

Wdrażanie rozwiązań biometrycznych a ochrona danych osobowych

Problematyka wdrażania rozwiązań biometrycznych w urzędach jest bez wątpienia złożona i wielopłaszczyznowa. Zagadnienia te w odniesieniu do pracowników są przedmiotem decyzji Generalnego Inspektora Ochrony Danych Osobowych.

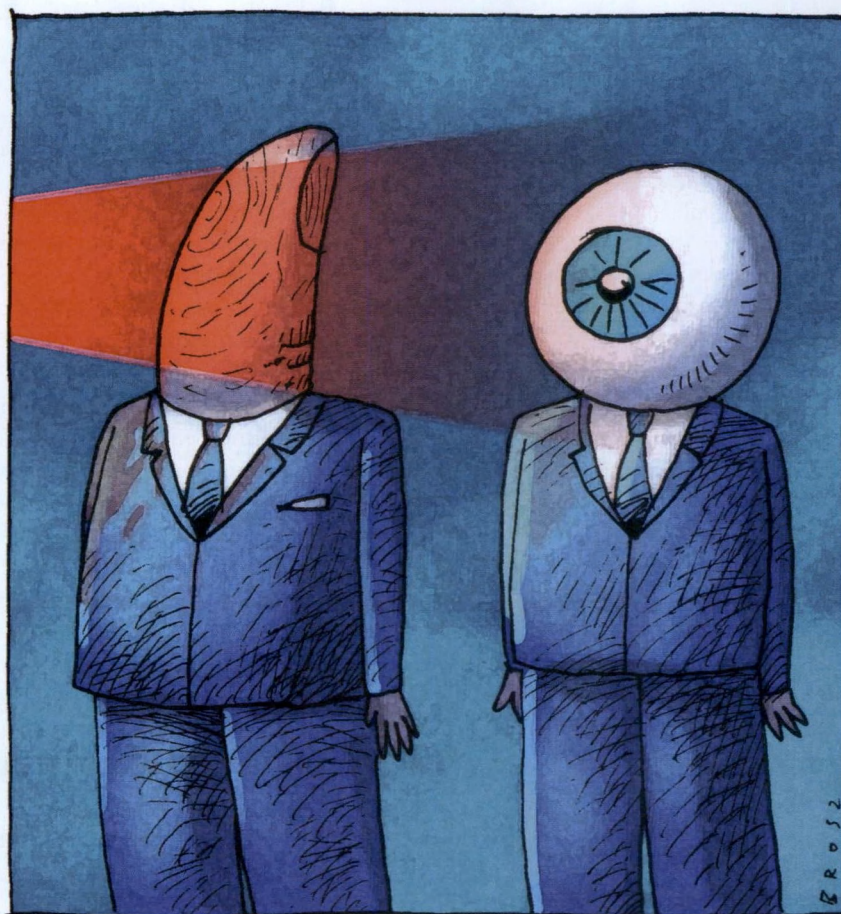
dr Edyta Bielak-Jomaa

W aktualnym stanie prawnym nie ma legalnej definicji danych biometrycznych. Dane te nie zostały również wprost zaliczone do zamkniętego katalogu tzw. danych wrażliwych zawartego w art. 27 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. z 2015 r. poz. 2135 ze zm.; uodo). Jak stanowi ten przepis, zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Można jednak założyć, że w pewnych przypadkach dane biometryczne mogą ujawniać pochodzenie rasowe lub etniczne, dane o stanie zdrowia lub kodzie genetycznym. Podmioty przetwarzające takie dane będą wówczas zobowiązane do legitymowania się jedną z przesłanek dopuszczalności przetwarzania danych wrażliwych, wymienionych w art. 27 ust. 2 uodo, a także do spełnienia założeń innym wymaganiom wynikającym z uodo, takim, jak chociażby zgłoszenie zbioru danych wrażliwych do rejestracji u Generalnego Inspektora Ochrony Danych Osobowych (GIODO) jeszcze przed rozpoczęciem ich przetwarzania.

