Dominika Czerniak

Warunki przetwarzania i czas przechowywania danych biometrycznych i genetycznych w związku z zapobieganiem i zwalczaniem przestępczości – standard strasburski a prawo krajowe

Dominika Czerniak

Magister nauk prawnych; asystent w Katedrze Postępowania Karnego na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

✉ dominika.czerniak@uwr.edu.pl

https://orcid.org/0000-0002-8970-4017

The Rules of Collecting and Safekeeping Time of Biometric and Genetic Data for the Purposes of the Prevention or Prosecution of Criminal Offences? European and National Standard

A biometric (fingerprints and police pictures) and genetic (DNA) data are a special type of personal data. As a rule, collecting, processing and safekeeping of the data shall be subject to the same condition as a sensu stricto *personal data (e.g. name, surname). Domestic law should provide additional procedural guarantees to prevent unnecessary and unproportioned interference of the realm of the individual's privacy. The European Court of Human Rights has created European standard of collecting, processing and safekeeping of a genetic and biometric data, which should be implemented in the national law. Does Polish law comply with the European standard? The next question is what kind of changes in the domestic law, should be taken to provide a standard of protection of the privacy of the individual in accordance with the requirements of the ECtHR.*

Słowa kluczowe: postępowanie karne, prawa człowieka, prawo do prywatności, ochrona danych osobowych

Key words: criminal proceedings, data protection, human rights, right to privacy

https://doi.org/10.32082/fp.1(69).2022.468

1. Prawo do ochrony danych biometrycznych i genetycznych jako jedno z praw podstawowych

Prawo do ochrony danych osobowych jest autonomicznym prawem podstawowym, ściśle związanym z prawem do prywatności[1]. Współcześnie – ze względu na rozwój technologii, globalizację oraz stale rozwijającą się współpracę międzynarodową w celu zwalczania i zapobiegania poważnej przestępczości – problematyka zasad gromadzenia, przetwarzania i przechowywania danych biometrycznych i genetycznych nie jest regulowana wyłącznie na poziomie krajowym (ustawodawstwa danego państwa). Konwencja Rady Europy z 28.01.1981 r.[2] o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych wraz z protokołem dodatkowym w związku z automatycznym przetwarzaniem danych osobowych dotyczącym organów nadzoru i transgranicznych przepływów danych została ratyfikowana nie tylko przez państwa Rady Europy, ale – wobec braku aktywności w tej sferze na forum ONZ – także przez państwa spoza Europy[3]. Na konieczność ochrony danych osobowych, w tym danych biometrycznych i genetycznych, zwraca również uwagę Europejski Trybunał Praw Człowieka (ETPC). Choć Europejska Konwencja Praw Człowieka nie odnosi się wprost do kwestii ochrony danych osobowych, to w orzecznictwie ETPC ta problematyka jest analizowana na gruncie art. 8 EKPC. Zakres prawa do prywatności w dużej mierze zależy bowiem od tego, jak będą chronione jej dane osobowe. Także Komitet Ministrów Rady Europy podejmuje działania w związku z ochroną danych osobowych. W 1987 r. przyjęte zostały Zalecenia Rec (87)15 dla państw członkowskich regulujące wykorzystywanie danych osobowych przez Policję[4], rekomendacje R(92)1 w sprawie stosowania analizy kwasu dezoksyrybonukleinowego (DNA) w sprawach karnych oraz rekomendacje R(2010) w sprawie ochrony osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania[5].

W Unii Europejskiej prawo do ochrony danych osobowych wprost wynika z art. 8 Karty Praw Podstawowych[6], a bardziej szczegółowe regulacje dotyczące ochrony danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości znajdują się w Dyrektywie Parlamentu Europejskiego i Rady 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 uchylająca decyzję ramową Rady 2008/977/WSiSW[7] (dalej: dyrektywa 2016/680; dyrektywa DODO). Zgodnie z art. 4 dyrek-

1 M. Kusak, *Ochrona danych osobowych w sprawach karnych – rekomendacje na tle transpozycji dyrektywy 2016/680/UE*, „Europejski Przegląd Sądowy" 2017, nr 10, s. 10. Autorka zwraca uwagę na rozwój technologii i globalizację oraz łatwość przekazywania i danych osobowych. Podkreśla również, że współcześnie wyzwaniem jest właściwa ochrona danych osobowych przed dostępem do nich przez osoby nieuprawnione.

2 W dniu 10 października 2018 r. uchwalony został protokół zmieniający Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, który zacznie obowiązywać po ratyfikacji przez wszystkie państwa – strony Konwencji z 1981 r. lub w dniu 11 października 2023 r., jeśli do tego momentu protokół zostanie ratyfikowany przez 38 państw – sygnatariuszy Konwencji. Polska podpisała protokół w dniu 16 maja 2019 r. i ratyfikowała go 20 czerwca 2020 r. Aktualny stan ratyfikacji: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures?p_auth=GSfsmaBr (dostęp 17.02.2022).

3 Argentynę, Burkina Faso, Republikę Zielonego Przylądka, Mauritius, Meksyk, Maroko, Senegal, Tunezję i Urugwaj, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=GSfsmaBr (dostęp: 17.02.2022 r.).

4 Zalecenia Komitetu Ministrów z dnia 17 września 1987 r.; https://rm.coe.int/168062dfd4 (dostęp 10.10.2020).

5 Zob. szerzej: M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020.

6 Karta Praw Podstawowych wyodrębnia prawo do ochrony danych osobowych z zakresu prawa do prywatności. Zob. art. 7 i 8 KPP UE.

7 Dz.Urz.UE z 2016, seria L, nr 119, poz. 89. Zgodnie z notyfikacją przedstawioną Komisji Europejskiej, Polska implementowała dyrektywę w dniu 6 maja 2018 r., https://eur-lex.europa.eu/legal-content/PL/NIM/?uri=CELEX:32016L0680 (dostęp 17.02.20220).

tywy 2016/680 dane osobowe muszą być przetwarzane zgodnie z prawem, zbierane w celach wyraźnie wskazanych w prawie i skonkretyzowanych, przechowywane przez czas nie dłuższy niż to konieczne i przetwarzane w sposób zapewniający bezpieczeństwo danych. W dyrektywie zwraca się także uwagę na konieczność rozróżnienia tego, czyje dane są przetwarzane[8], oraz jaki jest rodzaj tych danych[9]. Przepis art. 5 dyrektywy 2016/680 zobowiązuje państwa członkowskie do wprowadzenia maksymalnego terminu przechowywania danych, wskazując, że powinny zostać wskazane odpowiednie terminy usuwania danych osobowych lub okresowego przeglądu konieczności przechowywania danych osobowych.

Przepisy dyrektywy 2016/800 oraz Konwencji z 1981 r. pozostawiają państwom wielką swobodę w ustaleniu zasad i warunków gromadzenia, przetwarzania i przechowywania danych osobowych, w tym biometrycznych i genetycznych. Szczególnie wrażliwy charakter tych danych powinien skutkować większymi gwarancjami proceduralnymi dla jednostki, by zapobiegać arbitralności działania organów władzy publicznej i przetwarzaniu ich niezgodnie z celem.

Przepisy dyrektywy 2016/800 oraz Konwencji z 1981 r. wraz z protokołami dodatkowymi pozostawiają państwom szeroki margines swobody w ustaleniu zasad i warunków gromadzenia, przetwarzania i przechowywania danych osobowych, w tym danych biometrycznych i genetycznych[10]. Mimo że ogólne zasady

8 Przepis art. 6 dyrektywy 2016/680 nakazuje rozróżnić ze względów podmiotowych zasady gromadzenia, przetwarzania i przechowywania danych osobowych w zależności od osoby, której przetwarzanie danych dotyczy, tj. a) danych osób, w stosunku do których istnieją poważne podstawy, by przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony; b) osób skazanych za czyn zabroniony; c) pokrzywdzonych czynem zabronionym lub osób, w przypadku których określone fakty wskazują, że mogą stać się ofiarą czynu zabronionego; oraz d) osób innych w stosunku do czynu zabronionego, takie jak osoby, które mogą zostać wezwane do złożenia zeznań w ramach postępowania przygotowawczego w sprawie czynu zabronionego lub na dalszych etapach postępowania karnego, osoby, które mogą dostarczyć informacji o czynach zabronionych, lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w lit. a) i b).

9 Zob. art. 10 dyrektywy 2016/680.

10 Warto jednak wskazać, że w motywach do dyrektywy 2016/680 podkreślono konieczność zapewnienia spójnego, wysokiego stopnia ochrony danych osobowych osób fizycznych oraz ułatwienia wymiany danych osobowych między właściwymi organami państw członkowskich, ma to zasadnicze znaczenie dla zapewnienia skutecznej współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. W tym celu należy we wszystkich państwach członkowskich zapewnić równorzędny stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabro-

są takie same, to szczególnie wrażliwy charakter tych danych powinien wiązać się z większymi gwarancjami proceduralnymi dla jednostki, by zapobiegać arbitralności działania organów władzy publicznej i przetwarzaniu ich niezgodnie z celem[11]. W prawie krajowym powinno dążyć się do większej precyzji przepisów regulujących kwestie związane z danymi biometrycznymi i genetycznymi[12]. Na problematykę właściwej ochrony danych biometrycznych i genetycznych – pozyskanych i przetwarzanych w celu zapobiegania i zwalczania przestępczości – zwraca także uwagę Europejski Trybunał Praw Człowieka. Aktywność ETPC w odniesieniu do tego zagadnienia uzupełnia lukę w ochronie praw jednostek. Nie wszystkie państwa Rady Europy ratyfikowały Konwencję z 1981 r. i nie wszystkie państwa Rady Europy należą do Unii Europejskiej. Choć orzeczenia ETPC wydawane są w odniesieniu do konkretnych okoliczności danej sprawy, to Trybunał kreuje ogólny standard ochrony danych biometrycznych i genetycznych i każdorazowo przedstawia w formie *general prinicples*. Warto zatem ustalić, jaki jest strasburski standard ochrony danych biometrycznych i genetycznych, a następnie, czy ustawodawstwo krajowe jest zgodne z wymogami, jakie względem państw Rady Europy ma Trybunał strasburski.

