FUNDACJA PANOPTYKON

Warszawa, 16 października 2017 r.

Uwagi Fundacji Panoptykon[1]
w sprawie projektów ustawy o ochronie danych osobowych oraz ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych

1. Wprowadzenie

14 września br. Ministerstwo Cyfryzacji opublikowało dwa projekty ustaw: projekt ustawy o ochronie danych osobowych (dalej: **projekt ustawy**) oraz projekt ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych (dalej: **projekt ustawy wprowadzającej**). Fundacja Panoptykon poniżej przedstawia swoje najważniejsze uwagi do tych dwóch projektów. Dotyczą one przede wszystkim pozycji ustrojowej organu ochrony danych osobowych, postępowania przed organem, oraz niektórych zmian w przepisach sektorowych, takich jak Kodeks pracy, Prawo bankowe czy ustawa o działalności ubezpieczeniowej. Projekty stanowią odpowiedź polskiego ustawodawcy na reformę ochrony danych osobowych wynikającą z Rozporządzenia 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 osobowych, dalej**: RODO**).

Część 1. UWAGI DOTYCZĄCE PROJEKTU USTAWY O OCHRONIE DANYCH OSOBOWYCH

2. Prezes Urzędu Ochrony Danych Osobowych

a. Ograniczona niezależność Prezesa

W naszej ocenie projekt wprowadza niewystarczające mechanizmy gwarantujące niezależność Prezesa Urzędu Ochrony Danych Osobowych. Świadczy o tym zaproponowana formuła wyboru Prezesa, a także jego zastępców.

i. Tryb wyboru Prezesa

Wybór Prezesa przez Parlament (wzorowany na dzisiejszym trybie wyboru Generalnego Inspektora Ochrony Danych Osobowych) zapewnia wysoki standard niezależności i przejrzystości trybu wyboru jedynie wówczas, gdy możliwe jest przedstawienie więcej niż jednego kandydata na obsadzane stanowisko.

W tym świetle krytycznie oceniamy zaproponowany w ustawie sposób wyboru Prezesa. Przyznanie możliwości arbitralnego wskazania kandydata na Prezesa wyłącznie Prezesowi Rady Ministrów oznacza ograniczenie możliwości wyboru Prezesa na podstawie przesłanek merytorycznych i wyboru kandydata, który przedstawi najlepszy plan działań podczas swojej

[1] Opinia przygotowana przez Wojciecha Klickiego oraz Jędrzeja Niklasa.

kadencji. Jest to bowiem możliwe jedynie wówczas, gdy Parlament dysponuje realnym wyborem spośród kilku kandydatów. W zaproponowanym modelu rola Parlamentu sprowadza się natomiast jedynie do zatwierdzenia wyboru osoby wskazanej przez Premiera.

Jednocześnie zaproponowany model nie sprzyja przejrzystości procesu wyboru, albowiem organizacje społeczne nie będą miały – tak jak dotychczas – możliwości przeprowadzenia obywatelskiego monitoringu wyboru kandydatów na stanowisko Prezesa.

Jednak co najważniejsze, kluczowa rola Prezesa Rady Ministrów w wyborze Prezesa Urzędu, osłabia jego pozycję względem administracji rządowej i stawia pod znakiem zapytania jego niezależność. Tymczasem zagwarantowanie Prezesowi Urzędu niezależności ma fundamentalne znaczenie, ponieważ będzie on kontrolował także przetwarzanie danych osobowych przez organy administracji rządowej. W zasadniczy sposób odróżnia go to od innych urzędów, takich jak Prezes Urzędu Regulacji Energetyki czy Urzędu Ochrony Konkurencji i Konsumentów.

W naszej ocenie istniejący dziś model wyboru Generalnego Inspektora Ochrony Danych Osobowych jest najkorzystniejszy, ponieważ pozwala parlamentarzystom na wybór najlepszego kandydata na stanowisko GIODO. W modelu tym niezwykle wartościowa jest również możliwość przedstawiania kandydatów przez posłów z różnych opcji politycznych. Sprzyja to demokratycznej i transparentnej dyskusji nad kierunkiem działań organu. Istniejąca dziś procedura pozwala także na aktywny udział partnerów społecznych. W związku z tym postulujemy ukształtowanie w projekcie trybu wyboru w takim samym kształcie, jak w ustawie o ochronie danych osobowych z 29 sierpnia 1997 r.

