Ochrona danych osobowych w działalności dziennikarskiej

Dobrochna Ossowska-Salamonowicz

Ochrona danych osobowych w działalności dziennikarskiej

Wydawnictwo
Uniwersytetu Warmińsko-Mazurskiego
w Olsztynie

E-seria Monografie Wydziału Prawa i Administracji UWM

Kolegium Wydawnicze UWM
Przewodniczący
Zbigniew Chojnowski
Redaktor Działu
Małgorzata Szwejkowska

Redaktor prowadzący serii
Dorota Lis-Staranowicz

Recenzent
Marek Chmaj

Projekt okładki
Adam Głowacki

Skład i łamanie
Urszula Trzeciecka

ISBN 978–83–7299–957–3

Wydawnictwo UWM
ul. Jana Heweliusza 14, 10-718 Olsztyn
tel. 89 523 36 61, fax 89 523 34 38
www.uwm.edu.pl/wydawnictwo/
e-mail: wydawca@uwm.edu.pl

Ark. wyd. 11,8; ark. druk. 10
Druk: Zakład Poligraficzny UWM w Olsztynie, zam. nr 400

Spis treści

Wstęp

Każdy ma prawo do posiadania, pozyskiwania i rozpowszechniania informacji, jednak nie każdy korzystając z tego prawa – tak jak jest to w przypadku dziennikarzy – musi zachować szczególną rzetelność i staranność i równocześnie pamiętać, że jego misją jest służba społeczeństwu oraz państwu. Zdarzają się sytuacje, kiedy dziennikarz musi rozstrzygać dylemat komu ma służyć i czyj interes jest ważniejszy. Czy ujawnić informację powołując się na interes społeczny, czy nie podawać informacji do wiadomości publicznej ze względu na interes państwa. Musi też wiedzieć, jakie konsekwencje prawne może ponieść, nawet jeśli w słusznym interesie społecznym ujawni czyjeś dane osobowe.

Zarówno wolność pozyskiwania i rozpowszechniania informacji, jak i prawo dostępu do informacji publicznej, przewidziane w Konstytucji, nie mają absolutnego charakteru i podlegają ograniczeniom wynikającym z konieczności ochrony określonych dóbr i wartości. Może dochodzić do kolizji określonych dóbr prawnie chronionych: np. prawa do kontroli i jawności życia publicznego z ochroną danych osobowych osób pełniących funkcje publiczne. Z faktu, że konstytucyjnie chronioną wartością jest prawo obywatela do uzyskania informacji publicznej, wynika szereg problemów wynikających z konieczności interpretacji pojęć kluczowych, np. zakresu stosowania przesłanek umożliwiających odmowę udostępnienia informacji publicznej (np. ze względu na ochronę prywatności).

Rozważenia wymaga również celowość i skuteczność m.in. karnoprawnej reakcji na naruszenie przepisów o ochronie danych osobowych czy nieudostępnienie informacji publicznej zwłaszcza z uwagi na trudności z wykładnią przepisów w tym zakresie oraz niespójne orzecznictwo sądów. Szereg już obowiązujących regulacji prawnych w zakresie ochrony danych osobowych oraz szereg inicjatyw legislacyjnych w tym zakresie, (także na gruncie prawa europejskiego) wprowadzających ograniczenia dostępu do określonej kategorii danych, informacji, stanowi źródło wielu utrudnień. Przy wielu mało konkretnych przepisach regulujących ochronę danych osobowych (np. podejrzanego, oskarżonego, pokrzywdzonego) istnieje pokusa nadużywania przez nierzetelnych dziennikarzy swoich uprawnień.

Z drugiej jednak strony obecnie obowiązujące prawo nie ułatwia dziennikarzowi zbierania informacji. Po wejściu w życie przepisów ustawy o dostępie do informacji publicznej (od 2001) dziennikarz został pozbawiony monopolu na uzyskiwanie informacji. Ponadto w okresie między 13 listopada 1997 – 1 maja 2004 ustawa o ochronie danych osobowych z całym swoim rygoryzmem odnosiła się do działalności dziennikarskiej, skutecznie utrudniając dziennikarzom pracę. Dopiero z chwilą wejścia w życie art. 3a ust. 2 ustawy o ochronie danych

osobowych do działalności dziennikarskiej stosuje się tylko niektóre przepisy ustawy (np. o uprawnieniach kontrolnych GIODO i obowiązkach administratora zbioru danych osobowych).

To że prasa ma gwarancję swobody zbierania i wykorzystywania materiałów prasowych (m.in. dzięki określonemu w art. 44 prawa prasowego zakazowi utrudniania zbierania materiałów krytycznych i tłumienia krytyki), nie oznacza zgody na całkowity woluntaryzm. Jeśli bowiem dziennikarze przestają dążyć do odkrycia prawdy, to dają uzasadniony powód do ograniczania wolności mediów. Coraz bardziej popularni blogerzy (vlogerzy, czy chociażby użytkownicy Facebooka) szybko demaskują oszustwa mediów i równocześnie stanowią alternatywne źródło informacji. Zdarza się też coraz częściej, że ludzie nie mają czasu na czytanie prasy, ale za to czytają wpisy znajomych na Facebooku czy forach internetowych. Blogerzy w przeciwieństwie do mediów z reguły nie przywiązują wagi do jakości swoich tekstów (materiałów), media zaś muszą pamiętać nie tylko o obowiązkach wynikających chociażby z prawa prasowego, ale przede wszystkim o swojej wiarygodności zawodowej i wiarygodności medium dla którego pracują.

W pracy omówione zostały różnego rodzaju ustalenia prawne podejmujące problem ochrony danych osobowych. Tym samym dokonano opisu historycznego pokazującego narastanie świadomości prawnej i pojawiania się potrzeb uzasadniających konieczność wypracowania coraz bardziej precyzyjnych narzędzi służących ochronie jednostki. Ponadto opis doktryny – poczynając od uregulowań mających charakter postulatywny, czyli niewiążący (Powszechna Deklaracja Praw Człowieka, Rezolucje ONZ i Rady Europy, Rekomendacje Zgromadzenia Parlamentarnego Rady Europy czy dyrektywy unijne) po akty o charakterze wiążącym (Konstytucja RP z 1997, ustawy, konwencje Rady Europy i Unii Europejskiej) pokazują kontekst ogólny, w jakim kształtowała się w Polsce świadomość prawna określająca reguły ochrony danych osobowych. Polska ustawa o ochronie danych osobowych jako zbiór przepisów kompleksowo regulujących tę kwestię, obowiązuje dopiero od szesnastu lat. Wcześniej przepisów o ochronie danych osobowych należało szukać w regulacjach sektorowych (k.c., k.k. itp.). Oczywiste zatem jest, że dopiero tworzy się i utrwala coś, co można by nazwać kulturą prawną, czyli schematy i wzory rozumienia oraz postępowania z danymi osobowymi szanujące prawa jednostki w demokratycznym społeczeństwie. O aktualnym stanie świadomości pragmatyki prawa świadczy bogate orzecznictwo sądów krajowych oraz europejskich.

Wykaz skrótów

ABI	–	Administrator Bezpieczeństwa Informacji
BIP	–	Biuletyn Informacji Publicznej
CBA	–	Centralne Biuro Antykorupcyjne
C-SIS	–	Centralny System Informacyjny Schengen
CS-SIS	–	Centralny System SIS II zawierający bank danych SIS II
EFRG	–	Europejski Fundusz Rolnej Gwarancji
EFRROW	–	Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Rolnych
EIOD	–	Europejski Inspektor Ochrony Danych
EKPC	–	Europejska Konwencja Praw Człowieka
ETPC	–	Europejski Trybunał Praw Człowieka
GIODO	–	Generalny Inspektor Ochrony Danych Osobowych
IPN	–	Instytut Pamięci Narodowej
k.c.	–	kodeks cywilny
k.k.	–	kodeks karny
k.k.s.	–	kodeks karny skarbowy
k.p.a.	–	kodeks postępowania administracyjnego
k.p.k.	–	kodeks postępowania karnego
k.r.o.	–	kodeks rodzinny i opiekuńczy
Konstytucja	–	Konstytucja RP z 1997 r.
Konwencja	–	Konwencja nr 108 Rady Europy
KPP	–	Karta Praw Podstawowych
MKPC	–	Międzynarodowa Karta Praw Człowieka
MPPOiP	–	Międzynarodowy Pakt Praw Obywatelskich i Politycznych
MPPOiP	–	Międzynarodowy Pakt Praw Obywatelskich i Politycznych
NI-SIS	–	Narodowy Interfejs SIS II
NSA	–	Naczelny Sąd Administracyjny
N-SIS	–	Krajowy System Informacyjny Schengen
OECD	–	Organizacja Europejskiej Współpracy Gospodarczej
p.p.s.a.	–	prawo o postępowaniu przed sądami administracyjnymi
SA	–	Sąd Apelacyjny
SABAM	–	Belgijski Zarząd Autorów, Kompozytorów i Wydawców
SIS	–	System Informacyjny Schengen
SN	–	Sąd Najwyższy
TK	–	Trybunał Konstytucyjny
TS UE	–	Trybunał Sprawiedliwości UE (ETS)
TWE	–	Traktat Wspólnoty Europejskiej
UE	–	Unia Europejska
WE	–	Wspólnota Europejska
WSA	–	Wojewódzki Sąd Administracyjny

Rozdział 1. Uniwersalna ochrona danych osobowych

ONZ

Powszechna Deklaracja Praw Człowieka

Charakter prawnomiędzynarodowy Powszechnej Deklaracji Praw Człowieka z dnia 10 grudnia 1948 jest sporny. Niektórzy polscy prawnicy uznają, że jest dokumentem niewiążącym, inni zaś uznają Deklarację za element prawa zwyczajowego[1]. Z pewnością jest ona pierwszym dokumentem, który szczegółowo określił prawa i podstawowe wolności człowieka. Z tego przede wszystkim powodu Deklaracja spotkała się z szerokim poparciem międzynarodowej opinii publicznej i została uznana za kamień milowy w walce o prawa człowieka na świecie. Można też spotkać pogląd, że Deklaracja jest aktem prawa międzynarodowego, w którym po raz pierwszy pojawiła się formuła prawa do prywatności[2].

Powszechna Deklaracja Praw Człowieka uznaje, że „przyrodzona godność wszystkich członków wspólnoty ludzkiej jest podstawą wolności, sprawiedliwości i pokoju świata". W art. 12[3] wprowadza zakaz arbitralnego wkraczania w życie prywatne, rodzinę, mieszkanie lub korespondencję. Chroni też przed zamachami na honor i reputację. W myśl jej postanowień, każdy jest uprawniony do ochrony prawnej przed takim wkraczaniem lub takimi zamachami. Jednak zgodnie z postanowieniami art. 29 każdy w korzystaniu ze swych praw (i wolności) podlega pewnym ograniczeniom. Muszą one wynikać z przepisów prawa i służyć:

1) poszanowaniu praw i wolności innych osób,
2) zaspokojeniu słusznych wymagań moralności,

---

[1] Roman Kuźniar uważa, że: „fakt, iż deklaracja nie została uchwalona jako obowiązujący traktat międzynarodowy, stał się powodem do szerokiej dyskusji na temat charakteru zobowiązań, jakie ten dokument za sobą pociąga. Autorzy deklaracji mieli świadomość, iż dokument, nad którym pracują, nie będzie miał charakteru prawnego. […] Deklaracja to nie tylko intencje, ale również zobowiązania państw, aczkolwiek pozbawione sankcji prawa międzynarodowego". R. Kuźniar, *Prawa człowieka. Prawo, instytucje, stosunki międzynarodowe*, Warszawa 2008, s. 66.

[2] J. Braciak, *Prawo do prywatności*, Warszawa 2004, s. 63.

[3] „Artykuł 12 Nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu. <http://www.unic.un.org.pl/prawa_czlowieka/dok_powszechna_deklaracja.php>, dostęp: 26 lutego 2014.

3) porządku publicznego,

4) powszechnego dobrobytu w społeczeństwie demokratycznym.

Nie można również korzystać z praw i wolności wbrew Celom i Zasadom Narodów Zjednoczonych[4].

Międzynarodowy Pakt Praw Obywatelskich i Politycznych

Międzynarodowy Pakt Praw Obywatelskich i Politycznych w art. 17 również gwarantuje każdemu prawo do ochrony prawnej przed bezprawną lub samowolną ingerencją w jego życie prywatne, rodzinne, mir domowy, korespondencję, cześć czy dobre imię[5]. Obejmuje on ochroną także billingi czyli tzw. dane ruchome. Są to informacje np. o chwili rozpoczęcia oraz trwania rozmowy, dacie oraz wybranym numerze telefonu. Dane billingowe pozwalają na identyfikację abonenta, dlatego też podlegają ochronie m.in. na podstawie art. 17 MPPOiP[6]. Z Komentarza ogólnego nr 16 z dnia 8 kwietnia 1988 do art. 17 MPPOiP wynika, że przetwarzanie danych (gromadzenie i przechowywanie) osobowych w komputerach, bankach danych czy za pomocą innych urządzeń zarówno przez władze publiczne, jak i prywatne podmioty musi być regulowane przez prawo. Zatem każda jednostka musi mieć prawo do ustalenia w przystępnej formie, czy i jeśli tak, to jakie dane osobowe (jej dotyczące) są przechowywane w automatycznych bazach danych i do jakich celów[7]. Jednak przyjęta przez

---

[4] Celem Organizacji Narodów Zjednoczonych jest m.in.: utrzymanie międzynarodowego pokoju i bezpieczeństwa, rozwijanie przyjaznych stosunków między narodami, opartych na poszanowaniu zasady równouprawnienia i samoistnienia narodów, współdziałanie międzynarodowe w rozwiązywaniu zagadnień o charakterze gospodarczym, społecznym, kulturalnym lub humanitarnym. Dla osiągnięcia celów Organizacja NZ i jej członkowie zobowiązują się do postępowania według pewnych zasad: zasady suwerennej równości wszystkich członków, wszyscy członkowie wykonywać będą w dobrej wierze zobowiązania przyjęte przez nich zgodnie z niniejszą Kartą, wszyscy członkowie załatwiać będą swe spory międzynarodowe środkami pokojowymi, wszyscy członkowie powstrzymają się w swych stosunkach międzynarodowych od stosowania groźby lub użycia siły (przeciwko całości terytorialnej lub niepodległości któregokolwiek państwa), członkowie Organizacji powstrzymają się od udzielenia pomocy jakiemukolwiek państwu, przeciwko któremu Organizacja zastosowała akcję prewencji lub przymusu. Artykuł 1 i 2 Karty Narodów Zjednoczonych z dnia 26 czerwca 1945, Dz. U. 1947, nr 23, poz. 90.

[5] Międzynarodowy Pakt Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966, Dz. U. 1977, nr 38, poz. 167.

[6] Podlegają też ochronie na podstawie art. 49 Konstytucji RP z dnia 2 kwietnia 1997, Dz. U., nr 78, poz. 483 oraz art. 8 EKPCz z dnia 4 listopada 1950, Dz. U. 1993, nr 61, poz. 284. Więcej: S. Hoc, *Glosa do uchwały SN z dnia 22 stycznia 2003, I KZP 45/02*, „Przegląd Sądowy" 2003, nr 11–12, s. 201–206.

[7] A. Gliszczyńska-Grabias i K. Sękowska-Kozłowska w Komentarzu do art. 17 MPPOiP przywołują orzeczenie *(Ngambi i Nébol przeciwko Francji)* w którym Komitet Praw Człowieka odniósł się do problematyki ochrony informacji (danych osobowych). Skarżący podnosili, że nadanie statusu uchodźcy jednemu z małżonków i równocześnie odmowa udzielenia wizy drugiemu z małżonków poprzedzona badaniem autentyczności zawarcia małżeństwa oraz więzi łączących małżonków,

Komitet Praw Człowieka w 1988 interpretacja art. 17 MPPOiP nie jest wystarczająca w obecnej sytuacji m.in. z powodu, że: Internet stał się pierwszym (zasadniczym) sposobem komunikacji; stosowane są coraz bardziej zaawansowane technologie zbierania i przetwarzania danych; naruszenie prawa do prywatności może skutkować także naruszeniem wolności wypowiedzi czy wolności zrzeszania się a przede wszystkim dlatego, że Komitet Praw Człowieka podjął decyzję o rewizji komentarza ogólnego nr 16 ze względu na coraz większą liczbę wpływających do niego spraw[8].

Państwo, które przyjęło MPPOiP (wraz z Protokołem Fakultatywnym[9]) jest zobowiązane do niepodejmowania jakichkolwiek czynności, które mogłyby naruszyć wyznaczoną w przepisach sferę wolności. Międzynarodowy Pakt Praw Obywatelskich i Politycznych nakłada na państwa dwa rodzaje obowiązków: po pierwsze – obowiązek poszanowania praw człowieka (np. poprzez zakaz ingerencji), a po drugie – obowiązek podjęcia działań zabezpieczających jednostkę przed naruszeniem przysługujących jej praw przez inne osoby lub organizacje. Zakaz bezprawnej ingerencji oznacza, że niedopuszczalna jest jakakolwiek ingerencja z wyjątkiem sytuacji przewidzianych w ustawie. Ustawodawstwo krajowe musi być zgodne z postanowieniami oraz celem i przedmiotem MPPOiP. Zakaz arbitralnej ingerencji odnosi się do działań organów państwowych, podejmowanych na podstawie norm prawnych i gwarantuje, że ingerencja państwa będzie podejmowana w rozsądnych granicach, odpowiednio do okoliczności. W uwagach ogólnych do art. 17 MPPOiP uznaje się, że gromadzenie i przechowywanie danych osobowych musi zostać uregulowane prawem. Państwa zaś powinny podejmować wszelkie skuteczne środki gwarantujące, że informacje dotyczące sfery życia prywatnego nie dostaną się w nieupoważnione ręce i nie zostaną nigdy użyte w celach niezgodnych z MPPOiP. Każda osoba powinna mieć prawo do ustalenia i upewnienia się, w dostępnej dla niej formie, czy i jakie dane osobowe są zgromadzone w skomputeryzowanych kartotekach i w jakich celach. Jeżeli dane te zawierają błędne, nieprecyzyjne informacje albo zostały zebrane (przetworzone) w sposób niezgodny z prawem, każdy powinien mieć prawo do

---

stanowi naruszenie ich prawa do prywatności. Problemem, według Komitetu, może być w tym przypadku zbyt duża liczba gromadzonych i przetwarzanych danych osobowych. A. Gliszczyńska-Grabias, K. Sękowska-Kozłowska, *Komentarz do art. 17 Międzynarodowego paktu praw obywatelskich i politycznych*, [w:] *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych. Komentarz*, pod red. R. Wieruszewskiego, Warszawa 2012, LEX nr 135319.

[8] *Privacy Rights in the Digital Age, A Proposal for a New General Comment on the Right to Privacy under Article 17 on the International Covenant and Political Rights: A Draft Report and General Comment by the American Civil Liberties Union* <https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf>, dostęp: 27 stycznia 2015.

[9] Protokół Fakultatywny do Międzynarodowego Paktu Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966, Dz. U. 1994, nr 23, poz. 80 określa procedury implementacji Paktu.

żądania usunięcia danych lub ich sprostowania. Każdy powinien również wiedzieć, jakie organy państwowe, osoby prywatne (grupy osób) sprawują lub mogą sprawować kontrolę nad jego danymi osobowymi[10].

Kontrolę realizacji postanowień MPPOiP sprawuje Komitet Praw Człowieka[11]. Rozpatruje on sprawozdania przedkładane przez Państwa–Strony. Formułuje uwagi ogólne mające na celu dokonanie wykładni postanowień MPPOiP. Rozpatruje skargi, w których jedno państwo twierdzi, że inne nie wywiązuje się ze swoich zobowiązań (wynikających z postanowień MPPOiP) oraz rozpatruje skargi jednostek, które twierdzą, że zostały naruszone ich prawa przewidziane w Pakcie.

Powszechna Deklaracja UNESCO

Powszechna Deklaracja UNESCO z dnia 11 listopada 1997 w sprawie genomu ludzkiego i praw człowieka[12] gwarantuje w art. 7 poufność danych genetycznych dotyczących osoby podlegającej identyfikacji i przechowywanych lub przetwarzanych

---

[10] Więcej: A. Michalska, *Komitet Praw Człowieka. Kompetencje, funkcjonowanie, orzecznictwo*, Warszawa 1994.

[11] Kompetencje Komitetu Praw Człowieka i zasady jego funkcjonowania uregulowane są w Pakcie, Protokole Fakultatywnym oraz Regulaminie Komitetu. Komitet nie jest organem ONZ, ale jest ściśle związany z Organizacją. Są to związki o charakterze: techniczno-organizacyjnym (Sekretariat Komitetu organizowany jest przez Sekretarza Generalnego ONZ, który zapewnia personel oraz wszelkie ułatwienia techniczno-organizacyjne niezbędne do właściwego funkcjonowania Komitetu, Sekretarz Generalny ONZ zwołuje pierwsze posiedzenie Komitetu, Komitet zbiera się w siedzibie ONZ w Nowym Jorku lub biurze ONZ w Genewie), finansowym (Członkowie Komitetu otrzymują wynagrodzenie z funduszów ONZ) podporządkowującym (chodzi o tryb zgłaszania i uchwalania poprawek do Paktu. Każda poprawka przyjęta przez Komitet jest przedłożona Zgromadzeniu Ogólnemu ONZ do zatwierdzenia).

[12] Najbardziej zaawansowane prace nad wypracowaniem standardów w dziedzinie bioetyki odbywają się w Radzie Europy. Europejska Konwencja o Prawach Człowieka i Biomedycynie z dnia 4 kwietnia 1997, określa podstawowe zasady biomedycyny. W przeciwieństwie do Deklaracji, wywołuje określone skutki prawne (jeśli państwo ją ratyfikuje), a jeśli jest to możliwe, jest stosowana bezpośrednio. Ponadto zakłada stopniowy rozwój przepisów szczegółowych w poszczególnych dziedzinach. Artykuł 10 Konwencji stanowi, że:

„1. Każdy ma prawo do poszanowania jego życia prywatnego w zakresie informacji dotyczących jego zdrowia.

2. Każdy ma prawo zapoznania się z wszelkimi informacjami zebranymi na temat jego zdrowia. Należy jednak respektować życzenia osób, które nie chcą zapoznać się z tymi informacjami. 3. W wyjątkowych przypadkach prawo wewnętrzne może wprowadzić, w interesie osoby zainteresowanej, ograniczenia w wykonywaniu praw określonych w ustępie 2."

