DAGMARA JAROSZEWSKA-CHORAŚ

BIOMETRIA W HONGKONGU NA PRZYKŁADZIE PROBLEMU WYKORZYSTANIA ODCISKÓW PALCÓW DO KONTROLI CZASU PRACY

Wprowadzenie[1]

Celem niniejszego opracowania jest przedstawienie zagadnienia biometrii w kontekście obowiązujących przepisów odnoszących się do ochrony danych osobowych w Hongkongu.

Termin biometria pochodzi z języka greckiego, w którym *bios* oznacza życie, *metron* natomiast znaczy mierzyć. Wyniki pomiarów biometrycznych po opracowaniu metodami statystyki matematycznej są wykorzystywane między innymi w antropologii, fizjologii, genetyce, hodowli, medycynie, paleontologii[2]. Biometrię stosuje się przy dokonywaniu pomiarów w celu automatycznego uwierzytelniania tożsamości. Rozpoznawanie biometryczne lub inaczej biometria odnosi się do ustalania tożsamości osoby na podstawie jej cech fizjologicznych lub behawioralnych[3].

Metody identyfikacji człowieka towarzyszą ludzkości od dawna. Oczywiście w przeszłości sposoby weryfikacji określonych cech człowieka były mniej skomplikowane niż współcześnie. W starożytnych Chinach palce odciskano na urzędowych pieczęciach. Oficjalne dokumenty z szesnastowiecznej Persji były sygnowane przez decydenta kciukiem maczanym w farbie. W Babilonii odcisk palca na glinianej tabliczce stanowił potwierdzenie zawarcia transakcji. Pierwsze próby biometrycznego oznaczania osób stosowano w Imperium Rzymskim, gdzie nacinano, wypalano lub tatuowano skórę najemników, by utrudnić im dezercję[4].

Znaczący rozwój biometrii rozpoczął się w latach 60. XX w. i zbiegł się z rozwojem systemów komputerowych. Wiązał się on głównie z wykorzystywaniem odci-

[1] Wprowadzenie zostało opracowane na podstawie rozprawy doktorskiej autorki pt. *Prawne aspekty stosowania biometrii.*

[2] F. Jasiński, *Zagadnienia biometrii w Unii Europejskiej. Materiały robocze 4(8)/06*, Centrum Europejskie – Natolin, Warszawa 2006, s. 8.

[3] R.M. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha, A.W. Senior, *Biometria*, Warszawa 2008, s. XXIX.

[4] K. Krasowski, I. Sołtyszewski, *Biometria – zarys problematyki*, „Problemy Kryminalistyki" 2006, nr 252, s. 39.

sków palców. Liczba poszukiwań osób za pomocą odcisków palców była tak duża, że ręczne wyszukiwanie stawało się zbyt pracochłonne. Rozpoczęto więc prace nad stworzeniem systemu AFIS (*Automated Fingeprint Identification System*). W latach 80. XX w. rozwijała się technologia skanowania dokumentów, a wykorzystywanie komputerów osobistych stawało się coraz powszechniejsze. W następstwie tych okoliczności rozpoznawanie odcisków palców znalazło swoje zastosowanie nie tylko w kryminalistyce[5], medycynie sądowej[6], ale również w życiu codziennym, jak np. na lotniskach w celu zapewnienia szybkiej odprawy pasażerów[7] czy też w celu uzyskania dostępu do strzeżonych pomieszczeń[8].

Technologie biometryczne są również wykorzystywane w systemach rejestrujących informacje o obywatelach. W Europie w 2004 r. wprowadzone zostały paszporty biometryczne, w których wykorzystywane są dwie cechy biometryczne – wizerunek twarzy, a od 2009 r. również odciski palców[9]. Warto podkreślić, że prace nad elektronicznymi dokumentami podróży trwały od połowy lat 90. XX w. Wówczas Organizacja Międzynarodowego Lotnictwa Cywilnego (ICAO) nadzorowała prace nad wprowadzeniem danych biometrycznych do dokumentów podróży[10].

Powszechne jest także wykorzystywanie biometrii w celu realizacji polityki w zakresie swobodnego przepływu osób oraz w ramach polityki azylowej i imigracyjnej. Od kilku lat funkcjonują scentralizowane bazy danych, w których przetwarzane są między innymi odcisków palców pobierane od uchodźców, cudzoziemców, osób

---

[5] Dane biometryczne mają powszechne zastosowanie w postępowaniach kryminalnych, w ramach których wykorzystywane są między innymi odciski palców, fotografie twarzy oraz DNA.

[6] W medycynie sądowej systemy biometryczne są wykorzystywane w celu identyfikacji osób, która polega na rozpoznaniu nieznanej osoby poprzez badanie jednej lub kilku jej cech biometrycznych. System porównuje aktualny obraz zapisany przez odpowiednie urządzenie ze wzorcami zapisanymi w scentralizowanej bazie danych. Zob. E. Filipowicz, J. Kwiecień, M. Kłys, B. Filipowicz, *Analiza możliwości zastosowania metod sztucznej inteligencji w medycynie sądowej*, „Bio-Algorithms and Med-Systems" 2005, vol. 1, no. 1/2, s. 3–8.

[7] Na lotnisku Schiphol w Amsterdamie od 2001 r. testowany był pierwszy europejski system identyfikacji biometrycznej w oparciu o obraz tęczówki oka. Więcej informacji na temat zastosowań biometrii zob. K. Krassowski, I. Sołtyszewski, *Zastosowania biometrii – przegląd kluczowych programów i rozwiązań w zakresie ochrony państwa*, „Problemy Kryminalistyki" 2007, nr 255, s. 5–9.