Jeśli jednak projektodawca zdecyduje się utrzymać kompetencje Prezesa Rady Ministrów do wskazywania kandydatów na Prezesa, postulujemy takie rozbudowanie procedury wyboru, by Premier wskazywał kandydata np. spośród osób wyłonionych w drodze otwartego i konkurencyjnego naboru.

ii. Wybór zastępców

Ryzyko braku niezależności Prezesa względem administracji rządowej zwiększa zaproponowany sposób wyboru jego zastępców. Zgodnie z obowiązującą dzisiaj ustawą o ochronie danych osobowych, zastępcy GIODO powoływani są na wniosek GIODO przez Marszałka Sejmu. Tymczasem projekt zakłada powoływanie zastępców przez Prezesa Rady Ministrów na wniosek ministra właściwego do spraw informatyzacji lub ministra spraw wewnętrznych.

Takie ukształtowanie procedury wyboru zastępców:

- obniża dotychczasowy standard niezależności kadrowej organu, w bezpośredni sposób uzależniając jego skład od decyzji politycznej odpowiednich ministrów;
- jest instytucją nieznaną w polskim systemie prawnym (por. sposób wyboru zastępców Rzecznika Praw Obywatelskich czy Rzecznika Praw Dziecka);
- może stać w sprzeczności z motywem 121 RODO, zgodnie z którym „organ nadzorczy powinien dysponować własnym personelem, który jest dobierany przez ten organ nadzorczy".

Ryzyko zależności Urzędu Ochrony Danych Osobowych od Prezesa Rady Ministrów zwiększa art. 20 ust. 10 projektu, zgodnie z którym w przypadku odwołania lub wygaśnięcia kadencji Prezesa, jego obowiązki pełni zastępca wskazany przez Premiera. Wobec braku wskazania w projekcie

terminu, w którym Prezes Rady Ministrów zobowiązany jest złożyć do Sejmu wniosek o powołanie Prezesa Urzędu, oznacza to ryzyko, że obowiązki Prezesa Urzędu pełnić będzie osoba arbitralnie wskazana przez Premiera, nie posiadająca legitymacji płynącej z wyboru przez Parlament.

Jednocześnie za zupełnie nieprzekonujące uważamy przedstawione uzasadnienie przedstawionego wyżej trybu wyboru zastępców Prezesa. Projektodawca uzasadnia zaproponowany w art. 22 ust. 3 wpływ ministra do spraw wewnętrznych (wniosek o powołanie zastępcy) oraz Ministra Sprawiedliwości, Ministra Obrony Narodowej, ministra właściwego do spraw finansów publicznych oraz Prokuratora Generalnego (zaopiniowanie powyższego wniosku) przyznaniem Prezesowi kompetencji organu nadzorczego w rozumieniu dyrektywy Parlamentu Europejskiego i Rady UE 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (dalej: **dyrektywa policyjna**).

Prezes, pełniąc funkcje organu nadzorczego w rozumieniu dyrektywy policyjnej, weryfikować będzie zgodność z prawem działań instytucji podległych wymienionych wyżej ministrom (np. Policji czy Krajowej Administracji Skarbowej). W związku z tym uważamy za niebezpieczne dla niezależności organu przyznanie możliwości wpływu na wybór zastępcy Prezesa instytucjom, które następnie będą przez Urząd Ochrony Danych Osobowych nadzorowane.

Na marginesie zwracamy uwagę, że zarówno Prezes, jak i jego zastępcy poddani będą weryfikacji w trybie ustawy o ochronie informacji niejawnych (w kontekście dostępu do informacji niejawnych).

Bardzo pozytywnie oceniamy przepis upoważniający Prezesa Urzędu do samodzielnego ustalania statutu urzędu. Jednak to upoważnienie nie jest w stanie zniwelować wskazanego powyżej problemu braku wystarczających gwarancji niezależności Prezesa Urzędu i jego zastępców, które powinny zostać stworzone już na etapie ich wyboru.

b. Kadencja aktualnej Generalnej Inspektor Ochrony Danych Osobowych

Projekt ustawy nie rozstrzyga, jaki będzie wpływ uchylenia ustawy o ochronie danych osobowych z 29 sierpnia 1997 r. i powołanie urzędu Prezesa na kadencję Generalnej Inspektor Ochrony Danych Osobowych. Nie znane są nam powody pominięcia tej – jakże istotnej – kwestii w proponowanych przepisach. Prezes Urzędu będzie nowym organem administracji publicznej, niemniej zapewni także ciągłość działań podejmowanych aktualnie przez Generalną Inspektor Ochrony Danych Osobowych.