2. Gromadzenie, przetwarzanie i przechowywanie danych biometrycznych i genetycznych w orzecznictwie ETPC

Przepisy regulujące dopuszczalność i zasady gromadzenia, przetwarzania oraz usuwania danych biometrycznych i genetycznych powinny możliwie precyzyjnie wskazywać, w jakich sytuacjach organy państwa mogą ingerować w ten aspekt prywatności jednostki. Europejski Trybunał Praw Człowieka uznaje, że pobieranie i przechowywanie danych, które pozwalają na zidentyfikowanie konkretnej osoby, mieści się w zakresie art. 8 ust. 1 EKPC[13]. Już samo zatrzymywanie i przechowywanie danych osobowych przez organy publiczne należy traktować jako działania, które mają bezpośredni wpływ na życie prywatne danej osoby, niezależnie od tego, czy dane te w przyszłości zostaną wykorzystane[14]. Ingerencja w prawo do prywatności musi być uzasadniona celami wynikającymi z art. 8 ust. 2 EKPC i konieczne jest zachowanie odpowiedniej równowagi między interesem publicznym (zwalczaniem przestępczości) a konkurującym z nim interesem prywatnym jednostki. Trybunał w Strasburgu, badając zarzut naruszenia art. 8 ust. 1 EKPC, ocenia:

- czy ingerencja w prywatność jednostki była zgodna z prawem krajowym danego państwa (czy istniały przepisy krajowe, które pozwalały na pobraniem materiału do badań DNA lub pozyskanie danych biometrycznych);
- „jakość" prawa krajowego, tj. czy zapewnia ono wystarczającą ochronę przed arbitralnością działania organów władzy publicznej, jest odpowiednio precyzyjne, przewidywalne oraz dostępne dla jednostki[15];
- czy ingerencja w prywatność jednostki była uzasadniona celami wskazanymi w art. 8 ust. 2 EKPC[16];
- czy prawo krajowe zapewniało odpowiednie gwarancje przed niewłaściwym wykorzystaniem informacji ingerujących w prywatność[17].

nionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

11 Na zagrożenia związane z przetwarzaniem danych osobowych w związku ze zwalczaniem i zapobieganiem przestępczości zwraca uwagę m.in. Krzysztof Mróz. Zob. K. Mróz: *Zagrożenia dla prawa do prywatności jednostki w związku z przetwarzaniem danych osobowych w celu zapobiegania i zwalczania przestępczości*, „IusNovum" 2020, nr 1, s. 95–114.

12 Zwłaszcza że organy mogą nie udostępnić jednostce informacji, czy jej dane są przetwarzane w celach związanych ze zwalczaniem i zapobieganiem przestępczości. Zob. art. 15 dyrektywy 2016/680.

13 Wyrok ETPC z dnia 11 czerwca 2020 r. w sprawie P.N. p. Niemcom, skarga nr 74440/17; § 57. Wszystkie orzeczenia ETPC pochodzą ze strony https://hudoc.echr.coe.int/.

14 Wyrok ETPC (Wielka Izba) z dnia 4 grudnia 2008 r., w sprawie S. i Marper p. Zjednoczonemu Królestwu, skargi nr 30562/04 30566/04, § 67 i 121.

15 Wyrok ETPC (Wielka Izba) z dnia 4 grudnia 2008 r., w sprawie S. i Marper p. Zjednoczonemu Królestwu, skargi nr 30562/04 30566/04; § 95.

16 Wyrok ETPC z dnia 18 kwietnia 2013 r. w sprawie M.K. p. Francji, skarga nr 19522/09; § 33.

17 Wyrok ETPC z dnia 22 czerwca 2017 r. w sprawie Aycaguer p. Francji, skarga nr 8806/12; § 38.

Pobieranie danych biometrycznych i genetycznych w związku z prowadzonym postępowaniem karnym w celu identyfikacji osób podejrzewanych o popełnienie przestępstwa lub w celu zapobiegania i zwalczania przestępstw ETPC uznaje za uzasadnione działanie w świetle art. 8 ust. 2 EKPC[18]. Wskazuje jednak, że co do zasady nie powinny być przechowywane dane osób, które zostały uniewinnione od zarzutu popełnienia przestępstwa, a w odniesieniu do osób skazanych dane te nie mogą być przechowywane bezterminowo[19]. Za dopuszczalne uznaje jednak gromadzenie i przechowywanie danych *pro futoro*, tj. w celu zwalczania recydywy[20]. Jeśli istnieje uzasadnione przypuszczenie, że oskarżony może w przyszłości ponownie popełnić przestępstwo[21], to pobranie i przechowywanie jego danych biometrycznych i genetycznych jest uzasadnione w świetle art. 8 EKPC[22]. To, jakie dane zostaną zgromadzone – biometryczne np. wizerunek lub odciski palców – czy genetyczne zależy od okoliczności danej sprawy. Organy procesowe powinny jednak wykonywać czynności, które w najmniejszym stopniu ingerują w prywatność jednostki. Nie w każdej sprawie konieczne jest pobranie materiału do badań genetycznych. Podejmując decyzję o pobraniu próbek DNA, organy procesowe powinny wziąć pod uwagę m.in. wagę przestępstwa i charakter czynu zabronionego. Warto jednak zwrócić uwagę, że w niektórych sprawach – np. w sprawach o zgwałcenie – niezabezpieczenie materiału do badań genetycznych i niepobranie próbek do badań DNA Trybunał uznaje za naruszenie art. 3 EKPC w aspekcie proceduralnym[23].

Chcąc pobrać materiał do badań DNA, dopuszczalne jest użycie środków przymusu bezpośredniego. W decyzji w sprawie Caruana przeciwko Malcie[24] Trybunał wskazał, że pobranie wymazu do badań DNA jest czynnością trwającą bardzo krótko, nie wiąże się z żadną szczególną dolegliwością dla osoby, wobec której czynność ta jest wykonywana i ma dla niej niewielkie znaczenie[25]. Jeśli pobranie materiału do badań genetycznych jest konieczne dla ustalenia okoliczności sprawy, w tym motywu działania sprawcy przestępstwa, to dopuszczalne jest wykonanie niezbędnych czynności także wbrew woli świadka (osoby, która nie została oskarżona ani nie była podejrzewana o popełnienie przestępstwa)[26] – o ile przepisy krajowe dopuszczały taką możliwość. Ważne jednak, by przepisy prawa krajowego precyzyjnie wskazywały, kiedy dopuszczalne jest przełamanie woli danej osoby odnośnie do dostarczenia materiału do badań biometrycznych i genetycznych[27]. Jeśli prawo krajowe wymaga wyra-

18 Wyrok ETPC (Wielka Izba) z dnia 4 grudnia 2008 r., w sprawie S. i Marper p. Zjednoczonemu Królestwu, skargi nr 30562/04 30566/04; § 101–104.

19 W wyroku Gaughran przeciwko Zjednoczonemu Królestwu, Trybunał porównał prawo obowiązujące w różnych państwach Rady Europy. Zob. wyrok ETPC z dnia 13 lutego 2020 r. w sprawie Gaughran p. Zjednoczonemu Królestwu, skarga nr 45245/15; § 53–57.

20 Zob. wyrok ETPC z dnia 13 lutego 2020 r. w sprawie Trajkovski i Chipovski p. Macedonii Północnej, skargi nr 53205/13 i 63320/13; § 51.

21 Np. ze względu na jego dotychczasową „działalność" przestępczą. W wyrok P.N. przeciwko Niemcom Trybunał oceniał, czy pobranie próbek do badań DNA i zdjęć sygnalitycznych od oskarżonego chorego na reumatoidalne zapalenie stawów, który ma trudności z poruszaniem się nie stanowiło nieproporcjonalnej ingerencji w sferę prywatności jednostki. Rząd argumentował, że działania te były konieczne ze względu na dotychczasowy styl życia skarżącego i wielość uprzednio prowadzonych postępowań karnych. Zob. szerzej: wyrok ETPC z dnia 11 czerwca 2020 r. w sprawie P.N. p. Niemcom, skarga nr 74440/17; § 57.

22 Zob. wyrok ETPC z dnia 13 lutego 2020 r. w sprawie Trajkovski i Chipovski p. Macedonii Północnej, skargi nr 53205/13 i 63320/13; § 51.

23 Zob. m.in. wyrok ETPC z dnia 28 maja 2015 r. w sprawie Y. p. Słowenii, skarga nr 41107/10.

24 Decyzja ETPC z dnia 15 maja 2018 r. w sprawie Caruana p. Malcie, skarga nr 41079/16.

25 Decyzja ETPC z dnia 15 maja 2018 r. w sprawie Caruana p. Malcie, skarga nr 41079/16, § 41.

26 Decyzja ETPC z dnia 15 maja 2018 r. w sprawie Caruana p. Malcie, skarga nr 41079/16, § 41. Zob. jednak odmiennie: wyrok ETPC z dnia 14 kwietnia 2020 r. w sprawie Dragan Petrović p. Serbii, skarga nr 75229/10; § 79–83, w którym ETPC zakwestionował „zgodność z prawem" działania organów procesowych w odniesieniu do groźby zastosowania przymusu bezpośredniego, jeśli skarżący dobrowolnie nie podda się badaniom.