[8] R.M. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha, A.W. Senior, *Biometria*…, s. 35–36.

[9] W dniu 13 grudnia 2004 r. przyjęto rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i w dokumentach podróży wydawanych przez państwa członkowskie (Dz. Urz. UE L 385 z 29.12.2004 r., s. 1–6). Zmiany do rozporządzenia zostały wprowadzone rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 444/2009 z dnia 28 maja 2009 r. zmieniającym rozporządzenie Rady (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i w dokumentach podróży wydawanych przez państwa członkowskie (Dz. Urz. UE L 142 z 6.06.2009 r., s. 1–4).

[10] T. Petermann, A. Sauter, C. Scherz, *Biometrics at the borders – the challenges of a political technology*, „International Review of Law, Computers & Technology", March-July 2006, vol. 20, no. 1–2, s. 154.

ubiegających się o udzielenie ochrony międzynarodowej oraz osób składających wniosek o wizę[11]. Biometria jest również wykorzystywana jako rozwiązanie wspierające walkę z terroryzmem[12]. Znajduje szerokie zastosowanie w relacjach pracownik – pracodawca. Systemy biometryczne są stosowane np. w celu kontrolowania czasu pracy. Czytniki biometryczne sprawdzają się też w sytuacji, gdy pracownik musi dostać się do konkretnego pomieszczenia na terenie zakładu pracy (np. do laboratorium). Biometria jest więc wykorzystywana zarówno w sektorze publicznym, jak i prywatnym.

Prawo do ochrony danych osobowych w Hongkongu

Wzrost zainteresowania problematyką związaną z ochroną danych osobowych oraz prawa do prywatności w Hongkongu pojawił się w latach 70. XX w. z uwagi na rozwój technologii komputerowych[13]. W 1983 r. rząd powołał specjalną grupę

[11] Pierwsza baza danych o nazwie Eurodac zaczęła funkcjonować 15 stycznia 2003 r. System Eurodac został ustanowiony na mocy rozporządzenia Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczącego ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania konwencji dublińskiej (Dz. Urz. WE L 316 z 15.12.2000 r., s. 1). Natomiast 26 czerwca 2013 r. uchwalono nowe rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (wersja przekształcona) (Dz. Urz. UE L 180 z 29.06.2013 r., s. 1–30). Powyższa regulacja w zasadniczy sposób zmieniła pierwotne cele, dla których został powołany system. Nowe przepisy zaczęły obowiązywać od dnia 20 lipca 2015 r. Warto dodać, że według danych statystycznych z 2014 r. opracowanych przez Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-Lisa) w systemie Eurodac zgromadzono 2,7 mln zapisów odcisków palców (po 10 odcisków) i łącznie przeprowadzono 756 368 operacji. W związku z wprowadzonymi procedurami kontroli jakości wskaźnik odrzuceń odcisków niespełniających wymagań normy wyniósł 4,49%, co wiązało się z koniecznością ponownego pobrania i wprowadzenia odcisków. Zob. Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady. Dostępność i gotowość rozwiązań technologicznych umożliwiających identyfikację osoby na podstawie odcisków palców przechowywanych w Systemie Informacyjnym Schengen drugiej generacji (SIS II), COM(2016) 93 final, Bruksela, 29.02.2016 r., s. 5.

[12] F. Jasiński, *Zagadnienia biometrii*…, s. 7.

[13] Warto dodać, że Hongkong przed rokiem 1997 miał skomplikowany status prawny i międzynarodowy. Zbudowany był bowiem z trzech części, które zostały skolonizowane w różnych

roboczą, a wzorem Organizacji Współpracy Gospodarczej i Rozwoju (OECD) zostały opracowane wytyczne poświęcone tematyce związanej z ochroną danych osobowych[14].

Zasady dotyczące ochrony danych osobowych i prawa do prywatności zostały uregulowane między innymi w ustawie The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China (dalej: Basic Law)[15]. Warto w tym miejscu zwrócić uwagę na przepis zawarty w art. 30, który reguluje kwestię prawa do prywatności w zakresie wolności komunikacji. Zgodnie z art. 30 Basic Law: „wolność i prywatność komunikacji mieszkańców Hongkongu musi być chroniona przez prawo. Żaden departament (żadna instytucja) ani osoba nie może, pod żadnymi warunkami, naruszać wolności ani prywatności komunikacji rezydentów Hongkongu, za wyjątkiem odpowiednich władz, które mogą sprawdzać komunikację zgodnie z obowiązującymi procedurami i przepisami w celu zapewnienia bezpieczeństwa publicznego oraz w celu prowadzenia postępowań w zakresie popełnianych przestępstw".

Jednakże z punktu widzenia prawa do ochrony danych osobowych podstawowe znaczenie ma ustawa The Personal Data (Privacy) Ordinance (Cap. 486) z 1995 r. Hongkong jest drugim regionem w Azji, który wprowadził ustawę w całości poświęconą ochronie danych osobowych[16]. W lipcu 2012 r. ustawa została znowelizowana. Większość zmian zaczęła obowiązywać 1 października 2012 r. Dwie kolejne istotne nowelizacje (dotyczące zastosowań marketingu bezpośredniego oraz nowych uprawnień dla komisarza ds. prywatności i ochrony danych osobowych) weszły w życie 1 kwietnia 2013 r.[17] Podmioty, które zbierają, przechowują i wykorzystują dane osobowe (w tym również dane biometryczne), są zobligowane do przestrzegania przepisów ustawy The Personal Data (Privacy) Ordinance.

