IUS ET ADMINISTRATIO ISSN 2300-4797

NR 1/2024 (54) DOI: 10.15584/iuseta.2024.1.5

dr Paweł Siejak

ORCID: 0000-0002-5075-1959
Wyższa Szkoła Administracji Publicznej w Kielcach

Standardy Rady Europy w obszarze ochrony danych w świetle nowych wyzwań cywilizacyjnych

Council of Europe standards in the area of data protection in the light of new civilization challenges

Abstract

The article presents the efforts made by the Council of Europe in the area of data protection. It was verified whether these activities were identical or original to those undertaken by the European Union. An attempt was made to compare which solutions are more effective.

Keywords: personal data, Council of Europe, Convention 108+, Protocol 223.

Streszczenie

Artykuł przedstawia działania podejmowane przez Radę Europy w zakresie ochrony danych. Zweryfikowano, czy działania te są tożsame z tymi podejmowanymi przez Unię Europejską, czy też mają charakter oryginalny. Podjęto próbę porównania, które rozwiązania są bardziej skuteczne.

Słowa kluczowe: dane osobowe, Rada Europy, Konwencja 108+, Protokół 223.

1. Wstęp

Ochrona danych osobowych jest zagadnieniem niezwykle aktualnym w dobie rozwoju nowych technologii i sztucznej inteligencji. Rada Europy jako organizacja zajmująca się tworzeniem standardów ochrony praw człowieka podejmuje wysiłki również w tych obszarach. Źródłem jest oczywiście Konwencja o ochronie praw człowieka i podstawowych wolności z 1950 roku, która zawiera postanowienia o poszanowaniu prawa do prywatności.

Nowe wyzwania cywilizacyjne w obszarze biotechnologii, sztucznej inteligencji, masowego wykorzystania mediów społecznościowych sprawiają, że ochrona

prywatności jest bardzo aktualna. Obecnie przed tą organizacją stoi wiele wyzwań i konieczność wypracowania takich standardów, by nadrzędna wartość, jaką jest prywatność, była chroniona. Drugim zadaniem stojącym przed instytucjami Rady Europy jest wypracowanie mechanizmu monitorowania tych standardów w państwach członkowskich. Obecna Konwencja Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 1981 roku[1] wraz z protokołami zmieniającymi z 2001 roku[2] oraz 2018 roku[3] są podstawowymi instrumentami w przedmiotowym obszarze.

Celem niniejszego artykułu jest zweryfikowanie, jak standardy Rady Europy w obszarze ochrony danych osobowych dopasowują się do wyzwań współczesnego świata. Czy w świetle działań podejmowanych przez Unię Europejską inicjatywy Rady Europy w obszarze formowania wspólnych standardów w tej dziedzinie są celowe? Czy Rada Europy stworzyła spójny system monitorowania wypracowanych standardów? Czy w chwili, kiedy RODO[4] stało się instrumentem prawnym regulującym kwestie ochrony danych osobowych w 27 państwach europejskich, istnieje potrzeba wprowadzania dodatkowych standardów? Czy Rada Europy jest w stanie wypracować oryginalne podejście w obszarze ochrony danych osobowych, czy jest prekursorem, czy jedynie powiela rozwiązania Unii Europejskiej? Starając się odpowiedzieć na tak postawione pytania, dokonano analizy systemowej oraz analizy treści konwencji, rezolucji, raportów i innych materiałów opracowanych w ramach działań Rady Europy oraz Unii Europejskiej.

Literatura w obszarze ochrony danych osobowych jest bardzo bogata, również w kontekście standardów międzynarodowych, jednak w większości dotyczy dorobku Unii Europejskiej. Niniejszy artykuł wypełnia lukę badawczą, przedstawiając dorobek innej europejskiej organizacji międzynarodowej, czyli Rady Europy, która swoim działaniem w obszarze ochrony danych wpływa na systemy prawne niemal wszystkich państw europejskich, a także tych spoza kontynentu.

---

[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

[2] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181).

[3] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 2016, nr 119, s. 1 ze zm.).

2. Znaczenie Konwencji 108 i proces jej nowelizacji

Ochrona danych osobowych wywodzi się z prawa do ochrony prywatności jako dobra niematerialnego podlegającego ochronie. Już w Konwencji o ochronie praw człowieka i podstawowych wolności z 1950 roku (dalej: EKPC), w art. 8 ust. 1[5], wskazano, że prywatność zasługuje na ochronę prawną. Stąd też szersze zainteresowanie Rady Europy ochroną danych osobowych jako zagadnieniem węższym, wywodzącym się z prawa do prywatności, jest niczym innym jak rozszerzeniem standardów określonych w EKPC. Zaznaczyć należy, że jakkolwiek pojęcie danych osobowych łączy się z pojęciem prywatności, to nie są to zagadnienia tożsame. Dane osobowe to informacje pozwalające zidentyfikować osobę fizyczną, a w konsekwencji ich ujawnienie może doprowadzić do naruszenia prywatności. Nie należy jednak prawa ochrony danych osobowych zaliczać bezpośrednio do prawa nowych technologii. Jak słusznie zauważa M. Kawecki, nowe technologie mają istotny wpływ na ochronę danych osobowych, lecz nie są z tym pojęciem tożsame[6]. Prawo ochrony danych osobowych powinno być traktowane jako odrębna gałąź prawa[7].

Rada Europy podjęła i nadal podejmuje konkretne działania celem wypracowania wspólnych dla państw członkowskich standardów w obszarze ochrony danych osobowych. Ważne jest, że w obszarze swoich prac organizacja ta nie zamyka się wyłącznie na Europę. Co więcej, Rada Europy była prekursorem w zakresie tworzenia wspólnych ram ochrony danych. W 1973 roku przyjęto rezolucję (73) 22 dotyczącą ochrony prywatności jednostek w odniesieniu do elektronicznych banków danych w sektorze prywatnym[8], rok później przyjęto kolejną rezolucję[9]. W obu tych dokumentach określono pierwszy raz w formie wytycznych, zasady przetwarzania danych (przetwarzanie rozumiane jako gromadzenie, przetwarzanie *sensu stricte*, retencja), takie jak: zasada celowości, weryfikacji sposobu pozyskiwania danych, czasowości ich przetwarzania, ograniczenia przekazywania danych, informowania osób, których dane dotyczą,

[5] Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005).