27 W sprawie Trajkovski i Chipovski p. Macedonii Północnej ETPC krytycznie ocenił ustawodawstwo krajowe. Zwrócił uwagę, że przepisy były nieprecyzyjne – sąd mógł nakazać

żenia zgody przez osobę przesłuchiwaną na poddanie się czynnościom związanym z pobraniem materiału do badań biometrycznych i genetycznych, to niedopuszczalne jest wpływanie na wolę tej osoby groźbą lub przymusem. W sprawie Dragan Petrović przeciwko Serbii Trybunał wskazał, że nie można uznać za dobrowolne oddanie materiału do badań genetycznych, jeśli skarżącego poinformowano, że jeśli nie podda się czynności, to próbki zostaną pobrane z zastosowaniem środków przymusu bezpośredniego[28].

Na gruncie art. 8 EKPC problematyczne jest także to, czy organy procesowe mogą przechowywać dane genetyczne osoby skazanej, jeśli w toku postępowania karnego próbki DNA nie zostały wykorzystane, a samo ich pobranie nie było konieczne. W wyroku Trajkovski i Chipovski przeciwko Macedonii Północnej Trybunał nie uznał takiego działania za naruszające Konwencję, o ile prawo krajowe określa maksymalny termin przechowywania takich danych[29] oraz wskazuje, jakie okoliczności podmiotowe lub przedmiotowe[30] mogą uzasadniać ich przechowywanie.

W zależności od danych biometrycznych, jakie zostały pobrane na potrzeby postępowania karnego, dopuszczalność ich pobrania, przetwarzania i przechowywania może być różna. Najbardziej rygorystycznie ETPC ocenia przepisy dotyczące danych DNA[31], uznając, że w największym stopniu ingerują w sferę prywatności jednostki. Najmniejszy stopień precyzji jest wymagany od regulacji odnoszących się do gromadzenia wizerunku osób podejrzewanych i skazanych[32]. Choć nie sposób uznać, by między państwami Rady Europy istniał konsens odnośnie do gromadzenia, przechowywania, przetwarzania i usuwania danych biometrycznych, to margines swobody w uregulowaniu tej kwestii jest limitowany niedopuszczalnością bezterminowego przechowywania profili DNA osób skazanych[33] oraz odpowiednią „jakością" przepisów krajowych[34]. Ani z dokumentów Rady Europy[35], ani

pobranie próbek krwi lub przeprowadzenie „innych procedur medycznych", jeśli uzna to za konieczne z medycznego punktu widzenia w celu ustalenia faktów „ważnych" dla dochodzenia, bez wyraźnego wskazania, że można również pobrać próbki do badań DNA. Zob.: wyrok ETPC z dnia 13 lutego 2020 r. w sprawie Trajkovski i Chipovski p. Macedonii Północnej, skargi nr 53205/13 i 63320/13.

28 Wyrok ETPC z dnia 14 kwietnia 2020 r. w sprawie Dragan Petrović p. Serbii, skarga nr 75229/10; § 79–83. Trybunał analizował również kwestię naruszenia art. 6 ust. 3 lit. a EKPC. Skarżącego formalnie bowiem przesłuchano w charakterze świadka, choć organy procesowe uznawały go za podejrzewanego w prowadzonym postępowaniu karnym.

29 Termin ten powinien być możliwy do zweryfikowania. W sprawie Trajkovski i Chipovski przeciwko Macedonii Północnej Trybunał uznał, że oznaczenie czas przechowywania danych do momentu, do kiedy nie zrealizują celu pobrania danych (*may be retained until it has fulfilled the purpose for which it has been taken*) nie wprowadza żadnego maksymalnego terminu i pozwala na masowe gromadzenie danych o jednostkach. Zob. wyrok ETPC z dnia 13 lutego 2020 r. w sprawie Trajkovski i Chipovski p. Macedonii Północnej, skargi nr 53205/13 i 63320/13, § 52.

30 M.in. waga i charakter przestępstwa, wiek oskarżonego, stan zdrowia. Zob.: wyrok ETPC (Wielka Izba) z dnia 4 grudnia 2008 r., w sprawie S. i Marper p. Zjednoczonemu Królestwu, skargi nr 30562/04 30566/04, § 119.

31 Ze względu na zakres informacji o jednostce, które wynikają z tych danych.

32 Warto wskazać, że przez długi czas ETPC uznawał, że gromadzenie wizerunku na potrzeby procesu karnego nie mieści się w zakresie art. 8 ust. 1. Zob. wyrok ETPC z dnia 13 lutego 2020 r. w sprawie Gaughran p. Zjednoczonemu Królestwu, skarga nr 45245/15, § 65 i wskazane tam orzecznictwo.

33 ETPC zwraca uwagę na wadliwość przepisów obowiązujących w Zjednoczonym Królestwie, gdzie kwestia przechowywania danych biometrycznych i genetycznych osób podejrzewanych o popełnienie przestępstwa nie spełnia wymogów strasburskich. Warto zwrócić uwagę na ugody zwierane przez ETPC przez Zjednoczone Królestwo ze skarżącymi podnoszącymi zarzut naruszenia art. 8 EKPC: decyzja ETPC z dnia 6 lutego 2018 r. w sprawie Djalo p. Zjednoczonemu Królestwu, skarga nr 17770/10, § 16 i wskazane tam orzecznictwo; decyzja ETPC z dnia 6 lutego 2018 r. w sprawie Gare-Simmons p. Zjednoczonemu Królestwu, skarga nr 71358/12.

34 Wyrok ETPC z dnia 13 lutego 2020 r. w sprawie Gaughran p. Zjednoczonemu Królestwu, skarga nr 45245/15, § 82.

35 Zalecenia Rec (87)15 dla państw członkowskich regulujące wykorzystywanie danych osobowych przez policję, rekomendacje R(92)1 w sprawie stosowania analizy kwasu dezoksyrybonukleinowego (DNA) w sprawach karnych oraz rekomendacje R(2010) w sprawie ochrony osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania. coe.int/treatyoffice.

orzecznictwa ETPC nie wynika jednak maksymalny dopuszczalny termin przechowywania i przetwarzania danych biometrycznych. Wskazuje się jedynie, że powinien on być „odpowiedni" dla realizacji celów z art. 8 ust. 2 EKPC[36], ale Trybunał w odniesieniu do konkretnych okoliczności danej sprawy ocenia rozwiązania poszczególnych państw Rady Europy. Bada również, czy ze względu na czas przechowywania danych biometrycznych i genetycznych służby policyjne nie gromadzą masowo wrażliwych danych dotyczących jednostek[37]. W wyroku P.N. przeciwko Niemcom Trybunał uznał, że 5- lub 10-letni, w zależności od wagi czynu zabronionego[38], termin przechowywania danych biometrycznych (odcisków palców) jest odpowiedni dla realizacji celów z art. 8 ust. 2 EKPC.

Warto także podkreślić, że Trybunał za celowe uznaje ustanowienie sądowej kontroli nad przetwarzaniem i gromadzeniem danych biometrycznych i genetycznych[39]. Jednostka, znając przepisy regulujące kwestię pobierania i przechowywania szczególnie wrażliwych danych osobowych, powinna mieć zagwarantowaną możliwość żądania ich usunięcia z baz danych, jeśli zostały pozyskane z naruszeniem prawa lub są przetwarzane wbrew przepisom prawa krajowego[40]. W związku z powyższym, przepisy prawa krajowego muszą być odpowiednio precyzyjne lub musi istnieć utrwalona linia orzecznicza, wyjaśniająca, w jaki sposób należy interpretować nieostre sformułowania normatywne[41].

Najbardziej rygorystycznie ETPC ocenia przepisy dotyczące danych DNA, uznając, że w największym stopniu ingerują w sferę prywatności jednostki. Najmniejszy stopień precyzji jest wymagany od regulacji odnoszących się do gromadzenia wizerunku (zdjęć) osób podejrzewanych i skazanych.

Podsumowując, Trybunał pozostawia państwom Rady Europy szeroki margines swobody w uregulowaniu kwestii gromadzenia, przechowywania i usuwania danych biometrycznych i genetycznych. Zwraca jednak uwagę na jakość przepisów krajowych, tj. czy są zrozumiałe dla jednostki i czy zapewniają jej ochronę przed arbitralnym, niekontrolowanym i bezterminowym przetwarzaniem danych. Im bardziej dolegliwa ingerencja w prywatność jednostki, tym unormowania krajowe powinny być bardziej precyzyjne. Prawo krajowe musi wprowadzać maksymalny termin przecho-

36 Zob. wyrok ETPC (Wielka Izba) z dnia 24 stycznia 2019 r. w sprawie Catt p. Zjednoczonemu Królestwu, skarga nr 43514/15, § 109, wyrok ETPC z dnia 13 lutego 2020 r. w sprawie Gaughran p. Zjednoczonemu Królestwu, skarga nr 45245/15, § 88.

37 Problem masowego gromadzenia informacji był analizowany m.in. w wyroku ETPC z dnia 13 września 2018 r. w sprawie Big Brother Watch i inni p. Zjednoczonemu Królestwu, skargi nr 58170/13, 62322/14 i 24960/15 oraz wyroku ETPC z 30.01.2020 r. w sprawie Bayer p. Niemcom, skarga nr 50001/12.

38 Zob. analizę ustawodawstwa niemieckiego zawartą w wyroku ETPC z dnia 11 czerwca 2020 r. w sprawie P.N. p. Niemcom, skarga nr 74440/17, § 25 i 26.

39 Zob. wyrok ETPC z dnia 14 kwietnia 2020 r. w sprawie Dragan Petrović p. Serbii, skarga nr 75229/10.

40 Zob.: wyrok ETPC z dnia 13 lutego 2020 r. w sprawie Trajkovski i Chipovski p. Macedonii Północnej, skargi nr 53205/13 i 63320/13.

41 Zob.: wyrok ETPC z dnia 11 czerwca 2020 r. w sprawie P.N. p. Niemcom, skarga nr 74440/17, § 77.

wywania danych – a zwłaszcza danych genetycznych jako najbardziej wrażliwych[42]. Jednostka zaś powinna mieć możliwość zweryfikowania legalności i celowości przetwarzania jej danych biometrycznych i genetycznych, a kontrola powinna być sprawowana przez sąd.