Nadchodzą nowe regulacje

Sytuacja ulegnie zmianie, gdy zacznie obowiązywać unijne rozporządzenie ogólne o ochronie danych osobowych,



którego przepisy uznają dane biometryczne za dane szczególnej kategorii i dają państwom członkowskim Unii Europejskiej prawo do zachowania lub wprowadzenia innych zasad, w tym prawo do ograniczenia ich przetwarzania. Rozporządzenie będzie obowiązywać bezpośrednio, bez konieczności implementacji w polskim porządku prawnym, i zastąpi uodo. Jego formalne uchwalenie przez Parlament Europejski nastąpiło 14 kwietnia 2016 r., natomiast 20 dni po opublikowaniu, które miało miejsce 4 maja 2016 r. (DzUrz UE L 119),

rozpoczął się okres dwuletniego *vacatio legis*. Po jego upływie, a więc od 25 maja 2018 r., przepisy rozporządzenia będą stosowane we wszystkich państwach członkowskich.

Także Grupa Robocza Art. 29 – niezależny europejski organ doradczy Komisji Europejskiej w zakresie ochrony danych osobowych i prywatności, którą zgodnie z unijnym rozporządzeniem zastąpi Europejska Rada Ochrony Danych – przyjęła 27 kwietnia 2012 r. „Opinię 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych”. Grupa

Biometria w bankach

GIODO odpowiadał na zapytanie dotyczące przetwarzania danych biometrycznych przez banki w celu zabezpieczenia działalności bankowej. Organ wskazał, że podmioty przetwarzające dane osobowe są obowiązane do stosowania uodo, o ile przepisy innych aktów prawnych nie określają w sposób szczególny procesu przetwarzania danych osobowych. Przepisy ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (tekst jedn. DzU z 2015 r. poz. 128) nie dają natomiast bankom uprawnień do przetwarzania

danych osobowych w zakresie danych biometrycznych, w tym związanych z zabezpieczeniem działalności bankowej. Co więcej, przetwarzanie danych biometrycznych może być oceniane przez organ do spraw ochrony danych osobowych jako prowadzące do naruszenia zasady adekwatności przetwarzania danych, o której mowa w art. 26 ust. 1 pkt 3 uodo. Wskazał także, że musi zostać zachowana opcjonalność takiego rozwiązania. Szczególną uwagę należy też poświęcić aspektom przechowywania i zabezpieczenia tych

danych. Trzeba przy tym pamiętać o zasadzie czasowego ograniczenia przechowywania danych do momentu realizacji wyznaczonego celu przetwarzania. Gdy cel przetwarzania danych jest sprecyzowany (weryfikacja klientów), a jego realizacja dobiegła końca (np. gdy rozwiązano umowę, gdy odwołano zgodę), nie można mówić o zgodności dalszego przetwarzania danych osobowych z przepisami dotyczącymi ich ochrony. Dochodziłoby bowiem wówczas do przetwarzania danych bez podstawy prawnej, która wygasta dla celu ich uprzedniego przetwarzania. Rze-

telnie dopełniony powinien być obowiązek informacyjny wynikający z art. 24 i 25 uodo oraz obowiązek określony w art. 26 ust. 1 pkt 2 i 3 uodo, dotyczący dokończenia należytej staranności w celu ochrony interesów osób, których dane dotyczą, poprzez zapewnienie, aby dane te były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, dla jakich są przetwarzane. Niedopuszczalne będzie na ich podstawie np. profilowanie klientów.

wskazuje w niej, że systemy biometryczne są ściśle związane z daną osobą, ponieważ dzięki nim możliwe jest wykorzystanie określonej niepowtarzalnej cechy danej osoby fizycznej do celów identyfikacji lub uwierzytelnienia. Dane biometryczne konkretnej osoby można usunąć lub zmienić, ale źródła, z którego dane te pochodzą, nie da się zasadniczo ani zmienić, ani usunąć. Grupa Robocza Art. 29 przyznała także, że wraz z rozwojem tych technologii pojawiły się również nowe zagrożenia dla praw podstawowych, m.in. dyskryminacja genetyczna oraz kradzież tożsamości. W swojej analizie prawnej Grupa Robocza Art. 29 wskazała także, że dane biometryczne można przetwarzać tylko wtedy, gdy istnieje ku temu podstawa prawna i jeżeli przetwarzane dane są prawidłowe, odpowiednio oraz nienadmierne w stosunku do celów, dla których zostały zgromadzone lub dalej przetworzone.