Konwencja obowiązuje od dnia 1 grudnia 1999. Do tej pory ratyfikowało ją 29 państw. Polska nie jest jeszcze stroną Konwencji, choć ją podpisała. Tekst Konwencji dostępny na stronie <www.coe.int./t/dg3/healthbioethic/texts_and_documents/ETS164Polish.pdf>, dostęp: 25 lutego 2014. Więcej: M. Safjan, *Rozwój nauk biomedycznych a granice ochrony prawnej*, [w:] *Współczesne problemy bioetyki w obszarze regulacji prawnych. Materiały z konferencji zorganizowanej przez Komisję Nauki i Edukacji Narodowej pod patronatem Marszałek Sejmu prof. dr hab. Alicji Grześkowiak, 3 kwietnia 2001*, Warszawa 2001.

dla celów badawczych lub jakichkolwiek innych. Ograniczenia zasady zgody i poufności muszą zostać przewidziane przez prawo z powodów najwyższej rangi, w zakresie nie naruszającym międzynarodowego prawa publicznego i międzynarodowego prawa dotyczącego praw człowieka[13]. Dane genetyczne obejmują nie tylko informacje o osobie bezpośrednio zainteresowanej lecz o całej linii genetycznej (krewnych bliskiego stopnia). Dostarczają precyzyjnej wiedzy m.in. o pochodzeniu biologicznym, stylu życia, stanie zdrowia, skłonnościach genetycznych. Ujawnienie takich danych może wpłynąć na pozycję jednostki w społeczeństwie, np.: jej karierę, pracę, ubezpieczenie społeczne. Dlatego też konieczne jest wyważenie sfery interesów jednostki, osób trzecich oraz społeczeństwa.

Rezolucja 45/95

Rezolucja 45/95 Zgromadzenia Ogólnego ONZ z dnia 14 grudnia 1990 zawiera wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych, ale nie wyklucza stosowania w odniesieniu do kartotek manualnych. Wytyczne powinny być stosowane zarówno w sektorze publicznym, jak i prywatnym. Postanowienia rezolucji można rozszerzyć na kartoteki zawierające informacje o osobach prawnych. Rezolucja określa zasady: zgodności z prawem i słuszności zbierania danych, akuratności, celowości, dostępu osoby zainteresowanej, niedyskryminacji, bezpieczeństwa oraz transgranicznego przepływu danych. Dopuszcza wprowadzenie wyjątków przewidzianych prawem ze względu na ochronę bezpieczeństwa narodowego, porządku publicznego, zdrowia publicznego i moralności oraz między innymi praw i wolności innych osób. W przypadku danych wrażliwych dodatkowym kryterium wprowadzenia wyjątków jest to, aby mieściły się one w ramach wyjątków określonych w Międzynarodowej Karcie Praw Człowieka[14] . Zobowiązuje państwa do określenia w prawie wewnętrznym organu odpowiedzialnego za kontrolę przestrzegania tych zasad (który potem będzie

---

[13] Powszechna Deklaracja o Genomie Ludzkim i Prawach Człowieka z 11 listopada 1997 w preambule uznaje, że badania nad genomem ludzkim i wynikające z nich zastosowania stwarzają ogromne perspektywy dla polepszenia stanu zdrowia jednostek i ludzkości jako takiej, ale podkreśla jednocześnie, że takie badania powinny w pełni szanować ludzką godność, wolność i prawa człowieka, a także respektować zakaz wszelkiej dyskryminacji opartej na cechach genetycznych <http://libr.sejm.gov.pl/tek01/txt/inne/1997.html>, dostęp: 25 lutego 2014.

[14] Międzynarodowa Karta Praw Człowieka obejmuje Powszechną Deklarację Praw Człowieka, Międzynarodowy Pakt Praw Gospodarczych, Społecznych i Kulturalnych, Międzynarodowy Pakt Praw Obywatelskich i Politycznych, a także Drugi Protokół Fakultatywny do Międzynarodowego Paktu Praw Obywatelskich i Politycznych w sprawie Zniesienia Kary Śmierci. Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ustanowienia instrumentu finansowego na rzecz wspierania demokracji i praw człowieka na świecie (Europejski instrument na rzecz demokracji i praw człowieka) <http://bip.ms.gov.pl/pl/prawa-czlowieka/onz-i-prawa-czlowieka/wspolpraca-w-ramach-systemu-onz/>, dostęp: 26 lutego 2014 oraz M. A. Glendon, *Knowing the Universal Declaration of Human Rights*, 73 „Notre Dame Law Review" 1153 (1998).

zdawał sprawozdanie z ich przestrzegania) oraz określenie sankcji za naruszenie przepisów. Zaznacza, że transgraniczne przekazywanie danych jest dozwolone tylko wtedy, gdy kraje tym zainteresowane przewidują porównywalne gwarancje ochrony prywatności. Jeżeli gwarancji wzajemnych brakuje, państwa mogą nałożyć ograniczenia, ale tylko w takim stopniu, w jakim wymaga tego ochrona prawa do prywatności. Ponadto rezolucja wspomina o kartotekach danych osobowych prowadzonych przez rządowe organizacje międzynarodowe, do których również powinno się stosować powyższe zasady. Odstępstwo od nich możliwe jest wówczas, gdy celem kartoteki jest ochrona praw człowieka i podstawowych wolności bądź świadczenie pomocy humanitarnej[15].

Rezolucja 34/169

Rezolucja 34/169 Zgromadzenia Ogólnego ONZ z dnia 17 grudnia 1979 zaleca w art. 4, aby funkcjonariusz publiczny[16] korzystał z poufnych informacji z zachowaniem dyskrecji, chyba że ściśle określone zadania lub dobro wymiaru sprawiedliwości pozwalają mu postąpić inaczej. Wszelkie wyjawianie tych danych do innych celów jest absolutnie naganne (niewłaściwe)[17]. Może to szkodzić interesom (a zwłaszcza reputacji) tych osób. Funkcjonariusze publiczni powinni więc wykazać możliwie największą troskę w związku z przechowywaniem i wykorzystywaniem danych osobowych.

---

[15] Guidelines for the Regulation of Computerized Personal Data Files adopted by General Assembly resolution 45/95 of 14 December 1990 <http://www.un.org/documents/ga/res/45/a45r095.htm>, dostęp: 26 lutego 2014.

[16] Tadeusz Jasudowicz tłumaczy rezolucję jako Kodeks Postępowania (ONZ) Funkcjonariuszy Porządku Prawnego, i używa pojęcia „funkcjonariusz porządku prawnego". Pojęciem tym obejmuje wszystkich przedstawicieli porządku prawnego, którzy wypełniają kompetencje policyjne, a w państwach, w których kompetencje policyjne wypełniane są przez władze wojskowe – również na funkcjonariuszy takich służb.

Więcej: *Ochrona danych. Standardy europejskie.Zbiór materiałów*, pod red. T. Jasudowicza, Toruń 1998.

[17] „Article 4 Matters of a confidential nature in the possession of law enforcement officials shall be kept confidential, unless the performance of duty or the needs of justice strictly require otherwise. Commentary: By the nature of their duties, law enforcement officials obtain information which may relate to private lives or be potentially harmful to the interests, and especially the reputation, of others. Great care should be exercised in safeguarding and using such information, which should be disclosed only in the performance of duty or to serve the needs of justice. Any disclosure of such information for other purposes is wholly improper."

<http://www.un.org/documents/ga/res/34/a34res169.pdf>, dostęp: 26 lutego 2014.

OECD

Rekomendacja OECD z dnia 23 września 1980 w sprawie wytycznych dotyczących ochrony prywatności i przepływu danych osobowych przez granice z samej swej istoty nie jest wiążąca dla krajów członkowskich. Wytyczne określają dane osobowe jako wszelkie informacje o określonych lub dających się zidentyfikować osobach fizycznych. Krajom podpisującym pozostawiono swobodę rozszerzenia kręgu podmiotów objętych ochroną na grupy osób i organizacje. W rekomendacji wprowadzono zasadę, że przedmiot regulacji stanowić mają wszelkie, występujące w sektorze publicznym i prywatnym, przypadki przetwarzania danych, które ze względu na swój charakter, naturę lub ze względu na wzajemne powiązania mogą ingerować w sferę prywatności jednostki i jej podstawowe wolności.

Wytyczne dotyczące przetwarzania danych wprowadzają:

1) zasadę ograniczenia zbierania danych (*collection limitation principle*) – z zastrzeżeniem uzyskiwania ich w sposób zgodny z prawem i dobrymi obyczajami za wiedzą lub zgodą osób (w zależności od możliwości), których dane dotyczą;

2) zasadę jakości danych (*data quality principle*) – która nakazuje sprawdzać w jakim zakresie, ze względu na cel, któremu służyć ma zbiór, określone dane są konieczne i istotne, a także prawidłowe oraz autentyczne i kompletne;

3) zasadę określenia celu przetwarzania danych (*purpose specification principle*) – cel powinien być określony i ujawniony najpóźniej w momencie zbierania danych;

4) zasadę ograniczonego przetwarzania danych (*use limitation principle*), chyba że zostanie uzyskana zgoda zainteresowanych lub wynikać to będzie z upoważnienia ustawowego;

5) zasadę wprowadzenia odpowiednich zabezpieczeń (*security safeguards principle*), która ma chronić dane osobowe przed ryzykiem utraty, nieuprawnionym dostępem, zniszczeniem, eksploatacją, zamianą lub odtworzeniem;

6) zasadę jawności (*openness principle*) – ułatwiającą skuteczne realizowanie roszczeń osób, których dane dotyczą (poprzez ustalenie faktu zbierania i gromadzenia danych, celu i charakteru ich eksploatacji oraz ustalenia podmiotu odpowiedzialnego za przetwarzanie danych);

7) zasadę indywidualnego uczestnictwa (*individual participation principle*) – która zapewnia każdemu prawo do otrzymywania w rozsądnym terminie, w odpowiedni sposób, w odpowiedniej formie i bez nadmiernych kosztów, informacji o dotyczących go danych, oraz prawo do korygowania ich oraz żądania ich usunięcia;

8) zasadę odpowiedzialności (*accountability principle*) podmiotu przetwarzającego dane za przestrzeganie powyższych zasad.

Rozdział trzeci poświęcony został zasadom swobodnego przepływu danych osobowych między państwami. Państwa członkowskie OECD zostały zobowiązane do wzięcia pod uwagę skutków, jakie może wywołać przetwarzanie danych osobowych w jednym kraju i ich reeksport do innych krajów. Celem tych postanowień jest ochrona znajdujących się w obrocie międzynarodowym danych przed nieupoważnionym dostępem czy zniszczeniem. W związku z tym wszelkie przedsięwzięcia powinny być zgodne z systemem łączności i międzynarodowymi umowami w tym zakresie oraz gwarantować szybką wymianę i ochronę tajemnicy korespondencji (państwo eksportujące dane i państwo uzyskujące dane muszą gwarantować równoważną ochronę). Państwa mogą wprowadzić restrykcje odnośnie przypływu danych osobowych przez granice z trzech powodów:

1) gdy eksport danych zmierza do obejścia ustawodawstwa, czyli rozpowszechniania danych w kraju, który nie uznaje wytycznych OECD;

2) gdy w wyniku przekazania informacji do innego państwa udaremniony zostaje cel, jaki ma spełniać ustawodawstwo krajowe o ochronie danych osobowych;

3) gdy jest to związane z pewnymi kategoriami danych (danymi „wrażliwymi").

Żaden kraj nie powinien, powołując się na dopuszczalne restrykcje, ograniczać eksportu danych do innego kraju lub uzależniać ich przekazania od specjalnej zgody, jeśli zamierza osiągnąć inne faktyczne cele, których nie ujawnia. Z drugiej strony państwa członkowskie OECD mają pełną swobodę w zakresie regulowania wolnego handlu, ceł, zatrudnienia i warunków gospodarczych międzynarodowego obrotu danymi (traktowanymi jako towar).

Wzajemna pomoc i współpraca określona jest w rozdziale piątym. Zaleca on krajom członkowskim wzajemne informowanie się o realizacji wytycznych oraz wprowadzenie postępowania umożliwiającego wymianę doświadczeń i wzajemną pomoc. Ponadto państwa powinny harmonizować (ujednolicać) przepisy regulujące kwestię kontroli eksportu i importu danych oraz określić reguły kolizyjne stosowane w przypadku konfliktu przepisów[18].

[18] <www.oecd.org/sti/ieconomy/oecdquidelinesontheprotectionofprivacyandtrancborderflowsofpersnoldata.htm>, dostęp: 30 marca 2015.

Rozdział 2. Ochrona danych osobowych w europejskim systemie ochrony praw człowieka

System Rady Europy

Europejska konwencja o ochronie praw człowieka i podstawowych wolności

Celem EKPC jest jak najskuteczniejsza ochrona praw i wolności jednostki[1]. Europejska Konwencja Praw Człowieka gwarantuje każdemu ochronę praw bez względu na płeć, rasę, kolor skóry, religię, poglądy polityczne lub inne poglądy, pochodzenie narodowe lub socjalne, przynależność do mniejszości narodowej, majątek czy urodzenie. Katalog chronionych praw ulega rozszerzaniu w drodze przyjmowania kolejnych protokołów.

W art. 8 EKPC znajduje się prawo do poszanowania życia prywatnego i rodzinnego, mieszkania oraz tajemnicy korespondencji[2]. Europejska Konwencja Praw Człowieka dopuszcza pod pewnymi warunkami ograniczenie tych praw, jeśli będzie to wynikało z przepisów wewnętrznych. Jakakolwiek ingerencja przez władze publiczne w wykonywanie tych praw jest dopuszczalna tylko wtedy, gdy:

1) następuje na podstawie ustawowego upoważnienia
2) służy zapewnieniu w demokratycznym społeczeństwie:
   a) bezpieczeństwa narodowego,
   b) porządku i spokoju publicznego,
   c) gospodarczego dobra kraju,
   d) obrony ładu (przeciwdziałaniu czynom karalnym),
   e) ochrony zdrowia i moralności,
   f) ochrony praw i wolności innych osób.

---

[1] Państwa nowo przyjmowane do Rady Europy są zobowiązane do podpisanie EKPC z chwilą przyznania członkostwa RE oraz do jej ratyfikacji w ciągu roku od tego momentu. Orzeczenie Europejskiego Trybunału Praw Człowieka jest wiążące dla państwa, do którego jest skierowane (wiąże organy krajowe). Konsekwencją orzeczenia ETPC może być obowiązek wypłaty skarżącemu zadośćuczynienia, jak również konieczność dokonania zmian w prawie wewnętrznym. Więcej: A. Bisztyga, *Ochrona praw człowieka w systemie Rady Europy*, [w:] *System ochrony praw człowieka*, B. Banaszak, A. Bisztyga, K. Complak, M. Jabłoński, R. Wieruszewski, K. Wójtowicz, Kraków 2005, s. 127–130.

[2] Artykuł 8 EKPC otwiera grupę czterech praw formułujących klasyczne prawa i wolności jednostki: poszanowanie życia prywatnego, rodzinnego i korespondencji; wolność myśli sumienia i wyznania (art. 9); wolność wyrażania opinii (art. 10) i wolność zgromadzania się i zrzeszania (art. 11).

Z przywołanego przepisu nie wynika wprost, że ochronie podlegają dane osobowe. Wynika to, jednak z interpretacji pojęć „życie prywatne" i „życie rodzinne". Orzecznictwo na podstawie art. 8 też nie wskazuje na jednolite stanowisko w sprawie wykładni „życia prywatnego" w odniesieniu do gromadzenia (przetwarzania, zmieniania, usuwania i przekazywania) danych osobowych[3]. Przyjęcie szerokiego zakresu pojęcia „życie prywatne" jest słusznym zabiegiem prawodawcy, gdyż pozwala na rozwój „precedensów orzeczniczych" i ewolucję tego pojęcia. Zatem na pojęcie „życia prywatnego" składają się: swoboda (autonomia) jednostki pozostawania poza ingerencją władzy publicznej, integralność fizyczna i psychiczna jednostki (w tym reputacja, dobre imię, honor), ale także ochrona związana z gromadzeniem i udostępnianiem danych osobowych. Leszek Garlicki uważa, orzecznictwo strasburskie od dawna zajmuje się kwestiami gromadzenia i udostępniania danych osobowych. Przeszło jednak ewolucję od tolerowania uznaniowego podejścia urzędów w kwestii gromadzenia danych osobowych do wymagania od państwa, by przyjęły bardzo szczegółowe regulacje w tym zakresie i ograniczyły ingerencje w prywatność do rzeczywiście koniecznych sytuacji (np. sprawa Amman przeciwko Szwajcarii, wyrok z dnia 16 lutego 2000 oraz sprawa Rotaru przeciwko Rumunii, wyrok z dnia 4 maja 2000). Trybunał Konstytucyjny wielokrotnie w swoich orzeczeniach podkreślał, iż dostrzega „istnienie systemu niejawnego gromadzenia informacji służących ochronie bezpieczeństwa państwa, który to może stwarzać ryzyko podważenia (lub nawet zniszczenia) demokracji w imię jej ochrony" (Klass 49, Leander 60).

Problem ochrony danych osobowych w orzecznictwie Europejskiego Trybunału Praw Człowieka

Jedno z pierwszych orzeczeń związanych z ochroną danych osobowych zapadło w sprawie X przeciwko RFN. Europejska Komisja Praw Człowieka w 1973 stwierdziła, że zbieranie i przechowywanie informacji przez policję nie jest sprzeczne z art. 8 EKPC, nawet jeśli osoba, której dane dotyczą, nie była wcześniej notowana. Istotną okolicznością w sprawie był fakt, że dane te były udostępniane osobom trzecim.

---

[3] W nauce podejmowano wiele prób zdefiniowania prywatności i życia prywatnego. Dr S. Mahkonem oparł swoją definicję na przeciwieństwach: samostanowienie i wspólnota, rozgłos i nieujawnianie, izolacja i towarzyskość oraz nietykalność i dostępność. Prywatność jest więc prawem do: wpływu i decydowania o wykorzystaniu danych osobowych, organizowania życia prywatnego bez zbędnej ingerencji z zewnątrz, podlegania ocenie na podstawie właściwych i dokładnych danych, oczekiwania wystarczającego poziomu bezpieczeństwa danych. Więcej: R. Aarnio L. L. M, *Ochrona danych w życiu zawodowym (Data Protection in working life)*, [w:] *Ochrona danych osobowych wczoraj, dziś, jutro. Personal data protection yesterday, today, tomorrow*, Warszawa 2006, s. 27–39 (16–27).

Interesująca jest też ze względu na konflikt między prawem do ochrony danych osobowych obywatela, a prawem państwa do ochrony własnych istotnych interesów, sprawa Leander przeciwko Szwecji. Torsten Leander domagał się dostępu do informacji zebranych na jego temat (oraz możliwości ustosunkowania się do nich), jako że stanowiły one podstawę odmowy zatrudnienia. W sierpniu 1979 Leander starał się o zatrudnienie w Muzeum Morskim w Karlskronie. Ze względu na sąsiedztwo z bazą morską, fakt ten musiał być poprzedzony kontrolą bezpieczeństwa. Po zapoznaniu się z informacjami przechowywanymi w tajnym policyjnym rejestrze, nie zgodzono się na jego zatrudnienie, nie dano również Leanderowi możliwości zapoznania się z tajnymi informacjami i tym samym ich skomentowania. Domagał się więc oświadczenia, że spełnia warunki by być zatrudnionym, z czym władze się nie zgodziły. W skardze do Europejskiej Komisji Praw Człowieka Leander zarzucił szwedzkim władzom naruszenie art. 6, 8, 10, 13 EKPC. Trybunał Konstytucyjny zajął się w pierwszej kolejności zarzutem z art. 8 i stwierdził, iż przechowywanie, jak i udostępnianie informacji, wraz z odmową zezwolenia Leanderowi na ich sprostowanie, jest ingerencją w prawo do poszanowania życia prywatnego. Trybunał Konstytucyjny zwrócił uwagę, iż cel kontroli kadrowej (szwedzkiego systemu) był uprawniony. Musiał więc ocenić, czy ingerencja była przewidziana przez ustawę i konieczna w demokratycznym społeczeństwie. Po analizie TK stwierdził, że prawo szwedzkie spełnia wymóg przewidywalności. Co do warunku konieczności TK uznał, że Szwecja ma szeroki zakres swobody, nie ma również wątpliwości co do potrzeby ustalania, czy określone osoby mogą być zatrudniane na stanowiskach ważnych ze względu na bezpieczeństwo państwa. Z drugiej strony TK zauważył, że istnieją odpowiednie i skuteczne gwarancje przeciwko nadużyciom ze strony państwa i orzekł, że nie naruszono art. 8 EKPC[4]. Odnośnie zarzutu do art. 10 uznano, że rządy państw nie mogą wprowadzać ograniczeń w otrzymywaniu informacji od osób trzecich, jeśli te chcą ich udzielić. Artykuł 10 nie gwarantuje osobie prawa dostępu do rejestru zawierającego o niej informacje[5].

---

[4] Więcej: M. A. Nowicki, *Europejski Trybunał Praw Człowieka. Orzecznictwo*, tom 2, Kraków 2002, s. 625–627.

[5] Z art. 10 wynika zaś prawo do wolności wypowiedzi, na którą składają się: wolność poglądów, otrzymywania informacji bez cenzury i bez względu na granice państwowe. Jednak korzystanie z tych praw też może podlegać ograniczeniom i sankcjom. Ograniczenia muszą wynikać z prawa i być niezbędne w demokratycznym społeczeństwie ze względu na: bezpieczeństwo narodowe, integralność terytorialną, bezpieczeństwo publiczne, zapobieganie zamieszkom, zagwarantowanie bezstronności sądownictwa, ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz zapobieganie ujawnianiu informacji poufnych.

[6] Trybunał położył nacisk na: 1) przewidywalność, czyli dostateczną jasność ustawy pozwalającej władzom na zbieranie danych osobowych obywateli, prawowitość celu ale przede wszystkim gwarancje ochrony przed arbitralnym działaniem; 2) w odniesieniu do gromadzenia danych przez służby ustawa powinna określać rodzaje gromadzonych danych, kategorie osób tym objętych, procedury, które muszą być przy tym przestrzegane, wskazanie osób uprawnionych do dostępu do

O ile jeszcze w tej sprawie TK uznał za wystarczająco spełniony wymóg „dostępności" i „przewidywalności" prawa krajowego (na podstawie którego zbierane były dane), to później wypracował już bardziej rozbudowany wzorzec kontroli[6].