3. Gromadzenie, przetwarzanie i przechowywanie danych biometrycznych i genetycznych w prawie krajowym

3.1. Przesłanki i podstawy normatywne pobrania danych biometrycznych i genetycznych

Na potrzeby procesu karnego pobieranie danych biometrycznych i genetycznych od osób podejrzewanych oraz oskarżonych o popełnienie przestępstwa jest możliwe na podstawie art. 74 § 2 k.p.k. Każda osoba, wobec której istnieją podstawy do przypuszczania, że mogła popełnić przestępstwo, jest zobowiązania do poddania się czynnościom związanym z pobraniem odcisków palców, wykonaniem zdjęć sygnalitycznych czy pobraniem wymazów do badań DNA[43]. W celu wymuszenia spełnienia obowiązków procesowych organy procesowe mogą stosować środki przymusu bezpośredniego (art. 74 § 3 k.p.k.). Jeśli czynności z art. 74 § 2 k.p.k. są podejmowane wobec osoby początkowo wezwanej w charakterze świadka[44], to mogą one sugerować zmianę roli procesowej. Osoba taka staje się osobą podejrzaną, a organy procesowe wykonały pierwsze czynności nakierowane na jej ściganie. W takiej sytuacji, przed przystąpieniem do czynności związanych z pobraniem próbek do badań biometrycznych i genetycznych, niezbędne jest poinformowanie osoby przesłuchiwanej o przedmiocie postępowania karnego. Nie chodzi o formalne przedstawienie zarzutów – na wczesnym etapie postępowania pobranie próbek DNA może służyć zawężeniu kręgu osób podejrzewanych o popełnienie przestępstwa – ale o poinformowanie, o jaki czyn zabroniony prowadzone jest postępowanie i dlaczego organy procesowe uznały za konieczne przeprowadzenie badań genetycznych czy biometrycznych. Świadek nie musi się bowiem zgodzić na poddanie się badaniom; nie musi się podporządkować poleceniu funkcjonariusza Policji i nie można także wymusić na nim zmiany decyzji, grożąc np. zastosowaniem środków przymusu bezpośredniego[45].

Im bardziej dolegliwa ingerencja w prywatność jednostki, tym unormowania krajowe powinny być bardziej precyzyjne.

Podstawy do przeprowadzenia badań biometrycznych i pobrania wymazów do badań genetycznych wynikają także z ustaw policyjnych[46]. W odniesieniu do uprawnień funkcjonariuszy Policji to zgodnie z art. 20 ust. 1k w zw. z art. 15 ust. 1 pkt 3a lit d ustawy

42 I z których wynika najwięcej informacji o jednostce.

43 Rozporządzenie Ministra Sprawiedliwości z dnia 23 lutego 2005 r. w sprawie poddawania badaniom lub wykonywania czynności z udziałem oskarżonego oraz osoby podejrzanej (Dz.U. z 2005, nr 33, poz. 299) określa zasady i warunki przeprowadzenia badań i czynności z art. 74 § 2 k.p.k. Zgodnie z § 2 ust. 1 powyższego wskazanego rozporządzenia, osoba podejrzana lub oskarżona obowiązana jest poddać się czynnościom służącym pozyskaniu danych biometrycznych lub genetycznych na pisemne polecenie organu prowadzącego postępowanie, a w wypadkach niecierpiących zwłoki – na polecenie organu procesowego, po okazaniu legitymacji służbowej. Ustne polecenie powinno zostać w ciągu 7 dni potwierdzone na piśmie.

44 Zgodnie z art. 192 § 4 k.p.k. pobranie od świadka odcisków palców, czy dokonanie oględzin uzależnione jest od zgody tego uczestnika postępowania.

45 Pojawia się jednak pytanie, czy jeśli świadek odmówi oddania próbek do badań genetycznych lub biometrycznych, to organy procesowe automatycznie nie uznają, że jest on osobą podejrzaną i jako podstawę przeprowadzenia badań podany zostanie art. 74 § 2 k.p.k.

46 M.in. ustawy o Straży Granicznej. Ustawa z dnia 12 października 1990 r. o Straży Granicznej, Dz.U. z 2020, poz. 305.

o Policji funkcjonariusze Policji mogą pobierać od osób podejrzewanych o popełnienie przestępstwa lub podejrzanych odciski linii papilarnych lub wymaz ze śluzówki policzków w celu identyfikacji lub wykrywania sprawców przestępstw. W odniesieniu do osoby zatrzymanej na postawie art. 15 ust. 1 pkt 3 ustawy o Policji[47] daktyloskopowanie, fotografowanie lub pobranie próbek w celu przeprowadzenia badań genetycznych jest dopuszczalne tylko wtedy, gdy jej tożsamość nie może być ustalona w inny sposób[48]. Dodatkowe sytuacje, w których Policja lub inne służby policyjne mogą przeprowadzić czynności w celu pozyskania danych biometrycznych lub genetycznych zostały wskazane w tzw. ustawie antyterrorystycznej. W związku z podejmowaniem działań antyterrorystycznych funkcjonariusze ABW, Policji i Straży Granicznej są uprawnieni do pobierania obrazu linii papilarnych lub utrwalania wizerunku twarzy lub nieinwazyjnego pobierania materiału biologicznego w celu oznaczenia profilu DNA osoby niebędącej obywatelem Rzeczypospolitej Polskiej w przypadku gdy:

- istnieje wątpliwość co do tożsamości osoby, lub
- istnieje podejrzenie nielegalnego przekroczenia granicy Rzeczypospolitej Polskiej albo wątpliwość co do deklarowanego celu pobytu na terytorium Rzeczypospolitej Polskiej, lub
- istnieje podejrzenie co do zamiaru nielegalnego przebywania na terytorium Rzeczypospolitej Polskiej, lub
- istnieje podejrzenie związku osoby ze zdarzeniem o charakterze terrorystycznym, lub
- osoba mogła uczestniczyć w szkoleniu terrorystycznym[49].

Zasady i sposób pobierania danych biometrycznych są precyzowane w rozporządzeniu Rady Ministrów z dnia 4 lutego 2020 r. w sprawie postępowania przy wykonywaniu niektórych uprawnień policjantów[50]. Z pobrania wymazu ze śluzówki lub przeprowadzenia czynności służących pozyskaniu danych biometrycznych sporządza się protokół[51] (§ 12 ust. 1 – dotyczący danych daktyloskopijnych, § 16 ust. 1 – w odniesieniu do utrwalania wizerunku)[52]. Dane biometryczne – na wniosek funkcjonariusza Policji lub innej służby[53] – wprowadza się do odpowiedniego zbioru danych Krajowego Systemu Informacyjnego Policji[54], gdzie są one automatycznie przetwarzane[55].

47 Zatrzymanie osób stwarzających w sposób oczywisty bezpośrednie zagrożenie dla życia lub zdrowia ludzkiego, a także dla mienia, które nie musi wiązać się z podejrzeniem popełnienia przestępstwa.

48 Zob. art. 15 ust. 4 ustawy o Policji. Ustawa z dnia 6 kwietnia 1990 o Policji, Dz.U. z 2020, poz. 360.

49 Przesłanki pobrania materiału do badań genetycznych i biometrycznych na podstawie ustawy antyterrorystycznej są bardzo szerokie. Nie wyjaśniono również, co należy rozumieć przez pojęcie „podejrzenie", tj. jaki stopień prawdopodobieństwa powinien zaistnieć, by podjęcie działań z art. 10 ust. 1 ustawy antyterrorystycznej było dopuszczalne i jaka musi być podstawa dowodowa owego podejrzenia. Na wątpliwości wynikające z niejasnych sformułowań, jakimi posłużył się ustawodawca we wskazanym przepisie zwracał uwagę M. Gabriel-Węglowski. Zob. szerzej: M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*, Warszawa 2018.

50 § 1 i 2 i § 14, Dz.U. z 2020, poz. 192. Zob. także: Rozporządzenie Ministra Obrony Narodowej z dnia 8 stycznia 2020 r. w sprawie przetwarzania danych biometrycznych oraz danych genetycznych przez Żandarmerię Wojskową; Dz.U. z 2020, poz. 87; Rozporządzenie Rady Ministrów z dnia 4 lutego 2020 r. w sprawie wykonywania niektórych uprawnień przez funkcjonariuszy Straży Granicznej, Dz.U. z 2020, poz. 187.

51 Wzór protokołu jest dostępny na stronie: https://www.policja.pl/pol/kgp/biuro-kryminalne/dokumenty/zagadnienia-procesu-kar/formularze-procesowe/125060,Protokol-pobrania-materialu-porownawczego.html (dostęp 17.02.2022). W protokole wskazuje się podstawę prawną pobrania materiału do badań porównawczych, funkcjonariusza, który dokonał czynności oraz określa się, jaki materiał pobrano (zdjęcia sygnalityczne, odciski daktyloskopijne, próbki DNA), czas i miejsce pobrania próbek oraz sposób zabezpieczenia.

52 Zob. również § 13 w/w rozporządzenia.

53 Warto zauważyć, że Żandarmeria Wojskowa posiada również lokalną bazę danych biometrycznych, do której dostęp mają funkcjonariusze tej służby.

54 Zob. Zarządzenie Nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji; Dz.Urz.KGP z 2019, poz. 114. Administratorem danych jest Komendant Główny Policji, a w zależności od rodzaju danych biometrycznych, informacje są umieszczane w bazie danych DNA, bazie danych Krajowego Centrum Informacji Kryminalnych, czy w bazie AFIS.

55 Zob. art. 21b ustawy o Policji (w odniesieniu do danych DNA) art. 21i ustawy o Policji (w odniesieniu do danych daktyloskopijnych).