Dane biometryczne stanowią dane osobowe o szczególnym charakterze, odnoszą się bowiem do behawioralnych i fizjologicznych cech danej osoby i mogą

---

okresach przez Wielką Brytanię. Jedna z części, tzw. Wielkie Terytoria, która stanowiła 92% ogólnej powierzchni, została wydzierżawiona na 99 lat, natomiast pozostałe części zostały scedowane na rzecz Wielkiej Brytanii. Po 154 latach brytyjskiego panowania, od 1 lipca 1997 r. Hongkong stanowi specjalny region administracyjny należący do Chin. Szerzej zob. K. Żakowski, *Hongkong w nowej rzeczywistości* [w:] *Współczesne Chiny. Kultura – polityka – gospodarka*, red. M. Pietrasiak, Łódź 2005, s. 86–98.

[14] G. Greenleaf, *Comparative Study*, *Different Approaches to New Privacy Challenges in particular in the light of technological developments*, *B.3 – Hongkong*, European Commision, Directorate – General Justice, Freedom and Security, May 2010, s. 7.

[15] Tekst ustawy dostępny na stronie: http://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw_full_text_en.pdf (dostęp: 16.08.2016).

[16] Zob. C. Rich, *Privacy Law in Asia*, seria: Privacy and Security Law Report, s. 2, https://media2.mofo.com/documents/140422privacylawsasia.pdf (dostęp: 13.07.2016).

[17] Data Protecion Laws of the World, s. 181, https://www.dlapiperdataprotection.com/#handbook/world-map-section (dostęp: 24.07.2016).

prowadzić do jej bezpośredniej identyfikacji[18]. Dane te można zdefiniować jako właściwości biologiczne, cechy fizjologiczne, cechy życiowe lub powtarzalne czynności, przy czym te cechy i/lub czynności dotyczą wyłącznie danej osoby, a jednocześnie są wymierne, nawet jeżeli schematy używane w praktyce do ich pomiaru charakteryzuje pewien stopień prawdopodobieństwa[19]. Typowymi przykładami danych biometrycznych są odciski palców, wzorzec siatkówki, struktura twarzy, głos, ale także geometria dłoni, układ żył lub nawet pewne głęboko zakorzenione umiejętności lub inne cechy i zachowania, takie jak np. własnoręczny podpis, uderzenie w klawisze komputera, szczególny sposób chodzenia lub mówienia[20]. Wykorzystywanie technologii biometrycznych w celu autoryzacji i uwierzytelnienia wiąże się z przetwarzaniem szczególnej kategorii danych osobowych, czyli danych biometrycznych. Z kolei przetwarzanie danych osobowych, w tym danych biometrycznych, musi się odbywać zgodnie z podstawowymi zasadami prawa w zakresie ochrony danych osobowych.

The Personal Data (Privacy) Ordinance zawiera sześć podstawowych zasad dotyczących ochrony danych osobowych[21]. Mają one duże znaczenie w kontekście przetwarzania danych, w tym danych biometrycznych.

Pierwsza zasada reguluje celowość i sposób zbierania danych osobowych[22]. Zgodnie z nią dane osobowe muszą być zbierane uczciwie i zgodnie z poszanowaniem prawa, wyłącznie do celów bezpośrednio związanych z działalnością administratora danych. Natomiast osoby, od których pobierane są dane osobowe, muszą zostać poinformowane o tym, w jakim celu zbierane są ich dane oraz o tym, kto będzie miał do nich dostęp. Ponadto pobieranie danych powinno odbywać się zgodnie z zasadą proporcjonalności.

Kolejna zasada odnosi się do kwestii dokładności oraz okresu przetrzymywania danych osobowych[23]. Dane osobowe muszą być dokładne i nie powinny być prze-

---

[18] Grupa Robocza Art. 29 ds. Ochrony Danych Osobowych, *Working dokument on biometrics*, 1.08.2003 r., 12168/02/EN, WP 80, s. 2. Grupa Robocza Art. 29 ds. Ochrony Danych Osobowych to niezależny europejski organ doradczy w sprawach ochrony danych i prywatności, powołany na mocy art. 29 dyrektywy o ochronie danych 95/46/WE. Grupę Roboczą tworzą przedstawiciele krajowych organów ochrony danych z państw członkowskich UE, Europejskiego Inspektora Ochrony Danych oraz Komisji Europejskiej. Podstawowe zadania Grupy zostały opisane w art. 30 dyrektywy 95/46/WE oraz w art. 15 dyrektywy 2002/58/WE.

[19] Grupa Robocza Art. 29 ds. Ochrony Danych, Opinion 3/2012 *on developments in biometric technologies*, 27.04.2012 r., 00720/12/EN, WP 193, s. 4.

[20] Opinia Grupy Roboczej Art. 29 ds. Ochrony Danych, Opinia WP 136, 4/2007 *w sprawie pojęcia danych osobowych*, 20.06.2007 r., s. 8.

[21] Sections 72, 73 schedule 1 The Personal Data (Privacy) Ordinance, s. 51–54. Zob. też: Y. Ming Tham, J. Lee, *Hong Kong* [w:] *The Privacy Data Protection and Cybersecurity Law Review*, ed. A.Ch. Raud, 2nd ed., Derbyshire, UK 2015, s. 137–140.

[22] Principle 1 – purpose and manner of collection of personal data.

[23] Principle 2 – accuracy and duration of retention of personal data.

trzymywane dłużej, niż jest to konieczne dla realizacji celu, do którego są wykorzystywane. Zgodnie z Personal Data (Privacy) Ordinance dane osobowe mogą być wykorzystywane wyłącznie do celu, do którego zostały pobrane lub bezpośrednio związanego z pierwotnym celem przetwarzania. Należy jednak zaznaczyć, że przepisy ustawy umożliwiają administratorowi danych przetwarzanie danych osobowych w innym celu, ale tylko wówczas, gdy osoba, od której zostały one pobrane, wyrazi na to zgodę[24].