Odcisk palca a czas pracy

Jednym z najczęściej pojawiających się problemów w praktyce GODO jest kwestia skanowania linii papilarnych pracowników do celów ewidencjonowania czasu ich pracy. GODO wielokrotnie zajmował stanowisko w tej kwestii – w swoich decyzjach i wystąpieniach oraz udzielając odpowiedzi na pytania zadawane przez

różne podmioty. Zdaniem organu przetwarzanie danych osobowych pracowników w postaci charakterystycznych punktów linii papilarnych odbywa się bez podstawy prawnej. Zgodnie bowiem z art. 22¹ § 1 Kodeksu pracy pracodawca może żądać od pracownika podania danych tylko w takim zakresie, jaki został wskazany w tym przepisie. Złożenie przez pracownika oświadczenia, którego treścią jest wyrażenie zgody na rejestrację czasu

W jednej ze swoich decyzji GODO nakazał spółce usunięcie danych osobowych pracowników obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców oraz zaprzestanie zbierania tych danych osobowych na potrzeby rejestracji czasu pracy oraz ewidencjonowania wejść i wyjść (decyzja z 22 lutego 2008 r.; sygn. DIS/DEC-134/4605/08). Zastosowany w tym zakładzie pracy system

W aktualnym stanie prawnym nie ma legalnej definicji danych biometrycznych. Dane te nie zostały również wprost zaliczone do zamkniętego katalogu tzw. danych wrażliwych.

pracy za pomocą czytnika palców, nie stanowi przesłanki legalizującej przetwarzanie danych osobowych pracowników, o której mowa w art. 23 ust. 1 pkt 1 uodo. Co istotne, GODO stoi na stanowisku, że niedopuszczalne jest stosowanie urządzeń biometrycznych do monitorowania czasu pracy niezależnie od zastosowanej technologii. Zatem czytnik biometryczny przetwarzający dane jedynie w postaci kształtu dłoni, jej grubości i długości (bez linii papilarnych) zastosowany do potrzeb ewidencji czasu pracy również jest niedopuszczalny.

obejmował czytniki kart radiowych oraz czytniki linii papilarnych wraz z oprogramowaniem służącym do pozyskiwania linii papilarnych oraz do rejestracji wejść i wyjść na podstawie rejestrowanych linii papilarnych. Linie papilarne pobierane były z palców dłoni poprzez służący do tego czytnik, który skanował obraz linii papilarnych, nie zachowując ich obrazu w pamięci. Z informacji uzyskanych od dostawcy wynikało, że czytnik przysyłał obraz do oprogramowania, które przetwarzało obraz linii papilarnych na zapis cyfrowy (kod w postaci ciągu cyfr) →

→ na podstawie 12 charakterystycznych punktów zeskanowanych linii. Obraz linii papilarnych oraz punktów nie był zapisywany. Na serwerze zainstalowana była usługa służąca do komunikacji z terminalami (czytnikami służącymi do rejestracji wejść i wyjść za pomocą linii papilarnych) oraz z czytnikiem do pobierania danych biometrycznych. Informacja dotycząca każdego pracownika zapisywana była w osobnym pliku w określonym miejscu na serwerze. Dodatkowo w pliku tym zapisywane były: imię i nazwisko osoby, której linii papilarne zeskanowano, numer identyfikacyjny (ID) danego wpisu oraz dane o objętym systemem kontroli pomieszczeniu, do którego dany pracownik w ramach nadanych mu uprawnień miał dostęp.

W stosowanym systemie nadawany był taki sam numer Card ID, jaki figuruje na karcie, którą posługiwał się pracownik (od czasu wprowadzenia systemu kontroli dostępu za pomocą linii papilarnych). Następnie dane były przesyłane z serwera do poszczególnych czytników linii papilarnych służących do ewidencji wejść i wyjść. Dane przesyłane z serwera obejmowały numer ID oraz kod w postaci ciągu cyfr. Biorąc za podstawę definicję danych osobowych sformułowaną w art. 6 uodo, GİODO uznał, że dane pracowników spółki pozyskane przez nią i przetworzone do postaci zapisu cyfrowego stanowią dane osobowe, gdyż w wyniku zestawienia kodu cyfrowego zarejestrowanego w systemie informatycznym z palcem pracownika przyłożonym do urządzania skanującego i pozostałymi informacjami możliwa jest identyfikacja konkretnej osoby.