W odniesieniu do podstaw prawnych pobrania odcisków palców, wykonania zdjęć sygnalitycznych i przeprowadzenia badań genetycznych warto zauważyć, że przepisy nie wprowadzają odrębnych przesłanek do przeprowadzenia tych czynności. Formalnie zatem zarówno w sprawie o drobną kradzież, jak i zgwałcenie czy zabójstwo możliwe jest wykonanie tych samych czynności z art. 74 § 2 k.p.k. i wprowadzenie wrażliwych danych dotyczących danej osoby do systemów policyjnych[56]. Analizując jednak dane statystyczne, wydaje się, że w praktyce organy procesowe kierują się zasadą proporcjonalności. Najwięcej danych znajduje się w zbiorach zdjęć sygnalitycznych, a najmniej – w bazie DNA[57]. W polskiej bazie danych daktyloskopijnych jest natomiast ponad 3,8 miliona danych[58]. Brak jest jednak danych, które wskazywałyby, w sprawach o jakie przestępstwa pobrane zostały dane biometryczne lub genetyczne. Uwzględniając orzecznictwo ETPC, celowe wydaje się ustawowe powiązanie dopuszczalności pobrania próbek do badań genetycznych z ciężarem gatunkowym przestępstwa, o którego popełnienie podejrzewana jest dana osoba, lub z ustawowym zagrożeniem karą. W odniesieniu do tego rodzaju badań, Trybunał strasburski wymaga szczególnej precyzji, by zapewnić jednostce ochronę przed nieuprawnioną ingerencją w sferę prawa do prywatności i arbitralnością działania organów władzy publicznej.

Gromadzenie wrażliwych danych o jednostce w celach prewencyjnych, bez powiązania z przeszłością kryminalną danej osoby, jest niedopuszczalne w demokratycznym państwie prawnym.

Z przepisów prawa krajowego nie wynika wyraźnie dopuszczalność gromadzenia danych biometrycznych i genetycznych *pro futuro*, tj. w celu zwalczania recydywy. Obowiązujące regulacje odnoszą się jedynie do celowości przeprowadzenia tych czynności i przydatności danych do „wykrywania przestępstw" – bez wskazania, czy chodzi o przestępstwa już popełnione, czy takie, które – w ocenie organów procesowych – dana osoba może popełnić w przyszłości. Gromadzenie wrażliwych danych o jednostce w celach prewencyjnych, bez powiązania z przeszłością kryminalną danej osoby, jest niedopuszczalne w demokratycznym państwie prawnym. Takie stanowisko wynika także z orzecznictwa Trybunału Konstytucyjnego, który

56 Przepis § 40 ust. 7 Wytycznych nr 3 Komendanta Głównego Policji z dnia 30 sierpnia 2017 r. w sprawie wykonywania niektórych czynności dochodzeniowo – śledczych przez policjantów (Dz.Urz. KGP z 2017, poz. 59) uprawnia policjantów do pobrania odcisków palców, gdy tożsamość podejrzanego – ustalona zgodnie z § 18 ust. 5 powyższych wytycznych – budzi wątpliwości. Wytyczne częściowo precyzują, w jakich sytuacjach możliwe jest pobranie danych biometrycznych, ale nie wyczerpują katalogu sytuacji, kiedy policjanci będą pobierali od podejrzanych odciski palców.

57 Dane statystyczne są dostępne pod adresem: https://clkp.policja.pl/clk/baza-danych-dna/dane-statystyczne/109310,Liczba-profili.html (dostęp 17.02.2022). Na dzień 31 grudnia 2021 r. w bazie DNA było 153 000 profili podejrzanych o popełnienie przestępstwa (a 2019 było tych profili 93 241) i 19 199 śladów nieznanych sprawców przestępstw (w 2019 r. było tych danych 14.917). W 2021 r. baza DNA powiększyła się o 47 126 profili.

58 Dane dotyczące odcisków daktyloskopijnych dostępne sąd pod adresem: https://clkp.policja.pl/clk/zbiory-danych-d/dane-statystycz/163191,Liczba-kart-w-zbiorze-danych-daktyloskopijnych.html. (dostęp 17.02.2022). Na dzień 9 maja 2018 r. w bazie znajdowały się dane 3 958 000 osób. Nie ma dostępnych danych na rok 2021.

w jednym z orzeczeń wskazał, że w demokratycznym państwie prawnym dane na temat obywateli nie powinny być gromadzone ze względu na potencjalną przydatność tych informacji, a ingerencja w prywatność może być stosowana tylko „w związku z konkretnym postępowaniem, prowadzonym na podstawie ustawy dopuszczającej ograniczenie wolności ze względu na bezpieczeństwo państwa i porządek publiczny. Ingerencja policji w sferę praw i wolności obywatelskich, związana z czynnościami operacyjnymi podejmowanymi w interesie publicznym, nie może być nieograniczona”[59]. Obecnie obowiązujące, nieprecyzyjne przepisy pozwalają służbom policyjnym na gromadzenie danych, zawsze gdy dany funkcjonariusz uzna to za konieczne. Trudno oczekiwać, by dążąc do zwalczania przestępczości, bez wyraźnego wskazania ustawowego, funkcjonariusze dobrowolnie ograniczali sobie możliwości pozyskania potrzebnych informacji, stosując zasadę proporcjonalności.

3.2. Przetwarzanie danych biometrycznych i genetycznych

Dostęp do policyjnych baz danych jest możliwy po uzyskaniu przez funkcjonariusza Policji upoważnienia do dostępu do jednej z baz danych Krajowego Systemu Informacyjnego Policji[60]. Uprawnienie może wiązać się z możliwością wprowadzenia danych do systemu, przetwarzania ich (przeglądania) oraz wykonywania innych, określonych przez prawo operacji związanych z przetwarzaniem danych osobowych[61]. Procedura nadawania uprawnień dostępu do danych znajdujących się w rejestrach policyjnych została uregulowana w § 12 Zarządzenia nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji[62]. Na pisemny wniosek kierownika komórki organizacyjnej, w której pełni służbę policjant lub jest zatrudniony pracownik Policji, skierowany do dyrektora biura Komendanta Głównego Policji właściwego w sprawach wywiadu kryminalnego[63], kierownika komórki organizacyjnej właściwej w sprawach wywiadu kryminalnego właściwej miejscowo komendy wojewódzkiej Policji (Komendy Stołecznej Policji)[64], kierownika komórki organizacyjnej CBŚP właściwej w sprawach wywiadu kryminalnego[65], kierownika komórki organizacyjnej BSWP właściwej w sprawach administrowania systemami teleinformatycznymi przeznaczonymi do przetwarzania informacji niejawnych i jawnych[66]. We wniosku należy określić indywidualny zakres upoważnienia dostępu do policyjnych baz danych (rodzaj udostępnionego zbioru), zakres i rodzaj informacji, do których będzie miał dostęp funkcjonariusz Policji, wskazać rodzaje operacji przetwarzania danych, a ponadto podać wykaz zadań służbowych realizowanych przez policjanta[67]. Konieczne jest dołączenie oświadczenia policjanta lub pracownika Policji objętego wnioskiem o zobowiązaniu się do zapewnienia bezpieczeństwa danych osobowych przetwarzanych w KSIP oraz dostępnych w systemach teleinformatycznych KSIP, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych osobowych oraz ich przypadkową utratą,

59 Zob.: wyrok TK z dnia 12 grudnia 2005, K 32/04, OTK-A 2005, nr 11, poz. 132.

60 Zob. § 11 Zarządzenia nr 70 KGP, Dz.Urz.KGP z 2019, poz. 114.

61 Zob. również: Zarządzenie nr 28 Komendanta Głównego Policji z dnia 11 sierpnia 2020 r. w sprawie zbiorów danych daktyloskopijnych; Dz.Urz. KGP z 2020, poz. 44.

62 Uprawniony podmiot składa wniosek go KGP, w którym wskazywane są dane osobowe policjanta, ubiegającego się o dostęp do danych KSIP. Zob. szerzej: § 12 ust. 4 Zarządzenia nr 70 KGP, Dz.Urz.KGP z 2019, poz. 114.

63 W odniesieniu do policjantów pełniących służbę lub pracowników Policji zatrudnionych w Komendzie Głównej Policji, BOA, CLKP, szkołach policyjnych oraz w Wyższej Szkole Policji w Szczytnie; zob. § 12 ust. 1 pkt 1 Zarządzenie nr 70.

64 W przypadku policjantów pełniących służbę lub pracowników Policji zatrudnionych w jednostkach i komórkach organizacyjnych Policji podległych komendantowi wojewódzkiemu Policji (Komendantowi Stołecznemu Policji) oraz w samodzielnych oddziałach i pododdziałach prewencji Policji lub samodzielnych pododdziałach kontrterrorystycznych Policji.

65 W przypadku policjantów i pracowników Policji pełniących służbę i zatrudnionych w CBŚP.

66 W przypadku policjantów i pracowników Policji pełniących służbę i zatrudnionych w BSWP.

67 § 12 ust. 4 Zarządzenia Nr 70 KGP.

zniszczeniem lub uszkodzeniem[68]. Zgoda na dostęp do baz danych udzielana jest na okres wskazany we wniosku z możliwością dalszego przedłużenia. Dyrektor biura Komendanta Głównego Policji lub miejscowo właściwy komendant wojewódzki Policji niezwłocznie zatwierdzają wniosek, jeśli uznają go za uzasadniony[69]. Właściwy kierownik jednostki organizacyjnej Policji jest zobowiązany do kontrolowania – na bieżąco – celowości nadania uprawnień dostępu do baz KSIP i ich zakresu, a w przypadku m.in. zmiany zakresu lub rodzaju czynności służbowych realizowanych przez uprawnionego policjanta lub pracownika Policji lub przeniesienia do innej jednostki organizacyjnej Policji – powinien wystąpić o cofnięcie lub zmianę zakresu upoważnienia dostępu do baz danych.

