Pracodawcy czy handlarze danych osobowych?

19 lutego 2023

Do roku 2018 dane pracowników były chronione w sposób poważny. Za zbieranie nadmiarowych danych osobowych groziły kary finansowe, które były egzekwowane. Nie było mowy o tym, aby pracodawca mógł zmuszać pracownika do transmisji swojego wizerunku przez internet (o ile zawód na tym nie polegał – np. dziennikarza). Nie było mowy o tym, aby pracodawca zbierał odciski palców. Mimo prób obejścia przepisów poprzez stosowanie skrótów odcisków – wymierzano kary. Pracownik mógł się poskarżyć do GIODO a ten wszczynał kontrolę i dochodzenie (zazwyczaj wykorzystywał obydwa swoje uprawnienia).

Osłabienie ochrony danych osobowych nastąpiło wraz z wprowadzeniem tzw. RODO. Rozporządzenie to zdaje się nie być tak na prawdę rozporządzeniem o ochronie danych, ale o ich swobodnym przepływie. Mimo, że przedsiębiorcy tak bardzo się bali wprowadzenia tego rozporządzenia, jakość ochrony danych jaką zapewnia jest dużo niższa niż w przypadku starej ustawy o ochronie danych osobowych.

Kolejne osłabienie jakości ochrony danych osobowych nastąpiło

po roku 2020, kiedy wprowadzono, że pracodawca ma prawo przetwarzać dane biometryczne ze względu na bezpieczeństwo (art. 221b Kodeksu pracy). Kończyć się to może pod przykrywką tzw. „bespieczeństfa" na zbieraniu odcisków palców od osób, które mają dostęp danych do kontaktów firmowych lub baz danych klientów. Bo czemu nie kazać tym osobom logować się do komputera odciskiem palca lub buziakiem w monitor? Oczywiście nie ma to z bezpieczeństwem nic wspólnego, ponieważ odcisk palca też da się podrobić i nie jest to trudne w dobie kamer 50-megapixelowych. Można to skutecznie zrobić w domu pozyskując od pracownika odcisk w autobusie. Hasło byłoby ciężej pozyskać. Mniej więcej w podobnym czasie weszły przepisy, że ze względów „bespieczeństfa" można podglądać pracowników w toaletach.

W roku 2023 doszło do kolejnego doładowania żarłocznych pracowdawców – możliwością zbierania danych o zdrowiu (art 221c i kolejne). O tym czy pracownik choruje na padaczkę, nowotwór, nerwicę, depresję i inne zaburzenia psychiczne. Dano bowiem możliwość sprawdzania przez pracodawcę stężenia benzodiazepin i opioidów we krwi oraz w ślinie. Jeżeli pracownik odmówi – zjawi się policja, a pracodawca dostanie wynik od policji. Dane te zostają wpisane do nowej zakładki w aktach osobowych.

Rekruterzy i pracodawcy zaczęli wbrew prawu do prywatności i prawu do zachowania bezpieczeństwa – żądać od kandydatów włączenia kamer i prowadzenia wideorozmów przez internet bez opcji i bez próby umożliwienia odbycia tej rozmowy face-to-face.

Jak działa transmisja wizerunku przez internet?

Aby poprawnie i całościowo dokonać analizy, czy pracodawca może żądać od pracownika lub kandydata transmisji biometrycznego wizerunku przez programy internetowe, najpierw trzeba przeanalizować jak zbudowane są urządzenia, przez które się to odbywa, jakie programy w tym uczestniczą i jakie mają polityki

prywatności i przetwarzania danych.

W przypadku transmisji wizerunku biometrycznego z kamery poprzez aplikację MS Teams używane są następujące programy:

– MS Teams z polityką prywatności Microsoftu – obowiązkową do zaakceptowania przez każdego użytkownika,

– system operacyjny Windows z polityką prywatności Microsoftu.

W tym miejscu należy zastanowić się:

– co jest zapisane w polityce prywatności programu MS Teams,

– co jest zapisane w polityce prywatności i licencji MS Windows,

– czy wolno z poszkodowaniem pracownika odmówić mu pracy tylko dlatego, że nie wyraził zgody na te polityki prywatności,

– czy wolno żądać od kandydata do pracy – danych biometrycznych lub też oddania ich osobie trzeciej (firmie Microsoft),

– czy dane są szyfrowane w taki sposób, żeby Microsoft nie był w stanie ich rozkodować (nie każdy typ szyfrowania to gwarantuje, jedynie niektóre zastosowania E2EE potrafią to zagwarantować),

– czy prawo amerykańskie zapewnia ochronę danych na poziomie Unii Europejskiej, czy niższe standardy.