[6] M. Kawecki, *Prawo ochrony danych osobowych jako nowa dziedzina prawa*, „Europejski Przegląd Sądowy" 2017, nr 5, s. 5.

[7] *Ibidem*, s. 9.

[8] Committee of Ministers Resolution (73) 22 on the Protection of the Privacy of Individuals Vis-a-vis Electronic Data Banks In the Private Sector, adopted on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

[9] Committee of Ministers Resolution (74) 29 on the Protection of the Privacy of Individuals Vis-a-vis Electronic Data Banks In the Private Sector, adopted on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

o ich przetwarzaniu, prawie do korekty danych, dbania o bezpieczeństwo danych. Opracowane rezolucje były wynikiem konferencji ministrów sprawiedliwości z 1972 roku, która poświęcona została ochronie prywatności w związku z coraz większym gromadzeniem danych osobowych w komputerach. Formułując treść rezolucji, wzorowano się na rozwiązaniach już przyjętych w Szwecji – pierwszym kraju na świecie, który podjął próbę uregulowania zasad przetwarzania danych osobowych[10]. Pamiętać należy, że rezolucje Komitetu Ministrów odnosiły się do zasad przetwarzania danych przez Radę Europy jako organizację. Dopiero 28 stycznia 1981 roku otwarto do podpisu Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[11] – był to pierwszy prawnie wiążący dokument o charakterze międzynarodowym odnoszący się do ochrony danych osobowych jako dokument wiążący już państwa-strony (dalej: Konwencja 108).

Konwencję 108 podpisało i ratyfikowało w sumie 55 państw, nie tylko członkowie Rady Europy, ale także Argentyna, Burkina Faso, Republika Zielonego Przylądka, Mauritius, Meksyk, Maroko, Federacja Rosyjska (państwo członkowskie Rady Europy do 2022 roku), Senegal, Tunezja i Urugwaj – zakres podmiotowy wskazuje, że Konwencja ma potencjał, aby stać się konwencją daleko wykraczającą poza granice Europy. Celem Konwencji było stworzenie ram prawnych dla podstawowych zasad ochrony danych osobowych i ich przetwarzania ze względu na szczególną wagę, jaką mają one w kontekście prawa do ochrony prywatności. Od tej pory państwa członkowskie miały obowiązek stworzyć lub dostosować krajowe normy prawne do zasad określonych w Konwencji.

W myśl postanowień Konwencji 108 dane osobowe powinny być przetwarzane zgodnie z celem, jaki towarzyszy przy ich gromadzeniu, i powinny być uaktualniane, a ich retencja winna nastąpić niezwłocznie po osiągnięciu celu ich przetwarzania[12]. Obowiązek retencji danych nie dotyczy sytuacji, kiedy dane osobowe zostaną zanonimizowane i wykorzystywane do celów statystycznych. Nałożono na państwa-strony obowiązek wymagania od podmiotów przetwarzających dane, zarówno publicznych, jak i prywatnych, podjęcia działań celem zabezpieczenia danych. Zawarto również podstawowy katalog praw osób, których dane są przetwarzane, takich jak: informacja o przetwarzaniu danych osobowych,

[10] K. Szwed, *Ewolucja ochrony danych osobowych na przykładzie Polski i Szwecji*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2011, nr 71, s. 199.

[11] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

[12] Wyrok ETPC w sprawie *L.H. przeciwko Łotwie* o przetwarzanie danych medycznych, skarga nr 52019/07.

poznanie celu ich przetwarzania oraz informacja o administratorze. Osoba, której dane dotyczą, ma zagwarantowane prawo do wglądu w dane, do ich sprostowania oraz żądania ich usunięcia, a także złożenia skargi w razie niezaspokojenia jednego z wymienionych praw. Postanowienia Konwencji 108 w zakresie ochrony praw człowieka i wolności są ważne z jeszcze jednego powodu. Konwencja zabrania swobodnego przetwarzania danych wrażliwych, takich jak np.: rasa, płeć, poglądy polityczne, religia, czy informacje o skazaniu. Oczywiście nie jest to zakaz bezwzględny, jednak wytyczono kierunek, który po latach jest nadal niezwykle aktualny – dane wrażliwe zasługują na szczególną ochronę prawną. Przepisy Konwencji nakładają na państwa-strony względny obowiązek swobodnego przepływu danych osobowych.

Państwa-strony mają obowiązek wprowadzenia do swoich systemów prawnych sankcji karnych i odszkodowawczych dla podmiotów łamiących przepisy krajowe odnoszące się do podstawowych zasad ochrony danych osobowych.

Obecnie prawa te, zwłaszcza w świetle dorobku Unii Europejskiej, wydają się być oczywiste, jednak należy pamiętać, że określono je ponad 40 lat temu – stąd ich znaczenie w ocenie odrobku Rady Europy w obszarze ochrony danych jest niebagatelne.

Celem stałego czuwania nad interpretacją Konwencji przez państwa-strony powołano Komitet Doradczy (T-PD). Jego rola odnosi się także do zajmowania stanowiska na temat nowelizacji Konwencji 108, tworzenia raportów, opracowań i wytycznych.

Dynamiczne zmiany społeczne i technologiczne w XXI wieku wymusiły na Radzie Europy podjęcie nowych działań w obszarze ochrony danych osobowych. Konwencja 108 jest nowelizowana. Trwa proces wejścia w życie Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (CETS nr 223). Został on otwarty do podpisu 10 października 2018 roku i dopiero po wejściu w życie Konwencja 108 wraz z Protokołem zmieniającym będzie tworzyła tzw. Konwencję 108+. Jednak droga do zmian była długa, a ich źródłem jest oczekiwanie ze strony członków Zgromadzenia Parlamentarnego Rady Europy, aby państwa członkowskie w większym stopniu zaangażowały się we wdrażanie prawa traktatowego[13]. Następnie w rezolucji 1732(2010)[14] uznano, że prawo traktatowe Rady Europy musi nadążać za zmianami w świecie

[13] Motion for recommendation "For a greater commitment of member states concerning the efficiency and implementation of the Council of Europe Treaty Law", doc. 11425, Strasbourg, 8.10.2007.