Kontrowersyjna i głośna była sprawa Z. przeciwko Finlandii. Sąd miejski w Helsinkach skazał męża Z., pana X. za gwałt na O. X. został poinformowany o tym, że jest nosicielem wirusa HIV. Policja wszczęła przeciwko niemu śledztwo o usiłowanie zabójstwa (uznała bowiem, że świadomie naraził O. na ryzyko zakażenia wirusem HIV). Policja próbowała przesłuchać panią Z., żonę X. Skorzystała ona jednak z prawa odmowy zeznań. Pan X. konsekwentnie odmawiał odpowiedzi, czy jego żona jest nosicielką wirusa HIV. Doktor L., naczelny lekarz szpitala, w którym małżonkowie się leczyli, ujawnił informacje dotyczące stanu zdrowia pani Z. Doktor D. potwierdził, że Z. jest zakażona. Z. przyznała się, że jest nosicielką wirusa i oświadczyła, że nie została zakażona przez męża. W efekcie X. został skazany za usiłowanie zabójstwa i gwałt. Sąd podał do publicznej wiadomości sentencję wyroku i skróconą wersję uzasadnienia. Pełne uzasadnienie oraz całość akt miały pozostać w tajemnicy przez 10 lat. Sąd apelacyjny zaostrzył karę do 11 lat, zaś w uzasadnieniu wymienił panią Z. jako zakażoną wirusem HIV. Utrzymał w mocy postanowienie o przechowywaniu akt w tajemnicy przez 10 lat. W skardze do Europejskiej Komisji Praw Człowieka pani Z. zarzuciła naruszenie art. 8 EKPC ze względu na: zakaz składania zeznań przez lekarzy oraz ujawnienie informacji na ich temat w postępowaniu karnym przeciwko mężowi, przejęcia dokumentacji lekarskiej i włączenie jej do śledztwa, decyzje sądów o ograniczeniu utrzymania w tajemnicy akt do dziesięciu lat, ujawnienie jej tożsamości i danych medycznych w wyroku apelacyjnym.

Niewątpliwie działania władz były ingerencją w prawo do poszanowania życia prywatnego i rodzinnego. Trybunał Konstytucyjny nie dopatrzył się jednak braku zgodności tych działań z prawem krajowym. Konsekwencje przepisów, zdaniem TK, były w wystarczającym stopniu przewidywalne. Ochrona danych osobowych, nie tylko medycznych, ma fundamentalne znaczenie dla poszanowania prywatności. Służy m.in. zachowaniu zaufania do lekarzy (i służby zdrowia). Szczególne znaczenie ma to dla osób zakażonych wirusem HIV. Ujawnienie takiej informacji może im wyrządzić szkodę nieproporcjonalnie większą do celu, jaki chce się osiągnąć[7] .

---

zebranych informacji a przede wszystkim określenie czasu przechowywania informacji. 3) gwarancje przeciwko nadużyciom czyli stworzenie systemu adekwatnych i skutecznych zabezpieczeń regulujących przetwarzanie danych osobowych. Zob. więcej: L. Garlicki, *Komentarz do art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*, [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom 1. Komentarz do artykułów 1–18*, pod red. L. Garlickiego, Warszawa 2010, s. 479–550.

[7] Marek Antoni Nowicki zauważa, że „od przepisów i paragrafów nie mniej ważna jest kultura bycia i zwyczajna ludzka wrażliwość na prywatność drugiej osoby. [...] w tym właśnie tkwi sedno problemu. Wtedy nawet najlepsze prawo okazuje się bezsilne." M. A. Nowicki, *Interes pacjenta kontra interes śledztwa*, „Prawo i Życie" 2000, nr 6, s. 40–41.

Trybunał Konstytucyjny zgodził się z poglądem, że interes pacjenta i ochrona tajemnicy medycznej muszą ustąpić przed interesem śledztwa, ścigania przestępstw oraz jawności postępowania sądowego (jeśli wykaże się, że jawność postępowania sądowego jest ważniejsza). W tym przypadku Policja uzyskała zgodę sądu na przesłuchanie lekarzy. Akta zostały objęte tajemnicą. Ingerencja w życie prywatne i rodzinne była więc ograniczona. Zachowano proporcję między celem a środkami. Przejęcie dokumentacji lekarskiej do śledztwa służyło tylko uzupełnieniu zeznań lekarzy i również tym działaniem nie naruszono art. 8 EKPC. Odnośnie zarzutu, że dane medyczne będą ogólnie dostępne po dziesięciu latach, TK uznał, że ujawnienie informacji o zakażeniu wirusem HIV bez zgody pani Z. byłoby dalszą ingerencją w życie prywatne i rodzinne i nie ma dalszego uzasadnienia. W razie wykonania postanowienia w 2002 doszłoby do nieproporcjonalnej ingerencji. Również w przypadku ujawnienia danych osobowych pani Z. w wyroku sądu apelacyjnego TK uznał, że publikacja nie miała żadnego poważnego uzasadnienia i nastąpiło naruszenie art. 8 EKPC. Zgodnie z prawem sąd fiński (apelacyjny) mógł nie umieszczać w wyroku danych pozwalających zidentyfikować Z. Wystarczyłaby publikacja skróconej wersji, treść sentencji i wskazanie przepisów, które stanowiły jego podstawę (tak jak to uczynił sąd miejski).

Finlandia miała zapłacić pani Z. 100 tysięcy marek fińskich tytułem zadośćuczynienia za szkody moralne, oraz 160 tysięcy marek tytułem zwrotu kosztów i wydatków[8].

Duży rozgłos zyskała także sprawa Gaskin przeciwko Wielkiej Brytanii. Dotyczyła obowiązku państwa udostępnienia osobie zainteresowanej zbioru danych na jej temat. Gaskin po śmierci matki przebywał z małymi przerwami w kilku rodzinach zastępczych aż do osiągnięcia pełnoletniości (w 1977). Prawo Wielkiej Brytanii zobowiązywało władze lokalne do prowadzenia poufnych akt dotyczących każdego dziecka pozostającego pod ich opieką. Po osiągnięciu pełnoletności Gaskin chciał poznać swoją przeszłość. Urzędnik Rady Miejskiej w Liverpoolu pozwolił mu zajrzeć do akt, a Gaskin samowolnie wyniósł je do domu na trzy dni. W związku z tym następnym razem odmówiono mu wglądu do akt. Wobec tego wystąpił do sądu o nakazanie organom administracji ujawnienia mu całości akt[9]. Sąd uznał, że interes indywidualny Gaskina musi w tym wypadku podporządkować się interesowi publicznemu i pozew oddalił. Sąd apelacyjny utrzymał wyrok w mocy, a Izba Lordów nie przyjęła sprawy do rozpatrzenia.

---

[8] M. A. Nowicki, *Europejski Trybunał Praw Człowieka. Orzecznictwo*, tom 2, Kraków 2002, s. 672–677.

[9] Akta zawierały zapisy lekarzy, nauczycieli, policjantów, rodziców zastępczych, którzy udzielali informacji pod rygorem ścisłej poufności.

Niedługo potem Rada Miejska Liverpoolu powołała komisję ds. akt opieki nad dziećmi. Zdecydowano, że informacje sprzed 1 marca 1983, mogą być udostępnione wyłącznie za zgodą osób, które je dostarczyły. Departament Zdrowia i Ubezpieczeń Społecznych wydał okólnik, który nakazywał dostęp do akt. Można było odmówić tylko z powodu ochrony: osoby trzeciej (która przekazała poufne informacje), źródeł informacji oraz poufnych ocen pracowników socjalnych.

W skardze do Europejskiej Komisji Praw Człowieka Gaskin zarzucił, że odmowa dostępu do całości dotyczących go akt narusza prawo do poszanowania życia prywatnego i rodzinnego (art. 8 EKPC) oraz prawo dostępu do informacji (art.10). Komisja uznała (głos decydujący przy remisie miał przewodniczący), że pogwałcono art. 8 z powodu procedury i decyzji, których rezultatem była odmowa dostępu do akt. Nie doszło do naruszenia art. 10 EKPC.

Europejska Komisja Praw Człowieka zwróciła uwagę, że poszanowanie życia prywatnego wymaga, aby każdy mógł ustalić szczegóły swojej tożsamości, i władze nie mogą bez wyraźnego usprawiedliwienia ograniczać dostępu do tak podstawowych informacji. Powołała się na orzeczenie w sprawie Leander przeciwko Szwecji.

Zdaniem TK odmówienie Gaskinowi dostępu do całości akt nie mogło być traktowane jako ingerencja w jego życie prywatne i rodzinne. Trybunał Konstytucyjny uważał, że poufność akt pomagała w skutecznym działaniu systemu opieki nad dziećmi i służyła ochronie praw współpracowników służb specjalnych oraz dzieci potrzebujących opieki. Z jednej strony, osoby znajdujące się w takiej sytuacji jak Gaskin mają żywotny interes w otrzymaniu informacji o swoim dzieciństwie. Z drugiej strony poufność akt publicznych jest ważna ze względu na potrzebę posiadania obiektywnych informacji i ochronę osób trzecich. Trybunał uznał, że interesy osoby, która domaga się dostępu do akt dotyczących jej życia prywatnego i rodzinnego muszą być zagwarantowane także wtedy, gdy współpracownik służb socjalnych, który złożył oświadczenie, nie jest osiągalny lub bezpodstawnie odmówił zgody. Ostatecznie o wyrażeniu zgody w takich przypadkach orzeka niezależny organ. Gaskin nie miał możliwości skorzystania z takiej procedury, a ówcześnie istniejąca nie gwarantowała poszanowania jego życia prywatnego i rodzinnego. Wielka Brytania naruszyła więc art. 8 EKPC. Trybunał Konstytucyjny nie stwierdził naruszenia art. 10, ponieważ tenże artykuł nie obejmuje zobowiązania państwa do przekazania informacji.

Wielka Brytania zobowiązana została zapłacić Gaskinowi pięć tysięcy funtów jako zadośćuczynienie za krzywdę moralną i jedenaście tysięcy funtów jako zwrot kosztów i wydatków[10] .

---

[10] M. A. Nowicki, *Europejski Trybunał Praw Człowieka. Orzecznictwo*, tom 2, Kraków 2002, s. 639–641.

Problem ochrony danych osobowych w orzecznictwie sądów polskich

Na gruncie polskiego orzecznictwa do art. 8 EKPC można zauważyć, że sfera życia prywatnego (w tym intymnego) nie jest chroniona w sposób absolutny. Sąd Apelacyjny w Krakowie rozpatrywał sprawę z powództwa Primae przeciwko Secundam o wydanie i zapłatę. Powódka domagała się od pozwanej wydania (oddania) jej intymnych zdjęć i zasądzenia pewnej kwoty pieniędzy na rzecz Towarzystwa Przyjaciół Dzieci w Krakowie. Wskazywała, że pozwana weszła nielegalnie w posiadanie jej zdjęć, a potem pokazywała je robotnikom podczas remontu mieszkania, udostępniła żonie konkubenta powódki i chciała postawić ją (powódkę) w złym świetle oraz narazić na wstyd i straty moralne. Pozwana twierdziła, że zdjęcia powódki znalazła przypadkowo podczas remontu mieszkania, z którego wcześniej wyprowadziła się powódka. Zdjęcia pokazała tylko najbliższym i tylko i wyłącznie dla ochrony uzasadnionego interesu społecznego (dobra dziecka powódki).

Sąd I instancji zasądził od pozwanej na rzecz Towarzystwa Przyjaciół Dzieci w Krakowie 2500 zł, a w pozostałym zakresie powództwo oddalił.

Pozwana postanowiła wykorzystać zdjęcia powódki w postępowaniu o ograniczenie władzy rodzicielskiej i udostępniła je: prokuratorowi, kuratorowi sądowemu dla nieletnich, adwokatowi (który reprezentował pozwaną) oraz żonie konkubenta powódki (swojej córki). Sąd okręgowy uznał, że pozwana dopuściła się naruszenia praw osobistych powódki poprzez naruszenie jej gwarancji poszanowania życia intymnego i dobrego imienia, zwłaszcza iż ujawnienie zdjęć powódki żonie konkubenta miało na celu ośmieszenie powódki i dostarczenie żonie jej konkubenta dowodów w sprawie rozwodowej. Odnośnie ujawnienia zdjęć prokuratorowi, kuratorowi i pełnomocnikowi pozwanej sąd uznał, w jednym miejscu, że takie zachowanie pozwanej nie nosi znamion bezprawności (które jest konieczne dla uznania, że doszło do naruszenia dóbr osobistych). W innym natomiast uzasadniał, że zdjęcia te nie były przedmiotem postępowania dowodowego w sprawie opiekuńczej i te okazania były rozpowszechnieniem tajemnicy życia intymnego powódki.

Sąd apelacyjny orzekł, iż nie jest zasadna ocena okazania spornych zdjęć prokuratorowi, kuratorowi i adwokatowi jako działania bezprawnego. Zarówno z treści art. 47 Konstytucji (i art. 24 k.c.) oraz art. 8 EKPC wynika, że sfera życia prywatnego (a w tym intymnego) nie jest chroniona w sposób absolutny. W pewnych okolicznościach można skutecznie uchylić się od zarzutu naruszenia sfery czyjegoś życia prywatnego. Zwłaszcza, gdy ujawnienie faktów ze sfery życia prywatnego następuje w związku z dochodzeniem lub obroną własnych praw. Z drugiej strony należy pamiętać, że nawet niepubliczne udostępnianie erotycznych zdjęć narusza sferę życia intymnego. W tym przypadku nie można, jednak pozwanej przypisać bezprawnego działania, gdyż działała ona w ramach

porządku prawnego. Ujawnienie zdjęć powódki miało służyć jako dowód wskazujący na nienależyte wykonywanie władzy rodzicielskiej.

Sąd apelacyjny uznał, że nie są zasadne – podniesione w apelacji – zarzuty co do oceny bezprawności pokazania żonie konkubenta powódki zdjęć erotycznych przedstawiających intymne relacje między powódką a konkubentem. Pozwana powoływała się na prawo żony konkubenta do wiedzy o jego kontaktach seksualnych, bo małżeństwo polega na dzieleniu się ze sobą szczegółami życia, zarówno przykrymi, jak i przyjemnymi. Niezależnie od kontrowersyjności takiego twierdzenia bezsporny jest fakt, iż zdjęcia dotyczą w równym stopniu życia intymnego powódki, jak i konkubenta, a interesy żony konkubenta nie mogą usprawiedliwiać ingerencji osoby trzeciej (pozwanej) w życie intymne powódki[11].

W sprawie Niedbała przeciwko Polsce TK orzekł, iż doszło do naruszenia prawa do korespondencji poprzez kontrolowanie i opóźnienie doręczenia listów do Rzecznika Praw Obywatelskich. Skarżący, Maciej Niedbała został aresztowany (2 września 1994) w związku z podejrzeniem popełnienia przestępstwa kradzieży samochodu. Sąd skazał go jednak za paserstwo i uchylił areszt (20 marca 1995), jednak wkrótce (21 kwietnia 1995) aresztowano go ponownie za usiłowanie kradzieży samochodu. Sąd Apelacyjny w Katowicach zmienił wyrok sądu pierwszej instancji i skazał Niedbałę za pomoc w sprzedaży skradzionych przedmiotów. Niedbała, w skardze zarzucił, m.in. naruszenie art. 5 ust. 3 (aresztowanie na podstawie postanowienia prokuratora), art. 5 ust. 4 (postępowanie dotyczące kontroli sądowej podstaw aresztowania nie było kontradyktoryjne) oraz art. 8 (kontrola i opóźnienie doręczania listów do RPO). W związku z zarzutem na podstawie art. 8 TK orzekł, że doszło do ingerencji w prawo skarżącego do poszanowania korespondencji, gdyż prawo krajowe musi wskazywać wyraźnie zakres i sposób korzystania przez władze publiczne z prawa do ingerencji, zaś przepisy prawa polskiego obowiązującego w tamtym czasie zezwalały na automatyczną kontrolę korespondencji więźniów przez ograny prowadzące postępowanie karne. Z przepisów tych nie wynikały żadne zasady regulujące sprawowanie takiej kontroli, nie określały też sposobu i terminów, w których można było jej dokonać. Wynika z tego, że kwestionowana kontrola korespondencji więźniów nie była przewidziana przez prawo. Chodziło bowiem o cenzurę przez prokuratora, a wtedy skarżący nie mógł się odwołać do prezesa jakiegokolwiek sądu. W związku z powyższym nastąpiło naruszenie art. 8 i nie było już konieczne badanie innych przesłanek określonych w art. 8 ust. 2 EKPC. Orzeczenie zapadło jednogłośnie w każdym punkcie, a Polska została zobowiązana do zapłaty skarżącemu 2 tys. zł zadośćuczynienia za krzywdę moralną oraz 10 800 zł (pomniejszone o pomoc prawną Rady Europy) jako zwrot kosztów i wydatków[12].

---

[11] Wyrok SA w Krakowie z dnia 11 kwietnia 2001, I ACa 244/01, LEX nr 82416.

[12] M. A. Nowicki, *Europejski Trybunał Praw Człowieka. Orzecznictwo*, tom 2, Kraków 2002, s. 132–135.

Konwencja nr 108 Rady Europy

Konwencja 108 Rady Europy z dnia 28 stycznia 1981 dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych[13], ma wzmocnić prawną ochronę jednostek do poszanowania prywatności w związku z automatycznym przetwarzaniem danych. Konieczność ochrony została wymuszona poprzez rosnące wykorzystanie informatyki do zarządzania danymi. Problem ochrony danych czy ogólniej informacji nie pojawił się wraz ze stworzeniem pierwszego komputera. Przed wynalezieniem pisma ochrona informacji sprowadzała się do dyskrecji osób, którym te informacje powierzono. Wprowadzenie pisma stworzyło nowe problemy. W pierwszych latach informatyki, w maszynie cyfrowej działał na raz tylko jeden program. Po zakończeniu działania operator maszyny (użytkownik) naciskał klawisz „czyść pamięć" i wprowadzał do maszyny nowy program. Dane dzieliło się na zwykłe i poufne. Przy przetwarzaniu danych poufnych stosowano np.: zasłanianie okna ośrodka obliczeniowego, czy zasłaniano drukarkę drukującą wyniki, tak aby nikt ich nie przeczytał[14].

Konwencja 108 Rady Europy jest aktem bezpośrednio wiążącym Państwa––Strony. Nie uniknięto jednak różnorodnego traktowania danych osobowych. Ustawodawstwo krajowe poszczególnych państw okazało się na tyle zróżnicowane, że wymagało wypracowania i przyjęcia Dyrektywy.

Celem Konwencji jest zapewnienie na obszarze państw członkowskich każdemu, niezależnie od obywatelstwa i zamieszkania, ochrony jego praw i wolności, a w szczególności prawa do prywatności w związku z automatycznym przetwarzaniem danych osobowych. Pod pojęciem „zautomatyzowanych zbiorów danych" rozumie się każdy ogół informacji ujęty do automatycznego przetwarzania, zaś „automatyczne przetwarzanie" to działania prowadzone w całości lub w części za pomocą zautomatyzowanych procesów, tj. gromadzenie danych, przeprowadzanie logicznych i rachunkowych operacji z tymi danymi, przekształcanie, usuwanie, odzyskiwanie i ujawnianie danych[15], zaś „dane osobowe" to

[13] Akt ten zaczął obowiązywać od dnia 1 października 1985 (po tym jak ratyfikowało go pięć państw: Francja, RFN, Norwegia, Hiszpania i Szwecja). Polska mogła stać się stroną Konwencji dopiero po uchwaleniu ustawy o ochronie danych osobowych, gdyż jednym z warunków wejścia z życie konwencji, określonym w art. 4, jest istnienie w prawie wewnętrznym danego państwa odpowiednich gwarancji prawnej ochrony danych osobowych. Z punktu widzenia prawa międzynarodowego jest to pierwsza umowa międzynarodowa dotycząca przetwarzania danych osobowych. Więcej: A. Mednis, *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej*, „Państwo i Prawo" 1997, nr 6, s. 29–41. Tekst Konwencji [w:] Dz. U. 2003, nr 3, poz. 25.

[14] Więcej na temat historii ochrony danych: M. Kotowski, *Wstęp do ochrony danych. Materiały szkoleniowe*, Warszawa 1979.

[15] Arwid Mednis uważa, że Konwencja nakłada na państwa–strony obowiązek stosowania jej postanowień także do kartotek (jak i przetwarzania automatycznego danych osobowych), A. Mednis, *Ochrona danych* […], s. 33–34.

wszelkie informacje o określonych lub dających się określić osobach fizycznych. Może być to każda informacja dotycząca konkretnej osoby lub takiej osoby, którą można zidentyfikować (np.: nazwisko, pesel, NIP, zdjęcia, film, DNA). Identyfikowalność danej osoby zależy od posiadanych o niej danych osobowych lub od tego jakimi środkami dysponujemy w celu ustalenia jej tożsamości (identyfikacja ma doprowadzić do wskazania „fizycznie" konkretnej osoby). Przyjmuje się, że osoba nie jest identyfikowalna, jeśli ustalenie jej tożsamości wymaga nieproporcjonalnie dużo czasu i kosztów. Nie można z góry jakiejś kategorii danych przypisać charakter osobowy, ponieważ to, czy pozwalają na identyfikację osoby, wynika z okoliczności w jakich się pojawiają.

Konwencja 108 Rady Europy nie obejmuje ochroną danych osób prawnych (w kontekście gromadzenia, przetwarzania i udostępniania danych). Wykazuje pewną elastyczność. Pozwala krajom do niej przystępującym na ograniczenie lub poszerzenie zakresu jej działania. Państwo musi złożyć oświadczenie o wyłączeniu stosowania Konwencji do określonych, wymienionych rodzajów zautomatyzowanych zbiorów danych osobowych. Jednocześnie nie może się domagać od innych krajów ochrony tych kategorii zbiorów danych osobowych, których sam nie objął ochroną. Zakazane jest wyłączenie ochrony takich zbiorów, które na podstawie prawa wewnętrznego danego kraju podlegają przepisom o ochronie danych. Państwa–Strony konwencji mogą również objąć ochroną:

1) informacje o grupach osób, fundacjach, związkach, stowarzyszeniach, korporacjach i innych organizacjach (które bezpośrednio lub pośrednio składają się z osób fizycznych, niezależnie od tego czy posiadają osobowość prawną)[16];

2) zbiory danych osobowych, które nie są automatycznie przetwarzane[17].

Kraj, który rozszerza na swoim terytorium stosowanie Konwencji, może zastrzec, iż dotyczy to tylko wskazanych kategorii danych czy zbiorów. Nie jest zobowiązany do zapewnienia rozszerzonej ochrony względem innych krajów członkowskich, jeśli państwa te takich rozszerzeń również nie wprowadziły. Konwencja 108 Rady Europy może mieć zastosowanie w przypadku każdej informacji osobowej przetwarzanej automatycznie, niezależnie od tego czy występuje ona pojedynczo czy w zbiorze, oraz jeśli państwa rozciągnęły ochronę na zbiory ręczne, również pojedyncze lub w zbiór danych osobowych.