Zacznę tutaj analizę od początku. Każdy, aby móc używać MS Teams, musi zaakceptować politykę prywatności firmy Microsoft (dotyczy zarówno systemu operacyjnego Windows jak i MS Teams). Poniżej znajdują się fragmenty zapisów tego dokumentu.

Polityka prywatności Microsoftu

„Użytkownik może decydować o tym, z jakich technologii będzie korzystać i jakie dane udostępni. Gdy poprosimy użytkownika o

podanie swoich danych osobowych, może odmówić. Jeśli użytkownik chce korzystać z usług firmy Microsoft, w przypadku wielu naszych produktów musi podać pewne dane osobowe. Jeśli użytkownik nie zdecyduje się na dostarczenie nam danych niezbędnych do udostępnienia mu określonego produktu lub funkcji, nie będzie mógł z nich korzystać".

Z tego fragmentu dowiadujemy się, że użytkownik musi podać niektóre dane (takie jak imię, nazwisko, adres e-mail), które po użyciu narzędzia MS Teams zostaną przekazane wraz z wizerunkiem i głosem (głos to też dana biometryczna!) firmie Microsoft. Nie można więc mówić o pozostaniu osobą anonimową lub o tożsamości trudnej do ustalenia. Dochodzi do przetwarzania danych osobowych podstawowych i danych o charakterze biometrycznym, a nawet zdrowotnym, takie jak możliwość stwierdzenia czy osoba ma objawy tocznia rumieniowatego czy też zaawansowaną próchnicę. Pracodawca nie dając możliwości umówienia się na spotkanie F2F zmusza pracownika do przekazania minimum Microsoftowi informacji o tych chorobach i danych biometrycznych, bowiem szyfrowanie nie nosi znamion procesu E2EE (o tym będzie dalej).

Teraz będzie dość niewinna formułka „Polityki prywatności Microsoftu", którą stosują prawie wszystkie większe firmy i tak na prawdę tu kryje się niebezpieczeństwo, z którego większość ludzi korzystających z MS Teams może nie zdawać sobie sprawy lub też to wypierać.

„Firma Microsoft wykorzystuje gromadzone dane w celu zapewnienia kompleksowej, interaktywnej obsługi użytkownika. W szczególności wykorzystujemy te dane do następujących celów:

– udostępnianie naszych produktów, obejmujące m.in. ich aktualizację i zabezpieczanie oraz rozwiązywanie związanych z nimi problemów, a także zapewnianie pomocy technicznej; obejmuje to również udostępnianie danych, gdy jest to wymagane do świadczenia usług lub przeprowadzania transakcji, których zażądał użytkownik;

– ulepszanie i rozwój naszych produktów;

– personalizowanie naszych produktów i formułowanie rekomendacji;

– reklamowanie i sprzedaż produktów użytkownikowi, w tym wysyłanie materiałów promocyjnych, reklamy ukierunkowane oraz prezentowanie użytkownikowi odpowiednich ofert”.

W pojęciu ulepszania i rozwoju produktów nie kryje się tylko ulepszanie samego MS Teams. Nawet gdyby tak było, nie wiemy nad czym pracuje Microsoft w tej dziedzinie i jest to tajemnicą przedsiębiorstwa. Wiadome jest jednak, że firmy takie jak Google, Apple, Facebook i Microsoft pracują nad rozwojem sztucznej inteligencji. Tajemnicą poliszynela jest to, że OpenAI jest bliskim partnerem Microsoftu. Czy na pewno pracownik musi uczestniczyć w rozwoju czyjejś sztucznej inteligencji, aby mógł być przyjęty do pracy? Czy pracodawca uświadomił pracownikowi ten punkt polityki prywatności i zapytał czy pracownik uznaje to za etyczne i wyraża na to dobrowolną zgodę? „Dobrowolną zgodę” na wykorzystanie przez Microsoft wizerunku i głosu użytkownika pod zastraszeniem kandydata, że nie uzyska umowy o pracę, gdy odmówi. Tak ma wyglądać dobrowolność? To ma być taka sama dobrowolność jak z „preparatami”?