W naszej ocenie kadencja aktualnej GIODO powinna biec nieprzerwanie, mimo przekształcenia podległego jej urzędu. Nie tylko zapewni to ciągłość pracy urzędu, ale też nie stworzy niebezpiecznego precedensu umożliwiającego usunięcie ze stanowiska urzędnika wybranego na określoną kadencję ze względu na ustawowe zmiany dotyczące piastowanego przez niego stanowiska.

c. Dodatkowe uwagi

- **Powierzenie Prezesowi funkcji organu nadzorczego w rozumieniu dyrektywy policyjnej**

Pozytywnie oceniamy przyjęcie rozwiązania, zgodnie z którym Prezes Urzędu będzie organem nadzorczym w rozumieniu dyrektywy policyjnej. Naszym zdaniem powierzenie realizacji zadań nadzorczych wynikających z RODO i dyrektywy policyjnej jednemu organowi zwiększy jego efektywność i spójność podejmowanych działań.

- **Wymogi formalne stawiane kandydatom na stanowisko Prezesa oraz Zastępców Prezesa**

Projekt w art. 20 ust. 4 wymienia katalog warunków, jakie ma spełniać Prezes Urzędu. W naszej ocenie, najważniejszym punktem jest wyróżniająca się wiedza z zakresu ochrony danych osobowych. Jednak (jak wskazaliśmy w powyższych uwagach) zaproponowany w ustawie tryb wyboru Prezesa nie gwarantuje faktycznego wyboru osoby, która w zadowalającym stopniu spełnia ten wymóg.

Przy okazji zwracamy uwagę na niezrozumiałe skrócenie wymaganej długości (z 5 do 4 lat) wymaganego okresu wykonywania czynności bezpośrednio związanych z ochroną danych osobowych w przypadku zastępców Prezesa Urzędu.

- **Rada do spraw ochrony danych osobowych**

Pozytywnie oceniamy propozycję powołania Rady do spraw ochrony danych osobowych jako organu doradczego Prezesa. Jej funkcjonowanie może wzmocnić Prezesa, który – dzięki osobom zasiadającym w Radzie – będzie mógł na bieżąco konsultować swoje najważniejsze decyzje z osobami dysponującymi szeroką wiedzą w obszarze ochrony danych osobowych oraz – podobnie jak w przypadku Rady ds. Cyfryzacji - wnoszących różne doświadczenie i perspektywę.

Na marginesie zwracamy jedynie uwagę, że niejasne jest dla nas – zaczerpnięte z ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne – ograniczenie możliwości rekomendowania kandydatów do Rady do spraw ochrony danych osobowych jedynie przez stowarzyszenia (por. art. 34 ust. 7 pkt 9), co wyklucza inne organizacje społeczne specjalizujące się w działalności na rzecz ochrony danych osobowych. Przy czym, biorąc pod uwagę, że Prezes Urzędu będzie samodzielnie wybierać członków Rady – można rozważyć całkowite zniesienie systemu rekomendacji kandydatów, a w jego miejsce wprowadzić model otwartego konkursu, w którym każdy może się zgłosić, odpowiednio uzasadniając swoją kandydaturę, a Prezes Urzędu zachowuje swobodę w wyborze swoich doradców.

3. Udział organizacji społecznych w postępowaniu dotyczącym naruszenia ochrony danych osobowych

Zapewnienie możliwie szerokiego udziału organizacji społecznych w postępowaniu związanym ze stosowaniem RODO ma fundamentalne znaczenie z racji na poziom skomplikowania materii, a także wagę właściwej implementacji i późniejszego stosowania rozporządzenia (oraz przepisów krajowych) dla praw podstawowych.

Udział organizacji społecznych w postępowaniach dotyczących ochrony danych osobowych reguluje art. 80 RODO oraz art. 45 projektu, który dotyka sytuacji przewidzianych w ust. 2 art. 80 RODO. Projekt umożliwia organizacji społecznej wystąpienie z żądaniem wszczęcia postępowania lub dopuszczenia jej do udziału w toczącym się już postępowaniu, pod następującymi warunkami: (i) jest to uzasadnione celami statutowymi organizacji, (ii) przemawia za tym interes osoby, której prawa zostały naruszone.