Prawodawca wprowadził również zasadę odnoszącą się do bezpieczeństwa danych, zgodnie z którą administrator danych osobowych musi wdrożyć praktyczne mechanizmy ich zabezpieczenia przed przypadkowym lub nieautoryzowanym dostępem do nich, ich przetwarzaniem, usunięciem czy też utratą[25]. Natomiast zgodnie z zasadą przejrzystości danych osobowych ich administrator musi udostępnić polityki i praktyki dotyczące przetwarzania danych, szczególnie w zakresie typów danych, które przetwarza oraz informacji o tym, w jaki sposób są one wykorzystywane[26]. Z kolei w myśl zasady dostępu do danych osobowych osoba, której dane są przetwarzane, powinna otrzymać do nich dostęp i mieć możliwość ich korekty, gdy są niedokładne[27].

Podstawowe zalecenia dotyczące wykorzystywania danych biometrycznych

Przepisy zawarte w The Personal Data (Privacy) Ordinance nie odnoszą się wprost do kwestii przetwarzania danych biometrycznych. Natomiast zasadnicze wymogi dotyczące ochrony danych biometrycznych zostały opracowane w wytycznych z dnia 20 lipca 2015 r. Guidance on Collection and use of Biometric Data, przygotowanych przez komisarza ds. prywatności i ochrony danych osobowych (Privacy Commissioner for Personal Data, dalej: komisarz)[28]. Wypracowane w podręczniku standardy ułatwiają instytucjom przetwarzającym dane biometryczne działanie zgodne z obowiązującym prawem do ochrony danych osobowych.

Wytyczne z lipca 2015 r. regulują sześć podstawowych obszarów: 1) konieczność „rozważnego" przetwarzania wrażliwych danych biometrycznych; 2) uzasadnienie

[24] Principle 3 – use of personal data.

[25] Principle 4 – security of personal data.

[26] Principle 5 – information to be generally available.

[27] Principle 6 – access to personal data.

[28] Zastąpiły one zasady opracowane w 2012 r. Warto podkreślić, że komisarz wydał kilka opracowań dotyczących ochrony danych osobowych w kontekście nowoczesnych technologii. Jednym z nich jest np. Guidance on CCTV Surveillance and Use of Drones (the CCTV Guidance) z dnia 31 marca 2015 r.

dla zbierania i przetwarzania danych biometrycznych; 3) wykorzystanie technik minimalizacji ryzyk dotyczących przetwarzania danych biometrycznych; 4) potrzeba stosowania metodologii PIA (ocena wpływu na prywatność); 5) nieprzymuszona i świadoma możliwość wyboru (czy dane biometryczne danej osoby będą wykorzystywane); 6) wymagania dotyczące prywatności podczas przetwarzania danych biometrycznych.

Zgodnie ze stanowiskiem zaprezentowanym przez komisarza dane biometryczne można zakwalifikować do kategorii wrażliwych danych osobowych[29], gdyż mogą zawierać między innymi informacje dotyczące pochodzenia rasowego, etnicznego czy też stanu zdrowia, w tym psychicznego[30]. Istnieją przesłanki, że możliwe jest rozpoznawanie niektórych chorób na podstawie danych pochodzących z odcisków palców (np. nowotwór piersi, zespół różyczki wrodzonej oraz niektóre zaburzenia chromosomów, takie jak zespół Downa czy zespół Turnera). Medyczne badania naukowe wskazują, że dane tęczówki mogą być powiązane z cukrzycą, miażdżycą, nadciśnieniem, HIV oraz nadużywaniem alkoholu i narkotyków[31].

W wytycznych komisarz podkreślił, że nieprawidłowe wykorzystywanie danych biometrycznych może prowadzić do dyskryminacji, ponieważ mogą zostać ujawnione intymne informacje na temat danej osoby. Należy zauważyć, że komisarz już wcześniej sygnalizował, iż niewłaściwe przetwarzanie danych biometrycznych

---

[29] Na przykład w prawodawstwie europejskim dane wrażliwe stanowią specjalną kategorię danych osobowych, w stosunku do której istnieje co do zasady zakaz ich przetwarzania. Zgodnie z obowiązującą nadal dyrektywą 95/46/WE: „Państwa Członkowskie zabraniają przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego"(art. 8 ust. 1). Należy zaznaczyć, że 4 maja 2016 r. zostało opublikowane nowe rozporządzenie Parlamentu Europejskiego i Rady dotyczące ochrony danych osobowych. Przepisy rozporządzenia będą stosowane od 25 maja 2018 r. Zgodnie z art. 9 ust. 1 powyższej regulacji: „Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby". Przetwarzanie danych wrażliwych jest jednak możliwe wówczas, gdy spełnione zostaną określone prawem warunki. W art. 9 ust. 2 wskazano bowiem 10 przesłanek umożliwiających przetwarzanie tej szczególnej kategorii danych osobowych. Szczegóły zob. rozporządzenie 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. EU L 119 z 4.05.2016 r., s. 1–88).

[30] Guidance on Collection and use of Biometric Data, s. 2.