Naruszenie praw pracownika

Sprawa ta trafiła do Naczelnego Sądu Administracyjnego, który wyrokiem z 1 grudnia 2009 r. (I OSK 249/09) stwierdził, że wyrażona na życzenie pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie jego danych osobowych w postaci linii papilarnych narusza prawa pracownika i swobodę wyrażenia przez niego woli. Za takim stanowiskiem przemawia zależność pracownika od pracodawcy. Brak równowagi w relacji pracodawca – pracownik stawia pod znakiem zapytania dobrowolność

Privacy by design

Idea by privacy design zrodziła się jako sposób spojrzenia na budowanie systemów teleinformatycznych. Zakłada, że każde przetwarzanie danych osobowych powinno być planowane z uwzględnieniem koncepcji ochrony prywatności w fazie projektowania. Privacy by design polega na tym, by od samego początku tworzenia jakiegos systemu na każdym etapie rozważać wpływ tworzonego rozwiązania na sferę prywatności i nie tyle odpowiadać na pojawiające się problemy, co przewidywać najważniejsze z nich i im prewencyjnie przeciwdziałać.

w wyrażeniu zgody na pobieranie i przetworzenie danych osobowych (biometrycznych). Z tego względu ustawodawca ograniczył art. 22¹ Kodeksu pracy katalog danych, których pracodawca może żądać od pracownika. Uznanie faktu wyrażenia zgody przez pracownika za okoliczność legalizującą pobranie od pracownika innych danych niż wskazane w art. 22¹ Kodeksu pracy stanowiłoby naruszenie tego przepisu. NSA powołał się także na przyjęty przez Grupę Roboczą Art. 29 w dniu 1 sierpnia 2003 r. dokument roboczy w sprawie biometrii, w którym przyjęto jako niezbędne zasady proporcjonalności i legalności. Oznacza to, że ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności wyrażona w art. 26 ust. 1 pkt 3 uodo jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników zatrudnionych w spółce jest nieproporcjonalne do zamierzonego celu ich przetwarzania. We wspomnianym dokumencie Grupa Robocza Art. 29 stwierdziła, że: „(...) pracodawca popełnia błąd, jeśli próbuje zalegalizować przetwarzanie danych pochodzących od pracownika za pomocą uzyskanej od niego zgody. Można posłużyć się zgodą, jeśli odnosi się ona do przypadku, w którym pracownik ma

całkowitą swobodę jej udzielenia i może odmówić udzielenia takiej zgody bez poniesienia szkody”. Naczelny Sąd Administracyjny w pełni zaaprobował pogląd wyrażony w dokumencie Grupy Roboczej Art. 29.

Ta linia orzecnicza została utrzymana w kolejnym wyroku NSA z 6 września 2011 r. (I OSK 1476/10) w sprawie skargi Naczelnika Urzędu Skarbowego na decyzję GİODO (sygn. sprawy DIS/DEC-1172/43212/09), która dotyczyła przywrócenia stanu zgodnego z prawem przez m.in. usunięcie i zaprzestanie zbierania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników przetwarzanych w celu ewidencji czasu pracy.