Przyznane organizacjom społecznym rodzą uwagi na dwóch poziomach:

a. Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych (przed Prezesem)

Aktualne brzmienie art. 45 nasuwa wątpliwość, czy organizacja społeczna żądając wszczęcia postępowania musi wskazać konkretną osobę, której prawa zostały naruszone. W naszej ocenie konieczne jest usunięcie tych wątpliwości na etapie legislacyjnym i takie sformułowanie art. 45 ustawy, żeby warunkiem wszczęcia postępowania przed PUODO **nie było** wskazanie szczegółowych informacji na temat konkretnej osoby, której prawa zostały naruszone.

Takie sformułowanie przepisów odpowie na problem wysokiego poziomu skomplikowania tematu ochrony danych osobowych i ryzyka występowania sytuacji, w których osoba, której prawa zostały naruszone nie ma świadomości tego faktu, a jednocześnie jej interes przemawia za przeprowadzeniem postępowania w sprawie naruszenia przepisów o ochronie danych osobowych.

W naszej ocenie intencją unijnego pracodawcy (art. 80 ust. 2 RODO) było upoważnienie organizacji do inicjowania postępowań, w których dochodzi do naruszenia praw bliżej niewskazanych osób, np. użytkowników danego portalu. Zwracamy uwagę, że przyjęcie odwrotnej interpretacji (konieczność podania danych osobowych, której prawa zostały naruszone) prowadzi do wniosku, że norma ta będzie niemal pusta, ponieważ organizacje społeczne nie mają podstaw i możliwości do gromadzenia oraz wyszukiwania informacji na temat konkretnych osób, których prawa zostały naruszone.

Postulujemy także jednoznaczne określenie (na kształt art. 31 § 3 Kodeksu postępowania administracyjnego), że organizacja społeczna działa w omówionej wyżej sytuacji na prawach strony. Ma to znaczenie w kontekście uprawnień przysługujących stronie w postępowaniach administracyjnych, np. wglądu do akt postępowania czy możliwości ustanowienia pełnomocnika.

b. Inne postępowania

Jednocześnie krytycznie oceniamy decyzję ustawodawcy o nieskorzystaniu z możliwości wynikającej z art. 80 ust. 2 RODO i nieprzyznaniu organizacjom społecznym uprawnień, o których mowa w art. 78 i 79 RODO, czyli zaskarżania decyzji Prezesa Urzędu, a także realizacji uprawnień, o których mowa w art. 78 projektu.

W naszej ocenie przyznanie tych uprawnień, zwłaszcza w zakresie zaskarżenia decyzji Prezesa Urzędu wydanych w postępowaniu wszczętym na wniosek organizacji, jest niezbędnym elementem mechanizmu umożliwiającego organizacjom społecznym skuteczne działania na rzecz ochrony danych osobowych. Skoro bowiem na wniosek organizacji może zostać wszczęte postępowanie przed Prezesem, to jego decyzja – podobnie jak decyzja wydana w „normalnym" postępowaniu zainicjowanym na wniosek osoby fizycznej – powinna podlegać kontroli sądu administracyjnego.

Realizacja tego postulatu wymaga (jak już to zostało podniesione wyżej) przyznania organizacjom społecznym możliwości działania na prawach strony

Dodatkowo zwracamy uwagę, że fundamentalne znaczenie dla wykładni nowych przepisów i realnego poziomu ochrony danych osobowych w poszczególnych branżach będą mieć prowadzone przez Prezesa postępowania certyfikacyjne oraz zatwierdzane kodeksy postępowań. Zgodnie z art. 40 ust. 2 RODO kodeksy postępowań będą mogły precyzować kwestie, które mają fundamentalne znaczenie z perspektywy praw podmiotów danych, np.

wykonywanie przez te osoby przysługujących im praw czy przekazywanie danych osobowych do państw trzecich. Dlatego należy w taki sposób uregulować sposób ich przyjmowania, by zapewnić maksymalnie duży udział w ich tworzeniu osób, których praw będą one dotyczyć, a także organizacji społecznych, wśród których celów statutowych znajduje się m.in. ochrona danych osobowych.

Zgodnie z motywem 99 RODO, sporządzając lub zmieniając kodeks postępowania administratorzy powinni „konsultować się z odpowiednimi stronami, których sprawa dotyczy, w tym, jeżeli jest to wykonalne, z osobami, których dane dotyczą oraz mieć na względzie uwagi i opinie otrzymane w ramach takich konsultacji". Obecna konstrukcja przepisów regulujących przyjmowanie kodeksów postępowań nie zakłada etapu konsultacji.