Politykę prywatności do celów analizy można skończyć czytać w tym miejscu. Wykorzystanie danych (w tym biometrycznych) do szkolenia sztucznej inteligencji jest wystarczającym wykazaniem, że dojdzie do nadmiernego przetwarzania danych. Pracownik oddałby mniej danych o sobie jadąc na spotkanie prywatnym autem lub komunikacją (kamery w tramwaju dają obraz mało wyraźny w stosunku do kamery 30 centymetrów od twarzy).

Czy wolno żądać więcej danych niż to potrzebne?

Każdy pracodawca ma możliwość zaprosić pracownika na rozmowę

kwalifikacyjną do biura, gdzie zapewni kandydatowi to, że żadna osoba trzecia nie uzyska danych osobowych pracownika, w szczególności bez wiedzy pracownika. Pracownik może dotrzeć pieszo, własnym autem lub komunikacją miejską według własnego nieprzymuszonego wyboru. Pracownikowi za wybór pójścia pieszo względem pojechania samochodem nic nie grozi. Umowę jak ma otrzymać, to otrzyma.

W sytuacji, gdy od pracownika żąda się włączenia kamery i przekazania danych biometrycznych firmie Microsoft – dochodzi do żądania przekazania danych, co prawda nie pracodawcy, ale osobie trzeciej. Jednak dochodzi do przekazania tych danych, czego kandydat mógł uniknąć. Jest to więc nadmierne przetwarzanie danych, szczególnie, gdy kandydat miał 15 minut do biura. W przepisach pracy mówi się o oddaleniu zakładu pracy nawet o 90 minut w jedną stronę jako odległości nie nadmiernej do podjęcia pracy (a więc też pierwszej rozmowy).

Kandydat ma możliwość (ale nie obowiązek) podania więcej danych – w takim wypadku, gdy kandydat zgodziłby się dobrowolnie na przeprowadzenie rozmowy kwalifikacyjnej przez MS Teams – jest to jego wybór. Jednak nie można tego wymuszać, bowiem RODO w art. 5 i 6 wskazuje, że zbieranie danych musi być minimalne, a za niepodanie dodatkowych danych nie mogą spotkać kandydata nieprzyjemności.

„Art. 6.1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów”.

„Art. 5.1. 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 inte-

resie 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")".

Sprzedanie danych osoby ubiegającej się o pracę Microsoftowi poprzez żądanie oddania Microsoftowi wizerunku kandydata, imienia i nazwiska wraz z adresem e-mail nie jest minimalne w celu odbycia rozmowy rekrutacyjnej. Forma tradycyjna tej rozmowy nie powoduje oddania tych danych firmie trzeciej.

O zakazie odmowy zatrudnienia z powodu nieprzekazania większej ilości danych niż to jest wskazane w „Kodeksie pracy" mówi Art. 221.

„Art. 221a. § 1. Zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę innych danych osobowych niż wymienione w art. 221 § 1 i 3, z wyjątkiem danych osobowych, o których mowa w art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.2)), zwanego dalej „rozporządzeniem 2016/679".

„Art. 221a. § 2. Brak zgody, o której mowa w § 1, lub jej wycofanie, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę".

„Art. 221b. § 1. Zgoda osoby ubiegającej się o zatrudnienie

lub pracownika może stanowić podstawę przetwarzania przez pracodawcę danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika. Przepis art. 221a § 2 stosuje się odpowiednio".

Słabe szyfrowanie danych biometrycznych

Nie można w tym miejscu obronić argumentu spotykanego na wielu stronach, że przekaz wizerunku nie nosi znamion przekazu danych biometrycznych bo jest czynnością czysto techniczną.

Już czynność czysto techniczną kopiowania dowodów osobistych przez banki i inne instytucje (Urzędy Pracy) podważono. Nie jest to czynność czysto techniczna. Taki skan bowiem można wykorzystać do wyrobienia «kolekcjonerskiego dowodu osobistego», który wiadomo po co się wyrabia z cudzymi danymi. Na pewno nie tylko do tego, żeby kolekcjonować.

W tym przypadku może dojść do zapisania potajemnie wizerunku na komputerze rekrutera lub pracodawcy i wykorzystania takiego wizerunku wraz z imieniem, nazwiskiem, datą urodzenia, adresem zamieszkania (oprócz wizerunku – te dane ma prawo przetwarzać pracodawca względem kandydata).