---

[16] Stosowanie Konwencji wobec podmiotów innych niż osoby fizyczne („non natural person") przyjęły m.in. Austria, Bułgaria, Francja, Islandia, Włochy, Lichtenstein, Luksemburg, Polska, Rumunia oraz Szwajcaria

[17] Konwencję stosuje się wobec zbiorów przetwarzanych ręcznie m.in. w: Albanii, Austrii, Belgii, Bułgarii, Chorwacji, Cyprze, Czechach, Danii, Estonii, Finlandii, Francji, Grecji, Hiszpanii, Holandii, Islandii, Litwie, Lichtensteinie, Luksemburgu, Łotwie, Macedonii, Malcie, Niemczech, Norwegii, Polsce, Portugalii, Rumunii, Serbii, Słowacji, Słowenii, Szwecji, Szwajcarii oraz Wielkiej Brytanii.

Konwencja 108 Rady Europy zobowiązuje Państwa–Strony do wprowadzenia do swojego prawa wewnętrznego przepisów przewidujących sankcje i środki prawne na wypadek naruszenia ochrony danych osobowych oraz środki właściwe do zabezpieczenia przed przypadkowym lub bezprawnym dostępem (zniszczeniem, utratą, ujawnieniem) danych osobowych umieszczonych w zautomatyzowanych zbiorach.

Konwencja 108 Rady Europy, w art. 5 i 6 określa zasady postępowania z automatycznie przetwarzanymi danymi osobowymi. Wymaga, aby dane osobowe były:

1) uzyskiwane i przetwarzane w „dobrej wierze" i w sposób zgodny z prawem;

2) gromadzone i wykorzystywane tylko dla określonych celów (zgodnych z prawem);

3) odpowiednie i istotne dla celów, dla których są gromadzone;

4) aktualne i poprawne;

5) przechowywane tylko taki czas, jaki jest potrzebny do realizacji celu dla którego były zbierane.

Szczególną ochroną objęte są tzw. dane wrażliwe (sensytywne) – które ujawniają pochodzenie rasowe, poglądy polityczne lub religijne albo innego rodzaju przekonania, dane dotyczące stanu zdrowia, preferencji seksualnych lub orzeczeń karnych. Mogą być one przetwarzane tylko wówczas, gdy przepisy wewnętrzne danego państwa zapewniają właściwą ochronę.

Konwencja 108 Rady Europy zapewnia każdemu prawo do:

1) informacji o istnieniu zautomatyzowanego zbioru, jego celu, miejscu siedziby lub pobytu podmiotu odpowiedzialnego za zbiór,

2) otrzymania bez nadmiernej zwłoki i nadmiernych kosztów w zrozumiałej dla siebie formie potwierdzenia, czy dane osobowe na jego temat są gromadzone w zautomatyzowanym zbiorze danych osobowych,

3) poprawienia ich lub usunięcia, jeśli zostały one przetwarzane wbrew przepisom prawa wewnętrznego,

4) rozporządzania środkami prawnymi, jeśli jego uprawnienia nie zostaną zrealizowane.

Ograniczenie tej ochrony jest dopuszczalne tylko gdy jest przewidziane w prawie danego państwa członkowskiego i stanowi środek konieczny w demokratycznym społeczeństwie do ochrony bezpieczeństwa państwowego oraz publicznego, interesów obronnych państwa, zwalczania czynów karalnych i ochrony osób, których dane dotyczą lub praw i wolności osób trzecich.

Każda ze stron Konwencji zobowiązana jest do udzielania sobie wzajemnie pomocy. W tym celu wyznacza jeden lub więcej organów administracji publicznej i informuje (o nazwie i adresie każdego z tych organów) Sekretarza Generalnego Rady Europy. Organ ten został zobowiązany do udzielenia, na żądanie

organu administracji publicznej innej strony, informacji o własnych przepisach prawnych i praktyce w zakresie ochrony danych osobowych, oraz udzielenia informacji o konkretnym automatycznym przetwarzaniu danych dokonanym na jego terytorium[18].

Ponadto Państwo–Strona Konwencji zobowiązane jest do udzielenia pomocy osobom mieszkającym za granicą w korzystaniu z praw przewidzianych w jej prawie wewnętrznym (realizujących zasady określone w art. 8 Konwencji). Osoba mieszkająca na obszarze kraju członkowskiego może złożyć wniosek o udzielenie pomocy do oznaczonego urzędu w tym kraju. Wniosek musi zawierać: nazwisko, imię i inne dane identyfikujące wnioskodawcę, zautomatyzowany zbiór danych osobowych, których wniosek dotyczy, podmiot odpowiedzialny za ten zbiór oraz cel wniosku. Nie może takiego wniosku złożyć sam urząd zagraniczny w imieniu osoby mieszkającej za granicą, bez jej wyraźnej zgody. Konwencja 108 Rady Europy zastrzega, że organ administracji publicznej nie może otrzymanej informacji wykorzystać dla celów innych, niż określone we wniosku. Za udzielaną pomoc nie mogą być pobierane żadne opłaty z wyjątkiem kosztów wynagrodzeń rzeczoznawców lub tłumaczy.

Odrzucenie wniosku lub prośby o udzielenie pomocy może nastąpić tylko w wypadkach: gdy wniosek wykracza poza uprawnienia organu zobowiązanego do udzielenia odpowiedzi, nie odpowiada postanowieniom Konwencji, ich spełnienie nie da się pogodzić z suwerennością, bezpieczeństwem lub porządkiem publicznym danego kraju członkowskiego albo z podstawowymi wolnościami osób podlegających jurysdykcji tej strony.

Zgodnie z postanowieniami rozdziału V Konwencji powołano Komitet Doradczy[19], który jest zwoływany przez Sekretarza Generalnego Rady Europy[20]. Składa się on z przedstawicieli (po jednym) wszystkich krajów członkowskich (ewentualnie jego zastępcę), oraz gdy państwo jest członkiem Rady Europy, a nie przystąpiło do Konwencji, wówczas może być reprezentowane w Komitecie Doradczym przez obserwatora. Komitet Doradczy może, na mocy jednomyślnej

---

[18] Nie jest zobowiązany do udostępnienia treści danych osobowych, które były przedmiotem tego przetwarzania. (art. 13 ust. 3a Konwencji).

[19] Statut Rady Europy przewiduje w art. 17 „Komitet Ministrów może powołać, dla wszelkich celów, które uzna za stosowne, komitety lub komisje o charakterze doradczym lub technicznym", zaś w art. 24 stanowi, że „Zgromadzenie Doradcze może, uwzględniając postanowienia art. 38d, powołać komitety lub komicje do zbadania wszelkich spraw należących do jego kompetencji, zgodnie z art. 23, i przedstawienia mu opracowanych sprawozdań oraz badania zagadnień znajdujących się w porządku dziennym i przedkładania mu opinii we wszystkich sprawach proceduralnych." Statut Rady Europy z dnia 5 maja 1949, Dz. U. 1994, nr 118, poz. 565.

[20] Pierwsze posiedzenie powinno się odbyć w ciągu 12 miesięcy od daty wejścia w życie tej Konwencji. Następne posiedzenia powinny odbywać się co najmniej raz na dwa lata, albo w każdym innym terminie na wniosek przynajmniej 1/3 przedstawicieli stron. Po każdym posiedzeniu Komitet Doradczy przedstawia Komitetowi Ministrów Rady Europy sprawozdanie ze swojej działalności i ze stanu przestrzegania Konwencji. (art. 20 Konwencji).

uchwały, zaprosić państwo nie będące członkiem Rady Europy na swoje posiedzenie. Do kompetencji Komitetu Doradczego należy: składanie propozycji co do ułatwienia lub poprawienia stosowania Konwencji, proponowanie zmian, wypowiadanie się co do proponowanych zmian oraz zajmowanie stanowiska, na prośbę państwa członkowskiego, co do wszystkich kwestii związanych ze stosowaniem Konwencji.

Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych[21] uszczegóławia materialne i formalne warunki dla przetwarzania danych osobowych. Zmniejsza różnice między postanowieniami Konwencji oraz postanowieniami dyrektywy 95/46/WE[22]. Różnice te nie są liczne. Dotyczą głównie dwóch kwestii: tworzenia organów nadzorujących i przekazywania danych pomiędzy krajami konwencji oraz ochrony danych osobowych w relacjach międzynarodowych. Konwencja 108 Rady Europy nie zawiera wyraźnie określonego zobowiązania do utworzenia organu(-ów) kontrolnych (nadzorczych), tak jak to przewiduje dyrektywa. Odnośnie kwestii przekazywania danych w relacjach międzynarodowych, Konwencja nie definiuje pojęcia „zadowalający poziom ochrony danych", równocześnie zobowiązuje kraje członkowskie do zapewnienia swobodnego przepływu danych. Taka sytuacja może doprowadzić do konfliktu, ponieważ Dyrektywa zakazuje państwom członkowskim przekazywania danych do krajów, które nie zapewniają „adekwatnej" ochrony[23].

Rezolucje (zalecenia) Rady Europy

W latach 1973–74 Rada Europy wydała dwie rezolucje o ochronie sfery prywatności osób fizycznych w aspekcie wykorzystywania elektronicznych banków danych:

– w sektorze prywatnym – Rezolucja nr 22
– w sektorze publicznym – Rezolucja nr 29

---

[21] Protokół Dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych z dnia 8 listopada 2001, Dz. U. 2001, nr 3, poz. 15.

[22] Polska zakończyła procedurę ratyfikacyjną dnia 12 lipca 2005, a Protokół opublikowano w Dz. U. 2006, nr 3, poz. 15.

[23] Jak wskazuje A. Mrózek, wprowadzenie w jednym państwie rygorystycznej ochrony danych, a w innych nie, może doprowadzić do umieszczania zbiorów danych na terenie państw, w których obowiązuje bardziej liberalne ustawodawstwo. Istnieje zatem obawa, że zróżnicowanie ochrony danych osobowych może doprowadzić do jej nieskuteczności. Mogą zacząć powstawać tzw. wyspy komputerowe lub inaczej zwane „raje informacyjne", które stworzą swoisty azyl dla nieskrępowanego przetwarzania danych osobowych wykorzystywanych przez międzynarodowe koncerny i korporacje. Więcej: A. Mrózek, *Ustawowe prawo ochrony danych. Analiza prawnoporównawcza*, Toruń 1981, s. 131–132.

Mają one charakter wyłącznie zaleceń mobilizujących państwa członkowskie do podjęcia wszelkich środków służących realizacji określonych w nich zasad oraz powiadomienia Sekretarza Generalnego o poczynionych krokach.

Rezolucja nr 22 (73)

Rezolucja nr 22 (73) formułuje następujące zasady:

1) gromadzone dane powinny być dokładne, aktualne i nie powinny prowadzić do dyskryminacji;

2) powinny być zbierane tylko te informacje, które dokładnie odpowiadają celowi zbierania;

3) informacje powinny być pozyskiwane legalnymi i uczciwymi sposobami (nie podstępnymi);

4) powinien być jasno oznaczony moment, do którego mogą być zbierane i gromadzone dane osobowe;

5) informacje nie powinny, bez odpowiedniego upoważnienia, być używane dla celów innych niż te, dla których były zbierane, ani też innym osobom udostępniane;

6) każdemu zainteresowanemu powinno się zagwarantować prawo do informacji o zbieraniu na jego temat informacji, o celu ich zbierania oraz szczegółach ich udostępniania;

7) państwa powinny zadbać o poprawianie informacji nieścisłych i usuwanie informacji przestarzałych lub uzyskanych w sposób bezprawny;

8) należy zastosować środki ostrożności zapobiegające niewłaściwemu lub podstępnemu wykorzystywaniu informacji oraz służące wykryciu informacji utraconych;

9) dane powinny być udostępniane wyłącznie osobom, które wykażą uzasadniony powód. Osoby obsługujące elektroniczny bank danych powinny być zobowiązane stosownymi przepisami do zachowania tajemnicy zawodowej;

10) dane statystyczne powinny być udostępniane tylko w formie zbiorczej, i w taki sposób aby nie była możliwa identyfikacja osób.

Rezolucja nr 29 (74)

Zasadniczo powtarza zasady przedstawione we wcześniejszej rezolucji. Uściśla zasadę, w myśl której powinno się wskazywać granicę czasową, według której dozwolone jest zbieranie i wykorzystywanie określonych kategorii danych; zastrzega jednocześnie możliwość wprowadzenia wyjątków i dopuszczenie nieograniczonego czasowo dostępu do danych, jeśli jest to usprawiedliwione celami statystycznymi, naukowymi lub historycznymi. Ponadto dane te nie powinny być swobodnie i bez żadnej kontroli udostępniane. Dane osobowe wykorzystywane

dla celów statystycznych mogą być rozpowszechniane tylko w taki sposób, który uniemożliwi zidentyfikowanie tych osób.

Nowością w tej rezolucji są dwa postulaty:

1) społeczeństwo powinno być informowane o zakładaniu w sektorze publicznym (eksploatowaniu i rozwijaniu) banków danych;

2) gdy przedmiot przetwarzania stanowią dane wrażliwe (należące do sfery intymnej), lub gdy przetwarzanie może prowadzić do nieusprawiedliwionej dyskryminacji:

a) założenie banków danych musi być przewidziane w ustawie (lub szczególnym rozporządzeniu) oraz musi być odpowiednio opublikowane,

b) ustawa (rozporządzenie) musi jasno określać cel, dla którego mogą być zbierane i wykorzystywane dane oraz warunki konieczne dla dalszego ich przekazywania,

c) gromadzone dane nie mogą być używane dla innych niż podane celów, chyba że wyjątek zostanie wyraźnie przewidziany w ustawie lub usankcjonowany przez kompetentną władzę[24].

Charakter zaleceń posiadają także rekomendacje wydane i przyjęte przez Komitet Ministrów Rady Europy. Ich celem jest uszczegółowienie rozwiązań przyjętych w Konwencji. Są to w szczególności:

W zakresie badań medycznych i opieki społecznej[25]:

1) Rekomendacja R (81) 1, z dnia 23 stycznia 1981, w sprawie regulacji mających zastosowanie do zautomatyzowanych banków danych medycznych. Dotyczy elektronicznych banków danych medycznych tworzonych dla celów opieki zdrowotnej, zdrowia publicznego, zarządzania usługami medycznymi lub zdrowiem publicznym, dla celów badań naukowych dotyczących zdrowia,

---

[24] Obok wyżej wymienionych rezolucji należy wspomnieć także o:

Rezolucji 29 (78) dotyczącą pobierania i przeszczepiania ludzkich tkanek i organów – <http://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Res%2878%2929E.pdf>, dostęp: 26 lutego 2014,

Rezolucji 3 (95) dotyczącą karty oceny zawodowej osób niepełnosprawnych, która wymaga aby wszystkie informacje zbierane dla oceny przydatności zawodowej niepełnosprawnych podlegały uregulowaniom dotyczącym ochronie danych osobowych oraz tajemnicy zawodowej i medycznej.

[25] Poza wymienionymi poniżej rekomendacjami wskazać można jeszcze wiele innych „specjalistycznych" dotyczących działalności medycznej. Są to: Rekomendacja R (87) 23 w sprawie systemów informatycznych w szpitalach, Rekomendacja R (89) 4 w sprawie zbierania danych epidemiologicznych w podstawowej opiece medycznej, Rekomendacja R (89) 14 w sprawie etycznych problemów zakażenia wirusem HIV w zakładach służby zdrowia i placówkach społecznych, Rekomendacja R (90) 3 w sprawie badań medycznych na istotach ludzkich, Rekomendacja R (90) 8 w sprawie napływu nowych technologii do służby zdrowia, Rekomendacja R (90) 13 w sprawie prenatalnych genetycznych badań przesiewowych, prenatalnej diagnostyki genetycznej oraz związanego z tym poradnictwa, Rekomendacja R (91) 15 w sprawie współpracy europejskiej w ramach badań epidemiologicznych w dziedzinie zdrowia psychicznego, Rekomendacja R (92) 1 w sprawie wykorzystania kwasu dezoksyrybonukleinowego (DNA) w postępowaniu karnym, Rekomendacja R (92) 3 w sprawie genetycznych badań diagnostycznych i przesiewowych wykorzystywanych dla celów opieki zdrowotnej.

w których są zgromadzone dane medyczne oraz, w niektórych przypadkach, powiązane z nimi dane socjalne lub administracyjne dotyczące osób zidentyfikowanych lub możliwych do identyfikacji. O zakładaniu banków danych medycznych (bądź zmianie już istniejących) muszą być informowane osoby zainteresowane. Regulamin banku powinien zawierać postanowienia dotyczące jego konkretnych celów, kategorii zarejestrowanych osób, udostępniania informacji osobom, których dane dotyczą, udostępniania osobom trzecim oraz bezpieczeństwa danych i urządzeń. Dostęp do informacji może być przyznany tylko osobom wykonującym zawód lekarski, jak również, o ile jest to przewidziane w prawie, członkom personelu paramedycznego[26].

2) Rekomendacja R (86) 1 w sprawie ochrony danych osobowych wykorzystywanych dla celów zabezpieczeń społecznych. Gromadzenie i rejestrowanie danych osobowych dla celów zabezpieczeń społecznych nie powinno wykraczać poza zakres niezbędny dla wypełnienia przez instytucje zabezpieczeń społecznych ich zadań. Gromadzenie danych ujawniające pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne przekonania jest dopuszczalne tylko wtedy, gdy jest to absolutnie konieczne dla udzielenia konkretnego świadczenia. W miarę możliwości instytucje te powinny pozyskiwać dane osobowe od osób, których one dotyczą, i o ile jest to niezbędne, pozyskiwać dane z innych źródeł. Dane osobowe nie powinny być przechowywane przez instytucje zabezpieczeń społecznych dłużej niż jest to uzasadnione wypełnianymi przez nie zadaniami lub interesem osoby, której dotyczą. Przepływ danych osobowych między tymi instytucjami jest dozwolony, o ile jest to konieczne dla wypełnienia zadań i zgodne z prawem międzynarodowym dotyczącym zabezpieczenia społecznego. Dane osobowe, które nie są już wykorzystywane dla celów zabezpieczeń społecznych, powinny być anonimizowane, nawet jeśli są one potrzebne do badań historycznych, naukowych i statystycznych[27].

3) Rekomendacja R (97) 5 w sprawie ochrony danych medycznych jest próbą pogodzenia prawa dostępu do informacji medycznych przez specjalistów z koniecznością zachowania poufności danych. Normuje zasady przetwarzania danych medycznych, prawa podmiotu tych danych, przypadki gdy dane mogą być wyjawione osobom trzecim, zasady przesyłania danych za granicę, przetwarzania danych w związku z badaniami naukowymi oraz środki służące zabezpieczeniu danych medycznych[28].

W zakresie badań naukowych i statystyki:

1) Rekomendacja R (83) 10 z dnia 23 września 1983, dotycząca ochrony danych osobowych wykorzystywanych w badaniach naukowych i statystyce

---

[26] <http://www.memex.pl/doc/rekomendacja_banki_medyczne.doc>, dostęp: 26 lutego 2014.

[27] <http://www.giodo.gov.pl/plik/id_p/351/t/pdf/j/pl/>, dostęp: 27 lutego 2014.

[28] M. Jackowski, *Ochrona danych medycznych*, Warszawa 2002, s. 71–72.

(w sektorach publicznym i prywatnym niezależnie czy są przetwarzane automatycznie czy ręcznie). Badania w miarę możliwości muszą posługiwać się danymi anonimowymi, a dane osobowe gromadzone dla celów badań naukowych nie mogą być wykorzystywane do innych celów. Szczególne środki ochrony danych muszą być podjęte w stosunku do osób, których dane zostały zgromadzone i które nie są w stanie bronić swoich interesów lub nie mają możliwości swobodnego wyrażenia zgody. Dane osobowe mogą być upublicznione tylko wtedy, gdy osoby, których dane dotyczą, wyraziły na to zgodę oraz zgodnie z innymi gwarancjami przewidzianymi prawem krajowym. Ponadto każdy projekt badań musi w miarę możliwości określać, czy po jego zakończeniu zgromadzone dane osobowe zostaną zniszczone, zanonimizowane czy przechowywane (i na jakich warunkach).

2) Rekomendacja R (97) 18 w sprawie ochrony danych osobowych gromadzonych i przetwarzanych w celach statystycznych określa zasady przetwarzania, czyli: zbierania, gromadzenia, wymiany, udostępniania danych oraz prawa osób, których dotyczą. Zaleca stosowanie zasad etyki dla instytucji zajmujących się zbieraniem danych dla celów statystycznych. Wszelkie dane zbierane dla tych celów powinny być anonimizowane.

W zakresie skomputeryzowanych usług informacji prawniczych, rejestrów karnych i policji:

1) Rekomendacja R (83) 3 w sprawie ochrony użytkowników skomputeryzowanych usług informacji prawniczej[29].

2) Rekomendacja R (84) 10 w sprawie rejestrów karnych i rehabilitacji osób skazanych. Zobowiązuje władze do zapewnienia, że informacja pochodząca z rejestrów karnych przekazywana będzie jedynie w postaci wyciągów, których treść ściśle ograniczona zostanie do uprawnionego interesu odbiorców. Tylko w wyjątkowym trybie, władze odpowiedzialne za system wymiaru sprawiedliwości lub osoby upoważnione uzyskają pełny wykaz elementów rejestru karnego. Rekomendacja ponadto postuluje podjęcie właściwych kroków na rzecz ochrony informacji zawartej w rejestrach karnych, w szczególności, gdy są one skomputeryzowane[30].

3) Rekomendacja R (87) 15 o korzystaniu z danych osobowych w działalności policji. Policja została zobowiązana do powiadamiania obywateli o zbieraniu dotyczących ich danych, chyba że wpływałoby to ujemnie na prowadzone dochodzenie. Z tym samym zastrzeżeniem możliwe jest udostępnianie policyjnych

---

[29] <http://www.giodo.gov.pl/plik/id_p/347/t/pdf/j/pl/>, dostęp: 27 lutego 2014. Skomputeryzowana służba informacji prawnej oznacza służbę dostarczającą środkami zautomatyzowanymi informacjo o: ustawodawstwie, orzeczeniach sądowych oraz literaturze prawniczej. Użytkownik skomputeryzowanej służby informacji prawnej oznacza osobę bądź instytucje, która dociera bezpośrednio do służby operacyjnej, działając bądź też nie działając na rzecz strony trzeciej.

[30] <http://www.giodo.gov.pl/plik/id_p/349/t/pdf/j/pl/>, dostęp: 27 lutego 2014.

zbiorów danych (ze zautomatyzowanych i ad hoc tworzonych kartotek) innym osobom (np. dziennikarzom). Nie jest zabronione przekazywanie danych osobowych pomiędzy jednostkami policji. Dane oparte na faktach i dane oparte na opiniach i ocenach powinny być przechowywane w oddzielnych zbiorach. Tylko zbiory danych dotyczące przestępców mogą być łączone (ale nie osób posiadających broń i np. cudzoziemców)[31].