W związku z powyższym, apelujemy o dopuszczenie organizacji społecznych do udziału w postępowaniu zatwierdzającym kodeksy postępowań, np. poprzez nałożenie na PUODO obowiązku publikacji projektów kodeksów i przyznanie osobom fizycznym oraz organizacjom społecznym (jeśli jest to uzasadnione ich celami statutowymi) przynajmniej 30 dniowego terminu na zgłaszanie uzasadnionych zastrzeżeń. Przy czym organ mógłby odstąpić od formalnych konsultacji, jeśli podmiot zgłaszający kodeks byłby w stanie wykazać, że – zgodnie z motywem 99 – sam już przeprowadził rzetelne konsultacje z udziałem odpowiednich interesariuszy.

Podsumowując, w naszej ocenie niezbędne jest:

- przyznanie szerszych uprawnień organizacjom społecznym; w szczególności przyznanie im możliwości działania na prawach strony oraz – w konsekwencji – zaskarżania decyzji Prezesa Urzędu do sądu administracyjnego;
- takie sformułowanie art. 45 projektu, by organizacje społeczne mogły żądać wszczęcia postępowania bez wskazywania konkretnej osoby, której prawa zostały naruszone.

W naszej opinii możliwie szerokie uprawnienia przysługujące organizacjom społecznym posłużą podwyższeniu poziomu ochrony danych osobowych. Dotyczy to w szczególności sytuacji, w której prawa zostały naruszone bez wiedzy osoby, której one dotyczą.

Zwracamy przy tym uwagę, że podnoszone w debacie publicznej argumenty, zgodnie z którymi przyznanie szerokich uprawnień organizacjom społecznym prowadzić będzie do swoistego nadużywania tego uprawnienia jest chybione. Mechanizmem gwarantującym, że uprawnienia przyznawane organizacjom nie będą nadużywane jest przyznanie Prezesowi Urzędu możliwości odmowy wszczęcia postępowania w sytuacji, w której uzna, że nie przemawia za tym interes osoby, której dane dotyczą. W sytuacji, w której administratorzy danych nie przestrzegają obowiązków nałożonych na nich przez RODO, działania organizacji zwracających uwagę na ten problem będą działaniami w interesie publicznym. Przy czym ryzyko prób wymuszenia określonego działania na administratorach danych minimalizuje również art. 56 projektu, zgodnie z którym – gdy waga naruszenia przepisów o ochronie danych osobowych jest znikoma, a strona zaprzestała naruszenia – Prezes może w drodze decyzji udzielić upomnienia.

4. Kary pieniężne

Popieramy konstrukcję, zgodnie z którą organ nadzorczy będzie mógł nakładać na podmioty publiczne kary finansowe. Takie rozwiązanie może wpłynąć w pozytywny sposób na faktyczny poziom ochrony praw obywateli. Przyjęcie innego rozwiązania – w którym organ publiczny nie

musi się liczyć z dotkliwymi dla budżetu konsekwencjami naruszenia przepisów o ochronie danych osobowych – mogłoby wpłynąć demobilizująco na sektor administracji publicznej.

Z drugiej strony zrozumiała jest decyzja o obniżeniu maksymalnej wysokości kary finansowej w przypadku organów publicznych w porównaniu do działalności podmiotów komercyjnych. Popieramy także wymóg udostępniania na stronach internetowych decyzji PUODO podejmowanych wobec organów publicznych oraz publikowania informacji o działaniach, które mają na celu wykonanie ww. decyzji.

5. Postępowanie przed sądem cywilnym i sądami administracyjnymi

W zakresie postępowań prowadzonych na podstawie art. 78 i następnych projektu, a także postępowań prowadzonych na skutek skargi na decyzję Prezesa Urzędu, w naszej ocenie kluczowe jest zapewnienie sprawności postępowania.

W tym kontekście postulujemy rozważenie, by postępowania toczone przed sądem administracyjnym w sprawie skarg na decyzje Prezesa Urzędu, były rozpatrywane w sposób priorytetowy. Przykładowym rozwiązaniem tego typu ustawodawca zastosował w ustawie o dostępie do informacji publicznej, która zobowiązuje sąd do rozpatrzenia skargi w terminie 30 dni od dnia jej otrzymania wraz z odpowiedzią na skargę (por. art. 21 pkt 2 ustawy o dostępie do informacji publicznej). Za przyjęciem przez ustawodawcę rozwiązań sprzyjających szybszemu rozpatrywaniu skarg na decyzje Prezesa Urzędu przemawia przede wszystkim charakter spraw z zakresu danych osobowych, które wiążą się z ingerencją w prawa podstawowe.