[14] Resolution 1732(2010) Reinforcing the effectiveness of Council of Europe treaty law, PACE, 21.05.2010.

i jako jedną z konwencji, która powinna być znowelizowana, wskazano właśnie Konwencję 108. Celem zmian jest dostosowanie przepisów do obecnej sytuacji społecznej i technologicznej, a precyzyjniej – zapewnienie zgodności między Konwencją 108 Rady Europy a prawem Unii Europejskiej, przede wszystkim rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)[15]. Odnosząc się do nieobowiązującej już dyrektywy 95/46 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu takich danych, należy zauważyć, że powstała ona na kanwie osiągnięć Konwencji 108, a w rezultacie stała się od niej bardziej precyzyjna i kompletna. To pokazuje, że standardy wypracowywane jednocześnie przez Radę Europy, a następnie przez Unię Europejską bywają w ścisłej korelacji. Nie jest to pierwsza zmiana – poprzednia dotyczyła rozszerzenia, aby stronami Konwencji mogły być nie tylko państwa, ale także organizacje[16]. Konwencja 108 nawet po nowelizacji nie osiągnie takiego stopnia szczegółowości jak prawo unijne, jednak należy pamiętać, że ma ona nieco inny cel. Jej zadaniem jest wyznaczenie wspólnych standardów i kierunku rozwoju prawodawstwa krajowego. Jedną z najważniejszych jednak zmian, jakie miały nastąpić, było wdrożenie mechanizmu monitorującego Konwencję, takiego, jaki znany jest w przypadku innych konwencji[17].

Projekt Protokołu zmieniającego przygotował Komitet *ad hoc* ds. ochrony danych[18], następnie doszło do konsultacji i ostatecznie 10 października 2018 roku Protokół 223 został otwarty do podpisu. Przewiduje on szereg zmian w Konwencji 108. Przede wszystkim zaostrzone zostaną zasady proporcjonalności[19], minimalizacji oraz legalności przetwarzania danych. Samo pojęcie przetwarzania danych będzie oznaczało każdą operację lub zestaw operacji wykonywanych

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), doc. 32016R0679.

[16] Amendment to Convention ETS No.108 allowing the European Communities to accede: Adopted 15 June 1999 (Entry into force: after acceptation by all Parties); Explanatory Memorandum on the amendments to Convention 108 allowing the accession of the European Communities.

[17] Framework Convention for the Protection of National Minorities (ETS No. 157).

[18] *Ad hoc* Committee on Data Protection (CAHDATA) – Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), *Working document containing the draft Protocol and highlighting reservations that have been made thereon*, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616e [dostęp: 14.04.2023].

[19] Wyrok ETPC uznający skargę *L.B. przeciwko Węgrom* z 9 marca 2023 r., skarga nr 36345/16.

na danych osobowych, takich jak gromadzenie, przechowywanie, konserwacja, zmiana, odzyskiwanie, ujawnianie, udostępnianie, usuwanie, niszczenie lub przeprowadzanie działań logicznych i/lub operacje arytmetyczne na takich danych. Poszerzona zostanie definicja administratora danych, wprowadzone zostanie pojęcie współadministratora. Pojęcie danych wrażliwych zostanie poszerzone o dane genetyczne i biometryczne, pochodzenie etniczne czy przynależność do związków zawodowych. Protokół przewiduje obowiązek zgłaszania naruszeń w związku z przetwarzaniem danych osobowych. Kolejnym *novum* jest wymóg zasady *privacy by design*, tzn. ochrony prywatności na każdym etapie projektu, którego elementem jest przetwarzanie danych osobowych[20]. Państwa-strony są zobowiązane do powołania wewnętrznego, niezależnego i wyposażonego w uprawnienia władcze organu nadzoru, którego celem będzie stanie na straży przestrzegania standardów określonych w znowelizowanej Konwencji 108. Ważne zmiany, jakie wprowadza Protokół 223, to względny obowiązek ochrony danych w sektorze publicznym, nawet wówczas, gdy dane te są przetwarzane w związku z bezpieczeństwem, a także ułatwienie w zakresie transgranicznego przepływu danych[21]. Europejski Trybunał Praw Człowieka m.in. w sprawie *Uzun przeciwko Niemcom* podkreślił, że nie dochodzi do złamania zasady proporcjonalności przetwarzania danych (w tym przypadku lokalizacja osoby fizycznej przez inwigilację sygnału GPS) ani łamania prawa do prywatności gwarantowanego przez art. 8 EKPC, jeżeli celem jest zapewnienie bezpieczeństwa państwa i ochrona zdrowia i życia obywateli[22].

Wreszcie najważniejsza kwestia, jaką przewiduje Protokół 223, to wdrożenie mechanizmu ewaluacji, czyli monitorowania przez Komitet Doradczy poziomu przestrzegania przepisów Konwencji przez strony. Mechanizm ten będzie opierał się na opiniach formułowanych przez Komitet Doradczy, a następnie na zaleceniach, jeżeli ten dostrzeże potrzebę zmian w prawie wewnętrznym strony.

Kolejnym organem mającym fundamentalny wpływ na przedmiotowy problem ma Komisarz Rady Europy ds. Ochrony Danych. Wybierany jest przez Komitet Doradczy z listy osób wskazanych przez Sekretarza Generalnego Rady Europy. Wcześniej organ ten był znany jako Komisarz Ochrony Danych[23]. Jest on wybierany na 4-letnią kadencję z możliwością jednej reelekcji. Do jego zadań należy nadzór nad przestrzeganiem zasad przetwarzania danych osobowych gromadzonych

[20] M. Ciechomska, *E-usługi a RODO*, Warszawa 2021, s. 223.