W sprawie zbierania, przetwarzania, przedstawiania i archiwizacji orzeczeń sądowych:

1) Rekomendacja R (95) 1 w sprawie zbierania, przetwarzania, przedstawiania i archiwizacji orzeczeń sądowych w skomputeryzowanych systemach dokumentacji sądowej. Określa kryteria i sposób selekcji dokumentów znajdujących się w dyspozycji sądów, metody identyfikacji tych dokumentów i ich przechowywania.

W zakresie marketingu bezpośredniego:

1) Rekomendacja R (85) 20 w sprawie ochrony danych osobowych wykorzystywanych dla celów marketingu bezpośredniego. Przewiduje ona, iż w granicach przewidzianych prawem, każda osoba powinna mieć możność zbierania danych osobowych do tego rodzaju potrzeb z pomocą publicznie dostępnych kartotek lub publikacji. Niedopuszczalne jest pozyskiwanie danych od osób prywatnych za pomocą środków oszukańczych. Każdy winien mieć prawo do sprzeciwienia się umieszczeniu jego danych na listach marketingowych. Rekomendacja reguluje także kwestie udostępniania list marketingowych osobom trzecim. Zaleca wprowadzenie wszelkich odpowiednich środków technicznych i organizacyjnych służących zagwarantowaniu bezpieczeństwa i poufności danych[32].

W związku z zatrudnieniem:

1) Rekomendacja R (89) 2 w sprawie ochrony danych osobowych wykorzystywanych w związku z zatrudnieniem. Dane osobowe powinny być pozyskiwane w zasadzie od pracownika. Konsultacje z innymi źródłami niż osoba są możliwe jedynie za zgodą osoby, lub gdy osobę poinformowano wcześniej o takiej możliwości. Nie powinno się przeprowadzać testów, analiz i innych procedur służących do oceny charakteru lub osobowości osoby bez jej zgody lub jeśli prawo krajowe nie przewiduje innych odpowiednich zabezpieczeń. Dane osobowe powinny być zabezpieczone i wykorzystywane wyłącznie dla celów zatrudnienia. Ich przechowywanie jest dozwolone tylko wtedy, gdy dane zebrano zgodnie z prawem. Można je przekazywać przedstawicielom pracowników, o ile takie dane są niezbędne do umożliwienia im reprezentowania interesów pracowników. W stosunku do organów publicznych przekazywanie danych osobowych jest

---

[31] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 79.

[32] <http://www.memex.pl/doc/rekomendacja_85_20.doc>, dostęp: 27 lutego 2014.

dopuszczalne tylko w granicach prawnych zobowiązań pracodawców lub zgodnie z innymi przepisami prawa krajowego, zaś przekazywanie danych organom publicznym do celów innych niż sprawowanie ich publicznych funkcji lub przekazywanie innym stronom (niż organy publiczne) możliwe jest gdy:

– przekazywanie jest niezbędne dla celów zatrudnienia, i nie są niezgodne z celami, dla których dane zostały pierwotnie zebrane oraz gdy pracownicy (lub ich przedstawiciele) zostaną o tym poinformowani;
– prawo krajowe zezwala na przekazywanie danych,
– pracownik udzieli wyraźnej i świadomej zgody.

W odniesieniu do danych szczególnie wrażliwych rekomendacja wymaga, aby były zbierane i przechowywane wyłącznie w określonych przypadkach w granicach określonych prawem i odpowiednio zabezpieczone. W przypadku braku takich zabezpieczeń, dane mogą być gromadzone i przechowywane tylko za wyraźną i świadomą zgodą pracowników. Dodatkowo dane dotyczące zdrowia (objęte tajemnicą lekarską) powinny być przechowywane oddzielnie od innych kategorii danych osobowych. Dane osobowe nie mogą być przechowywane przez pracodawcę przez okres dłuższy niż okres zatrudnienia i należy je usunąć także, gdy oferta pracy stała się nieaktualna.

W zakresie płatności i innych operacji finansowych:

1) Rekomendacja R (90) 19 w sprawie ochrony danych osobowych wykorzystywanych dla potrzeb płatności oraz innych operacji finansowych wymaga, aby banki i inne instytucje obsługujące obrót płatniczy nie gromadziły i nie przetwarzały danych osobowych służących dostarczaniu środków płatności, chyba że jest to niezbędne do realizacji celów, dla których były zbierane. Nie powinny być przechowywane przez czas dłuższy, niż jest to konieczne[33].

W zakresie przekazywania osobom trzecim danych osobowych pochodzących od instytucji publicznych:

1) Rekomendacja R (91) 10 w sprawie udostępniania osobom trzecim danych osobowych będących w posiadaniu instytucji publicznych. Zasady rekomendacji stosuje się do danych osobowych przetwarzanych w zautomatyzowanych zbiorach przez instytucje publiczne, ale państwa członkowskie mogą rozszerzyć zakres stosowania rekomendacji do zgromadzeń, towarzystw, zrzeszeń i danych osobowych w formie niezautomatyzowanej. Udostępniania osobom trzecim danych osobowych lub zbiorów zawierających dane może mieć miejsce pod warunkiem, że: jest to przewidziane prawem, dane są publicznie dostępne (np. na podstawie przepisów o dostępie do informacji publicznej), udostępnienie jest zgodne z przepisami ustawy o ochronie danych osobowych, osoba, której dane dotyczą, udzieliła wyraźnej i świadomej zgody. Dane osobowe wrażliwe nie powinny być rejestrowane w zbiorze (lub jego części) ogólnie

[33] <http://www.giodo.gov.pl/230/id_art/640/j/pl/>, dostęp: 4 grudnia 2014.

dostępnym dla osób trzecich. Rekomendacja reguluje także kwestię dostępu i udostępniania danych osobowych za pomocą środków elektronicznych (online). Zasadniczo zabronione jest łączenie, fuzja lub pobieranie drogą elektroniczną danych osobowych w celu tworzenia nowych zbiorów albo łączenie zbiorów w celu ich wzbogacania. Udostępnianie za granicę danych osobowych osobom trzecim do państwa, które ratyfikowało Konwencję, nie powinno być objęte szczególnymi przepisami ochrony prywatności. W przypadku, gdy zapewniona jest równoważna ochrona, nie powinno być ograniczeń w transgranicznym przekazywaniu danych. Nie powinno mieć miejsca udostępnianie danych osobowych osobom trzecim mającym siedzibę w państwie, które nie przestrzega Konwencji lub nie zapewnia równoważnej ochrony, chyba że osoba, której dane dotyczą wyraziła pisemną, wyraźną i świadomą zgodę oraz posiada możliwość wycofania swojej zgody w dowolnym momencie lub gdy zostały podjęte niezbędne środki w celu poszanowania zasad Konwencji i Rekomendacji[34].

W dziedzinie usług telekomunikacyjnych:

1) Rekomendacja R (95) 4 w sprawie ochrony danych osobowych w dziedzinie usług telekomunikacyjnych. Zawiera zalecenia dla operatorów sieci i dostawców usług telekomunikacyjnych. Określa zasady odnoszące się do marketingu bezpośredniego przy wykorzystaniu telefonu lub innych środków teletransmisji. Niedopuszczalne jest podsłuchiwanie, kontrolowanie i przechwytywanie informacji, o ile prawo nie przewiduje takiej ingerencji ze względu na zasady obowiązujące w demokratycznym państwie prawa. Jeśli władze publiczne mają prawo żądania danych osobowych od użytkownika sieci lub wykonawcy usług, wówczas dane powinny być przekazane jedynie tej instytucji. Dane osobowe nie powinny być gromadzone, chyba że jest to konieczne dla potrzeb podłączenia do sieci, realizacji konkretnej usługi telekomunikacyjnej lub dla celów płatności. Abonentom przysługuje prawo wyrażenia zgody lub odmowy umieszczenia swoich danych w spisie. Jeśli chodzi o telefonię przenośną, abonenci powinni być informowani o ryzyku naruszenia tajemnicy rozmowy, zwłaszcza gdy rozmowy nie są szyfrowane. Rachunki za użytkowanie telefonów nie powinny zawierać danych zbyt szczegółowo lokalizujących abonenta i jego rozmówcę[35].

W zakresie ochrony prywatności w Internecie[36]:

1) Rekomendacja R (99) 5 w sprawie ochrony prywatności w Internecie zawiera zalecenia skierowane zarówno do użytkowników Internetu, jak i dostaw-

---

[34] <http://www.giodo.gov.pl/plik/id_p/1011/t/pdf/j/pl/>, dostęp: 20 sierpnia 2014.

[35] <http://www.giodo.gov.pl/230j/od/12/j/>, dostęp: 20 sierpnia 2014.

[36] Rekomendacja R (97) 3, z dnia 3 grudnia 1997, przyjęta przez Grupę Roboczą ds. Ochrony Danych „Anonimowość w Internecie" zakłada, że pozostawienie jednostce decyzji w sprawie zachowania anonimowości ma zasadnicze znaczenie dla zapewnienia prywatności, jednak nie w każdych okolicznościach takie rozwiązanie jest uzasadnione. Niezbędne jest wyważenie z jednej strony prawa do prywatności (i prawa do wyrażania opinii), a z drugiej strony uwzględnienie interesów

ców usług internetowych. Ostrzega użytkowników Internetu, że każda czynność w Internecie pozostawia ślady i nie jest to bezpieczne miejsce. Zwraca uwagę, że nie jest możliwa zupełna anonimowość, ale anonimowy dostęp i korzystanie z usług stanowi najlepszą ochronę prywatności. Przypomina, że adres elektroniczny jest daną osobową i można się nim posłużyć do realizacji różnych celów. Zakazuje dostawcom usług internetowych ingerowania w treść wiadomości, przechowywania danych przez okres dłuższy niż jest to konieczne dla osiągnięcia celu przetwarzania, udostępniania danych osobom trzecim. Zobowiązuje ich do poinformowania użytkowników o środkach technicznych służących zmniejszeniu zagrożenia bezpieczeństwa danych oraz o potencjalnych zagrożeniach wynikających z korzystania z Internetu[37].

2) Rekomendacja Rec (2010) 13 z dnia 23 listopada 2010 w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych podczas tworzenia profili zaleca państwom członkowskim podjęcie działań mających na celu ochronę godności ludzkiej i innych podstawowych praw i wolności, zwłaszcza mając na uwadze mobilność obywateli, globalizację rynków i wykorzystywanie nowych technologii do transgranicznej wymiany informacji. Rekomendacja ta nawiązuje do wcześniej wydanych R (97) 18 oraz Rec (2002) 9 oraz do art. 8 EKPC i konwencji budapeszteńskiej w sprawie cyberprzestępczości. Nawet bowiem legalne wykorzystanie profili bez ostrzeżeń i odpowiednich zabezpieczeń może prowadzić do naruszenia prywatności i dyskryminacji ze względu na płeć, pochodzenie rasowe i etniczne, wyznanie, przekonania, niepełnosprawność, wiek czy orientację seksualną[38].

W zakresie ubezpieczeń:

1) Rekomendacja R (86) 1 dotycząca ochrony danych osobowych dla potrzeb ubezpieczenia społecznego wychodzi naprzeciwko potrzebie chronienia prywatności osób wobec coraz szerszego posługiwania się informatyką w dziedzinie zabezpieczeń społecznych. Państwa członkowskie zostały zobowiązane do zapewnienia poszanowania prywatności już w czasie gromadzenia danych używanych dla celów społecznych. Zaś samo gromadzenie i rejestrowanie danych nie powinno wykraczać poza zakres niezbędny dla wypełniania przez instytucje ich zadań. W każdej instytucji zabezpieczeń społecznych powinny być wprowadzone środki nadzoru zapewniające wystarczającą ochronę danych.

---

państwa, zwłaszcza jeśli chodzi o zwalczanie przestępczości. Rekomendacja proponuje umożliwienie zachowania anonimowości np. przy wysyłaniu e-maili i przeglądaniu witryn www oraz robieniu zakupów przez Internet. Postuluje wprowadzenie kontroli dostawców informacji w Internecie. Anonimowość w Internecie ma być zapewniana przez anonimowy system płatności lub podpis cyfrowy. Więcej: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 231–232.

[37] <http://www.giodo.gov.pl/plik/id_p/1012/t/pdf/j/pl/>, dostęp: 20 sierpnia 2014.

[38] <http:/www.giodo.gov.pl/230/od/0/j/pl>, dostęp: 20 sierpnia 2014.

2) Rekomendacja R (2002) 9 w sprawie ochrony danych osobowych zbieranych i przetwarzanych dla celów ubezpieczeniowych ustala reguły przetwarzania i ochrony danych uwzględniające specyfikę sektorową tego rodzaju działalności. Wskazuje podstawy dopuszczalności przetwarzania danych, precyzuje cele, w jakich mogą być zbierane i wykorzystywane oraz określa uprawnienia osób, których dane dotyczą. Ma umożliwić racjonalne i ekonomiczne zarządzanie ubezpieczeniami. Nakazuje zagwarantowanie poufnego charakteru danych oraz ich bezpieczeństwo.

Rekomendacje Zgromadzenia Parlamentarnego Rady Europy

Odrębną grupę regulacji z zakresu ochrony danych osobowych tworzą rekomendacje Zgromadzenia Parlamentarnego Rady Europy.

1) Rekomendacja R (77) 818 dotycząca sytuacji osób psychicznie chorych. Zaleca, aby państwa członkowskie zapewniły, że wszelkie rejestry przechowywane w placówkach psychiatrycznych dotyczące byłych pacjentów (oraz związana z nimi dokumentacja) były objęte tajemnicą lekarską i nie mogły być użyte w taki sposób, żeby wyrządzić szkodę byłym pacjentom[39].

2) Rekomendacja R (82) 934 dotycząca inżynierii genetycznej zaleca, aby przygotowywanie, przechowanie, zabezpieczanie i wykorzystanie informacji genetycznej na temat poszczególnych osób odbywało się z uwzględnieniem ich prawa do prywatności oraz stosownie do postanowień Konwencji[40].

3) Rekomendacja R (86) 1037 w sprawie ochrony danych i wolności wypowiedzi zleca Komitetowi Ekspertów do spraw Ochrony Danych określenie kryteriów i zasad, zgodnie z którymi można będzie pogodzić ochronę danych i prawo do informacji (np.; informacji publicznej) oraz przygotowanie stosownego dokumentu prawnego[41].

4) Rekomendacja R (89) 1116 „AIDS a prawa człowieka". Uznaje za nadrzędną potrzebę ochrony tajemnicy lekarskiej oraz zapewnienie anonimowości ofiarom AIDS i osobom seropozytywnym. Zaleca, o ile państwa jeszcze tego nie uczyniły, ratyfikowanie Konwencji nr 108 o ochronie jednostek w kontekście automatycznie przetwarzanych danych osobowych. Komitet Ekspertów do spraw Ochrony Danych został zobowiązany do zbadania problemów wynikających w związku ze skomputeryzowanymi danymi dotyczącymi nosicieli wirusa HIV[42] .

---

[39] <http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta77/erec818.htm>, dostęp: 5 grudnia 2014.

[40] <http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta82/erec934.htm>, dostęp: 5 grudnia 2014.

[41] <http://www.aip-bg.org/pdf/rec1037.pdf >, dostęp: 5 grudnia 2014.

[42] *Ochrona danych osobowych. Standardy europejskie. Zbiór materiałów*, pod red. T. Jasudowicza, Toruń 1998, s. 133.

5) Rekomendacja R (92) 1181 w sprawie współdziałania policji oraz ochrony danych osobowych w sektorze policyjnym nakazuje, aby dane osobowe były ścisłe, istotne, nie wykraczające poza cel w jakim są gromadzone, a w razie konieczności również aktualizowane. Powinny również być utajnione, zanim będą podlegać przechowywaniu. Każdy powinien mieć prawo do informacji o przechowywaniu jego danych osobowych i prawo dostępu do nich i ewentualnie żądania ich usunięcia. Jednostki, którym odmówiona prawa dostępu do dotyczących ich materiałów, powinny mieć prawo odwołania się do niezależnej władzy. Postuluje, by dane w sektorze Policji mogły podlegać wymianie między państwami członkowskimi oraz państwami członkowskimi i Interpolem, jedynie w trybie przewidzianym w Konwencji[43].

6) Rekomendacja R (93) 1210 dotyczy bezpieczeństwa systemów informatycznych wysokiego ryzyka.

Unia Europejska

Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE

Zgodnie z art. 249 Traktatu ustanawiającego WE dyrektywa wiąże każde państwo członkowskie, do którego jest kierowana, w odniesieniu do rezultatu, który ma być osiągnięty, pozostawia jednak organom krajowym swobodę wyboru formy i środków.

Do wydania Dyrektywy Parlamentu Europejskiego i Rady (95/46/WE) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych doszło 24 października 1995[44]. Głównym jej celem jest pogodzenie prawa do prywatności osób fizycznych i zagwarantowanie swobodnej wymiany informacji (traktowanej jako towar) oraz doprowadzenie do wyrównania poziomu ochrony (dzięki ujednoliceniu przepisów państw członkowskich[45]). Cel ten nie może być realizowany przez poszczególne państwa samodzielnie, zwłaszcza w sytuacji rozbieżności między przepisami w różnych krajach. Niewątpliwie impulsem tworzenia dyrektywy były obawy związane z rozwojem nowych metod przetwarzania danych osobowych.

---

[43] <http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?FileID=15215&lang=EN>, dostęp: 5 grudnia 2014.

[44] Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995, w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych 95/46/WE, Dz. Urz. WE L 281/31. Wersja polska np.: <http://www.giodo.gov.pl/plik/id_p/476/t/pdf/j/pl/>, dostęp: 4 grudnia 2014.

[45] Dążenie do harmonizacji i zbliżania ustawodawstw poszczególnych państw wynika z art. 94 i 95 Traktatu ustanawiającego Wspólnotę Europejską. Tekst [w:] I. C.Kamiński, *Unia Europejska. Podstawowe akty prawne*, Warszawa 2005.

Jeśli chodzi o zakres stosowania dyrektywy, to w zasadzie powtarza on postanowienia art. 1 Konwencji. Zobowiązuje państwa członkowskie do ochrony podstawowych praw i wolności osób fizycznych. Konwencja 108 Rady Europy przewidywała możliwość objęcia ochroną także danych dotyczących ugrupowań, stowarzyszeń, fundacji, spółek, korporacji i innych organizacji skupiających osoby fizyczne. Ma zastosowanie do przetwarzania danych osobowych zautomatyzowanego w całości lub w części oraz do przetwarzania danych osobowych zawartych lub mających być w zbiorze (zbiory ręczne). Taki zapis wymusiły doświadczenia zebrane podczas obowiązywania samej tylko Konwencji. Okazało się, bowiem że mimo postępującej informatyzacji życia, nadal istnieją zbiory przetwarzane ręcznie. Zarówno na podstawie Konwencji i dyrektywy ochronie nie będą podlegały dane osobowe nie będące elementem zbioru ani przedmiotem przetwarzania automatycznego.

Dane osobowe to informacje pozwalające na identyfikację osoby. Osobowy charakter informacji nie jest przypisany z góry żadnej kategorii danych. To, czy zebrane informacje pozwalają na identyfikację, zależy od kontekstu. Osoba fizyczna nie jest identyfikowalna, jeśli ustalenie jej tożsamości wymaga nieproporcjonalnie dużo czasu, kosztów i nakładu pracy. Zidentyfikować osobę można albo bezpośrednio, albo pośrednio, na podstawie cech przynależnych tej osobie. Według dyrektywy (art. 2b) przetwarzanie danych to operacja lub zespół operacji wykonanych za pomocą lub bez pomocy procedur automatycznych i zastosowanych wobec danych osobowych, takich jak gromadzenie, zarejestrowanie, zorganizowanie, przechowywanie, adaptacja lub zamiana, wyprowadzanie, zapoznawanie, używanie, komunikowanie przez transmisję, rozpowszechnianie lub jakąkolwiek inną formę przekazania, łączenie, połączenie, blokowanie, wymazanie lub niszczenie. Z treści definicji wynika, że dyrektywa obejmuje ochroną dane już na etapie ich zbierania, jeśli dane te mają być umieszczone w zbiorze.

Zbiór danych, to każdy posiadający strukturę zespół danych o charakterze osobowym dostępnych według określonych kryteriów, niezależnie od tego czy zespół ten jest scentralizowany, zdecentralizowany lub podzielony funkcyjnie albo geograficznie (art. 2c dyrektywy). Administratorem danych jest osoba fizyczna lub prawna, urząd publiczny, agenda lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych. Jeżeli cele i sposoby przetwarzania danych są określane w ustawach i innych przepisach krajowych lub przepisach Wspólnoty, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub ustawodawstwo Wspólnoty. Od administratora danych należy odróżnić organ administrujący, który tylko przetwarza dane w imieniu administratora danych, a nie decyduje o celach ich przetwarzania.

Dyrektywa Parlamentu Europejskiego i Rady w rozdziale II określa ogólne zasady legalności przetwarzania danych osobowych. Państwa członkowskie

zostały zobowiązane do zapewnienia, że dane osobowe są przetwarzane rzetelnie i legalnie, i są prawidłowe, a w razie konieczności będą aktualizowane. Gromadzone są dla określonych, wyraźnych i legalnych celów oraz, że nie będą poddawane dalszemu przetwarzaniu w sposób niezgodny z tymi celami. Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych będzie dopuszczalne pod warunkiem stworzenia przez państwo odpowiednich zabezpieczeń. Powinny być przechowywane w formie umożliwiającej identyfikację osób tylko przez taki okres, przez jaki jest to niezbędne dla osiągnięcia celów, dla których zostały zebrane.

Dyrektywa Parlamentu Europejskiego i Rady (w art. 7), w przeciwieństwie do Konwencji, wymienia sześć sytuacji, w których przetwarzanie danych powinno być dopuszczalne. Przede wszystkich wtedy, gdy:

1) osoba zainteresowana wyraziła na to zgodę w sposób nie budzący wątpliwości;

2) jest to niezbędne do wykonania umowy, której osoba zainteresowana jest stroną;

3) jest to niezbędne do wykonania przez podmiot odpowiedzialny za zbiór spoczywającego na nim obowiązku ustawowego (np. współpracy z policją, służbą celną, podatkową);

4) jest to niezbędne do zabezpieczenia żywotnego interesu osoby, której dane dotyczą (np. ze względu na ochronę zdrowia);

5) jest to niezbędne do wykonania zadania w interesie publicznym;

6) jest to niezbędne do realizacji interesu prawnego podmiotu odpowiedzialnego za przetwarzanie danych lub innych podmiotów, którym dane mają być przekazywane, pod warunkiem, że ten interes nie przeważa nad interesem lub podstawowymi prawami i wolnościami obywatelskimi osoby, której dane dotyczą.