Część 2. UWAGI DOTYCZĄCE PROJEKTU USTAWY – PRZEPISY WPROWADZAJĄCE USTAWĘ O OCHRONIE DANYCH OSOBOWYCH

Z racji na szeroki zakres ustawy wprowadzającej, przedstawiamy poniżej uwagi jedynie do niektórych proponowanych zmian, które w naszej ocenie w sposób szczególny wiążą się z zagrożeniami dla ochrony danych osobowych.

6. Kodeks pracy

Zgodnie z art. 88 RODO, państwa mogą wprowadzać bardziej szczegółowe przepisy dotyczące przetwarzania danych w związku z zatrudnieniem czy do celów rekrutacji. Projekt ustawy wprowadzającej proponuje zmiany względem przetwarzania danych osobowych w związku z ubieganiem się o zatrudnienie i w związku ze stosunkiem zatrudnienia. Projekt utrzymuje w mocy katalog danych, które pracodawca może pozyskiwać od pracownika lub kandydata do pracy (imiona, datę urodzenia, PESEL etc.). Dodatkowe dane (dane biometryczne i inne dane, których katalog nie został określony), będę mogły zostać przetwarzane, gdy dotyczą stosunku pracy i tylko za zgodą udzieloną przez pracownika. Co więcej, nowe przepisy mówią o trzech kategoriach danych (zdrowie, nałogi i orientacja seksualna), których przetwarzanie będzie możliwe wyłącznie, gdy wymagają tego dodatkowe przepisy prawne.

a. Zakres przetwarzanych danych

Naszym zdaniem projekt ustawy powinien zostać zmieniony w zakresie katalogu danych, które może dodatkowo pozyskać pracodawca za zgodą pracownika. Zbytnia dowolność w tym obszarze może przynosić negatywne konsekwencje społeczne. Warto wskazać, że np. liberalny dostęp pracodawców w USA do informacji o zadłużeniu pracowników, powoduje ograniczenie

dostępu do rynku pracy osób zadłużonych[2]. Rozwiązanie to uderza w osoby uboższe i uniemożliwia im wyjście ze spirali zadłużenia. Podobne zastrzeżenia związane są np. z przetwarzaniem na szeroką skalę informacji pochodzących z Krajowego Rejestru Karnego. Niestety projektodawca nie wskazuje na tego typu ryzyka na poziomie uzasadnienia, nie wprowadza też żadnych konstrukcji prawnych, które mogłyby im zapobiegać.

Pewne wątpliwości wiążą się także z przetwarzaniem tzw. danych biometrycznych. Dane te zostały zaliczone do szczególnej kategorii informacji, które wymagają odpowiedniej ochrony, o czym wielokrotnie wspominały krajowe i międzynarodowe organy ochrony danych osobowych[3]. Systemy kontroli oparte na korzystaniu z cech biometrycznych historycznie były kojarzone z sytuacjami opresji lub ograniczenia wolności. Bardzo często gromadzenie m.in. odcisków linii papilarnych było narzędziem służącym do stygmatyzacji społecznej. Stosowanie na szeroką skalę danych biometrycznych nie tylko wzbudza wątpliwości na gruncie ochrony prawa do prywatności, ale także poszanowania integralności cielesnej i ochrony ludzkiej godności. W Polsce mamy przykłady protestów pracowników, których pracodawcy próbowali wprowadzić systemy biometrycznego kontrolowania czasu pracy[4].

W naszej ocenie propozycja projektodawcy, umożliwiająca pracodawcy przetwarzanie danych biometrycznych mających związek ze stosunkiem pracy, pod warunkiem uzyskania zgody pracownika, doprowadzi do wykorzystywania tych danych na masową skalę. Zwracamy bowiem uwagę na wadliwość zgody wyrażanej w stosunku pracy – jak wielokrotnie wskazywały sądy administracyjne zgoda wyrażona w relacji pracownik-pracodawca nie ma dobrowolnego charakteru. W naszej ocenie niezbędne jest zagwarantowanie – zwłaszcza w kontekście danych biometrycznych –zasady adekwatności ograniczającej możliwość pracodawcy, nawet mimo uzyskania zgody pracowników, na zbieranie danych osobowych wówczas, gdy nie jest to konieczne. Przykładem takiej sytuacji jest chociażby powszechne wprowadzenie kontroli dostępu do pomieszczeń za pomocą danych biometrycznych. O ile taki wyższy poziom zabezpieczenia będzie zrozumiały np. w sektorze bankowym, to trudno uzasadnić stosowanie odcisku palca przy standardowej kontroli wejścia do biurowca.