[21] Resolution CM/Res(2022)14 on establishing the Council of Europe Regulations on the Protection of Personal Data, Strasbourg, 15.01.2022.

[22] Wyrok ETPC o nieuznaniu skargi *Uzun przeciwko Niemcom* w sprawie o monitoring GPS, skarga nr 35623/05.

[23] Secretary General's Regulation of 17 April 1989 instituting a system of data protection for personal data files at the Council of Europe, Strasbourg, 17.04.1989.

i przetwarzanych przez organy Rady Europy. Co roku przedstawia on raport ze swojej działalności Komitetowi Doradczemu oraz Sekretarzowi Generalnemu Rady Europy.

Do jego zadań określonych w Regulaminie Rady Europy o ochronie danych w uchwale CM/Res(2022)14 (dalej: Regulamin) należy:

- monitorowanie i zapewnienie stosowania postanowień Regulaminu;
- rozpatrywanie skarg osób, których dane dotyczą, w odniesieniu do domniemanego naruszenia ich praw wynikających z Regulaminu oraz w razie potrzeby nakazania podjęcia działań naprawczych;
- prowadzenie dochodzeń w sprawie stosowania Regulaminu z własnej inicjatywy lub w celu rozpatrzenia skargi osoby, której dane dotyczą;
- formułowanie opinii na zlecenie Inspektora Ochrony Danych lub administratora w każdej sprawie związanej ze standardami ochrony danych określonych w Konwencji 108 i w Regulaminie;
- kierowanie zaleceń do administratora, który następnie składa Rzecznikowi sprawozdanie z ich wykonania;
- współpraca z krajowymi lub międzynarodowymi organami ochrony danych lub organami ochrony danych organizacji międzynarodowych w zakresie niezbędnym do wykonywania jej funkcji i wykonywania jej uprawnień;
- uczestniczenie na żądanie w pracach Komitetu Doradczego powołanego na podstawie art. 22 Konwencji 108 oraz w pracach innych komitetów Konwencji lub komitetów międzyrządowych.

Komisarz Rady Europy ds. Ochrony Danych jest uprawniony również do uzyskania dostępu do wszystkich danych osobowych przetwarzanych przez Radę Europy. Ma on prawo do nałożenia na organy Rady Europy czasowego lub całkowitego zakazu przetwarzania niektórych danych lub sposobu, w jaki są one przetwarzane. Może nakazać zawiadomić osobę, której dane dotyczą, o naruszeniu zasad ich przetwarzania. Komisarz ma prawo do podjęcia działań, których celem jest sprostowanie lub usunięcie danych, jeżeli były one przetwarzane niezgodnie z przepisami Regulaminu. Do władczych uprawnień Komisarza należy też prawo domagania się, aby spełniono żądania osoby, której dane dotyczą, jeżeli uzna, że żądanie to jest zgodne z Konwencją 108 oraz z Regulaminem.

Konwencja 108 stanowi podstawowy instrument prawny w obszarze ochrony danych osobowych. Zakończenie procedury wchodzenia w życie jej znowelizowanej wersji zdecydowanie przyczyni się do poprawy jej efektywności.

Nowelizacja Konwencji 108 jest ważnym krokiem do zwiększenia ochrony danych osobowych, jednak pojawia się ważne pytanie, czy jej działalność nie jest kalką prawną rozwiązań, które wdrożyła już Unia Europejska, przede

wszystkim w RODO. Jest ono, podobnie jak przyszła Konwencja 108+, oparte na zasadzie ryzyka i *privacy by design* (art. 25 ust. 1 RODO) oraz domyślnej ochronie prywatności. Zasady przetwarzania danych określone w art. 5 RODO są bardziej rozbudowane od zasad określonych w art. 5 Protokołu 223, chociaż powyższe są ze sobą zbieżne. Zasady retencji danych są szerzej opisane, w sposób kauzalny wraz z odwołaniem do innych przepisów prawa krajowego (art. 25, 47 RODO), gdy w Konwencji 108 ta kwestia jest potraktowana bardziej ogólnikowo. Tego rodzaju przykładów jest więcej, jak chociażby rola i kompetencje współadministratora danych (art. 26 RODO), pojęcie danych wrażliwych, zasady odpowiedzialności cywilnej za przetwarzanie danych, podjęcie środków bezpieczeństwa w procesie przetwarzania danych. Reasumując – Konwencja 108 po wejściu w życie Protokołu 223 i powstaniu tzw. Konwencji 108+ nie będzie zawierała przepisów wykluczających się czy sprzecznych z przepisami RODO. Wynika to też z faktu, że prace negocjacyjne w ramach Rady Europy ze strony państw członkowskich prowadziła Komisja Europejska.

3. Zgromadzenie Parlamentarne Rady Europy oraz Komitet Ministrów – działania na rzecz poprawy ochrony danych

Dorobek prawny Rady Europy w obszarze tworzenia standardów ochrony danych osobowych nie zamyka się jednak tylko w działaniach związanych z Konwencją 108. Już w 1968 roku Zgromadzenie Parlamentarne Rady Europy (PACE) wydało zalecenie[24] dla Komitetu Ministrów, by ten za pośrednictwem Komitetu Ekspertów ds. Praw Człowieka badał i informował, czy ustawodawstwo krajowe w państwach członkowskich odpowiednio chroni prawo do prywatności przed naruszeniami, które mogą zostać popełnione przy użyciu nowoczesnych metod naukowych i technicznych, jak podsłuchy telefoniczne, podsłuchiwanie, ukradkowa obserwacja czy też bezprawne wykorzystywanie oficjalnych statystyk. Celem było zapewnienie ochrony obywatelom przed łamaniem art. 8 EKPC. Istotna jest uchwała PACE z 1980 roku[25], w której zwrócono się do Parlamentu Europejskiego, by podjął działania, których celem będzie synergia wysiłków Wspólnot Europejskich i Rady Europy w obszarze ochrony prywatności i danych osobowych.

[24] Recommendation 509, Human rights and modern scientific and technological development, Strasbourg, 31.01.1968.