Dane biometryczne (odciski daktyloskopijne)[70] mogą być przetwarzane w celu prowadzenia czynności identyfikacyjnych i wykrywczych, a dane genetyczne – w celu prowadzenia czynności wykrywczych i eliminacyjnych. Warto jednak podkreślić, że dane zgromadzone np. w celach eliminacyjnych mogą być wykorzystane (przetwarzane) w celach wykrywczych. Organy śledcze nie są ograniczone podstawą pozyskania danych biometrycznych lub genetycznych i w zależności od bieżących potrzeb prowadzonego postępowania mogą przetwarzać dane w inny sposób. Zmiana celu jest możliwa w granicach ustawowych zadań danego organu. Zgodnie z art. 13 ust. 2 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości dopuszczalne jest przetwarzanie danych osobowych, w innych nowych celach, o których mowa, o ile: 1) administratorowi wolno przetwarzać takie dane osobowe w innym nowym celu na mocy odrębnych przepisów; 2) przetwarzanie jest niezbędne i proporcjonalne w tym innym nowym celu na mocy odrębnych przepisów.

Dane genetyczne i biometryczne mogą być udostępniane organom prowadzącym postępowanie karne, postępowanie w sprawach nieletnich lub prowadzącym czynności wykrywcze lub identyfikacyjne[71], m.in. CBA[72], ABW[73], SKW[74] czy Straży Granicznej[75]. W odniesieniu do udostępniania informacji ze zbiorów DNA i daktyloskopijnych można mieć wątpliwości odnośnie do transparentności działań i zgodności z prawem unijnym. Przetwarzanie danych osobowych w związku z zapewnieniem bezpieczeństwa narodowego, w tym zapobieganiu terroryzmowi, nie podlega zasadom określonym w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[76]. Konsekwencją owego wyłączenia jest ograniczenie sądowej kontroli przetwarzania danych osobowych[77] oraz pozbawienie jednostki możliwości zweryfikowania, w jaki sposób jej dane są wykorzystywane przez organy państwa[78]. Ustawodawca wyłączył zastosowanie wyżej wskazanej ustawy w zakresie dotyczącym realizacji ustawowych zadań Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego. O ile w odniesieniu do ABW, AW, SKW i SWW wyłączenie jest zasadne[79], o tyle trudno uznać, by CBA realizowała zadania

68 § 12 ust. 4 pkt 6 Zarządzenia Nr 70 KGP.

69 W tym samym trybie dokonywana jest zmiana lub cofnięcie uprawnień dostępu do baz KSIP.

70 Por. art. 20k ustawy o Policji.

71 Zob. art. 21c i 21j ustawy o Policji.

72 Zob. art. 22a Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2018 r. poz. 2104 i 2399 oraz z 2019 r. poz. 53)

73 Zob. art. 34 Ustawy z dnia 24 maja 2002 r. Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2018 r. poz. 2387, 2245 i 2399 oraz z 2019 r. poz. 53).

74 Zob. art. 38 Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j.: Dz.U. z 2019, poz. 687).

75 Zob. art. 10a Ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz.U. z 2017 r. poz. 2365, z późn. zm.)

76 Zob. art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

77 Zob. art. 51 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości.

78 Wyłączone jest stosowanie art. 23 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości.

79 Zob. szerzej: M. Kusak, P. Wiliński, *Ochrona*…, s. 118. Autorzy wskazują jednak, że nie należy każdej z czynności wskazanych służb automatycznie uznawać jako służącej

związane z zapewnieniem bezpieczeństwa narodowego. W uzasadnieniu do projektu ustawy wskazano, że jednym z zadań CBA jest rozpoznawanie, zapobieganie i wykrywanie przestępstw przeciwko interesom ekonomicznym państwa, co jest „częścią składową" bezpieczeństwa narodowego[80]. Trudno jednak zgodzić się z tą argumentacją. Po pierwsze, jednym z zadań ABW jest ochrona „podstaw ekonomicznych państwa", co dotyczy bardziej fundamentalnych kwestii niż interesy ekonomiczne państwa[81]. Po drugie, działania związane z zapewnieniem bezpieczeństwa narodowego koncentrują się przede wszystkim na „obronności, nienaruszalności terytorium, zagrożeniu międzynarodowym terroryzmem czy przeciwdziałaniu militarnym zagrożeniom", czyli przestępstwach o najwyższym ciężarze gatunkowym. Same kwestie ekonomiczne – choć istotne – trudno uznać za porównywalne np. z zapewnieniem integralności państwa czy nienaruszalnością terytorium. CBA zajmuje się przede wszystkim zwalczaniem korupcji w jednostkach dysponujących środkami publicznymi, co nie sposób uznać za mieszczące się w zakresie zapewnienia bezpieczeństwa narodowego. Paweł Wiliński i Martyna Kusak słusznie wskazują, że biorąc pod uwagę zakres zadań i liczbę postępowań prowadzonych przez CBA oraz pozostałe służby, „potencjalna szansa przetwarzania danych osobowych konkretnej osoby przez CBA jest dużo wyższa aniżeli przez ABW, AW, SKW czy SWW", a dane te będą przetwarzane na niższym poziomie rzetelności gwarancyjności niż wynika z dyrektywy 2016/680[82].

Uprzywilejowanie CBA i zezwolenie na przetwarzanie danych osobowych jednostki na specjalnych – mniej korzystnych i mniej transparentnych – warunkach jest nieuzasadnione również z perspektywy strasburskiej. Z przepisów nie wynika, na jakich zasadach i kiedy Policja może udostępnić CBA dane biometryczne i genetyczne. Biorąc pod uwagę zadania Centralnego Biura Antykorupcyjnego, należy stwierdzić, że może to nastąpić wyłącznie w odniesieniu do przestępstw, w sprawach o które CBA może prowadzić postępowania karne. Niemniej brak zewnętrznej kontroli nad udostępnianiem i przekazywaniem danych może sprzyjać nadużyciom.

3.3. Usuwanie danych biometrycznych i genetycznych z baz danych

Przepisy krajowe regulują kwestię usunięcie danych z bazy zbiorów odcisków palców i bazy DNA. Dane te[83] – jeśli zostały zebrane w celu wykrywania sprawców przestępstw i zwalczania przestępczości – usuwa się z policyjnych baz danych[84], jeśli:

- postępowanie karne zostało umorzone postępowanie z uwagi na to, że czynu stanowiącego podstawę wprowadzenia danych osobowych do zbioru danych nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia[85];

zapewnieniu bezpieczeństwa narodowego, ale powinno się oceniać konkretnie prowadzone postępowanie.

80 Zob. art. 1 ust. 1 ustawy o CBA. Także jednym z zadań ABW jest ochrona „podstaw ekonomicznych państwa", co dotyczy bardziej fundamentalnych kwestii niż interesy ekonomiczne państwa. Tak: M. Kusak, P. Wiliński, *Ochrona*…, s. 116–124.

81 Tak: M. Kusak, P. Wiliński, *Ochrona*…, s. 116–124.

82 *Ibidem*.

83 W odniesieniu do danych genetycznych zob. art. 21e ust. 2 ustawy o Policji; w odniesieniu do danych daktyloskopijnych – art. 21l ust. 2 ustawy o Policji.

84 Dane biometryczne i genetyczne mogą zostać usunięte przez administratora, jeśli oceni on, że zostały zebrane lub są przetwarzane niezgodnie z przepisami ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości (art. 24 ust. 4 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości). Ze względu na ogólne przesłanki, które pozwalają na gromadzenie i przetwarzanie danych, wydaje się, że usunięcie danych z urzędu przez administratora może dotyczyć wyłącznie rażącego naruszenia przepisów ustaw, tj. takiego które jest widoczne na pierwszy rzut oka. Np. przetwarzane dane są nieprawidłowe, dane pobrano od świadka-pokrzywdzonego z zastosowaniem środków przymusu bezpośredniego albo w sposób oczywisty są przetwarzane w innym celu niż zwalczanie i zapobieganie przestępczości. Nie wydaje się, by ta instytucja mogła mieć szerokie zastosowanie w praktyce. Trudno, bez analizy okoliczności danej sprawy ocenić, czy czynności organów procesowych były zgodne z prawem i celowe.

85 Na marginesie warto zwrócić uwagę, że Trybunał Konstytucyjny w wyroku z 12.12.2005 r. K 32/04 dopuścił możliwości

– zdarzenie lub okoliczność, w związku z którymi wprowadzono dane osobowe do zbioru danych, nie ma znamion czynu zabronionego;
– osoba, której dane dotyczą: a) została uniewinniona prawomocnym wyrokiem sądu, b) ukończyła 100. rok życia, c) zmarła;
– tożsamość zwłok ludzkich została ustalona;
– upłynął okres przedawnienia karalności przestępstwa, na wniosek organu prowadzącego postępowanie karne – w odniesieniu do śladów nieznanych sprawców przestępstw.