Projektodawca nie wykazał jasno uzasadnienia dla zaproponowanego zakresu danych, który pracodawca nie powinien zbierać - nawet za zgodą pracownika (por. proponowany art. 22^2 §5 Kodeksu pracy). Wśród tego typu informacji są dane o nałogach, stanie zdrowia czy orientacji seksualnej. Jak wskazuje uzasadnienie projektu ustawy wprowadzającej wyróżnienie tego typu informacji jest podyktowane ochroną strefy intymnej. Projektodawca wydaje się nie zauważać, że istnieją też inne informacje, których przetwarzanie może pociągać daleko idące konsekwencje, chociażby w postaci dyskryminacji[5]. Na przykład trudno zrozumieć, dlaczego w ww. katalogu nie ma informacji o pochodzeniu etnicznym i rasowym lub wyznaniu. Podobne zastrzeżenia mogłoby budzić pobieranie informacji od kandydatów do pracy danych o przynależności do związków zawodowych czy partii politycznych. Z drugiej strony, dane o orientacji seksualnej (których gromadzenie nie jest dopuszczalne nawet za zgodą) mogłyby służyć jako podstawa tworzenia polityk równościowych w miejscu pracy. W związku z tym

[2] Demos, Discredited: How Employment Credit Checks Keep Qualified Workers out of a Job, http://www.demos.org/sites/default/files/publications/Discredited-Demos.pdf
[3] Por. np. opinia 03/2012 na temat rozwoju technologii biometrycznych przyjętą przez Grupę Roboczą Art. 29.
[4] Gazeta Wyborcza: Biometria na wejściówki w szpitalu, Dyrektor szpitala nadepnął lekarzom na odcisk http://wroclaw.wyborcza.pl/wroclaw/1,35771,7004640,Dyrektor_szpitala_nadepnal_lekarzom_na_odcisk.html
[5] Szerzej w S. Barocas, A. Selbst, Big Data's Disparate Impact, https://pdfs.semanticscholar.org/1d17/4f0e3c391368d0f3384a144a6c7487f2a143.pdf

należy przeanalizować, czy przetwarzanie tego typu informacji powinno być bezwzględnie niedozwolone[6].

Naszym zdaniem projektodawca powinien rozszerzyć katalog danych, których przetwarzanie przez pracodawcę jest niedozwolone nawet za zgodą pracownika lub ewentualnie precyzyjnie określić katalog danych, których przetwarzanie jest dozwolone – bez możliwości jego rozszerzania za zgodą pracownika. Co więcej uważamy, że w przypadku dodatkowych kategorii danych oraz danych biometrycznych, zgoda jest wadliwą podstawą ich przetwarzania. W zależności od przyjętego modelu zarządzania i funkcjonowania zakładu pracy, relacje pracownik-pracodawca mogą być obarczone większą lub mniejszą nierównością. W takiej sytuacji trudno wyobrazić sobie, żeby zgoda pracownika spełniała kryteria dobrowolności.

b. Monitoring wizyjny

Doceniamy starania uregulowania kwestii monitoringu w miejscu pracy, jednak naszym zdaniem zaproponowane rozwiązania są niewystarczające. Przede wszystkim należy zauważyć, że projekt ustawy wprowadzającej ogranicza się tylko do monitoringu wizyjnego, pozostawiające w sferze nieuregulowanej (lub uregulowanej przepisami ogólnym) inne instrumenty kontroli pracowników - jak monitoring dźwięku, monitoring aktywności w Internecie, wgląd do korespondencji elektronicznej itp. Fundacja Panoptykon wielokrotnie apelowała o uregulowanie tych kwestii[7].

Co więcej zaproponowane w projekcie ustawy wprowadzającej przepisy (np. w zakresie dopuszczalnego okresu przechowywania danych) dotyczą tylko danych osobowych. Tymczasem w kontekście stosowania monitoringu wizyjnego bardzo żywa jest debata o tym, w jakim zakresie i kiedy takie nagranie zawiera dane osobowe. W związku z tym wymogi w zakresie przechowywania powinny dotyczyć ogólnie nagrań z monitoringu, nie tylko tych zaklasyfikowanych jako zawierające dane osobowe. Ten sam problem można przełożyć na inne zagadnienia dotyczące monitoringu wizyjnego tj. celowość, uprawnienia osób nagrywanych itp. Ogólne rekomendacje w tym zakresie zawiera opinia Fundacji Panoptykon dotycząca założeń do ustawy o monitoringu wizyjnym[8].