[31] Zob. G Hornung, *The European Regulation on Biometric Passports: Legislative Procedures*, *Political Interactions*, *Legal Framework and Technical Safeguards*, (2007) 4:3 *SCRIPTed* 246, s. 9, http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.asp (dostęp: 16.08.2016).

może prowadzić do negatywnych następstw, takich jak profilowanie[32], kontrolowanie jednostek czy kradzież tożsamości[33]. Przechowywanie danych biometrycznych w bazach danych w powiązaniu np. ze skradzionym dokumentem tożsamości może prowadzić do poważnych konsekwencji dla posiadacza skradzionego dokumentu. Ryzyko kradzieży tożsamości może wynikać również z niedokładności technologii biometrycznych. Niestety, w przypadku kradzieży danych biometrycznych nie można zapewnić osobie nowych danych, tak jak w innych systemach identyfikacji (np. nadanie nowego hasła, nowego numeru PIN). W odniesieniu do odcisków palców ryzyko kradzieży tożsamości jest szczególnie wysokie.

W podręczniku wskazano także, że przechowywanie danych biometrycznych w oryginalnym formacie (np. odciski linii papilarnych, fotografie twarzy) stwarza większe zagrożenie dla praw człowieka, w szczególności prawa do prywatności, niż przechowywanie takich informacji w formie szablonów (wzorców biometrycznych)[34]. Z tego względu, zdaniem komisarza, dane biometryczne muszą być jak najszybciej przetwarzane do postaci szablonów[35].

---

[32] Profilowanie wiąże się z kategoryzowaniem osób według ich cech „niezmiennych" (takich jak: płeć, wiek, pochodzenie etniczne, wzrost) czy „zmiennych" (takich jak: zwyczaje, preferencje i inne elementy zachowania). Szczegóły zob. Agencja Praw Podstawowych, *Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu: przewodnik*, Luksemburg 2010, s. 8. W Europie kwestia profilowania została również zdefiniowana w rozporządzeniu 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). Zgodnie z art. 4 pkt 4 rozporządzenia profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

[33] R.B. Woo, *Challenges Posed by Biometric Technology on Data Privacy Protection and the Way Forward* [w:] *Ethics and Policy of Biometrics*, eds. A. Kumar, D. Zhang, Berlin–Heidelberg 2010, s. 2.

[34] Należy w tym miejscu wyjaśnić, czym jest wzorzec biometryczny. Z danych biometrycznych w formie nieprzetworzonej (np. fotografia twarzy, odciski palców) można wyodrębnić kluczowe identyfikatory biometryczne (np. wymiary twarzy z fotografii), które można przechowywać do celów późniejszego przetworzenia zamiast samych danych nieprzetworzonych. Na podstawie takich cech tworzy się wzorzec biometryczny danych. Bardzo ważną kwestią jest określenie wielkości (liczby informacji) wzorca. Tworzenie wzorca powinno być procesem jednokierunkowym, tak aby na jego podstawie nie można było odtworzyć nieprzetworzonych danych biometrycznych. Szczegóły zob. Opinia Grupy Roboczej Art. 29 ds. Ochrony Danych, Opinion 3/2012 (…), s. 4.

[35] Guidance on Collection and use of Biometric Data, s. 3.

Wykorzystywanie danych biometrycznych w miejscu pracy

Szybko rozwijającym się sektorem, w ramach którego są stosowane technologie biometryczne, jest obszar związany z funkcjonowaniem rynku pracy. Na szeroką skalę wykorzystywane są zabezpieczenia biometryczne mające na celu kontrolowanie czasu pracy oraz zabezpieczenie pomieszczeń przed dostępem nieuprawnionych osób.

Z punktu widzenia przepisów prawa te dwa wskazane zastosowania mają znaczenie, gdyż różne będą cele związane z przetwarzaniem danych biometrycznych. To z kolei ma związek z zasadą proporcjonalności. Pojawia się bowiem pytanie: czy kontrolowanie czasu pracy pracownika, np. za pomocą odcisków palców, jest zgodne z powyższą zasadą, skoro można wykorzystać sposoby mniej inwazyjne dla prywatności. Stosowanie czytników biometrycznych w miejscu pracy nadal wzbudza wiele kontrowersji.

Na wstępie należy zaznaczyć, że zagadnienie dotyczące wykorzystywania przez pracodawcę odcisków palców pobieranych od pracowników nie zostało uregulowane w przepisach prawa w Hongkongu. Natomiast zasady te zostały opracowane w dokumencie Guidance on Collection and use of Biometric Data[36]. Naczelna reguła dotyczy tzw. „nieprzymuszonej i świadomej możliwości wyboru (czy dane biometryczne danej osoby będą wykorzystywane)". Osoba, której dane biometryczne mają być wykorzystywane, musi w sposób świadomy i swobodny wyrazić na to zgodę. Dodatkowo należy poinformować ją o wpływie technologii biometrycznych na prawo do prywatności.

Administrator danych osobowych jest zobowiązany, aby poinformować osobę, której dane biometryczne są lub będą przetwarzane, o kilku zasadniczych kwestiach. Po pierwsze, czy przekazywanie danych biometrycznych ma charakter dobrowolny, czy obowiązkowy? Po drugie, jeżeli przetwarzanie danych biometrycznych ma charakter obowiązkowy, to jakie będą konsekwencje dla osoby, która nie chce takich danych przekazać? Po trzecie, jaki będzie cel przetwarzania takich danych? Po czwarte, kto będzie miał do nich dostęp? Ponadto osoba, której dane biometryczne mają być przetwarzane, musi zostać poinformowana o sposobie dostępu do swoich danych osobowych oraz możliwości ich korekty[37].