[25] Resolution 721, Data processing and the protection of human rights, Strasbourg, 1.02.1980.

Już w latach 90. Komitet Ministrów zwrócił uwagę na potrzebę ochrony danych medycznych, wydając zalecenie z 1997 roku[26]. W tym samym roku do podpisu otwarto Konwencję o ochronie praw człowieka i godności istoty ludzkiej w zakresie zastosowań biologii i medycyny, zwaną Konwencją o prawach człowieka i biomedycynie lub Konwencją z Oviedo[27]. Ustanowiono w niej zasadę, że predykcyjne testy genetyczne mogą być przeprowadzane wyłącznie w celach medycznych, a informacje z takich testów podlegają szczególnej ochronie. Konwencja zakazuje również tworzenia ludzkich embrionów w celach badawczych, co odnosi się do ochrony wrażliwych danych genetycznych i osobistych w kontekście postępu technologicznego i bioetyki. PACE podejmowało również kolejne działania w tym obszarze, czego przykładem była uchwała z 2011 roku w sprawie *Potrzeby globalnego rozważenia implikacji danych biometrycznych dla praw człowieka* (1797)[28]. Wydanie tej uchwały było odpowiedzią na rosnące zagrożenie terrorystyczne oraz praktyki wielu państw, które w celu zapewnienia bezpieczeństwa wprowadzały masowe przetwarzanie danych biometrycznych. Apelowano w tej uchwale o przestrzeganie ogólnych zasad ochrony danych, w tym danych biometrycznych jako szczególnie wrażliwych. Zalecono, by w ustawodawstwach krajowych znalazły się przepisy regulujące celowość i proporcjonalność. Zwrócono uwagę, że kwestia ochrony prywatności danych biometrycznych nie może być w żadnym stopniu bagatelizowana ze względu na bezpieczeństwo czy rozwój nauki. Warto w tym miejscu przywołać sprawę *Drelon przeciwko Francji*[29]. Dotyczyła ona bezpodstawnego przetwarzania danych bez zgody osoby, której dane dotyczyły, a co więcej – dane zebrane w chwili wywiadu medycznego przed oddaniem krwi przez skarżącego zostały nadinterpretowane. Podmiot przetwarzający dane oznaczył skarżącego jako osobę homoseksualną wyłącznie na podstawie odmowy skarżącego na pytanie o orientację seksualną. Trybunał uznał, że takie działanie jest jawnym łamaniem art. 8 EKPC oraz art. 5 Konwencji 108.

W późniejszym okresie, w odpowiedzi na dynamiczne zmiany w obszarze nowych technologii oraz rozwój mobilnych aplikacji do przetwarzania danych medycznych, wydano nowe zalecenie[30]. Ma ono na celu wsparcie państw członkowskich

[26] Recommendation No. R(97) 5 on the protection of medical data, Strasbourg, 13.02.1997.

[27] Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No. 164).

[28] Resolution 1797, The need for a global consideration of the human rights implications of biometrics, Strasbourg, 2011.

[29] Wyrok ETPC uznający skargę *Drelon przeciwko Francji* w sprawie o zbieranie i retencję danych osobowych przez EFS, skarga nr 3153/1627758/18.

[30] Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, 27.03.2019.

w tworzeniu regulacji i praktyk zgodnych z nowymi wyzwaniami technologicznymi, przy jednoczesnym poszanowaniu podstawowych praw człowieka, w tym prawa do prywatności i ochrony danych osobowych.

PACE zarekomendowało rozwój współpracy z Organizacją Narodów Zjednoczonych oraz Unią Europejską. Ograniczenie przetwarzania danych biometrycznych rekomendował także Komitet Ministrów w zaleceniu z 2016 roku[31]. Należy zauważyć, że zagadnienie ochrony prywatności w kontekście danych medycznych i biometrycznych ma szczególne znaczenie dla bioetyki, ponieważ dotyka kluczowych aspektów ochrony praw człowieka oraz godności jednostki w dynamicznie zmieniającym się świecie nowych technologii[32].

Uchwała PACE o ochronie prywatności i danych osobowych w Internecie i mediach internetowych (1843) z 2011 roku[33] była ważnym krokiem do dalszej promocji standardów Rady Europy w omawianym zakresie. PACE tym razem rekomendowało przede wszystkim szersze podjęcie współpracy z Organizacją Narodów Zjednoczonych i Unią celem rozległego promowania Konwencji 108 jako instrumentu prawnego, który może być zaakceptowany powszechnie. Zachęca się do jego przyjęcia przede wszystkim Stany Zjednoczone, Japonię czy Izrael. Do tej pory – stan na 17 kwietnia 2023 roku – Konwencję 108 przyjęły: Argentyna, Republika Zielonego Przylądka, Mauritius, Meksyk, Maroko, Rosyjska Federacja, Senegal, Tunezja oraz Urugwaj.

W zakresie cyberbezpieczeństwa i ochrony prywatności PACE zajęło stanowisko w 2014 roku, kiedy to w związku z upowszechnieniem dostępu do internetu wzrosła ilość ataków na jego użytkowników[34]. PACE rekomendowało zwiększenie współpracy w obszarze zabezpieczeń, stworzenie bardziej precyzyjnych ram prawnych, które determinowałyby poprawę bezpieczeństwa hot spotów oraz internetu rzeczy (*internet of things* – IoT). W tym celu padł apel o zacieśnienie współpracy takich organizacji, jak: Międzynarodowa Organizacja Normalizacyjna (International Organization for Standardization) oraz Internetowa Korporacja ds. Nadanych Nazw i Numerów (Internet Corporation for Assigned Names and Numbers – ICANN)) i IANA (Internet Assigned Numbers Authority). Ważne

[31] Recommendation CM/Rec(2016)8 of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, Strasbourg, 26.10.2016.

[32] Guide to Public Debate in Human Rights and Biomedicine, Adopted by the Committee on Bioethics at its 16th meeting, Strasbourg, 2019.

[33] Resolution 1843, The protection of privacy and personal data on the Internet and online media, Strasbourg, 2011.