Szereg wątpliwości wiąże się także z określeniem celów, dla których może być stosowany monitoring. Projekt ustawy wprowadzającej mówi o zapewnieniu bezpieczeństwa lub ochronie mienia. Zakazuje przy tym stosowania monitoringu do kontroli czasu i jakości pracy. Mamy obawy, że w praktyce powyższy zakaz będzie niezwykle trudny do wyegzekwowania w praktyce, zwłaszcza w przypadkach śledzenia nagrań miejsca pracy w czasie rzeczywistym. Co więcej, projekt nie określa czy konsekwencją naruszenia tego zakazu będzie niemożność wykorzystania nagrań z monitoringu dla celów dowodowych przez pracodawcę.

Rekomendujemy uzupełnienie katalogu pomieszczeń, których nie powinien obejmować monitoring wizyjny pracodawcy (por. proponowany art. 22^4 § 2 Kodeksu pracy) o pomieszczenia wykorzystywane przez związki zawodowe. Postulat ten związany jest bezpośrednio z wolnością wykonywania działalności związkowej.

---

[6] Szerzej o problemie etycznego zbierania danych dla celów równościowych w European Network Against Racism, Equality data collection, http://www.enar-eu.org/Equality-data-collection-151

[7] Stanowisko Fundacji Panoptykon w sprawie stosowani a nowoczesnych technologii do kontroli w miejscach pracy, https://panoptykon.org/sites/default/files/panoptykon_kontrola_w_miejscu_pracy_stanowisko_07_01.2016_0.pdf

[8] Stanowisko Fundacji Panoptykon w sprawie projektu założeń do projektu ustawy o monitoringu wizyjnym https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_msw_zalozenia-cctv-v2_opinia_14.08.2014_1.pdf

Rekomendujemy również wprowadzenie do ustawy wprowadzającej obowiązku konsultowania potrzeby i celów wprowadzenia monitoringu wizyjnego w miejscu pracy z pracownikami, a w szczególności z zakładową organizacją związkową lub inną formą przedstawicielstwa pracowników.

7. Profilowanie i automatyczne podejmowanie decyzji w ustawach sektorowych

Projekt ustawy wprowadzającej przyznaje bankom (por. art. 41 projektu ustawy wprowadzającej – zmiany w ustawie – Prawo bankowe) możliwość profilowania klientów i podejmowania wobec nich zautomatyzowanych decyzji. Jednocześnie projekt ustawy nie określa gwarancji poszanowania praw klientów w procesie profilowania i podejmowania zautomatyzowanych decyzji. Natomiast art. 22 ust. 2 lit. b RODO jasno wskazuje, że upoważnieniu do wydawania tego typu decyzji muszą towarzyszyć środki ochrony praw, wolności i prawnie uzasadnionych interesów osób, których dane dotyczą. Do takich środków należy zaliczyć m.in. prawo do ludzkiej interwencji, prawo do wyrażenia swojego stanowiska, prawo do sprzeciwu wobec decyzji oraz prawo do wyjaśnienia. Co więcej przywołany artykuł RODO mówi o „właściwych" środkach ochrony. W naszej ocenie środki te muszą być więc dostosowane do konkretnej sytuacji i sektora, który stosuje tego typu proces podejmowania decyzji. Uważamy, że projekt ustawy wprowadzającej powinien wprost wskazywać, jakie środki ochrony będą właściwe w sektorze bankowym oraz wprowadzić jednoznaczny obowiązek ich wprowadzenia w przypadku podejmowania automatycznych decyzji i profilowania.

Dodatkowo rekomendujemy wprowadzenie precyzyjnego katalogu danych, które mogą służyć do budowania profili przez banki lub określenie katalogu danych, które nie mogą być podstawą takiej operacji (np. pochodzenie etniczne, orientacja seksualna itp.) Stworzenie takiego katalogu służyłoby minimalizowaniu negatywnych skutków społecznych profilowania oraz przeciwdziałało dyskryminacji.

Analogiczne uwagi dotyczące profilowania i automatycznego podejmowania decyzji odnoszą się do zmian w ustawie o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, ustawie Prawo telekomunikacyjne oraz ustawie o działalności ubezpieczeniowej i reasekuracyjnej.