Zgodnie z postanowieniami opracowanymi przez urząd komisarza pracodawca, który zamierza przetwarzać dane biometryczne swoich pracowników, musi się upewnić, że pracownicy wyrazili zgodę (w sposób swobodny, nieprzymuszony) na pobranie i przetwarzanie danych biometrycznych. Zgodnie z wytycznymi zgoda udzielana przez pracownika powinna zostać sporządzona na piśmie (przede wszystkim dla celów dowodowych). Jeżeli pracownik wyraził w sposób swobodny zgodę

[36] Dodatkowo instytucje, które wykorzystują dane biometryczne, są zobligowane do przestrzegania przepisów ustawy The Personal Data (Privacy) Ordinance.

[37] Guidance on Collection and use of Biometric Data, s. 7.

na przetwarzanie jego danych osobowych, to taki wybór będzie respektowany przez komisarza. Natomiast w sytuacji, gdy zgoda na pobieranie danych biometrycznych została udzielona pod jakąkolwiek presją lub nie miała charakteru dobrowolnego, komisarz przeprowadza postępowanie kontrolne. W dokumencie podkreślono również, że pracodawca, aby minimalizować ryzyko naruszenia prawa do prywatności, powinien zaproponować alternatywne metody ewidencjonowania danych osobowych pracowników, takie jak karty chipowe, kamery.

W latach 2014–2015 do komisarza wpłynęło 1690 skarg, które w znacznym stopniu były związane ze stosowaniem nowoczesnych technologii informacyjnych[38]. Coraz więcej z nich dotyczy niezgodnego z prawem wykorzystywania danych biometrycznych w postaci odcisków palców w celu kontrolowania czasu pracy. Jednym z uprawnień komisarza jest możliwość wszczęcia postępowania kontrolnego w przypadku naruszeń przepisów dotyczących ochrony danych osobowych[39].

Takie postępowanie kontrolne zostało przeprowadzone w firmie Queenix (Asia) Limited. W dniu 21 lipca 2015 r. komisarz opublikował raport pokontrolny z przeprowadzonego dochodzenia[40].

Na początku stycznia 2014 r. skarżąca została zatrudniona w fimie Queenix (Asia) Limited. Natomiast 23 stycznia 2014 r. rozwiązała ona umowę o pracę. Już pierwszego dnia pracy pracodawca pobrał od niej odciski palców. Według skarżącej w firmie były dwa miejsca, w których wykorzystywano czytniki biometryczne. Jedno znajdowało się przy wejściu do biura, a drugie w salonie wystawowym. Zarówno jeden, jak i drugi system służył do kontrolowania obecności w pracy oraz miał na celu zapewnienie bezpieczeństwa (zabezpieczenie przed kradzieżami, które już wcześniej zdarzały się w firmie). Zdaniem skarżącej odciski palców mają charakter wrażliwych danych osobowych. Procedura ustalania tożsamości za ich pomocą była w kontrolowanej instytucji obowiązkowa. Skarżąca sugerowała pracodawcy, aby zapewnił mniej inwazyjne, alternatywne sposoby kontrolowania obecności w pracy. Pomimo jej próśb firma Queenix nie wdrożyła innych rozwiązań, więc, nie mając wyboru, skarżąca przekazała pracodawcy swoje odciski palców. Drugiego dnia w pracy zaprezentowała pracodawcy prosty formularz dotyczący zgody na przetwarzanie danych osobowych z propozycją, aby firma Queenix wykorzystywała podobny formularz do uzyskania zgody na przetwarzanie danych biometrycznych pobieranych od pozostałych pracowników. Pracodawca nie wziął pod uwagę tego rozwiązania.

---

[38] Y. Ming Tham, J. Lee, *Hong Kong*…, s. 135.

[39] Sekcja 38 The Personal Data (Privacy) Ordinance. Komisarz wszczyna postępowanie między innymi wówczas, gdy wpłynie do niego skarga od osoby fizycznej, w której wskazano, że doszło do naruszenia prawa do ochrony danych osobowych.

[40] Report Published under Section 48(2) of the The Personal Data (Privacy) Ordinance (Cap. 486), Investigation Report: Collection of Fingerprint Data by Queenix (Asia) Limited, Report Number: R15-2308, 21.07.2015, https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R15_2308_e.pdf (dostęp: 10.08.2016).

Skarżąca miała podejrzenia, że jej dane osobowe, w tym w szczególności jej dane biometryczne, nie są przetwarzane zgodnie z przepisami ustawy i w związku z tym złożyła skargę do komisarza, który rozpoczął kontrolę[41].

W trakcie podstępowania firma Queenix przyznała, że nie miała opracowanej pisemnej strategii związanej z przechowywaniem i przetwarzaniem danych biometrycznych w postaci odcisków palców. Nie zapewniono odpowiedniej polityki bezpieczeństwa przetwarzania danych osobowych w komputerowych bazach danych. Firma Queenix przyznała, że osoba rozpoczynająca pracę była informowana jedynie w sposób ustny, między innymi o tym, że dane o odciskach palców będą wykorzystywane do kontrolowania czasu pracy oraz w celu zapewnienia bezpieczeństwa[42].