[34] C. Banasiński, M. Rojszczak, J.M. Chmielewski, W. Hydzik, J. Łuczak, W. Nowak, K. Wańkowski, *Cyberbezpieczeństwo*, Warszawa 2020, s. 69.

z perspektywy ochrony danych osobowych są jeszcze dwie uchwały PACE: *o poprawie ochrony sygnalistów* (2060)[35] oraz *masowej inwigilacji*(2045)[36]. Pierwsza z nich odnosi się do szczególnej ochrony sygnalistów. PACE nawołuje do stworzenia konwencji o ochronie sygnalistów, w tym o szczególnej ochronie ich prywatności. Konwencja taka jak dotąd nie powstała[37]. Obecne regulacje Rady Europy w stosunku do ochrony sygnalistów znajdują się w Cywilnoprawnej konwencji o korupcji[38]. Uchwała w sprawie masowej inwigilacji była odpowiedzią na tzw. aferę E. Snowdena z 2013 roku. PACE zaapelowało o wprowadzenie do krajowych systemów prawnych przepisów ograniczających samowolę służb bezpieczeństwa w obszarze przetwarzania danych osobowych, w tym metadanych.

Inicjatywy podejmowane przez Komitet Ministrów można podzielić na dwa rodzaje: deklaracje i zalecenia. Do najważniejszych deklaracji należy Deklaracja Komitetu Ministrów w sprawie zagrożeń dla praw podstawowych wynikających ze śledzenia cyfrowego i innych technologii nadzoru[39], w której odwołano się do szczególnej potrzeby ograniczania eksportu technologii umożliwiających inwigilację i wzmożenia kontroli tych działań. Zwrócono w tym dokumencie również uwagę na koordynację działań w zakresie cyberbezpieczeństwa, ochrony danych (poprzez przestrzeganie zasad: *privacy by design* oraz domyślnej ochrony prywatności) i zarządzania internetem[40]. Koherentne z deklaracją jest zalecenie Komitetu Ministrów w sprawie ochrony i promowania prawa do wolności wypowiedzi oraz prawa do życia prywatnego w odniesieniu do neutralności sieci, które zawiera szereg postanowień nakładających na operatorów internetu wiele nakazów. Ich celem jest zapobieżenie dyskryminacji w korzystaniu z sieci[41].

Ważna jest również Deklaracja Komitetu Ministrów w sprawie konieczności ochrony prywatności dzieci w środowisku cyfrowym z 2021 roku[42] przyjęta

[35] Resolution 2060, Improving the protection of whistle-blowers, Strasbourg, 2015.

[36] Resolution 2045, Mass surveillance, Strasbourg, 2015.

[37] Zob. A. Kantor-Kilian, *Organizacja modelu kanałów sygnalizowania nieprawidłowości w świetle dyrektywy2019/1937* [w:] *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających nieprawidłowości*, red. B. Baran, M. Ożóg, Warszawa 2021, s. 37.

[38] Civil Law Convention on Corruption (ETS No. 174).

[39] Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, Strasbourg, 11.06.2013.

[40] Report by the Secretary General The Council of Europe Strategy on Internet Governance (2012–2015), CM(2016)9, 28.01.2016.

[41] Recommendation CM/Rec(2016) 1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, Strasbourg, 13.01.2016.

[42] Declaration by the Committee of Ministers on the need to protect children's privacy in the digital environment, Strasbourg, 28.04.2021.

w związku z zaleceniem Komitetu Ministrów dla państw członkowskich w sprawie wytycznych dotyczących poszanowania, ochrony i realizacji praw dziecka w środowisku cyfrowym[43]. Oba dokumenty są niezwykle istotne, podkreślono w nich, że dzieciom (rozumianym jako osoby do 18. roku życia) nie tylko należy się ochrona prywatności w sieci[44], ale także same dzieci jako autorzy treści internetowych powinny być edukowane w zakresie poszanowania praw innych osób, ze szczególnym uwzględnieniem ochrony prywatności. W pkt 3.4 zalecenia Komitetu Ministrów CM/Rec(2018)7 stwierdzono, że „dzieci mają prawo do życia prywatnego i rodzinnego w środowisku cyfrowym, co obejmuje ochronę ich danych osobowych oraz poszanowanie poufności ich korespondencji i komunikacji prywatnej". Naczelną zasadą przetwarzania danych dzieci powinna być minimalizacja.

Zalecenia Komitetu Ministrów w obszarze ochrony danych odnoszą się też do takich zagadnień jak ochrona danych osobowych w zatrudnieniu regulowana przez zalecenie CM/Rec (2015)5[45] wraz z memorandum wyjaśniającym. W zaleceniu tym zwrócono uwagę, że przetwarzanie danych pracowniczych oprócz tego, że musi być zgodne ze standardami określonymi w Konwencji 108+, to niezbędne jest także, aby pracodawca kierował się zasadą minimalizmu przetwarzania danych. W zaleceniu zwrócono uwagę, że prawo krajowe winno istotnie ograniczać możliwości przetwarzania danych niezwiązanych z wykonywaniem pracy lub zbędnych z punktu widzenia ochrony interesów pracodawcy. Wskazano tutaj dane zbierane z takich źródeł, jak: namierzanie lokalizacji pracownika, informacje udostępniane w mediach społecznościowych czy dane biometryczne lub genetyczne. Do naruszenia w obszarze przetwarzania danych pracowniczych doszło, jak stwierdził w wyroku Europejski Trybunał Praw Człowieka, w sprawie *Bărbulescu przeciwko Rumunii*. Dopuszczono się nadmiernego przetwarzania danych osobowych przez monitorowanie komputera pracownika[46].

Jednym ze sposobów przetwarzania danych jest profilowanie, czyli zautomatyzowane przetwarzanie danych osobowych, które dotyczy wykorzystania tych danych do oceny pewnych cech osobowych osoby fizycznej, takich jak np.

[43] Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Strasbourg, 4.07.2018.

[44] Zob. M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, s. 292.

[45] Recommendation CM/Rec(2015)5 of the Committee of Ministers to memberStates on the processing of personal data in the context of employment, Strasbourg, 1.04.2015.