Zasada adekwatności

Na niedopuszczalność stosowania czytników biometrycznych w celu ewidencjonowania czasu pracy GİODO zwracał uwagę również w swoich wystąpieniach przesyłanych do różnych podmiotów. Jedno z nich zostało skierowane do kuratora oświaty, a dotyczyło systemu rejestrującego wejścia i wyjścia pracowników tego urzędu przez pobieranie odcisku palca (sygn. sprawy DOLIS-035-116/10). W swoim piśmie GİODO wskazał na zasadę legalizmu, do przestrzegania której zobowiązane są organy władzy publicznej na mocy art. 7 Konstytucji RP. Przypomniat, że dane biometryczne określonej osoby (takie jak jej linie papilarne i obraz tęczy oka) niewątpliwie można uznać za dane osobowe w rozumieniu definicji zawartej w uodo. Dane biometryczne to szczególny rodzaj danych osobowych, gdyż pozwalają na ustalenie tożsamości osoby w sposób pewny. Z racji ich wyłącznej przynależności do danej osoby dane biometryczne stanowią swego rodzaju „identyfikator” osoby fizycznej. W obowiązującym w Polsce porządku prawnym nie ma powszechnie obowiązujących przepisów, na podstawie których pracodawca mógłby żądać udostępnienia przez pracowników ich danych biometrycznych, takich jak linie papilarne. Mając na uwadze powyższe, pozyskiwanie przez pracodawcę odcisków palców pracowników w celu ich

identyfikacji w związku z wprowadzeniem systemu dokonującego na ich podstawie ewidencji czasu pracy, GODO ocenia jako prowadzące do naruszenia zasady adekwatności przetwarzania danych, o której mowa w art. 26 ust. 1 pkt 3 uodo. Ponadto organ ds. ochrony danych osobowych podkreślił, że pozyskiwanie przedmiotowych danych prowadzi do zbyt daleko idącej ingerencji w prywatność pracownika.

Podobne pismo zostało skierowane do dyrektora zespołu szkół muzycznych (sygn. sprawy DOLiS-035-115/10) w związku z wprowadzeniem elektronicznego systemu kontroli dostępu, który odczytuje (skanuje) obraz linii papilarnych nauczycieli, pracowników i uczniów. GODO wskazał w nim, że gromadzenie odcisków palców od tych osób jest nieadekwatne do celu ich przetwarzania, czyli zapewnienia im bezpieczeństwa na terenie zespołu szkół. Zespół szkół – jako placówka oświatowa – jest bowiem obowiązany nie tylko czuwać nad bezpieczeństwem uczniów, lecz także dbać o to, aby nie dochodziło do sytuacji mogących spowodować niezgodne z prawem przetwarzanie danych osobowych uczniów. Tymczasem pozyskiwanie obrazów linii papilarnych uczniów w celu zapewnienia im poczucia bezpieczeństwa jest niezgodną z zasadami w obowiązujących przepisach (np. ustawy z dnia 7 września 1991 r. o systemie oświaty; tekst jedn. z 2015 r. poz. 2156) ingerencją w sferę ich konstytucyjnej wolności. Może też prowadzić do zlekceważenia przez młodych ludzi rangi ważności danych biometrycznych, jakimi są linie papilarne.

Odmienne należałoby rozpatrywać ewentualne pozyskiwanie danych biometrycznych celem zapewnienia bezpieczeństwa jedynie w szczególnie istotnych strefach na terenie zespołu szkół. W tym kontekście warto wskazać, że Grupa Robocza Art. 29 w przywołanej już opinii nr 3/2012 uznała, że pracodawca musi zawsze dążyć do zastosowania środków w jak najmniejszym stopniu ingerujących w prywatność i wybierać w miarę możliwości rozwiązania, w których nie wykorzystuje się danych biometrycznych. W przypadkach, w których można odpowiednio uzasadnić taką konieczność,

podstawę prawną takiego przetwarzania mógłby stanowić uzasadniony interes administratora danych określony w art. 7 lit. f) dyrektywy 95/46/WE. Oznacza to, że mogą wystąpić przypadki, w których stosowanie systemów biometrycznych może leżeć w uzasadnionym interesie administratora danych. Przykładowo, jeżeli należy w sposób szczególny zapewnić bezpieczeństwo stref wysokiego ryzyka – stosując mechanizm umożliwiający dokładne sprawdzenie, czy dane osoby mają prawo dostępu do tych stref – to zastosowanie systemu biometrycznego może leżeć w uzasadnionym interesie administratora danych.