W toku przeprowadzonej kontroli komisarz ustalił kilka zasadniczych kwestii. Po pierwsze, zwrócił uwagę na fakt, że odciski palców są danymi osobowymi w rozumieniu przepisów ustawy The Personal Data (Privacy) Ordinance[43]. Po drugie, stwierdził, że odciski palców stanowią dane wrażliwe, których utrata może rodzić poważne konsekwencje, włącznie z kradzieżą tożsamości. Komisarz uznał, że w przypadku firmy Queenix wykorzystywanie odcisków palców pracowników było nieproporcjonalne do zamierzonego celu ich przetwarzania. Według komisarza odciski palców są unikatowym wzorcem fizjologicznym, który pozwala zidentyfikować osobę. Po trzecie, zbieranie odcisków palców przez Queenix było działaniem nadmiernie ingerującym w prawo prywatności. W toku postępowania ustalono, że w tym konkretnym przypadku system bazujący na odciskach palców nie zwiększał bezpieczeństwa i był zbędny, gdyż wykorzystywano także inne, mniej inwazyjne metody, takie jak cyfrowe zamki, łańcuchy i monitoring[44]. Ponadto, w kontekście kontrolowania obecności czasu pracy komisarz uznał, że nie było konieczności wykorzystywania odcisków palców, a wystarczające byłyby tradycyjne metody (np. dziennik wejść – wyjść, tym bardziej że firma Queenix zatrudniała tylko 20 pracowników). Podsumowując, zdaniem komisarza system wykorzystujący odciski palców był nieproporcjonalny.

W toku przeprowadzonej kontroli komisarz wykazał, że wykorzystywanie przez firmę Queenix danych o odciskach palców pracowników stanowiło naruszenie zasady celowości i sposobu zbierania danych osobowych (zasada nr 1 ustawy The Personal Data (Privacy) Ordinance). Ponadto komisarz ustalił, że doszło również do

[41] *Ibidem*, s. 2 i 3.

[42] *Ibidem*, s. 11

[43] W oryginale: „Personal data means any data: a) relating directly or indirectly to a living individual; b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and c) in a form in which access to or processing of the data is practicable" (Section 2(1) The Personal Data (Privacy) Ordinance).

[44] Report Published under Section 48(2) of the The Personal Data (Privacy) Ordinance (…), s. 14.

naruszenia zasady dokładności oraz okresu przechowywania danych osobowych. Jego zdaniem przetwarzanie danych o odciskach palców „nie było w porządku"[45] wobec pracowników. W przypadku firmy Queenix pracownicy nie wyrazili dobrowolnie zgody na przetwarzanie danych o odciskach palców, gdyż system był obowiązkowy i nie zapewniono alternatywnych rozwiązań[46]. Firma ta nie przekazała pracownikom żadnych szczegółów dotyczących działania systemu biometrycznego (ani technicznych, ani organizacyjnych). Komisarz przedstawił w raporcie pokontrolnym również dodatkowe rekomendacje związane z przetwarzaniem danych biometrycznych. Podkreślił, że dokument Guidance on Collection and Use of Biometric Data stosuje się też do innych danych biometrycznych, takich jak DNA, siatkówka oka, podpis czy odcisk dłoni.

Na zakończenie tej części rozważań warto podkreślić, że podobne kwestie były także rozstrzygane przez europejskich inspektorów ds. ochrony danych osobowych. Na przykład włoski organ ochrony danych osobowych uznał, że wykorzystywanie odcisków palców w miejscu pracy w celu kontroli obecności pracowników lub też weryfikacji zgodności z godzinami pracy stanowi naruszenie zasady proporcjonalności, gdyż cel ten może być osiągnięty dzięki innym systemom, które są mniej „inwazyjne" dla prywatności i nie naruszają dobra, jakim jest godność człowieka[47].

W Polsce Generalny Inspektor Ochrony Danych Osobowych (GIODO) musiał zmierzyć się z analogicznym problemem. W 2008 r. GIODO wydał decyzję nakazującą usunięcie uchybień w procesie przetwarzania danych biometrycznych w firmie LG Electronics Mława. Zakres rozstrzyganej sprawy dotyczył przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U.

[45] W raporcie użyto słowa „unfair".

[46] Report Published under Section 48(2) of the The Personal Data (Privacy) Ordinance (…), s. 16.

[47] The Garante Per La Protezione dei Dati Personali, *Use of Fingerprints for Assiduity Control at the Workplace*, 21.07.2005 r., doc. n. 1166892, dostępne na stronie: http://www.garanteprivacy.it/garante/doc.jsp?ID=1166892. Podobną opinię przedstawił również grecki organ ds. ochrony danych osobowych, Data Protection Authority, Decision 245/9, 20.03.2000 r., Athens, *Identification through taking fingerprints*, dostępne na stronie: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/05%20DECISION%20NO.%20245_9%20-%2020.03.2000.DOC (dostęp: 7.08.2016). W podsumowaniu opinii włoskiego organu ochrony danych osobowych czytamy: „In line with Community law – whereby the processing of data entailing specific risks to data subjects' rights and fundamental freedoms, such as the one in question, is to be allowed only following a prior checking aimed at establishing that the processing is lawful and fair as well as laying down measures and instructions to safeguard data subjects (see Article 20 of EC Directive 95/46, and Section 17 of the DP Code) – it is hereby concluded that the prerequisites envisaged by the law to process data relating to fingerprints are not met in the case at issue. Therefore, the processing referred to in the submission is to be regarded as unlawful on the grounds described heretofore".

z 2016 r., poz. 922) oraz prawa pracy, tj. ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (tekst jedn.: Dz. U. z 2016 r., poz. 1666, dalej: k.p.).

W 2007 r. w firmie LG Electronic wprowadzono rejestrację wejść i wyjść pracowników za pomocą czytników linii papilarnych. Za podstawę prawną umożliwiającą przetwarzanie takich danych uznano art. 22^1 § 5 k.p. Przepis ten odsyła do ustawy o ochronie danych osobowych w kontekście przetwarzania danych na podstawie udzielonej przez osobę zgody[48]. Odbyło się to za zgodą pracowników wyrażoną w pisemnych oświadczeniach. Jednak GIODO nakazał usunięcie tych informacji i zaprzestanie ich pobierania, argumentując, że nie istnieje podstawa prawna do tego typu działań. Według jego opinii wyrażenie zgody przez pracowników niczego nie zmienia w tej kwestii. Sprawa została skierowana do Wojewódzkiego Sądu Administracyjnego, który w dniu 27 listopada 2008 r. wydał wyrok (II/SA/Wa 903/08) uchylający decyzję GIODO.