[46] Wyrok ETPC w sprawie *Bărbulescu przeciwko Rumunia* o monitorowanie komputerów pracowniczych z 5 września 2017 r., skarga nr 61496/08.

jej lokalizacja, zainteresowania, zdrowie czy sytuacja finansowa[47]. O profilowaniu jako sposobie przetwarzania danych mówi się, kiedy są spełnione te dwa wyżej wymienione elementy: automatyzacja przetwarzania i ocena czynników osobowych. Zagadnienie profilowania Komitet Ministrów podjął w zaleceniu dla państw członkowskich w sprawie ochrony osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania[48]. *Profilowanie* zdefiniowano w zaleceniu jako każdą formę zautomatyzowanego przetwarzania danych osobowych, w tym z wykorzystaniem systemów uczenia maszynowego, polegającego na wykorzystaniu danych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Natomiast *profil* to zestaw danych przypisanych do osoby fizycznej, charakteryzujących kategorię osób fizycznych lub przeznaczonych do zastosowania w odniesieniu do osoby fizycznej. Istotne jest, że w tym zaleceniu odniesiono się do profilowania w kontekście wykorzystania sztucznej inteligencji. Komitet Ministrów zaleca państwom członkowskim, aby wdrażały w prawie krajowym obowiązek certyfikacji systemów sztucznej inteligencji pod kątem ich zgodności ze standardami ochrony danych osobowych.

Działania Zgromadzenia Parlamentarnego Rady Europy oraz Komitetu Ministrów w obszarze ochrony danych osobowych mają charakter uzupełniający dla dorobku nowelizowanej Konwencji 108. Określone w uchwałach, deklaracjach i zaleceniach, są aktualne do zmieniającego się świata i nowych wyzwań. Zdecydowanie wpisują się w system standardów ochrony danych osobowych. W Unii Europejskiej standardy ochrony danych osobowych są ugruntowane w art. 8 Karty praw podstawowych Unii Europejskiej oraz art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, które gwarantują każdej osobie prawo do ochrony jej danych osobowych. Kluczowym instrumentem jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO), uzupełniane przez inne akty prawne, takie jak dyrektywa 2016/680 (tzw. dyrektywa policyjna)[49], regulująca

[47] M. Ciechomska, *Pra*wne *aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2017, nr 5, s. 37–42.

[48] Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Strasbourg, 3.11.2021.

[49] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 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,

przetwarzanie danych w kontekście egzekwowania prawa, oraz dyrektywa 2002/58/WE (dyrektywa ePrivacy)[50], która chroni prywatność w komunikacji elektronicznej.

W kontekście nowych technologii Unia Europejska podjęła również prace nad rozporządzeniem ePrivacy, które zastąpi dyrektywę ePrivacy i lepiej dostosuje przepisy do współczesnych wyzwań, takich jak komunikatory internetowe czy śledzenie aktywności w sieci. Ponadto wytyczne Europejskiej Rady Ochrony Danych (EROD) wzmacniają stosowanie RODO, dostarczając szczegółowych interpretacji przepisów w takich obszarach, jak profilowanie, transfery międzynarodowe czy sztuczna inteligencja.

4. Podsumowanie

Analizując dotychczasowe dokonania Rady Europy w zakresie tworzenia standardów ochrony danych osobowych, trzeba zwrócić uwagę nie tylko na Konwencję 108, ale także na niezwykle bogaty dorobek Zgromadzenia Parlamentarnego Rady Europy oraz Komitetu Ministrów. Synergia podjętych działań buduje obraz systemu zasad, których celem jest ochrona prywatności i promowanie wartości w państwach członkowskich w niezwykle rozbudowanej formie. Konwencja 108 stanowi pierwszy i jak dotąd jedyny wiążący prawnie międzynarodowy instrument wskazujący właściwe wytyczne dla zmian w prawie krajowym w odniesieniu do stron Konwencji. Trzeba też zauważyć, że jakkolwiek działania mające na celu nowelizację Konwencji (Protokół CETS 223) są motywowane zmianami w prawie Unii Europejskiej, to jednak nie są one kalką prawną, ale też nie są rozwiązaniami oryginalnymi. Sama filozofia i najważniejsze aspekty ochrony danych osobowych są tożsame, ale RODO opisuje je zdecydowanie precyzyjniej. Jest to rozporządzenie, czyli akt prawa Unii Europejskiej nadający się do bezpośredniego stosowania. Konwencja 108, nawet zmodernizowana, będzie potrzebowała doprecyzowania w systemach prawnych państw-stron. W przypadku 27 państw będących jednocześnie członkami Unii Europejskiej i Rady Europy tym aktem będzie RODO. Pojawia się więc pytanie, dla kogo jest Konwencja 108 w pierwotnej i zmienionej formie. Pierwotnie wyprzedzała ona rozwiązania

wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 2016, nr 119, s. 89 ze zm.).

[50] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. UE L 2002, nr 201, s. 37 ze zm.).

Wspólnot Europejskich, a następnie Unii Europejskiej. Obecnie stanowi ona powtarzanie rozwiązań, które już funkcjonują w większości jej państw członkowskich. Nasuwa się więc pytanie, czy Konwencja 108 wraz z Protokołem 223 nie powinna być eksportowana do państw trzecich jako mapa drogowa dla budowy globalnego systemu ochrony danych osobowych opartego na wspólnych, europejskich wartościach.

Można dostrzec pewną synergię wysiłków Rady Europy, Unii Europejskiej, a także Organizacji Narodów Zjednoczonych w obszarze ochrony danych osobowych i prawa do prywatności, jednak polegają one na uzupełnianiu się, a nie kopiowaniu rozwiązań prawnych. Zdecydowanie do tej pory, dopóki Protokół 223 nie wejdzie w życie, brakuje mechanizmu monitorującego.