Weryfikacja głosowa

GODO odpowiadał również na zapytanie operatora telekomunikacyjnego (sygn. sprawy DOLiS-035-1174/12) dotyczące możliwości zastosowania weryfikacji głosowej klienta metodą biometryczną podczas rozmowy z konsultantem infolinii. Jak zauważył GODO, ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (tekst jedn. z 2014 r. poz. 243; pt) dopuszcza przetwarzanie danych dotyczących użytkownika, gdy jest to przedmiotem usługi i następuje za jego zgodą. Zgodnie z art. 159 ust. 2 pt zakazane jest inne (niż wskazane w tym przepisie) wykorzystywanie treści lub

w szczególności z uodo i pt. Powinno być jednak realizowane z uwzględnieniem wszystkich określonych w tych aktach prawnych obowiązków administratorów danych (w tym przedsiębiorców telekomunikacyjnych). W pierwszej kolejności należy zwrócić uwagę na prawidłowe wypełnienie obowiązku wynikającego z art. 174 pt. Konieczność uzyskania stosownej zgody to obowiązek uzyskania jasnego, wyraźnego, nienasuwającego wątpliwości pozytywnego oświadczenia woli przy tak samo jednoznacznym określeniu przedmiotu, którego oświadczenie to (czyli zgoda) dotyczy. Pamiętać przy tym należy o możliwości wycofania zgody w każdym czasie w sposób prosty i wolny od opłat. GODO zaznaczył także, że podobnie jak w przypadku działalności banków musi zostać zachowana opcjonalność rozwiązania. Szczególną uwagę należy poświęcić aspektom przechowywania i zabezpieczenia tych danych – wzorców stanowiących podstawę identyfikacji osób. Należy przy tym pamiętać o zasadzie czasowego ograniczenia przechowywania danych do momentu realizacji wyznaczonego celu przetwarzania. Rzetelnie dopełniony powinien być także obowiązek informacyjny oraz określony art. 26 ust. 1 pkt 2 i 3 uodo obowiązek dołożenia należytej staranności w celu ochrony interesów

Jednym z najczęściej pojawiających się problemów w praktyce GODO jest kwestia skanowania linii papilarnych pracowników do celów ewidencjonowania czasu ich pracy. Zdaniem organu przetwarzanie danych osobowych pracowników w postaci charakterystycznych punktów linii papilarnych odbywa się bez podstawy prawnej.

danych objętych tajemnicą telekomunikacyjną (w tym szeroko rozumianych danych dotyczących użytkownika) przez osoby inne niż nadawca i odbiorca komunikatu, chyba że będzie to przedmiotem usługi lub będzie to niezbędne do jej wykonania albo nastąpi za zgodą nadawcy lub odbiorcy, których dane te dotyczą. Zdaniem GODO opisane przedsięwzięcie nie stoi w sprzeczności z prawem,

osób, których dane dotyczą, poprzez zapewnienie, aby dane te były: zbierane dla oznaczonych i zgodnych z prawem celów, niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, dla jakich są przetwarzane. Analogicznie wskazano na niedopuszczalność np. profilowania abonentów na podstawie tych danych.

→ W czerwcu 2015 r. GIODO zajmował się kwestią planowanego wprowadzenia nowego Systemu Informacji Telefonicznej w biurach Krajowej Informacji Podatkowej, w ramach którego wykorzystywany miał być m.in. system biometrii głosowej, opisanej w Kierunkowych założeniach nowej ordynacji podatkowej (sygn. sprawy DOLiS-033-230/15). Rozwiązanie to wzbudziło szczególne zaniepokojenie GIODO nie tylko ze względu na wątpliwości dotyczące jego zgodności z przepisami Konstytucji RP i uodo, lecz także z uwagi na to, że przetarg na zaprojektowanie, dostawę oraz wdrożenie systemu został rozpisany na rok przed zaprezentowaniem założeń nowej ustawy Ordynacja podatkowa (reguluje ona kwestie związane z funkcjonowaniem Krajowej Informacji Podatkowej). Jest to sprzeczne z ideą *privacy by design* (patrz: ramka „Privacy by design”).