Z kolei Naczelny Sąd Administracyjny w wyroku z dnia 1 grudnia 2009 r. (I OSK249/09) stwierdził, że brak równowagi w relacji pracodawca – pracownik stawia pod znakiem zapytania dobrowolność w wyrażeniu zgody na pobieranie i przetwarzanie danych osobowych (biometrycznych)[49]. Z tego względu ustawodawca ograniczył przepisem art. 22^1 k.p. katalog danych, których pracodawca może żądać od pracownika. Uznanie faktu wyrażenia zgody na podstawie art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych jako okoliczności legalizującej pobranie od pracownika innych danych niż wskazane w art. 22^1 k.p. stanowiłoby obejście tego przepisu. 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 ustawy o ochronie danych osobowych jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to należy stwierdzić, że wykorzystanie danych biometrycznych do kon-

[48] Zgodnie z art. 7 pkt 5 ustawy o ochronie danych osobowych poprzez zgodę rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

[49] Innym orzeczeniem związanym z przetwarzaniem danych biometrycznych pracowników jest wyrok NSA z dnia 6 września 2011 r. (I OSK 1476/10), oddalający skargę kasacyjną na decyzję GIODO w przedmiocie uchybień w procesie przetwarzania danych osobowych. Po przeprowadzeniu postępowania administracyjnego przez GIODO w sprawie przetwarzania danych osobowych przez Naczelnika Urzędu Skarbowego w siedzibie Urzędu Skarbowego GIODO wydał decyzję nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych. W kolejnym orzeczeniu sądu administracyjnego – z dnia 20 czerwca 2011 r. oddalono skargę złożoną przez pełnomocników szpitala na decyzję GIODO nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych między innymi poprzez zaprzestanie zbierania danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników szpitala. Szczegóły zob. wyrok SA w Warszawie z dnia 20 czerwca 2011 r., II SA/Wa 719/11.

troli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania[50].

Podsumowanie

Popularność technologii biometrycznych wciąż wzrasta i tym samym technologia ta wnika coraz głębiej w życie człowieka. Instytucje, które pobierają i przetwarzają dane biometryczne, muszą postępować zgodnie z podstawowymi zasadami dotyczącymi prawa do ochrony danych osobowych, przede wszystkim zasadami proporcjonalności, rzetelności, celowości, bezpieczeństwem danych. Rozsądne wdrażanie rozwiązań technologicznych w dziedzinie biometrii ułatwi społeczeństwu funkcjonowanie w wielu obszarach życia. Należy jednak uświadamiać użytkownikom systemów biometrycznych potencjalne zagrożenia wiążące się z biometrią. Takie zadanie ciąży np. na pracodawcach, którzy mają zamiar wykorzystywać dane biometryczne swoich pracowników. Warto podkreślić, że w tym obszarze niezwykle istotne są działania podejmowane przez organy do spraw ochrony danych osobowych. Komisarz do spraw prywatności i ochrony danych osobowych w Hongkongu podejmuje aktywne działania w dziedzinie prawa do ochrony danych osobowych.

Chociaż przepisy ustawy The Personal Data (Privacy) Ordinance nie odnoszą się wprost do biometrii i przetwarzania danych biometrycznych, to dzięki inicjatywom komisarza instytucje wykorzystujące technologie biometryczne mają jasno określone zasady postępowania. Wystarczy, że będą one postępować zgodnie z przepisami powyższej ustawy oraz przygotowanymi przez komisarza wytycznymi na temat zbierania i wykorzystywania danych biometrycznych. Przykład Hongkongu pokazuje również, że po spełnieniu odpowiednich warunków możliwe jest wykorzystywanie danych biometrycznych do kontrolowania czasu pracy.

[50] Warto podkreślić, że dopuszczalne jest stosowanie czytników biometrycznych, gdy np. pracownik musi się dostać do konkretnego pomieszczenia (np. sejf w banku). Takie stanowisko w jednej ze swoich wypowiedzi zaprezentował GIODO. Stwierdził on, że „Odmiennie należałoby rozpatrywać pozyskiwanie danych biometrycznych w celu ochrony szczególnych interesów pracodawcy, np. zapewnienia bezpieczeństwa poufnych informacji czy systemów, i jedynie, gdy pozyskiwanie danych biometrycznych dotyczyć będzie tylko wybranych pracowników i na potrzeby realizacji innych celów niż wynikające ze stosunku pracy. Jednakże wykorzystywanie odcisków palców w celu kontrolowania obecności pracowników w pracy należy uznać za nadmierną inwigilację w prawo do prywatności.", http://www.giodo.gov.pl/1520261/j/pl/ (dostęp: 22.07.2016).

SUMMARY

BIOMETRICS IN HONG KONG AS AN EXAMPLE
OF THE PROBLEM OF FINGERPRINTS USAGE
TO CONTROL THE WORKING TIME

The paper describes the current legal regulations and guidelines regarding the usage of biometric technologies in Hongkong. The Author discusses the regulations for data protection and privacy. In particular, the crucial legal act "The Personal Data (Privacy) Ordinance (Cap. 486) is presented. The „Guidance on Collection and use of Biometric" issued by the Privacy Commissioner for Personal Data of Hongkong is also discussed. Moreover, the results of the investigation about the Collection of Fingerprint Data by Queenix (Asia) Limited is discussed.