Inicjatywy podejmowane przez Radę Europy w kontekście działań, jakie na tym samym obszarze podejmuje Unia Europejska, są celowe. Rozwiązanie polegające na harmonizacji przepisów, jakim jest RODO, dotyczy państw członkowskich Unii Europejskiej. Natomiast instrumenty prawne Rady Europy są kierowane do większej grupy odbiorców. Kluczowe jest, aby w ramach kooperacji wypracowywane standardy były spójne i nie tworzyły zbędnych problemów w interpretacji dla administratorów danych.

W obecnej sytuacji Rada Europy tworzy pewne ramy prawne i rozwiązania, forsuje je za pomocą konwencji, uchwał ZPRE czy zaleceń i deklaracji Komitetu Ministrów, natomiast nadal nie ma narzędzi do weryfikacji poziomu ich wdrożenia w krajowych systemach prawnych, jak ma to miejsce w systemie Unii Europejskiej i znacznie skuteczniejszym funkcjonowaniu Trybunału Sprawiedliwości Unii Europejskiej. Tylko orzecznictwo Europejskiego Trybunału Praw Człowieka odgrywa pewną rolę w weryfikacji poziomu ochrony danych, jednak siłą rzeczy odnosi się ono wyłącznie do EKPC i jej art. 8 – gwarantującego prawo do prywatności i ochrony życia rodzinnego. Przed Radą Europy stają też nowe wyzwania w kontekście ochrony danych osobowych i rozwoju sztucznej inteligencji.

Bibliografia

Banasiński C., Rojszczak M., Chmielewski J.M., Hydzik W., Łuczak J., Nowak W., Waćkowski K., *Cyberbezpieczeństwo*, Warszawa 2020.

Ciechomska M., *E-usługi a RODO*, Warszawa 2021.

Ciechomska M., *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2017, nr 5.

Kantor-Kilian A., *Organizacja modelu kanałów sygnalizowania nieprawidłowości w świetle dyrektywy 2019/1937* [w:] *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających nieprawidłowości*, red. B. Baran, M. Ożóg, Warszawa 2021.

Kawecki M., *Prawo ochrony danych osobowych jako nowa dziedzina prawa*, „Europejski Przegląd Sądowy" 2017, nr 5.

Rojszczak M., *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.

Szwed K., *Ewolucja ochrony danych osobowych na przykładzie Polski i Szwecji*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2011, nr 71.

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 2016, nr 119, s. 1 ze zm.).

Dokumenty

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181).

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005).

Committee of Ministers Resolution (73) 22 on the Protection of the Privacy of Individuals Vis-a-vis Electronic Data Banks In the Private Sector, adopted on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

Committee of Ministers Resolution (74) 29 on the Protection of the Privacy of Individuals Vis-a-vis Electronic Data Banks In the Private Sector, adopted on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

Wyrok ETPC w sprawie *L.H. przeciwko Łotwie* o przetwarzanie danych medycznych, skarga nr 52019/07.

Motion for recommendation "For a greatercommitment of memberstatesconcerning the efficiency and implementation of the Council of Europe Treaty Law", doc. 11425, Strasbourg, 8.10.2007.

Resolution 1732(2010) Reinforcing the effectiveness of Council of Europe treaty law, PACE, 21.05.2010.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), doc. 32016R0679.

Official Journal of the European Communities, C 277, 5 November 1990.

Amendment to Convention ETS No.108 allowing the European Communities to accede: Adopted 15 June 1999 (Entry into force: after acceptation by all Parties); Explanatory Memorandum on the amendments to Convention 108 allowing the accession of the European Communities.

Framework Convention for the Protection of National Minorities (ETS No. 157).

Ad hoc Committee on Data Protection (CAHDATA) – Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), *Working document containing the draft Protocol and highlighting reservations that have been made thereon*, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616e [dostęp: 14.04.2023].

Wyrok ETPC uznający *skargę L.B. przeciwko Węgrom* z 9 marca 2023 r., skarga nr 36345/16.

Resolution CM/Res(2022)14 on establishing the Council of Europe Regulations on the Protection of Personal Data, Strasbourg, 15.01.2022.

Wyrok ETPC o nieuznaniu skargi *Uzun przeciwko Niemcom* w sprawie o monitoring GPS, skarga nr 35623/05.

Secretary General's Regulation of 17 April 1989 instituting a system of data protection for personal data files at the Council of Europe, Strasbourg, 17.04.1989.

Recommendation 509, Human rights and modern scientific and technological development, Strasbourg, 31.01.1968.

Resolution 721, Data processing and the protection of human rights, Strasbourg, 1.02.1980.

Resolution 1797, The need for a global consideration of the human rights implications of biometrics, Strasbourg, 2011.

Recommendation No. R(97) 5 on the protection of medical data, Strasbourg, 13.02.1997.

Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, 27.03.2019.

Guide to Public Debate in Human Rights and Biomedicine, Adopted by the Committee on Bioethics at its 16th meeting, Strasbourg, 2019.

Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No. 164).

Wyrok ETPC uznający skargę *Drelon przeciwko Francji* w sprawie o zbieranie i retencję danych osobowych przez EFS, skarga nr 3153/1627758/18.

Recommendation CM/Rec(2016)8 of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, Strasbourg, 26.10.2016.

Resolution 1843, The protection of privacy and personal data on the Internet and online media, Strasbourg, 2011.

Resolution 2060, Improving the protection of whistle-blowers, Strasbourg, 2015.

Resolution 2045, Mass surveillance, Strasbourg, 2015.

Civil Law Convention on Corruption (ETS No. 174).

Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, Strasbourg, 11.06.2013.

Report by the Secretary General The Council of Europe Strategy on Internet Governance (2012–2015), CM(2016)9, 28.01.2016.

Recommendation CM/Rec(2016)1of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, Strasbourg, 13.01.2016.

Declaration by the Committee of Ministers on the need to protect children's privacy in the digital environment, Strasbourg, 28.04.2021.

Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Strasbourg, 4.07.2018.

Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, Strasbourg, 1.04.2015.

Wyrok ETPC w sprawie *Bărbulescu przeciwko Rumunia* o monitorowanie komputerów pracowniczych z 5 września 2017 r., nr 61496/08.

Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Strasbourg, 3.11.2021.