W porównaniu z poprzednio obowiązującymi regulacjami[86] obecnie przepisy znacząco wydłużyły okres przechowywania danych DNA. Przepis art. 20d ustawy o Policji – w brzmieniu obowiązującym do dnia 28 stycznia 2019 r.[87] – stanowił, że dane genetyczne mogą być przechowywane przez okres do 20 lat. Niezależnie od okoliczności po upływie tego okresu dane zostawały usuwane. Obecnie obowiązujące przepisy nie wprowadzają ogólnego, maksymalnego terminu przechowywania danych, ale odnoszą go do wieku oskarżonego. W takiej sytuacji młodociany oskarżony, który został skazany na karę grzywny, nie ma żadnej gwarancji, że jego dane genetyczne i biometrycznie nie będą przechowywane przez kolejne lata. Takiej gwarancji nie daje art. 16 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości zobowiązujący administratora danych – czyli Komendanta Głównego Policji – do dokonania co 10 lat weryfikacji danych znajdujących się w policyjnych bazach danych „w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne". Nie określono jednak żadnych przesłanek, które administrator danych musi wziąć pod uwagę ani jakie okoliczności mogą mieć wpływ na podjęcie decyzji o usunięciu danych z systemu. Decyzja ma zatem charakter uznaniowy i nie podlega kontroli sądowej. Warto także podkreślić, że do momentu wejścia w życie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości kryteria oceny „przydatności" przetwarzania danych osobowych (w tym danych biometrycznych i genetycznych) wynikały z Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 23 sierpnia 2018 r. w sprawie przetwarzania informacji przez Policję[88]. Przepis § 29 ust. 1 rozporządzenia stanowił, że „oceniając dane zgromadzone w celu wykrywania przestępstw pod kątem ich przydatności, uwzględnia się:

– rodzaj i charakter popełnionego czynu wyczerpującego znamiona przestępstwa;
– rodzaj i charakter dobra chronionego prawem naruszonego popełnionym przestępstwem;
– formy sprawstwa i umyślności popełnienia przestępstwa;
– postaci zamiaru i skutki czynu, w tym rodzaj i rozmiar wyrządzonej lub grożącej szkody;
– zagrożenie sankcją karną za popełnione przestępstwo;
– liczbę popełnionych przestępstw;
– czas, który upłynął od momentu wprowadzenia danych do zbioru danych do momentu dokonywania oceny;
– inne zgromadzone informacje o osobie;
– podstawy uzyskania, pobrania lub zgromadzenia danych oraz ich prawdziwość;
– aktualność przesłanek legalności oraz niezbędności dalszego przetwarzania danych do wykonania zadań ustawowych Policji;
– wystąpienie okoliczności określonych w art. 20 ust. 17b i 18 ustawy o Policji, a w przypadku danych daktyloskopijnych wystąpienie okoliczności określonych w art. 21l ust. 2".

Pojawia się zatem pytanie, jak nieprecyzyjny przepis art. 16 ust. 1 ustawy implementującej DODO będzie stosowany w praktyce i czy okoliczności sprecyzowane w rozporządzeniu z 2018 r. nadal będą brane pod

przetwarzania danych osób, które zostały prawomocnie uniewinnione.

86 Zob. przepis art. 20d ustawy o Policji w brzmieniu nadanym ustawą DODO.

87 Do momentu wejścia w życie ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości.

88 Dz.U. z 2018, poz. 1636. Rozporządzenie zostało uchylone ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości i utraciło moc w dniu 7 lutego 2020 r. Dotychczas nie przyjęto nowych przepisów regulujących to zagadnienie.

uwagę[89]. Obecnie brak jest aktualnego orzecznictwa, które wyjaśniałoby, jak należy oceniać potencjalną przydatność danych. Inną kwestią jest możliwość usunięcia danych, które przekazano służbom, które zostały wyłączone z zakresu ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości, np. CBA. Nie wydaje się, by udostępnienie danych biometrycznych i genetycznych CBA czy ABW wiązało się z automatycznym uznaniem przydatności dalszego przechowywania tych danych. Chcąc ustalić, czy dane określonej osoby nadal powinny być przechowywane, administrator danych, tj. Komendant Główny Policji, powinien wystąpić z zapytaniem do kierownictwa odpowiedniej służby, czy dane te nadal są „przydatne", ale stanowisko odnośnie do przydatności dalszego przechowywania danych nie powinno być wiążące. Administrator danych – niezależnie od stanowiska kierownictwa ABW, CBA czy SKW – powinien mieć możliwość podjęcia decyzji o usunięciu danych, które można uznać za nieprzydatne, np. biorąc pod uwagę wiek osoby, której dane są przetwarzane, jej stan zdrowia czy inne informacje zgromadzone o tej osobie świadczące o tym, że nie popełni przestępstwa[90].

Warto także zwrócić uwagę, że administrator danych – uznając je za nieprzydatne – niekoniecznie ma obowiązek je usunąć. Zgodnie z art. 17 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości dane, które zostały uznane za zbędne, mogą zostać przekształcone w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo w taki sposób, że przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań. Pseudoanonimizacja danych osobowych jest możliwa na podstawie dyrektywy 2016/680[91] i może być prowadzona w celu określenia struktury przestępczości. Trudno przewidzieć, w jakim kierunku rozwinie się praktyka działania organów policyjnych i co będzie przemawiało za tym, by dane nieprzydatne jednak zachować. Kwestie te powinny zostać doprecyzowane w rozporządzeniu lub wytycznych Komendanta Głównego Policji. Niestety, przepisy wykonawcze nie odnoszą się do tego zagadnienia, więc decyzja o pseudoanonimizacji jest uznaniowa i nietransparentna dla jednostki. Ustawodawca wprowadził stopniowalność „nieprzydatności" danych osobowych, w tym danych szczególnie wrażliwych, nie formułując żadnych przesłanek pozwalających ocenić legalność i celowość dalszego przechowywania danych[92].

Trudno także zrozumieć, dlaczego ustawodawca pominął kwestię usunięcia danych biometrycznych i genetycznych osób, wobec których postępowanie karne zostało prawomocnie umorzone z przyczyn innych niż to, że czynu stanowiącego podstawę wprowadzenia danych osobowych do zbioru danych nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia (art. 17

89 W uzasadnieniu do projektu ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości nie wyjaśniono, jakie kryteria powinny być brane pod uwagę przy okresowej ocenie przydatności danych. Zob. uzasadnienie do Rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, druk sejmowy nr 2989.

90 Wydaje się, że w sytuacji, gdy dane biometryczne i genetyczne zostały udostępnione innym służbom, administrator danych może wziąć pod uwagę tylko czynniki obiektywne, świadczące o nieprzydatności danych. Policja nie ma bowiem dostępu do informacji o postępowaniach przygotowawczych czy czynnościach operacyjnych prowadzonych przez ABW, CBA itp. Niemniej o nieprzydatności danych może świadczyć np. długi czas od ich wprowadzenia do systemu.

91 M. Kusak i P. Wiliński zwracają uwagę, że art. 17 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości jest niezgodny z dyrektywą DODO. Przepisy unijne dopuszczają przekształcenie danych znajdujących się w rejestrach odpowiednich służb w sposób uniemożliwiający ich przyporządkowanie do konkretnej osoby. Polski ustawodawca pozwala natomiast na mniej dokładną anonimizację, a zatem – przy odpowiednich nakładach – będzie możliwe ustalenie tożsamości danej osoby. Zob. szerzej: M. Kusak, P. Wiliński, *Ochrona…*, s. 120–124.

92 Zwłaszcza, że pseudoanonimizacja może być odwrócona. Jednostka, które dane genetyczne i biometryczne nadal są przechowywane na podstawie art. 17 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości nie ma gwarancji, że proces ten w pewnym momencie nie zostanie odwrócony.

§ 1 pkt 1 k.p.k.) lub czyn nie zawierał znamion czynu zabronionego (art. 17 § 1 pkt 2 k.p.k.). Prawomocne umorzenie postępowania w skutkach prawnych nie różni się od uniewinnienia. Przepisy ustawy o Policji podważają jednak tę tezę. Osoba, wobec której postępowanie zostało prawomocnie umorzone, np. ze względu na niepodleganie karze (art. 17 § 1 pkt 4 k.p.k.), choć nie poniesie odpowiedzialności karnej, to jej dane będą przetwarzane w policyjnych bazach danych. Pojawia się pytanie o *ratio legis* tego rozwiązania. W uzasadnieniu do projektu ustawy nowelizującej art. 20d i 20e ustawy o Policji nie wyjaśniono tej rozbieżności.

4. Podsumowanie

Kwestie gromadzenia, przechowywania i przetwarzania danych biometrycznych i genetycznych regulują przede wszystkim: art. 74 § 2 k.p.k. ustawy o Policji, ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości oraz rozporządzenia i wytyczne Komendanta Głównego Policji. Pojawia się jednak wątpliwość, czy obowiązujące regulacje są wystarczająco precyzyjne i zapobiegają nieuprawnionemu wykorzystaniu informacji o jednostce.

Jeśli chodzi o podstawy gromadzenia danych biometrycznych i genetycznych, to oczywiste jest, że nie jest możliwe precyzyjne określenie *in abstracto* przesłanek, kiedy organy procesowe mogą pobrać materiał do badań DNA, a kiedy wykonać zdjęcia sygnalityczne czy zdjąć odciski palców. Konieczne jest pozostawienie przestrzeni do indywidualnej oceny każdej sprawy i dostosowania zakresu czynności procesowych do potrzeb danego postępowania. Niemniej ustawodawca w art. 74 § 2 k.p.k. i w art. 20 ust. 1k ustawy o Policji pozwala organom procesowych całkowicie dowolnie podjąć decyzję o tym, jakie dane wrażliwe zostaną pobrane. Zarówno w sprawie o drobne (np. zwykłą, drobną kradzież), jak i poważne przestępstwo formalnie dopuszczalne jest przeprowadzenie tych samych czynności, o ile organy procesowe uznają, że mają one znaczenie dowodowe, wykrywcze lub identyfikacyjne. Takie rozwiązanie nie jest prawidłowe. Stopień i zakres ingerencji w prywatność jednostki powinien być proporcjonalny do wagi czynu zabronionego. Ustawodawca powinien zapobiegać gromadzeniu danych o jednostkach „na wszelki wypadek", formalnie w celu wykrywania ewentualnych, przyszłych przestępstw. Sama potencjalna użyteczność pobrania danych biometrycznych i genetycznych – bez związku z prowadzonym postępowaniem – jest niewystarczającą podstawą ingerencji w prywatności jednostki.