Szczególnym zagrożeniem dla prywatności człowieka może być ujawnienie tzw. danych wrażliwych. Dyrektywa Parlamentu Europejskiego i Rady zakazuje więc przetwarzania danych ujawniających pochodzenie rasowe, etniczne, opinie polityczne, przekonania religijne lub inne, jak również dane dotyczące zdrowia i życia seksualnego oraz danych dotyczących karalności. Zezwala na przetwarzanie tych danych, ale tylko wtedy, gdy prawo wewnętrzne przewiduje odpowiednie gwarancje poszanowania prywatności. Zakaz przetwarzania danych wrażliwych nie obowiązuje gdy:

1) osoba, której dane dotyczą w sposób precyzyjny i wyraźny zgodziła się na przetwarzanie jej danych. Nie może być to jednak zgoda wymuszona;

2) pracodawca przetwarza dane o pracowniku (a prawo wewnętrzne gwarantuje odpowiednią ochronę prywatności pracownika);

3) przetwarzanie jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą (a osoba ta nie może samodzielnie wyrazić zgody);

4) fundacje, stowarzyszenia lub inne instytucje o charakterze politycznym, filozoficznym, religijnym lub związkowym przetwarzają informacje o swoich członkach lub osobach utrzymujących z tymi instytucjami regularne kontakty związane z celem danej instytucji. Instytucja może ujawniać dane tych osób na zewnątrz wyłącznie za ich zgodą;

5) przetwarzanie dotyczy danych już wcześniej upublicznionych przez osobę zainteresowaną;

6) jest to niezbędne dla stwierdzenia istnienia, skorzystania lub obrony prawa w postępowaniu sądowym;

7) przetwarzanie jest niezbędne dla celów medycyny zapobiegawczej, diagnozowania, administracji zdrowia oraz dla celów zarządzania ośrodkami zdrowia, i osoba, która przetwarza dane zobowiązana jest do przestrzegania tajemnicy lekarskiej (zawodowej).

Dla ochrony ważnego interesu publicznego państwa mogą ustanawiać wyjątki od zakazu przetwarzana danych wrażliwych. Muszą być one jednak wyraźnie przewidziane prawem. W kwestii informacji o karalności dyrektywa stwierdza, że dane te mogą być przetwarzane tylko wtedy, gdy odbywa się to pod kontrolą organu władzy publicznej lub jeśli ustawodawstwo krajowe ustanawia odpowiednie gwarancje. Organ władzy publicznej powinien kontrolować dostęp do zbioru danych o karalności (rejestru skazanych).

Dyrektywa Parlamentu Europejskiego i Rady gwarantuje każdemu prawo do informacji o zbiorze, w którym są przechowywane informacje jego dotyczące. Powinien też znać cel zbierania danych i dane o tym, kto jest administratorem zbioru. Każdemu przysługuje prawo do sprostowania błędnych danych oraz domagania się usunięcia danych przetwarzanych niezgodnie z prawem. Dyrektywa Parlamentu Europejskiego i Rady przewiduje ponadto prawo sprzeciwu. Osoba może sprzeciwić się, aby jej dane były przetwarzane, musi jednak podać powody sprzeciwu. W razie nieprzestrzegania tych praw, przysługuje jednostce prawo do odwołania się do organu ochrony danych osobowych.

Dyrektywa Parlamentu Europejskiego i Rady gwarantuje państwu prawo wprowadzenia wyjątków dotyczących zasad przetwarzania danych. Państwa mogą wprowadzić w ustawodawstwie wewnętrznym wyjątki, jeśli służyć mają one: bezpieczeństwu państwa, obronności, bezpieczeństwu publicznemu, zapobieganiu lub walce z przestępczością, ochronie osoby zainteresowanej, ochronie praw i wolności innych osób, ochronie ważnego interesu gospodarczego lub finansowego. Nakłada na administratorów danych obowiązek ich zabezpieczenia przed przypadkowym lub bezprawnym zniszczeniem, utratą, udostępnieniem ich osobom nieupoważnionym. Dodatkowo w celu ujednolicenia praktyki w poszczególnych państwach Dyrektywa przewiduje konieczność zawiadomienia organu właściwego w sprawach danych osobowych o przetwarzaniu danych.

Przekazywanie danych osobowych z WE do państw trzecich (nie należących do Europejskiego Obszaru Gospodarczego[46]) może nastąpić tylko wówczas, gdy dane państwo trzecie zapewni adekwatny stopień ochrony. Organem odpowiedzialnym za badanie stopnia ochrony jest Komisja Europejska. Ocenia ona ustawodawstwo państw trzecich i w zależności od oceny może, po uprzednim uzyskaniu opinii grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych[47] oraz Komitetu Ekspertów Krajowych[48], wykluczyć lub dopuścić możliwość przekazywania danych osobowych do tego państwa przez administratorów z poszczególnych państw członkowskich WE. Odpowiedni poziom ochrony jest oceniany w świetle wszystkich okoliczności związanych z przekazywaniem danych. Dotychczas Komisja Europejska uznała, że nie są konieczne klauzule umowne i adekwatny poziom ochrony danych osobowych zapewniają[49]:

1) Andora – C (2010) 7084 Dz. Urz. UE L 277/27 z 21.10.2010;
2) Argentyna – C (2003) 1731 Dz. Urz. UE L 168 z 5.7.2003;
3) Australia – Dz. Urz. UE L 213 z 8.8.2008, s. 49–57;
4) Kanada 2002/2 WE – Dz. Urz. WE L 2 z 4.1.2002, s. 13[50];
5) Szwajcaria 2000/518 WE – Dz. Urz. WE L 215/1 z 25.8.2000;
6) Wyspy Owcze – C (2010) 1130, Dz. Urz. UE L 58 z 9.3.20010, s. 17–19;

---

[46] Europejski Obszar Gospodarczy to strefa wolnego handlu obejmująca swoim obszarem kraje Unii Europejskiej oraz Europejskiego Stowarzyszenia Wolnego Handlu (z wyjątkiem Szwajcarii), opiera się na czterech fundamentalnych zasadach: swobodzie przepływu ludzi, kapitału, towarów i usług. Członkami EOG są: Austria, Belgia, Bułgaria, Czechy, Cypr, Dania, Estonia, Finlandia, Francja, Grecja, Hiszpania, Holandia, Irlandia, Islandia, Liechtenstein, Litwa, Luksemburg, Łotwa, Malta, Niemcy, Norwegia, Polska, Portugalia, Rumunia, Słowacja, Słowenia, Szwecja, Węgry, Wielka Brytania, Włochy.

[47] Niezależny podmiot o charakterze doradczym powołany na mocy art. 29 Dyrektywy 95/46/ /WE W skład zespołu roboczego wchodzą przedstawiciele organu (-ów) nadzorczych z każdego państwa członkowskiego, przedstawiciel organów ustanowionych dla instytucji i organów Wspólnoty oraz przedstawiciel Komisji. Podejmuje decyzje zwykłą większością głosów. Artykuł 30 Dyrektywy określa kompetencje zespołu roboczego.

[48] Komitet Ekspertów Krajowych to organ opiniodawczy przedstawiający Komisji projekt środków jakie należy podjąć. Wydaje opinie o projekcie w terminie wyznaczonym przez przewodniczącego w zależności od stopnia pilności sprawy. W jego skład wchodzą przedstawiciele państw członkowskich (przewodniczącym jest przedstawiciel Komisji).

[49] Więcej: <http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm>, dostęp: 28 lutego 2014.

[50] Komisja Europejska uznała, że kanadyjski „Personal Information Protection and Electronic Documents Act of 13 April 2000" (ustawa o ochronie danych osobowych oraz o dokumentach elektronicznych) zawiera podstawowe zasady gwarantujące adekwatną ochronę danych osobowych. Więcej: Canadian protection of personal data found compliant with exacting EU standars, International Law Update, Vol. 8, January 2002, p. 15.

Odnośnie Kanady Komisja podjęła decyzję 2006/253/WE z dnia 6 września 2005 w sprawie odpowiedniej ochrony danych osobowych zawartych w Imiennym Rejestrze Pasażerów linii lotniczych, przekazanym do Agencji Służb Granicznych Kanady (notyfikowana jako dokument nr C (2005) 3248) (Tekst mający znaczenie dla EOG) Dz.Urz. WE L 91/49 z dnia 29 marca 2006.

7) Guernsey 2003/821WE – Dz. U. UEL 308, s. 27;
8) Izrael C (2011) 332, Dz. Urz. UE L 27 z 1.2.2011, s. 39;
9) Wyspa Man 2004/11 WE – Dz. Urz. UE L 151, s. 48;
10) Wyspa Jersey – C (2008) 1746, Dz. Urz UE L 138 z 28.05.2008;
11) USA – transport powietrzny (PNR passenger name rekord) 2007/551/CFSP/JHA z 23.7.2007;
12) Nowa Zelandia – C (2012) 9557, Dz. Urz. UE L 28 z 30.1.2013;
13) „Safe Harbour" 2000/520 WE – Dz. Urz. WE L 215, s. 7;
14) Urugwaj – C (2012) 5704, Dz. Urz. UE L 227/11 z 23.8. 2012.

Jeśli Komisja Europejska uzna, że państwo trzecie nie zapewnia odpowiedniego poziomu ochrony, może albo zablokować przepływ danych osobowych do tego państwa, albo przystąpić do negocjacji (art. 25 ust. 4 i 5 dyrektywy).

Dyrektywy Parlamentu Europejskiego i Rady w sprawie komunikacji elektronicznej (97/66/WE, 2002/58/WE, 2006/24/WE, 2009/136/WE)

Dyrektywa Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 zmieniająca dyrektywy: 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów zwana jest dyrektywą „praw obywateli". W polskim prawodawstwie wdrożono już założenia tej dyrektywy w ustawie – prawo telekomunikacyjne. Dyrektywa Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 zakładała m.in. lepszą ochronę konsumenta przed naruszeniem ochrony danych osobowych oraz spamem, zwłaszcza gdy chodzi o dane: dotyczące połączeń telefonicznych oraz połączeń internetowych konsumenta, dostępne dostawcy usług, które nie powinny trafiać w niepowołane ręce. Na dostawców usług nałożono obowiązki w zakresie należytego przechowywania i przetwarzania tych danych. Operatorów zobowiązano do informowania konsumentów oraz odpowiednie organy o przypadkach naruszenia prawa dotyczącego ochrony danych osobowych. Wprowadzono również możliwość kontroli przez użytkownika Internetu tzw. Cookies, tak aby bez zgody użytkownika jego dane nie mogły być wykorzystywane przez właścicieli serwerów internetowych[51].

Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 (2002/58/WE) w sprawie przetwarzania danych osobowych oraz ochrony prywatności

[51] Więcej: <http://www.uke.gov.pl/uke/index.jsp?place=Lead01&news_cat_id=168&news_id=4850&layout=3&page=text>, dostęp: 28 lutego 2014.

w sektorze komunikacji elektronicznej jest odpowiedzią na coraz większe zagrożenie prywatności i dynamiczny rozwój telekomunikacji. Poprzednia dyrektywa z dnia 15 grudnia 1997 (97/66/WE[52]) w sprawie przetwarzania danych osobowych i ochrony prywatności w dziedzinie telekomunikacji, przeniosła wprost zasady określone w dyrektywie 95/46/WE do sektora telekomunikacji. Nie zapewniała jednak jednolitego poziomu ochrony danych osobowych oraz prywatności użytkowników usług łączności elektronicznej, niezależnie od stosowanych technologii, dlatego została zastąpiona nową dyrektywę, która również częściowo już została zmieniona DPEiR z dnia 15 marca 2006 (2006/24/WE) w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności.

Postanowienia dyrektywy z 2002 mają zapewnić realizację podstawowych zasad określonych w KPP UE, ze szczególnym uwzględnieniem postanowień art. 7 i 8 (o ochronie prywatności i danych osobowych). Celem dyrektywy jest z jednej strony ochrona podstawowych praw i wolności człowieka, a z drugiej strony zapewnienie swobodnego przepływu danych w ramach WE. Postanowienia dyrektywy nie mają zastosowania do działalności pozostającej poza zakresem TWE[53]. Zakres przedmiotowy dyrektywy ogranicza się do przetwarzania danych osobowych w związku ze świadczeniem publicznych usług łączności elektronicznej w publicznych sieciach łączności w obrębie WE, ale jest on i tak szerszy od pojęcia „usługi telekomunikacyjne" znanego z dyrektywy 97/66/WE. Takie wyłączenie jest krytykowane, ponieważ wyłącza usługi świadczone w zamkniętych grupach użytkowników, podczas gdy rośnie rola prywatnych sieci. Jeśli chodzi o podmiot, dyrektywa chroni zarówno osoby fizyczne (ich podstawowe prawa) jak i osoby prawne (np. interes abonentów).

Dyrektywa Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 nakłada na dostawców usług obowiązek zapewnienia bezpieczeństwa usług, a niekiedy także bezpieczeństwa sieci. Wymagany poziom zabezpieczenia ma być odpowiedni do ryzyka. Usługodawcy oferujący usługi łączności elektronicznej za pomocą Internetu powinni powiadomić abonentów (użytkowników) o środkach, jakie ci mogą podjąć, aby zapewnić sobie bezpieczeństwo przekazu. Oceny dokonuje się

---

[52] ETS w sprawie C-350/02 (Komisja Wspólnot Europejskich przeciwko Królestwu Holandii) uznał, że Królestwo Holandii uchybiło zobowiązaniom, które na nim ciążą z mocy dyrektywy, transponując w sposób niekompletny art. 6 i 9 Dyrektywy 97/66/WE, jak również fakt, że przepisy wykonawcze nie zostały zakomunikowane Komisji. Dz. U. WE C 2004/07, <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-350/02>, dostęp: 20 listopada 2014.

[53] Chodzi tutaj o obszar objęty Tytułami V i VI Traktatu o Unii Europejskiej, czyli o kwestie dotyczące wspólnej polityki zagranicznej i bezpieczeństwa, wspólnej polityki obronnej oraz współpracy policyjnej i sądowej w sprawach karnych.

na podstawie art. 17 dyrektywy 95/46/WE o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływie takich danych. Państwa członkowskie mają obowiązek zapewnić poufność przekazów i związanych z nimi danych transmisyjnych[54] poprzez zakaz ich słuchania, pobierania, przechowywania, przechwytywania bądź śledzenia. Istotne znaczenie ma tutaj możliwość legalnego podsłuchiwania rozmów telefonicznych w związku z prowadzeniem śledztw w sprawach karnych oraz ochroną interesów bezpieczeństwa narodowego. W świetle rekomendacji R (99) 2 w sprawie poszanowania prywatności w związku z telekomunikacyjnym podsłuchem, prawo krajowe w sprawie podsłuchu powinno:

1) wskazywać organy upoważnione do zezwalania na podsłuch (i podstawę prawną) oraz niezależne organy nadzorujące realizację podsłuchu;

2) określać cel dokonywania podsłuchu, wyraźnie okoliczności i warunki realizowania podsłuchu, środki bezpieczeństwa przewidziane dla przetwarzania danych osobowych;

3) wprowadzać zakaz „generalnego podsłuchu", gwarancje bezpieczeństwa dla danych osób pośrednio narażonych przez podsłuch, lub których przekazy zostały przypadkowo uzyskane, obowiązek informacji zainteresowanego o podsłuchu w najwcześniejszym momencie (uwzględniający cele śledztwa), zasady wniesienia sprzeciwu zainteresowanego przeciwko podsłuchowi, wymóg publikacji danych statystycznych o zakresie prowadzonego podsłuchu oraz zasady i warunki udostępnienia danych stronom trzecim w ramach dwustronnych i wielostronnych porozumień.

Dane o abonentach i użytkownikach przetwarzane i gromadzone przez dostawcę usługi muszą zostać usunięte lub zanonimizowane w momencie, gdy już nie są potrzebne do transmisji przekazu, natomiast dane transmisyjne niezbędne do naliczenia opłat abonenta oraz opłat międzyoperatorskich mogą być przedmiotem przetwarzania. Jest to jednak dozwolone tylko do końca okresu, w którym przysługuje odwołanie od przedstawionego rachunku bądź okresu jego ściągalności. Na potrzeby marketingu usług łączności elektronicznej bądź świadcze-

---

[54] Dane transmisyjne mogą zawierać informacje o nazwie, numerze i adresacie udostępnione przez nadawcę przekazu lub użytkownika oraz dane dotyczące kierowania, czasu trwania, daty lub objętości przekazu, zastosowanego protokołu, lokalizacji urządzenia końcowego nadawcy lub odbiorcy, sieci z której przekaz pochodzi lub do której została przesłana, może również dotyczyć formatu w jakim jest informacja w sieci. Dane o lokalizacji inne niż dane transmisyjne – wykraczają poza to, co jest konieczne dla celów telekomunikacyjnych i mogą być wykorzystywane do świadczenia usług o wartości dodanej. Mogą dotyczyć szerokości oraz długości geograficznej oraz wysokości końcowego urządzenia użytkownika, kierunku transmisji, szczegółowej informacji o lokalizacji, identyfikacji komórki sieciowej.

Art. 14 i 15 preambuły do dyrektywy 2002/58/WE z dnia 12 lipca 2002 w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej. Dz. Urz. WE L 2002/201, s. 37.

nia usług dodatkowych, dostawca może przetwarzać dane w zakresie i przez okres czasu niezbędny dla tego typu usług. Użytkownicy (abonenci) powinni mieć prawo wycofania swojej zgody na przetwarzanie danych transmisyjnych w dowolnym momencie. Przetwarzaniem danych mogą zajmować się wyłącznie osoby działające z upoważnienia dostawców, zajmujące się naliczaniem opłat, zarządzaniem transmisją, marketingiem, wykrywaniem oszustw[55]. Dostawcy publicznych usług łączności elektronicznej powinni udzielać swoim klientom wszelkich informacji o istniejących w danej sieci sposobach identyfikacji połączeń. Pozwoli to abonentom na świadome dokonanie wyboru dotyczącego wariantu ochrony prywatności. Powinni również zaoferować możliwość jednorazowego zablokowania prezentacji własnego numeru, jak również możliwość blokowania prezentacji identyfikacji numerów połączeń przychodzących. W sytuacji, gdy numer wywołujący może zostać zidentyfikowany, abonent musi mieć prawo odrzucenia (w prosty sposób) rozmów przychodzących[56].

Państwa członkowskie zostały zobowiązane do zapewnienia tam, gdzie oferowana jest identyfikacja numerów (wywołującego/wywoływanego), publicznej informacji o takim fakcie oraz do zapewnienia przejrzystych procedur nadzoru nad działalnością dostawcy usług. Ponieważ spisy abonentów są publicznie dostępne, prawo do prywatności osób fizycznych i uzasadniony interes osób prawnych wymagają tego, aby abonenci mieli prawo decydowania czy i ewentualnie jakie dane osobowe zostaną opublikowane. Dyrektywa Parlamentu Europejskiego i Rady z 12 lipca 2002 wprowadza więc pewne obowiązki. Przede wszystkim abonenci muszą być informowani (bez dodatkowych opłat i zanim ich dane zostaną umieszczone w spisie) o celu opracowania wykazu abonentów. Ewentualna korekta lub usunięcie danych powinno być wolne od opłat. W przypadku, gdy dane mogą być przesłane do osób (stron) trzecich, abonent powinien być powiadomiony o takiej możliwości. Jeśli dane osobowe mają być wykorzystane dla innych celów, niż te dla których zostały zebrane, wówczas abonent musi wyrazić nową zgodę.

Wiele emocji budzi kwestia zatrzymywania przez usługodawców danych o ruchu w sieciach telekomunikacyjnych rzekomo dla celów zapobiegania, dochodzenia, wykrywania i ścigania przestępstw (tzw. retencja danych). Zwolennicy gromadzenia i archiwizowania danych uważają, że jest to konieczne dla zapewnienia bezpieczeństwa publicznego w sytuacji globalnego zagrożenia terroryzmem,

---

[55] W. Gromski, J. Kolasa, A. Kozłowski, K. Wójtowicz, *Europejskie i polskie prawo telekomunikacyjne*, Warszawa 2004, s. 163–181.

[56] Abonenci powinni być chronieni przed otrzymywaniem niezamówionych marketingiem, spamem czy niechcianymi sms-ami, dlatego też państwo powinno zakazać tego typu bezpłatnych praktyk. Podjęcia takich kroków wymaga dyrektywa 99/5/WE Parlamentu Europejskiego i Rady z dnia 9 marca 1999 w sprawie urządzeń radiowych i urządzeń końcowych łączności elektronicznej oraz wzajemnego rozpoznawania ich zgodności. Dz. Urz. WE L 1999/91, s. 10.

natomiast przeciwnicy retencji zauważają, że jest to działanie stanowiące głęboką ingerencję w sferę praw i wolności człowieka. W związku z zaistniałą sytuacją 15 marca 2006 została wydana Dyrektywa Parlamentu Europejskiego i Rady 2006/24/WE w sprawie zatrzymania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE[57].

Dyrektywa Parlamentu Europejskiego i Rady z 15 marca 2006 nałożyła na państwa członkowskie obowiązek wprowadzenia do ustawodawstwa wewnętrznego rozwiązań zapewniających zatrzymywanie danych przez dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznej sieci łączności w trakcie świadczenia usług. Określiła w art. 5 jakie kategorie danych mają być gromadzone. Dane podzielono na grupy:

1) niezbędne do ustalenia źródła połączenia;
2) niezbędne do ustalenia odbiorcy połączenia;
3) niezbędne do określenia daty, godziny i czasu trwania połączenia;
4) niezbędne do określenia rodzaju połączenia;
5) niezbędne do określenia narzędzia komunikacji;
6) niezbędne do identyfikacji lokalizacji urządzenia.

Ustalono także, że dane mogą być gromadzone i przetrzymywane przez okres nie krótszy niż 6 miesięcy, i nie dłuższy niż 2 lata oraz sprecyzowano wymogi dotyczące zabezpieczenia tych danych.

Wyrokiem z dnia 8 kwietnia 2014 TS UE orzekł nieważność dyrektywy 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającą dyrektywę 2002/58/WE. Trybunał Sprawiedliwości UE uznał, że nakładając obowiązek zatrzymywania danych i umożliwiając dostęp do nich właściwym organom krajowym, dyrektywa ingeruje w sposób szczególnie poważny w prawa podstawowe do poszanowania życia społecznego i do ochrony danych osobowych. To, że dane są zatrzymywane a potem wykorzystywane danych jest dokonywane bez informowania o tym abonenta i zarejestrowanego użytkownika, może wywołać u zainteresowanych poczucie, iż ich życie prywatne podlega stałemu nadzorowi.