Na podstawie adresu zamieszkania możliwe jest w przypadku osób, które kupiły mieszkanie, ustalenie innych danych takich jak PESEL, imię ojca, imię matki) na podstawie ksiąg wieczystych. Są firmy, które sprzedają po niskich cenach numer księgi wieczystej przypisany do adresu.

Stąd już nie jest daleko, by kolejna osoba mogła „kolekcjonować dowody osobiste".

Innym powodem dla którego przekaz wizerunku w przypadku wykorzystania MS Teams nie jest czynnością czysto techniczną jest

to, że dane te służą do «doskonalenia usług» osobie trzeciej czyli Microsoftowi. Wizerunek jest szyfrowany kluczem ustalonym przez serwer, rozszyfrowywany i ponownie szyfrowany kluczem kolejnej osoby, do której obraz jest kierowany. W połączeniach wiele do wielu może być szyfrowany wspólnym kluczem znanym dla serwera.

Gdyby obraz był pozyskiwany na systemie Linux i na urządzeniu z Linuxem odbierany i doszłoby do wymiany klucza publicznego między użytkownikami wraz z zachowaniem klucza prywatnego w taki sposób, by Microsoft nie mógł rozszyfrować danych – można-by mówić o czynności technicznej. Tak jednak nie jest. Pracodawcy używają zazwyczaj systemu Windows, zaś szyfrowanie w MS Teams nie nosi cech szyfrowania E2EE. Jedyne stosowane tam szyfrowanie to jest SSL/TSL (podobnie jak w HTTPS) pomiędzy klientem a serwerem.

Korzystanie z kompleksowego szyfrowania połączeń w usłudze Teams (np. Microsoft Teams, Microsoft Teams dla instytucji edukacyjnych):

– „W przypadku sytuacji wymagających zwiększonej poufności Teams oferuje szyfrowanie end-to-end (E2EE) na połączenia jeden do jednego. W przypadku E2EE informacje o połączeniach są szyfrowane na ich początku i odszyfrowywowane w zamierzonych przez nich miejscu docelowym, dzięki czemu nie można odszyfrowywać informacji między tymi punktami;

– Domyślnie wszystkie Teams za pomocą standardowych branżowych technologii, takich jak Transport Layer Security (TLS) i Secure Real-Time Transport Protocol (SRTP). Aby uzyskać więcej informacji na temat Teams zabezpieczeń, zobacz Zabezpieczenia i Microsoft Teams. Jeśli administrator IT włączył szczegółowe szyfrowanie (E2EE) dla Twojego zespołu, możesz użyć go, aby dodatkowo zwiększyć poufność połączeń jeden na jeden. Obie osoby dzwoniące muszą włączyć E2EE, aby technologia działała”.

W rozmowach kwalifikacyjnych oprócz kandydata bierze udział

jeszcze 2 lub 3 osoby (z których 1–2 nie wiadomo, co w ogóle tam robią). Połączenie nie jest więc E2EE, ponieważ nie jest jeden do jednego, nie zobowiązano minimum jednej strony do jego włączenia (nie każdy kandydat o tym wie, szczególnie mniej techniczny – autorka tego artykułu też nie wie jak to włączyć) i nie wiadomo czy administrator IT włączył odpowiednie funkcje.

Nie są więc spełnione 3 warunki, które umożliwią działanie technologii E2EE, połączenie nie jest więc czysto techniczne, nawet, gdyby kandydat podał Microsoftowi fałszywe (lub tymczasowe) dane w zakresie imienia, nazwiska i adresu e-mail.

Co jest nie tak z Google Meet?

Zapisy umowy Google Meet są podobne, szczególnie w zakresie «doskonalenia swoich usług». Nie jest tajemnicą, że Google pracuje nad sztuczną inteligencją BARDacha. Google też przyznał się, że podsłuchuje użytkowników systemu Android bez ich wiedzy, „bo tak jest lepiej”.

Uważamy za mocne naruszenie już samo proponowanie rozmowy kwalifikacyjnej przez to konkretne narzędzie działające na systemie operacyjnym znanym z tego, że w myśl definicji polskiego prawa pozostaje nielegalnym podsłuchem. Dlaczego w ogóle nadal używacie tych smartfonów, skoro można kupić oparty na Linuxie PinePhone Pro? To pytanie kieruję szczególnie do przedsiębiorców – dlaczego nie dbają o prywatność swoich podwładnych?