Przetwarzanie danych osobowych odbywa się automatycznie, a przepisy wykonawcze szczegółowo regulują kwestie wprowadzania danych do systemów informatycznych, nadawania uprawnień do dostępu do baz danych, zakresu i czasu trwania upoważnienia. Krajowy System Informacji Policyjnej, w tym bazy DNA i odcisków linii papilarnych, jest podstawową bazą danych, z której korzystają inne służby, tj. ABW, CBA, Żandarmeria Wojskowa, Straż Graniczna, SKW i SWW. Policja ma obowiązek umożliwić dostęp do baz danych, jeśli dana służba tego zażąda w związku z wykonywaniem przez nią ustawowych zadań. W odniesieniu do udostępniania danych biometrycznych i genetycznych można mieć wątpliwość odnośnie do procedury udostępniania danych na wniosek CBA. Ze względu na ustawowe wyłączenie działalności tej służby spod zakresu ustawy o ochronie danych osobowych w związku z zapobieganiem

Nie jest możliwe precyzyjne określenie *in abstracto* przesłanek, kiedy organy procesowe mogą pobrać materiał do badań DNA, a kiedy wykonać zdjęcia sygnalityczne czy zdjąć odciski palców.

i zwalczeniem przestępczości[93], obowiązek udostępnienia danych biometrycznych i genetycznych przez Policję na żądanie CBA oraz praktycznie brak możliwości oceny celowości i zasadności tego żądania pojawia się niebezpieczeństwo niekontrolowanego przetwarzania danych osobowych. Osoba, której dane zostały przekazane CBA, nie może skorzystać z uprawnień wynikających z ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości, tj. prawa dostępu do informacji o przetwarzaniu danych osobowych (wynikającym z art. 23 ust. 1 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości) ani z sądowej kontroli przetwarzania danych osobowych (art. 51 ust. 1 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości).

Największe wątpliwości z perspektywy zgodności z orzecznictwem strasburskim[94] budzi czas przechowywania danych biometrycznych i genetycznych. Ustawodawca wprowadził takie same terminy przechowywania danych DNA i odcisków palców, choć wydaje się, że powinien odpowiednio zróżnicować czas przechowywania tych danych w zależności od tego, jaki zakres informacji o jednostce wynika z określonych danych. Przepisy krajowe, które obligują do usunięcia danych, jeśli osoba, której dane są przechowywane ukończyła 100 lat, zmarła lub nie było podstaw do prowadzenia przeciwko niej postępowania karnego z przyczyn wynikających z art. 17 § 1 pkt 1 i 2 k.p.k., tak naprawdę pozwalają na masowe gromadzenie informacji o jednostkach. Dane biometryczne i genetyczne będą przechowywane przez czas, który nie jest jednoznacznie zdefiniowany. Zagrożenia przed masowym gromadzeniem danych nie eliminuje mechanizm przewidziany w art. 16 ust. 1 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości, tj. okresowa ochrona przydatności danych. Ustawodawca nie wprowadził żadnych kryteriów oceny przydatności, pozostawiając administratorowi danych, tj. Komendantowi Głównemu Policji, całkowitą swobodę decyzyjną. Co więcej, uznając dane za nieprzydatne, administrator danych nie jest zobowiązany do ich usunięcia, ale może dokonać pseudoanonimizacji. Obecnie brak jest orzecznictwa, które wyjaśniałoby, dlaczego w niektórych sytuacjach dane uznane za nieprzydatne zostały usunięte, a w innej sytuacji – poddane pseudoanonimizacji. Trudno także zrozumieć, dlaczego z rejestrów policyjnych nie usuwa się danych biometrycznych i genetycznych osób, wobec których postępowanie karne zostało prawomocnie umorzone, np. z przyczyn wskazanych w art. 17 § 1 pkt 3 i 4 k.p.k. Na marginesie warto podkreślić, że obecnie obowiązujące, niekorzystne dla jednostki przepisy zostały wprowadzone pod pretekstem implementacji przepisów unijnych. Przed wejściem w życie ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości prawo krajowe przewidywało maksymalny, 20-letni termin przechowywania danych biometrycznych i genetycznych, a rozporządzenia wykonawcze do ustawy o Policji określały kryteria, które administrator danych musiał wziąć pod uwagę, oceniając przydatność (celowość) przechowywania tych danych. W uzasadnieniu do projektu ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości nie wyjaśniono, dlaczego – implementując przepisy unijne – obniżono standard krajowy, choć dyrektywa DODO wymagała wprowadzenia „odpowiednich" terminów przechowywania i usuwania danych. Poprzednio obowiązujące przepisy – w zakresie dotyczącym przechowywania i usuwania danych biometrycznych i genetycznych – były zgodne, bardziej gwarancyjne dla jednostki, z prawem unijnym i nie było potrzeby wprowadzania żadnych zmian.

Dane biometryczne i genetyczne mogą być gromadzone i przetwarzane w celach identyfikacyjnych, dowodowych, eliminacyjnych i wykrywczych. Organy procesowe nie są związane w celu wprowadzenia informacji o jednostce i np. odciski palców czy wyniki badań DNA wprowadzone w celach dowodowych mogą być wykorzystane w celach identyfikacyjnych. Konieczne jest zapewnienie możliwości efektywnego zwalczania przestępczości, więc przepisy krajowe nie mogą być nadmiernie formalistyczne i nie mogą utrudniać pracy organom ścigania. Wydaje się, że ustawodawca określił podstawy gromadzenia i przetwarzania danych

93 Zob. art. 3 pkt 2 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczeniem przestępczości.

94 I prawem unijnym.

osobowych na tyle precyzyjnie, na ile było to możliwe, a na prawidłowość stosowania tych przepisów w praktyce ustawodawca ma niewielki wpływ. Przestrzeganiu zasad gromadzenia i przetwarzania wrażliwych danych o jednostce sprzyja wprowadzenie zewnętrznej kontroli nad działaniami organów ścigania.

Ze względu na szeroki zakres wyłączenia z art. 3 pkt 2 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości osoba, której pobrano dane biometryczne i genetyczne, nie zawsze będzie mogła zweryfikować, w jaki sposób wykorzystywane są jej dane osobowe i czy służba, która nimi dysponuje, robi to w granicach swoich kompetencji. Jak to już zostało wcześniej wskazane, zastrzeżenia może budzić brak kontroli nad przetwarzaniem danych osobowych, w tym danych wrażliwych, przez CBA[95]. Ponadto dodatkowe gwarancje proceduralne, pozwalające na zewnętrzną kontrolę przetwarzania danych osobowych, wynikające z art. 24 ust. 1 ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości mają zastosowanie wyłącznie do naruszeń tej ustawy. Nie odnoszą się zatem do nieprawidłowości podczas przetwarzania danych biometrycznych i genetycznych stanowiących naruszenie innych ustaw, m.in. ustawy o Policji.

Podsumowując, prawo krajowe w odniesieniu do gromadzenia, przetwarzania i przechowywania danych biometrycznych i genetycznych nie jest w pełni zgodne z tym, czego od państw Rady Europy wymaga ETPC. Największe zastrzeżenia można mieć w zakresie czasu przechowywania i przetwarzania danych osobowych, który w praktyce pozwala na masowe gromadzenie danych o jednostkach. Problemu tego nie rozwiązuje możliwość wcześniejszego usunięcia danych biometrycznych i genetycznych na podstawie decyzji administratora danych – Komendanta Głównego Policji – ponieważ jest to decyzja całkowicie uznaniowa i nie sprecyzowano okoliczności, które powinien on wziąć pod uwagę, podejmując taką decyzję. Ponadto przepisy nie spełniają kryterium „jakości", na które zwraca uwagę Trybunał strasburski. Regulacje pozwalające na pobieranie danych biometrycznych i genetycznych nie gwarantują wystarczającej ochrony przed arbitralnością działania organów władzy publicznej ani nie zapewniają jednostce możliwości kontroli nad przetwarzaniem i przechowywaniem danych wrażliwych. Należy także podkreślić, że przyczyną niezgodności prawa krajowego ze standardem strasburskim nie była konieczność implementacji dyrektywy 2016/680. Ustawodawca wprowadził antygwarancyjne dla jednostki zmiany, uzasadniając je powinnością wdrożenia regulacji unijnych. Tymczasem prawodawca unijny pozostawił państwom Unii szeroki margines swobody w zakresie m.in. czasu przechowywania danych biometrycznych i genetycznych, podstaw normatywnych pozwalających na usunięcie wrażliwych informacji o jednostce, gdy poprzednio obowiązujące regulacje były zgodne z przepisami unijnymi. Sposób, w jaki została implementowana dyrektywa 2016/680, powoduje nie tylko to, że regulacje krajowe są niezgodne ze standardem strasburskim, ale naruszają także prawo unijne.

Artykuł powstał w grancie badawczym finansowanym przez Narodowe Centrum Nauki Nr 2017/27/B/HS5/00854, pt. „Dopuszczalność dowodów w procesie karnym. Między poznaniem prawdy a rzetelnością i sprawnością postępowania".

95 Zwłaszcza, że w odniesieniu do przestępstw korupcyjnych, badania DNA raczej nie są podstawową czynnością dochodzeniowo-śledczą.

Bibliografia

Gabriel-Węglowski M., *Działania antyterrorystyczne. Komentarz*, Warszawa 2018.

Kusak M., *Ochrona danych osobowych w sprawach karnych – rekomendacje na tle transpozycji dyrektywy 2016/680/UE*, „Europejski Przegląd Sądowy" 2017, nr 10, s. 10–19.

Kusak M., Wiliński P., *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020.

Mróz K., *Zagrożenia dla prawa do prywatności jednostki w związku z przetwarzaniem danych osobowych w celu zapobiegania i zwalczania przestępczości*, „IusNovum" 2020, nr 1, s. 95–114.