---

[57] Zmiana w dyrektywie 2002/58/WE miała na celu zharmonizowanie obydwu dyrektyw i polegała na dodaniu art. 15 ust. 1a. Artykuł 11 Zmiana dyrektywy 2002/58/WE. W art. 15 dyrektywy 2002/58/WE dodaje się ustęp w następującym brzmieniu: 1a. Ustępu 1 nie stosuje się do danych, których zatrzymywanie jest wyraźnie wymagane na mocy dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 w sprawie zatrzymywania danych wygenerowanych lub przetworzonych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności dla celów określonych w art. 1 ust. 1 tej dyrektywy. Dz. Urz. WE L 2006/105, s. 54.

Trybunał Sprawiedliwości UE stwierdził jednak, że przewidziane dyrektywą zatrzymywanie (retencja) danych nie narusza zasadniczej treści praw podstawowych do poszanowania życia prywatnego i do ochrony danych osobowych. Dyrektywa Parlamentu Europejskiego i Rady z 15 marca 2006 nie pozwala bowiem na zapoznawanie się z treścią komunikatów elektronicznych i stanowi, że dostawcy usług lub sieci powinni przestrzegać określonych zasad ochrony i bezpieczeństwa danych. Zatrzymanie danych w celu ich ewentualnego udostępnienia właściwym organom krajowym rzeczywiście odpowiada celowi w postaci interesu ogólnego, jakim jest zwalczanie poważnej przestępczości, a także – ostatecznie – bezpieczeństwo publiczne.

Mimo to, zdaniem TS UE, przyjmując dyrektywę w sprawie zatrzymywania danych, prawodawca UE przekroczył granice, które wyznacza poszanowanie zasady proporcjonalności ponieważ:

1) obejmując ogólnie wszystkie jednostki, środki łączności elektronicznej i dane o ruchu, dyrektywa nie przewiduje żadnego zróżnicowania w zależności od celu dotyczącego zwalczania poważnych przestępstw;

2) Dyrektywa nie przewiduje też żadnego obiektywnego kryterium gwarantującego, że właściwe organy krajowe będą miały dostęp do danych wyłącznie po to, by zapobiegać, wykrywać i ścigać przestępstwa, które mogą być uważane za wystarczająco poważne, by uzasadnić taką ingerencję w omawiane prawa podstawowe. Przeciwnie, dyrektywa ogranicza się do odesłania w sposób ogólny do pojęcia „poważnych przestępstw", które każde państwo członkowskie definiuje w prawie krajowym;

3) nie przewiduje również materialnych i proceduralnych przesłanek dostępu właściwych krajowych organów do danych podlegających retencji. Dostęp do danych nie jest w szczególności podporządkowany uprzedniej kontroli sądu lub niezależnego organu administracyjnego.

4) Dyrektywa przewiduje okres co najmniej 6 miesięcy na retencję danych, ale nie przeprowadza jakiegokolwiek rozróżnienia między kategoriami danych w zależności od zainteresowanych osób lub ewentualnej użyteczności danych w stosunku do zakładanego celu. Ponadto okres ten wynosi od co najmniej 6 miesięcy do co najwyżej 24 miesięcy, przy czym dyrektywa nie precyzuje obiektywnych kryteriów, na podstawie których należy ustalić okres retencji, by zagwarantować jej ograniczenie do tego co ściśle niezbędne;

5) nie gwarantuje nieodwracalnego zniszczenia danych po upływie ich okresu zatrzymania;

6) Dyrektywa nie przewiduje wystarczających gwarancji skutecznej ochrony danych przed niebezpieczeństwem nadużycia oraz przed jakimkolwiek dostępem do danych i ich wykorzystywaniem w sposób niedozwolony;

7) Dyrektywa nie nakłada obowiązku, by dane były zatrzymywane na obszarze Unii.

Obecnie trwa analiza wpływu orzeczenia na prawo krajowe w zakresie retencji danych i prawa właściwych organów krajowych do dostępu do takich danych[58].

Karta Praw Podstawowych Unii Europejskiej

Karta Praw Podstawowych została proklamowana przez Parlament Europejski, Radę i Komisję na szczycie w Nicei w 2000 i ma charakter porozumienia międzyinstytucjonalnego i początkowo miała sporny charakter[59]. Nie obowiązywała w znaczeniu prawnym, ale wywoływała skutki prawne[60]. Celem KPP miało być uwidocznienie praw, jakie posiadają mieszkańcy państw członkowskich Unii Europejskiej. Powtarza prawa zawarte w innych dokumentach (oraz aktach prawnych)[61]. Nie ustanawia żadnego nowego uprawnienia ani zadania dla WE

---

[58] Trybunał Sprawiedliwości UE rozpatrując sprawę o sygnaturze C- 293/12 musiał odpowiedzieć m.in. na pytania: czy dyrektywa 2006/24/WE jest zgodna z prawem do poszanowania życia prywatnego określonym w art. 7 Karty praw podstawowych Unii Europejskiej i art. 8 EKPC?; czy dyrektywa 2006/24/WE jest zgodna z prawem do ochrony danych osobowych określonym w art. 8 karty? oraz czy dyrektywa 2006/24/WE jest zgodna z prawem do wolności wypowiedzi określonym w art. 11 karty i art. 10 EKPC?

Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 8 kwietnia 2014, C-293/12 i C-594/12, <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=PL>, dostęp: 4 września 2014.

[59] Przeciwnicy nadania Karcie charakteru prawnie wiążącego uważali, że mogłoby to doprowadzić do stworzenia w ramach UE „elitarnego klubu", w którym funkcjonowałyby wyższe standardy praw podstawowych (ochrony danych osobowych) niż w systemie Rady Europy. Zob. więcej: J. Jaskiernia, *Karta Praw Podstawowych Unii Europejskiej a Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności – konflikt czy komplementarność?*, [w:] *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, pod red. A. Wróbla, Warszawa 2009, s. 163 i nast.

[60] Tekst Karty był gotowy już na przełomie września i października 2000 Został zatwierdzony nieformalnie na szczycie Rady Europejskiej 13–14 października w Biarritz, jednak uroczyście proklamowano Kartę 7 grudnia 2000, w Nicei. Szczyt Rady Europejskiej w Nicei uznał Kartę za „deklarację moralności europejskiej".

I. C. Kamiński, *Unia Europejska. Podstawowe akty prawne*, Warszawa 2005, s. 245. Andrzej Wróbel uważa, że [przed wejściem w życie Traktatu z Lizbony] „sądy unijne przyjmowały zgodnie, że wprawdzie „karta nie stanowi wiążącego aktu prawnego", to jednak: 1)prawodawca wspólnotowy uznaje jej wagę , „potwierdzając w motywie drugim dyrektywy, że dyrektywa ta przestrzega zasad uznanych nie tylko przez art. 8 EKPC, lecz również przez Kartę" […]; 2) jako źródło odniesień zawiera informacje o prawach podstawowych zagwarantowanych w prawie wspólnotowym lub prawa te potwierdza […]; 3) ma znaczenie w procesie wykładni prawa wspólnotowego […]; 4) potwierdza istnienie praw podstawowych uznanych dotychczas za zasady ogólne prawa unijnego."

A. Wróbel, *Wprowadzenie do Karty Praw Podstawowych UE*, [w:] *Karta Praw Podstawowych UE. Komentarz*, pod red. A. Wróbla, Warszawa 2013, s. 4–5.

[61] Z treści art. 52 ust. 2 karty wynika, że prawa uznane w Karcie, które wynikają z Traktatów wspólnotowych lub Traktatu o Unii Europejskiej, są wykonywane na warunkach oraz w granicach określonych przez te traktaty. Ustęp 3 art. 52 odnosi się do praw przewidzianych w Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności. Stanowi, że w sytuacji gdy Karta przewiduje takie same prawa co Konwencja, to znaczenie i zakres tych praw są takie same. Taki zapis miał zapobiegać niepotrzebnemu dublowaniu zakresu ochrony praw i wolności i hierarchizacji instrumentów ochrony praw człowieka.

lub UE. Nie konstruuje odrębnego mechanizmu służącego ochronie praw człowieka. W jednym dokumencie zebrano prawa ekonomiczne, socjalne, cywilne i polityczne, choć nie nadano im równej rangi. Niektóre z praw przysługują wyłącznie obywatelom UE, a niektóre przysługują każdemu, wobec kogo stosowane jest prawo Unii/Wspólnot. Karta Praw Podstawowych pełni istotną rolę w procesie wykładni norm prawa wspólnotowego. Do postanowień KPP nawiązują rzecznicy generalni (np. Rzecznik Praw Obywatelskich) w swoich opiniach przedkładanych TS UE. Do KPP odniósł się także w swym orzeczeniu sąd pierwszej instancji[62]. Zgodnie z przewidywaniami prof. Leszka Wiśniewskiego, KPP początkowo nie została włączona do Traktatu o Unii Europejskiej w randze prawa pierwotnego, ale ma taką samą moc prawną jak Traktaty[63]. Aby bowiem należycie funkcjonować, KPP musi być wkomponowana do demokratycznych zasad ustrojowych gwarantujących trwałość i realność zapisanego w niej katalogu wolności i praw[64]. W praktyce, od wejścia w życie Traktatu z Lizbony, KPP stanowi jeden z trzech filarów praw podstawowych UE. Ponadto prawa podstawowe, zagwarantowane w europejskiej konwencji o ochronie praw człowieka i podstawowych wolności oraz wynikające z tradycji konstytucyjnych wspólnych Państwom członkowskim, stanowią część prawa UE jako zasady ogólne prawa.

Na szczególną uwagę zasługują art. 7 i 8 KPP. Artykuł 7 gwarantuje każdemu prawo do poszanowania swojego życia prywatnego i rodzinnego, mieszkania i komunikowania, zaś art. 8 odnosi się do ochrony danych osobowych. Każdemu zapewnia się prawo do ochrony dotyczących go danych osobowych[65]. Dopuszczalne jest rzetelne przetwarzanie danych jedynie w określonych celach i za

---

[62] Więcej: K. Wójtowicz, *Ochrona prawa człowieka w Unii Europejskiej*, [w:] *System ochrony praw człowieka*, B. Banaszak, A. Bisztyga, K. Complak, M. Jabłoński, R. Wieruszewski, K. Wójtowicz, Kraków 2005.

[63] Karta Praw Podstawowych ogłoszona w 2007 ma taką samą moc jak Traktaty (o UE i funkcjonowaniu UE). Zgodnie z art. 6 ust. 1 Traktatu o Unii Europejskiej; „Unia uznaje prawa, wolności i zasady określone w Karcie praw podstawowych Unii Europejskiej z 7 grudnia 2000 r., w brzmieniu dostosowanym 12 grudnia 2007 r. w Strasburgu, która ma taką samą moc prawną jak Traktaty". Dz. Urz. UE C 2010/83, s. 19.

Karta Praw Podstawowych stała się faktycznie częścią prawa pierwotnego z chwilą wejścia w życie Traktatu z Lizbony, tj. 1 grudnia 2009.

[64] L. Wiśniewski, *Karta Praw Podstawowych Unii Europejskiej a konstytucyjny katalog praw człowieka*, [w:] *Sześć lat Konstytucji Rzeczypospolitej Polskiej. Doświadczenia i inspiracje*, Warszawa 2003, s. 316–323. A. Jackiewicz, *Karta Praw Podstawowych Unii Europejskiej (uwagi konstytucyjnoprawne)*, „Państwo i Prawo" 2002, nr 1, s. 67–78.

[65] Czyli tzw. prawo „do bycia pozostawionym w spokoju". Pojawienie się automatycznego przetwarzania danych spowodowało wzrost prawdopodobieństwa naruszenia prywatności. Więcej: J. L. Piñar Mañas, *The fundamental right to personal data protection, essential content and current challanges (Fundamentalne prawo do ochrony danych osobowych, jego istota i wiążące się z nim wyzwania)*, [w:] *Ochrona danych osobowych wczoraj, dziś, jutro*, Warszawa 2006, s. 337–338 (347–348).

zgodą osoby (której dane dotyczą) albo w innych uzasadnionych przypadkach, jeśli jest to przewidziane przez prawo. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i do ich sprostowania. Przestrzeganie tych zasad kontroluje niezależna instytucja – EIOD[66].

---

[66] Dz. Urz. UE C 2010, nr 83, s. 393. Europejski Inspektor Ochrony Danych jest organem powołanym na podstawie Rozporządzenia (WE) Nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych. Jest odpowiedzialny za zapewnienie, że podstawowe prawa i wolności osób fizycznych, w szczególności prawo do prywatności są respektowane przez instytucje i organy wspólnotowe w odniesieniu do przetwarzania danych osobowych. Powoływany jest na okres pięciu lat, na podstawie listy ustalonej przez Komisję po ogłoszeniu publicznego naboru dla kandydatów. W tej samej procedurze i na taki sam okres powoływany jest Zastępca Europejskiego Inspektora Ochrony Danych (od 1 stycznia 2015 roku będzie to dr Wojciech Wiewiórowski). Wybór dokonywany jest spośród osób, których niezależność jest niekwestionowana i o których wiadomo, że mają doświadczenie i umiejętności wymagane do spełniania obowiązków Europejskiego Inspektora Ochrony Danych. Po upływie pięcioletniej kadencji ta sama osoba może zostać ponownie wybrana na stanowisko Europejskiego Inspektora Ochrony Danych. Europejski Inspektor Ochrony Danych wykonuje swoje obowiązki w sposób całkowicie niezależny. Powinien powstrzymać się również od wszelkich czynności niezgodnych ze swoimi obowiązkami. Podczas swojej kadencji nie może wykonywać żadnej innej zarobkowej lub niezarobkowej działalności zawodowej.

Do zadań Europejskiego Inspektora Ochrony Danych w szczególności należy:

- rozpatrywanie skarg oraz informowanie osoby, której dane dotyczą o wyniku postępowania;
- przeprowadzanie dochodzeń zarówno z własnej inicjatywy, jak i na podstawie skarg oraz informowanie osób, których dane dotyczą, o ich wyniku;
- monitorowanie i zapewnianie stosowania przepisów Rozporządzenia i każdego innego aktu wspólnotowego odnoszącego się do ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucję lub organ Wspólnoty, z wyjątkiem Trybunału Sprawiedliwości Wspólnot Europejskich działającego z mocy prawa;
- doradztwo wszystkim instytucjom i organom wspólnotowym, we wszystkich kwestiach dotyczących przetwarzania danych osobowych, w szczególności przed przyjęciem przepisów wewnętrznych związanych z ochroną podstawowych praw i wolności w odniesieniu do przetwarzania danych osobowych;
- monitorowanie rozwoju odpowiednich dziedzin, o ile ma on wpływ na ochronę danych osobowych, w szczególności rozwój technologii informatycznych i telekomunikacyjnych;
- współpraca z krajowymi organami nadzoru, do których odnosi się art. 28 dyrektywy 95/46/WE w krajach, do których ta dyrektywa ma zastosowanie.
- współpraca z organami nadzoru w dziedzinie ochrony danych ustanowionymi przez tytuł VI Traktatu o Unii Europejskiej, w szczególności mając na względzie poprawę spójności i zastosowania reguł i procedur;
- uczestniczenie w działalności grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, o którym mówi art. 29 dyrektywy 95/46/WE;
- prowadzenie rejestru operacji przetwarzania, o których został powiadomiony na mocy art. 27 ust. 2 Rozporządzenia i które zostały zarejestrowane zgodnie z art. 27 ust. 5 Rozporządzenia oraz zapewnia metody dostępu do rejestrów prowadzonych przez rzeczników ochrony danych na mocy art. 26 Rozporządzenia;
- przeprowadzanie wstępnych kontroli przetwarzania, o których został powiadomiony;
- składanie rocznego sprawozdania ze swojej działalności Parlamentowi Europejskiemu, Radzie i Komisji z jednoczesną jego publikacją;

Prawo do prywatności (i ochrony danych osobowych) nie jest prawem absolutnym i podlega ograniczeniom przewidzianym w art. 52 KPP. Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie musi być wyraźnie określone w prawie i nie może wypaczać istoty tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności ograniczenia te mogą być wprowadzane tylko wtedy, gdy są konieczne i rzeczywiście służą celom publicznym uznanym przez UE, albo są niezbędne do ochrony praw i wolności innych osób.

Kilkakrotnie do KPP nawiązywał polski TS UE. W jednej ze spraw TK zwrócił uwagę, że KPP, choć została przyjęta przez szefów rządów państw UE, to nie została włączona do Traktatu Nicejskiego i orzekanie w sprawie zgodności z nią norm ustawowych przez TK jest niedopuszczalne[67]. Również SN kilka razy orzekał odnosząc się do KPP. W przypadku orzeczeń SN zasadą jest, że na Kartę powołują się strony, a sąd co najwyżej się do niej odnosi. Można tutaj przywołać postanowienie z dnia 8 czerwca 2004 (sygn. akt II KZ 27/04), w którym SN stwierdził, iż chybione jest powołanie się (w zażaleniu) na KPP i jej art. 8 jako *sui generis* wzorzec kontrolny w stosunku do przepisów polskiego kodeksu postępowania karnego oraz wykazywanie nadrzędności prawa wspólnotowego nad prawem wewnętrznym i ściśle powiązaną z nią zasadę bezpośredniego skutku tego prawa. Takie podejście do sprawy miałoby znaczenie, gdyby KPP była źródłem prawa (czyli ratyfikowaną umową międzynarodową albo jej częścią)[68].

- doradzanie osobom, których dane dotyczą, w kwestii korzystania z ich praw;
- przekazywanie spraw administratorom w przypadku domniemanego naruszenia przepisów rządzących przetwarzaniem danych osobowych i w miarę potrzeb, proponowanie środków prawnych dla usunięcia naruszeń i dla poprawy ochrony osób, których dane dotyczą;
- nakazywanie, aby przyjęte zostały wnioski o skorzystaniu z pewnych praw w odniesieniu do danych, gdy takie wnioski zostały odrzucone z naruszeniem art. 13-19 Rozporządzenia;
- ostrzeganie lub upominanie administratorów danych;
- nakazywanie poprawienia, zablokowania, wykasowania lub zniszczenia wszystkich danych, jeżeli były one przetwarzane z naruszeniem przepisów rządzących przetwarzaniem danych osobowych oraz powiadomienie o takich działaniach osób trzecich, którym dane zostały ujawnione;
- nakładanie czasowego lub całkowitego zakazu przetwarzania;
- przekazywanie sprawy odpowiedniej instytucji lub organowi Wspólnoty i jeśli to konieczne Parlamentowi Europejskiemu, Radzie i Komisji;
- przekazywanie sprawy Trybunałowi Sprawiedliwości Wspólnot Europejskich zgodnie z warunkami przewidzianymi w Traktacie;
- interweniowanie w sprawach wniesionych przed Trybunał Sprawiedliwości Wspólnot Europejskich.

[67] K 24/02, K 44/02, K 20/02, P 9/04, K 18/04, SK 30/05. Więcej: M. Zubik, *Karta Praw Podstawowych UE a polski Trybunał Konstytucyjny*, [w:] *5 lat Karty Praw Podstawowych UE. Materiały pokonferencyjne*, pod red. A. Gubrynowicza, Warszawa 2006, s. 39–48.

[68] Postanowienie SN z dnia 8 czerwca 2004, II KZ 27/04, LEX nr 121650. Interesujący jest również wyrok z dnia 17 marca 2005, III PK 83/04, w którym Sąd Najwyższy stwierdził, że przepisy Karty nie mogą być skutecznie powoływane przed sądami krajowymi jako samoistne źródło praw jednostki lub jako wzorzec oceny zgodności prawa krajowego z zawartymi w Karcie prawami. Mimo to, zgodnie z opiniami rzeczników generalnych ETS stanowi punkt wyjścia do poznania

Konwencja z Schengen

W 1985 podpisano Układ z Schengen[69], a 19 kwietnia 1990 Belgia, Holandia, Luksemburg, Francja, Hiszpania, Portugalia, RFN oraz Włochy podpisały Konwencję Wykonawczą do Układu z Schengen. Wejście w życie postanowień zawartych w Układzie i Konwencji nastąpiło 26 marca 1995. Podstawowym celem postanowień było zniesienie kontroli granicznej między państwami, które je przyjęły i skoncentrowanie się na zewnętrznych granicach „terytorium Schengen" oraz próba stworzenia międzynarodowej sieci bezpieczeństwa[70]. Konwencja z Schengen nie zamierzała jednak ujednolicać zasad ochrony danych osobowych w krajach członkowskich. Wprowadzono SIS, który jest skomputeryzowanym systemem informacyjnym przeznaczonym dla kontroli granicznej, celnej i policyjnej[71], i który miał zapewnić skuteczną realizację celów Konwencji z Schengen. Schengen Information System składa się z wielu krajowych systemów informacyjnych, które są wzajemnie dostępne. Część centralna C-SIS (centralny[72]) znajduje się w Strasburgu, a części N-SIS w każdym państwie

---

podstawowych praw gwarantowanych przez wspólnotowy porządek prawny. Więcej: A. Barbasiewicz, *Europejska Karta Praw Podstawowych w orzecznictwie polskiego Sądu Najwyższego*, [w:] *5 lat Karty Praw Podstawowych UE. Materiały pokonferencyjne*, pod red. A. Gubrynowicza, Warszawa 2006, s. 49–54.

[69] 14 czerwca 1985 w Schengen, małym miasteczku przygranicznym w Luksemburgu podpisano Porozumienie Schengeńskie w Sprawie Stopniowego Znoszenia Kontroli Granicznej na Wspólnych Granicach. Mimo, że Porozumienie jako całość weszło w życie 1 lipca 1987, to już 15 czerwca 1985 ograniczono kontrolę graniczną samochodów osobowych tylko do oglądu zewnętrznego, bez potrzeby zatrzymywania. S. M. Amin, J. Justyński, *Instytucje i porządek prawny Unii Europejskiej na tle tekstów prawnych oraz orzecznictwa Europejskiego Trybunału Sprawiedliwości*, Toruń 1999, s. 156.

[70] Monica den Boer twierdzi, że cele Układu z Schengen są „papierowym tygrysem", a najlepszym przykładem jest niespójna polityka prowadzona np. w kwestii zwalczania narkomanii. Holandię traktuje się jako państwo narkomanów na terytorium Europy i nazywa „eldorado narkotykowym". Wskazuje się, że np. kilogram haszyszu w Holandii jest nawet pięciokrotnie tańszy niż w Niemczech, a po wejściu w życie Układu z Schengen dużo łatwiej jest przekroczyć granicę. Więcej: M. Den Boer, *Międzynarodowe uprawnienia policyjne przyznane policji przez Układ z Schengen*, [w:]*Układ z Schengen. Współpraca policji i organów sprawiedliwości po Maastricht*, pod red. J. Beczały, Łódź 1998, s. 51–52.