Czy pracodawca może prowadzić rekrutację zdalną?

Tak, pracodawca może prowadzić rekrutację zdalną w zakresie w jakim nie przekaże osobom trzecim danych osobowych kandydata. Może sprawdzić umiejętności językowe za pomocą testów, po prostu wprowadzając spseudonimizowane dane do systemów firm trzecich. Może wykorzystać rozmowę telefoniczną, ponieważ kandydat

podał numer telefonu. To też forma rekrutacji zdalnej. Może wysłać zadania rekrutacyjne do zrobienia w domu. Ważne by adresu e-mail nie podawać bez zgody kandydata firmom trzecim, które mogą go użyć potem do rozsyłania spamu. Pracodawca może podać swój e-mail wybierając zadania np. w „codify” (oraz inne dane spseudonimizowane) i przekazać link do testu na adres pracownika ze swoim pośrednictwem.

Może przeprowadzić rozmowę kwalifikacyjną przez MS Teams lub Google Meet (polityka prywatności podobna do microsoftowej) pod warunkiem, że umożliwił kandydatowi również udział w spotkaniu face-to-face i nastąpiło to za dobrowolną zgodą.

Bezprawnym jest tutaj samo zmuszanie do odbycia rozmowy kwalifikacyjnej zdalnie. Nie można mówić o dobrowolnej zgodzie, gdy pracownikowi grozi odrzucenie kandydatury za wątpliwości wobec formy elektronicznej tej czynności (która wiąże się z przekazywaniem danych osobom trzecim).

Należy zawsze pamiętać czy to wobec kandydata czy pracownika, że włączenie kamery to nie jest samo włączenie kamery. Pracodawca nie napisał systemu operacyjnego i aplikacji do przekazu obrazu. Zrobiły to inne firmy, które mają własne polityki prywatności często nieakceptowalne dla normalnych i świadomych ludzi, którzy je raczą przeczytać.

Pracodawca wymusza rozmowę MS Teams – co robić?

W sytuacji, gdy pracodawca wymusza na Tobie rozmowę kwalifikacyjną zdalną i nie udostępnia Ci swojego biura (lub w biurze każe połączyć się zdalnie przez MS Teams), należy udać się do sądu i walczyć o prywatność i normalność. Właściwy może być tu sąd pracy lub sąd cywilny (właściwość miejscową i merytoryczną ustalić powinien prawnik w oparciu o aktualny porządek prawny). Postępowanie przed sądem pracy jest bezpłatne.

Zarzut, który należy formułować przeciwko pracodawcy to nie zarzut nadmiernego przetwarzania danych osobowych w tym biometrycznych przez pracodawcę, ale stosowanie przymusu wyrażenia zgody na przetwarzanie danych biometrycznych przez firmę trzecią (Microsoft w przypadku Teams, Google w przypadku Meet) oraz przymus zawarcia umowy z firmą Microsoft. Ważne też jest, aby wyjaśnić w piśmie procesowym, jak działa wideokonferencja MS Teams i Google Meet oraz jakie mają polityki prywatności. Niestety, ale nie wierzymy, by nietechniczny sąd lub nietechniczny UODO podjął właściwą decyzję, gdy brakuje im wiedzy technicznej i dodatkowo nie wiedzą, że im tej wiedzy może brakować. Przez to nie powołują odpowiedniego biegłego (UODO nie powołuje specjalistów – ich opinie musisz samodzielnie dostarczyć).

Kluczem do wygranej jest więc poprawne sformułowanie zarzutu w pozwie i wyjaśnienie tego, co nie jest oczywiste. To, że czegoś nie widać, nie oznacza, że nie istnieje.

Rozmowy telefoniczne, gdzie odmawia pracodawca rekrutacji tylko dlatego, że „nie chcesz włączyć kamerki” – koniecznie nagrywaj (nagrywaj wszystkie i potem kasuj, gdy nie są potrzebne do celów dowodowych). Będąc uczestnikiem rozmowy z definicji nie stosujesz podsłuchu a o fakcie nagrywania nie musisz informować, gdy nie prowadzisz rozmowy firmowej.