Nie można ograniczać praw

Wprowadzenie – bez jakiegokolwiek podstawy prawnej – systemu, którego funkcjonowanie prowadziłoby do ograniczenia konstytucyjnych wolności i praw, jest niedopuszczalne m.in. z uwagi na art. 31 ust. 3 Konstytucji RP. Zgodnie z jego brzmieniem ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw. Artykuł 51 ust. 2 Konstytucji RP stanowi, że władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Niewątpliwie cel i zakres pozyskiwanych danych powinny być podporządkowane zadaniom nałożonym na podmioty publiczne realizujące zadania w danym obszarze. Tylko wtedy bowiem zakres zbieranych danych nie będzie przekraczać kryterium „niezbędności w demokratycznym państwie prawnym”.

Prawo do ochrony prywatności i prawo do ochrony danych osobowych

Nie można dopuścić do tego, że osoby decydujące się na udostępnienie swoich danych biometrycznych będą traktowane w sposób bardziej uprzywilejowany niż osoby korzystające z innej formy kontaktu – szczególnie jeśli chodzi o usługę, która powinna być dostępna na równych zasadach dla wszystkich podatników.

są prawami osobistymi gwarantowanymi przez Konstytucję RP (art. 47 i art. 51), a więc ich ograniczenie wymaga regulacji rangi ustawowej. Powołane przepisy wyraźnie bowiem zastrzegają, że dopuszczalność zobowiązania kogoś do ujawnienia swoich danych osobowych oraz zasady i tryb gromadzenia i udostępniania tych danych oraz dostęp do urzędowych baz danych wymagają uregulowania ustawowego. Zgodnie zaś z art. 49 Konstytucji RP zapewnia się wolność i ochronę tajemnicy komunikowania się, a ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony. Tymczasem planowane rozwiązania polegające na nagrywaniu rozmów telefonicznych i analizie biometrycznej głosu, oprócz braku odpowiedniej podstawy prawnej, nie spełniają – w opinii GIODO – kryterium niezbędności. Zaprezentowane założenia jedynie ogólnikowo odnoszą się do kwestii stworzenia „systemu identyfikacji rozmówcy” i rejestrowania prowadzonych rozmów. Nie precyzują natomiast, na czym dokładnie te rozwiązania

miałyby polegać i nie wykazują niezbędności ich wprowadzenia ani konieczności ograniczenia konstytucyjnych wolności i praw. Poza tym przez projektodawcę nie został wskazany cel, jakiemu miałoby służyć takie ograniczenie prawa do prywatności, dlatego nie ma jasności, czy w ogóle jest ono uzasadnione. Projektodawca w pierwszej kolejności powinien wykazać niezbędność wprowadzenia danego rozwiązania, czyli że nie istnieje inny, mniej ingerujący w prywatność sposób realizacji danego celu. Należy zatem udowodnić, że z uwagi na ten cel system oparty na biometrii głosowej jest jedynym możliwym rozwiązaniem.

Zagrożenia przy stosowaniu biometrii

Rozważenia wymaga również, czy proponowany system gwarantuje równe prawa i dostęp do informacji podatkowej dla osób, które z uwagi na ochronę prywatności zdecydują się na formę kontaktu inną niż telefoniczna. Nie można bowiem dopuścić do tego, że osoby decydujące się na udostępnienie swoich danych biometrycznych będą w praktyce traktowane w sposób bardziej uprzywilejowany niż osoby korzystające z innej formy kontaktu, tym bardziej jeśli chodzi o usługę, która powinna być dostępna na równych zasadach dla wszystkich podatników. Należy ponadto zwrócić uwagę na potencjalne zagrożenia związane ze stosowaniem biometrii głosowej – przede wszystkim z punktu widzenia bezpieczeństwa tego rodzaju identyfikacji i ryzyka związanego z możliwością przechwycenia próbki głosu. Bez odpowiednich zabezpieczeń i funkcji pozwalających na identyfikowanie oszustw rozwiązanie zaprojektowane jako ułatwiające kontakt podatnika z administracją, w praktyce będzie się wiązało z licznymi zagrożeniami. Dlatego konieczne jest przeprowadzenie kompleksowej oceny i rzetelnej analizy planowanych rozwiązań tak, aby późniejsze propozycje zmian legislacyjnych były zgodne z opisanymi zasadami wynikającymi z prawa.

IT

Autorka jest Generalnym Inspektorem Ochrony Danych Osobowych.