[71] Zgodnie z artykułem 101 Konwencji Wykonawczej do Układu z Schengen dostęp do danych wprowadzanych do SIS oraz prawo do ich bezpośredniego przeglądania posiadają wyłącznie organy: kontroli granicznej, policyjnej i celnej oraz w określonym zakresie organy odpowiedzialne za rozpatrywanie wniosków wizowych oraz organy odpowiedzialne za wydawanie dokumentów pobytowych. Użytkownicy mogą przeglądać tylko te dane, które są im niezbędne do wykonywania ich zadań. Każda z Umawiających się Stron została zobowiązana do przedstawienia Komitetowi Wykonawczemu wykazu właściwych władz, które są upoważnione do bezpośredniego przeglądania danych. Dz. Urz. WE L 2000/ 239, s. 19.

[72] Zgodnie z art. 95 i 115 Konwencji odpowiedzialność techniczną za C-SIS ponosi Francja.

[73] Do SIS wprowadzane są także informacje o skradzionych: dokumentach wystawionych in blanco lub na określone nazwisko, broni palnej, banknotach czy przywłaszczonych lub zaginionych pojazdach. Dane osobowe wprowadzane do SIS dla celów śledzenia osób są przechowywane jedynie

członkowskim. Wszystkie N-SIS-y mają taką samą treść, gdyż przesyłane są do nich informacje z C-SIS-u.

W ramach tego systemu gromadzone są dane osobowe o:

1) osobach, wobec których wydano postanowienie o areszcie w celu ekstradycji;

2) cudzoziemcach, którym odmówiono wjazdu do jednego z krajów sygnatariuszy Układu z powodu zagrożenia porządku lub bezpieczeństwa publicznego;

3) osobach zaginionych lub przetrzymywanych dla własnego bezpieczeństwa i na podstawie decyzji sądu, w bezpiecznym miejscu;

4) osobach, których miejsce pobytu jest nieznane, a mają obowiązek stawić się przed sądem w sprawach karnych;

5) osobach, wobec których prowadzona jest obserwacja niejawna[73].

Dane osobowe dotyczące tych kategorii osób mogą zawierać co najwyżej informacje o:

1) imieniu i nazwisku;

2) pierwszej literze drugiego imienia;

3) szczególnych i widocznych cechach fizycznych;

4) dacie i miejscu urodzenia;

5) płci;

6) narodowości;

7) możliwości posiadania broni lub posiadaniu gwałtownego usposobienia (charakteru);

8) przyczynie sporządzenia raportu dotyczącego tej osoby oraz

9) czynnościach, jakie powinny być podjęte w stosunku do danej osoby[74].

Zabronione jest umieszczanie w systemie danych osobowych ujawniających pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne, jak również dane osobowe dotyczące stanu zdrowia lub życia seksualnego. Ponadto niedozwolone jest wykorzystywanie danych do innych celów, niż zostały zebrane (np. do celów administracyjnych)[75].

---

przez okres konieczny dla osiągnięcia celów, dla których zostały dostarczone. Przegląd takich danych odbywa się najpóźniej w trzy lata po ich wprowadzeniu. Dane osobowe inne niż dla celów śledzenia są przechowywane przez maksymalny okres 10 lat, dane na temat wydanych dokumentów tożsamości i podejrzanych banknotów przez maksymalny okres pięciu lat, a dane dotyczące pojazdów silnikowych, przyczep, i przyczep mieszkalnych przez maksymalny okres 3 lat. Dane, które zostały skreślone są przechowywane przez okres jednego roku w jednostce centralnej. Po upływie tego czasu dane powinny być zniszczone. Artykuł 112-113.Konwencji wykonawczej do układu z Schengen.

[74] Artykuł 94 Konwencji Wykonawczej do Układu z Schengen określa jakie kategorie danych umieszcza się w SIS-ie. Konwencja wykonawcza do Układu z Schengen z dnia 14 czerwca 1985, Dz. Urz. WE L 2000/239, s.19.

[75] Więcej: J. Justyński, *Acquis communautaire a acquis Schengen*, [w:] *Unia Europejska – wyzwanie dla polskiej Policji*, pod red. W. Pływaczewskiego, G. Kędzierskiej, P. Bogdalskiego, Szczytno 2003, s. 14–26. K. Napierała, *Prawne aspekty ochrony danych osobowych przetwarzanych w systemach informatycznych*, Warszawa 1997.

Każda osoba ma prawo domagać się:

1) informacji w każdym kraju grupy Schengen, czy dane jej dotyczące znajdują się w systemie SIS (art. 109 oraz art. 114);

2) dostępu do danych jej dotyczących zawartych w systemie SIS, na warunkach określonych w krajowej ustawie o ochronie danych osobowych (art. 109);

3) sprostowania lub usunięcia nieprawdziwych lub wprowadzonych niezgodnie z zasadami danych (art. 110);

4) odszkodowania (w razie niesprostowania lub nieusunięcia danych), w związku z wprowadzonym do SIS raportem na jej temat (art. 111 oraz art. 116)[76].

Konwencja z Schengen reguluje także możliwość wymiany danych osobowych pomiędzy krajami członkowskimi w odniesieniu do: udzielania azylu, międzynarodowej współpracy policji oraz wzajemnego udostępniania danych w związku z postępowaniem karnym.

Państwa–Strony Konwencji zostały zobowiązane do wyznaczenia niezależnego organu nadzorczego odpowiedzialnego za kontrolę, czy przetwarzanie i wykorzystywanie danych wprowadzanych do SIS nie narusza praw osób, których dane te dotyczą. Aby zapewnić należytą ochronę, państwa powinny przyjąć środki niezbędne w celu:

1) kontroli dostępu osób nieupoważnionych do sprzętu (służącego do przetwarzania danych osobowych);

2) zapobiegania nieupoważnionemu czytaniu, kopiowaniu, modyfikacji lub usuwaniu nośników danych;

3) kontroli wprowadzanych danych;

4) zapobiegania wykorzystaniu zautomatyzowanych systemów przetwarzania danych przez osoby nieupoważnione i wykorzystania sprzętu do przekazywania danych;

5) zapewnienia, że dostęp do danych osobowych posiadają jedynie osoby upoważnione;

---

[76] Konwencja z Schengen weszła w życie w 1995, jako umowa międzyrządowa. SIS, (jako część konwencji z Schengen) został następnie włączony do porządku prawnego UE na mocy Traktatu Amsterdamskiego. Z chwilą wejścia w życie Traktatu z Amsterdamu dorobek Schengen, w tym decyzje Komitetu Wykonawczego utworzonego przez układy z Schengen, które zostały wydane przed tą datą, stosuje się bezzwłocznie do 13 Państw Członkowskich (Belgii, Danii, RFN, Grecji, Hiszpanii, Francji, Włoch, Luksemburga, Holandii, Austrii, Portugalii, Finlandii i Szwecji), bez uszczerbku dla innych postanowień. Radę zastępuje Komitet Wykonawczy. Więcej: *Protokół włączający dorobek Schengen w ramy Unii Europejskiej wraz z załącznikiem Dorobek Schengen*, [w:]*Unia Europejska. Wspólnota Europejska. Zbiór dokumentów*, oprac. E. Wojtaszek-Mik, C. Mik, Kraków 2005, s. 336–341. Obecnie obowiązuje Protokół między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczący włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, Dz. Urz. UE L 2011/160, s. 21.

6) weryfikacji i stwierdzenia jakie dane wysyłane są do poszczególnych organów;

7) weryfikacji i stwierdzenia, kiedy i przez kogo dane osobowe zostały wprowadzone do systemu;

8) zapobiegania nieupoważnionemu czytaniu, kopiowaniu, modyfikacji i usuwaniu danych podczas przekazywania danych osobowych lub podczas przenoszenia nośników danych.

Wszystkie państwa obecnie włączone do SIS przyjęły wymagane środki krajowe dotyczące mechanizmów związanych z korzystaniem z praw przysługujących osobom, których dane dotyczą oraz odpowiedzialności za przetwarzanie danych osobowych oraz kontroli i nadzoru.

Od kilku lat dyskutuje się na temat utworzenia nowego SIS II[77]. SIS II miałby się składać z centralnej bazy danych CS-SIS powiązanej z krajowymi punktami dostępu określonymi przez każde państwo członkowskie NI-SIS. Państwa członkowskie będą przekazywać do SIS II dane dotyczące osób poszukiwanych w celu aresztowania, wydania lub ekstradycji, w celu przeprowadzenia procedur sądowych osób mających być umieszczone pod nadzorem lub wymagających szczególnych kontroli, osób którym należy odmówić wjazdu (na granicy zewnętrznej) oraz przedmiotów zagubionych lub ukradzionych. Nowością jest poszerzenie katalogu podmiotów mających dostęp do SIS (Europol, Eurojust, prokuratorzy krajowi, organy odpowiedzialne za rejestrację pojazdów), wprowadzenie wzajemnych połączeń pomiędzy wpisami, dodanie nowych kategorii danych (w tym biometrycznych, czyli odcisków palców i zdjęć[78]) oraz platforma techniczna dzielona z Systemem Informacji Wizowej. We wszystkich proponowanych aktach prawnych wydłużony jest okres przechowywana danych dla każdego rodzaju wpisu, bez wyjaśnienia powodów. Cel SIS II jest szerszy niż

---

[77] 1 czerwca 2005 Komisja Europejska przedstawiła trzy wnioski dotyczące utworzenia SIS II.

1. Wniosek dotyczący rozporządzenia opartego na tytule IV traktatu WE (wizy, azyl, imigracja oraz swobodny przepływ osób), obejmującego aspekty SIS II należące do I filaru (imigracja) – zwany „wnioskiem dotyczącym decyzji".

2. Wniosek dotyczący decyzji opartej na tytule VI traktatu UE (współpraca policyjna i sądowa w sprawach karnych), obejmująca aspekty SIS II należące do III filaru – zwany „wnioskiem dotyczącym decyzji".

3. Wniosek dotyczący rozporządzenia opartego na tytule V (transport), poświęcony dostępowi organów odpowiedzialnych za rejestrację pojazdów do danych zawartych w SIS.

Więcej: Opinia Grupy Roboczej ds. Ochrony Danych ustanowionej na mocy art. 29 nr 6/2005, przyjęta dnia 25 listopada 2005, 2067/05/PL.

[78] Hasło włączenia do SIS II biometrii pojawiło się w konkluzjach Rady z 26 maja 2003 (Dok. 9808/03), gdzie stwierdzono, iż nowy system musi umożliwiać przechowywanie, przekazywanie i przeszukiwanie danych biometrycznych. Ma to zapewnić niezawodną identyfikację osób, których dotyczy wpis (w bazie). SIS II powinien pozwalać na przetwarzanie danych osób w taki sposób, aby uniknąć błędnej identyfikacji. Więcej: F. Jasiński, *Zagadnienia biometrii w Unii Europejskiej. Materiały Robocze 4(8)/06*, Warszawa 2006, s. 35–42.

obecnego SIS, a jego realizacja ma umożliwić właściwym organom państw członkowskich wymianę informacji do celów kontroli osób i przedmiotów. SIS II dopuszcza przetwarzanie danych biometrycznych. Dostęp do bazy SIS II byłby przyznawany w trzech sytuacjach:

1) dla przeprowadzenia działań przewidzianych we wpisie (organ ma dostęp wyłącznie w celu przeprowadzenia określonych działań);

2) w celu innym niż cel SIS II, lecz pasującym do treści wniosków;

3) w celu innym niż cel SIS II, lecz niesprecyzowanym.

Im ogólniejszy jest cel dostępu, tym ściślejsze powinny być zabezpieczenia. W każdym przypadku dostępu udziela się wyłącznie wtedy, gdy jest on zgodny z ogólnym celem SIS II i spójny z jego podstawą prawną[79]. Prawo do informacji, dostępu do danych, ich poprawienia i usunięcia oraz środki odwoławcze przysługiwałoby każdej osobie. Projekt rozporządzenia nie przewiduje żadnego organu ochrony danych, do którego można by się było odwołać. Wprowadza termin sześćdziesięciu dni na odpowiedź w sprawie wniosku o udostępnienie danych. Każdemu przyznaje się prawo do złożenia odwołania od decyzji o dokonaniu wpisu podjętej przez organ administracyjny lub zwrócenia się z wnioskiem o kontrolę tej decyzji. Prawo dostępu do danych (ich poprawienia czy usunięcia) wykonywane ma być zgodnie z przepisami prawa państwa członkowskiego, przed którym powołano się na to prawo. Wspomina się, że monitorowanie czy przetwarzanie danych osobowych na danym terytorium odbywa się zgodnie z prawem, natomiast nie wspomina się, w jaki sposób należy je zapewnić. Wszystkie projekty wykluczają możliwość interweniowania przez Komisję w operacje przetwarzania danych. Zapewnienie odpowiedniej jakości danych należy do obowiązków państw członkowskich, a zasady nadzoru i kontroli mają być określone w prawie krajowym. W systemie SIS II nie zmieni się organ nadzoru na szczeblu krajowym, bo będzie on nadal sprawowany przez niezależny organ nadzorczy, zmieni się natomiast organ nadzoru na szczeblu centralnym. Wspólny Organ Nadzorczy zostanie zastąpiony przez EIOD. Projekt dopuszcza możliwość tworzenia krajowych kopii danych CS-SIS zamiast umożliwiania bezpośredniego dostępu do CS-SIS[80].

---

[79] Np. wniosek o dostęp do danych o imigracji musi być uzasadniony wspieraniem realizacji polityki związanej z przepływem osób. Należy również uzasadnić potrzebę dostępu do bazy SIS II. Sposób dostępu i warunki wykorzystania danych muszą być precyzyjnie sformułowane i ograniczone.

[80] Wnioski i uwagi EIOD do przedstawionych projektów znaleźć można w Opinii Europejskiego Inspektora Ochrony Danych, w sprawie wniosku dotyczącego decyzji Rady w sprawie utworzenia, działania i wykorzystania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (COM(2005)230 wersja ostateczna); wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie utworzenia, eksploatacji i wykorzystania Systemu Informacyjnego Schengen (SIS II) drugiej generacji (COM(2005)236 wersja ostateczna), oraz wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie dostępu służb odpowiedzialnych w Państwach Członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II) (COM(2005)237 wersja ostateczna) Dz. Urz. WE C 2006/91, s. 38.

Ochrona danych osobowych w orzecznictwie ETS (TS UE)

Orzecznictwo Europejskiego Trybunału Sprawiedliwości w zakresie poszanowania życia prywatnego, rodzinnego, mieszkania i korespondencji nie jest zbyt radykalne. W pierwszej kolejności korzysta z dorobku sądu strasburskiego. Orzecznictwo strasburskie nie wywiera formalnie wpływu na treść rozstrzygnięcia TS UE, jednak często bywa przywoływane w orzeczeniach ETS[81].

Pierwsze orzeczenie, w którym TS UE wyraził pogląd, że ochrona praw człowieka stanowi ogólną zasadę prawa wspólnotowego jest sprawa „maślana" Ericha Staudera. Powód, inwalida wojenny, uznał że władze miejskie naruszyły jego godność (też i prawa człowieka). Przyczyną tej sytuacji była nadprodukcja masła i jego sprzedaż po obniżonej cenie dla wybranych grup osób. Uprawnione osoby musiały się jednak wylegitymować przed sprzedawcą dokumentem tożsamości ujawniającym nazwisko i adres. Stauder uznał za obraźliwe umieszczenie swego nazwiska na „maślanej" kartce. Na jego korzyść świadczył fakt, że taki wymógł nie został jasno i precyzyjnie wyrażony w przepisach wspólnotowych w tłumaczeniach na inne języki. Trybunał Sprawiedliwości UE uznał za obowiązującą wersję bardziej liberalną i przyznał rację Stauderowi[82].

Inną ciekawą sprawą, ze względu na problem dopuszczalności publikacji danych osobowych (w tym danych wrażliwych) w Internecie, jest sprawa szwedzkiej katechetki i wolontariuszki Bodil Lindqvist. Zamieściła ona na własnej stronie internetowej dane osobowe swoich współpracowników (informacje o ich hobby, stanie zdrowia). Nie uzyskała wcześniej ich zgody na publikację tych danych w Internecie (nawet ich nie uprzedziła). Nie powiadomiła też Datainspektionen o funkcjonowaniu strony. Usunęła ją wraz z informacjami, kiedy dowiedziała się o proteście parafian. Mimo to prokurator wszczął przeciwko niej postępowanie o naruszenie (szwedzkiej) ustawy o ochronie danych osobowych. Bodil Lindqvist przyznała się do zarzucanych jej czynów (czyli: przetwarzania danych osobowych w sposób zautomatyzowany bez uprzedniego zgłoszenia tego faktu do Datainspektion; przetwarzania bez zezwolenia danych o stanie zdrowia parafianki; przekazania do państwa trzeciego danych osobowych przetwarzanych bez pozwolenia) ale nie przyznała się do popełnienia przestępstwa. Przez sąd I instancji została skazana na karę grzywny. Wniosła jednak apelację od tego wyroku.

Sąd apelacyjny skierował do ETS siedem pytań dotyczących interpretacji dyrektywy 95/46/WE o ochronie osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych. W odpowiedzi na postawione

---

[81] M. Dybowski, *Prawa fundamentalne w orzecznictwie ETS*, Warszawa 2007, s. 42–45, 118–121.

[82] Z. J. Pietraś, *Prawo wspólnotowe i integracja europejska*, Lublin 2006, s. 99.

pytania ETS stwierdził, iż zamieszczenie na stronie internetowej danych osobowych (imion, nazwisk, numerów telefonów, informacji o stanie zdrowia czy zainteresowaniach) jest działaniem przeprowadzanym automatycznie, a przetwarzanie tych danych nie stanowi wyjątku określonego w art. 3 ust. 2 dyrektywy, ponieważ charytatywne czy religijne działania nie są objęte wyjątkiem. Również przetwarzanie danych na własny użytek nie mieści się w katalogu wyjątków[83]. Ponadto pani Lindqvist naruszyła art. 8 ust. 1 dyrektywy, który m.in. zabrania przetwarzania danych dotyczących zdrowia (w tym przypadku ujawniła informację o uszkodzonej stopie jednej z osób).

Trybunał Sprawiedliwości UE przypomniał, iż celem dyrektywy jest utrzymanie równowagi pomiędzy wolnością przepływu danych a ochroną prywatności, a państwa członkowskie mają pełną swobodę w implementacji postanowień dyrektywy[84].

W doktrynie, w opiniach większości akceptującej to orzeczenie, można znaleźć pewne wątpliwości, kiedy strona internetowa zawierająca dane osobowe spełnia warunki strony „prywatnej", aby mogła być zaliczona do kategorii objętej art. 3 ust. 2. Trybunał Sprawiedliwości UE nie udzielił odpowiedzi, czy mniejszy stopień dostępności może czynić witrynę „prywatną". Wyrok nie określił mechanizmów, które wystarczyłyby do ograniczenia dostępu do strony internetowej, np.: poprzez zastosowanie hasła podczas logowania[85].

W sprawie The Bavarian Lager Co. Ltd przeciwko Komisji WE Sąd I Instancji powołał się na zasadę wyrażoną przez ETPC, że aby odpowiednio wyważyć sprzeczne ze sobą interesy publiczne i prywatne, należy przyznać odpowiednim władzom pewną swobodę działania. Jednak to swobodne uznanie związane jest z istnieniem kontroli sądowej nad nim i jego zakres uzależniony jest od

---

[83] „Art. 3 ust. 2 Niniejsza dyrektywa nie dotyczy przetwarzania danych osobowych: w ramach działalności wykraczającej poza zakres prawa Wspólnoty takiej, o której mowa w rozdziałach V (filar II – wspólna polityka zagraniczna i bezpieczeństwa)i VI (współpraca policyjna i sądowa w sprawach karnych) Traktatu o Unii Europejskiej, oraz w każdym przypadku przetwarzania związanego z bezpieczeństwem publicznym, obronnością, bezpieczeństwem państwa (łącznie ze stanem gospodarki państwa, kiedy przetwarzanie danych dotyczy bezpieczeństwa państwa) oraz z działalnością państwa w dziedzinach prawa karnego, przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze."

Dyrektywa 95/46/WE z dnia 24 października 1995, Dz. Urz. WE L 281/31.

[84] J. Klosek, *European Court establishes broad interpretation of data privacy law*, The Metropolitan Corporate Councel, 2004/03, s. 22. <http://www.goodwinprocter.com/getfile.aspx?filepath=//Files/publications/klosek_j_03_04.pdf>.

[85] Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 6 listopada 2003, C-101/01, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=154144>, dostęp: 4 grudnia 2014.

L. A. Bygrave, *Zapewnienie prywatności w Internecie*, [w:] *Prawo do prywatności – prawo do godności. Międzynarodowa Konferencja Ochrony Prywatności i Danych Osobowych 14–16 września 2004 Wrocław*, Warszawa 2006, s. 232–233.

czynników takich, jak charakter i znaczenie występujących w danej sprawie interesów oraz waga ingerencji. Sama okoliczność, iż dokument zawiera dane osobowe, nie oznacza, że mamy tu do czynienia z prywatnością lub integralnością fizyczną osób, których te dane dotyczą, choć działalność zawodowa nie jest co do zasady wykluczona z pojęcia „prywatności". Sąd uznał, że przy wykazywaniu istnienia ingerencji w prywatność nie ma znaczenia, iż zostały podane do wiadomości dane wrażliwe pracownika. Wystarczy bowiem, że pracodawca podał dane dotyczące dochodów pobieranych przez pracownika lub emeryta do wiadomości osób trzecich. Z drugiej jednak strony, jeśli podanie tych danych do wiadomości nie narusza przewidzianej w art. 4 ust. 1 lit. b) rozporządzenia nr 1049/2001 prawa do ochrony prywatności i integralności osoby fizycznej, odmowa ujawnienia tych danych przez osobę, której one dotyczą, nie może stanąć na przeszkodzie temu ujawnieniu. Publiczny dostęp do dokumentów instytucji stanowi zasadę prawną i możliwość odmowy jest wyjątkiem[86].

Trybunał Sprawiedliwości UE rozpatrując połączone sprawy C-92/09 oraz C-93/09 – Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) przeciwko Krajowi Związkowemu Hesja (orzeczenie z dnia 9 listopada 2010) musiał rozstrzygnąć m.in. kwestię publikowania danych osobowych beneficjentów programów unijnych oraz odpowiedzieć na pytanie, czy publikacja danych

---

[86] W uzasadnieniu do wyroku Sąd Pierwszej Instancji powołał m.in. się na dyrektywę 95/46/WE, rozporządzenie WE nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 o ochronie osób w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, art. 8 EKPC, art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej. W sprawie tej chodziło o ujawnienie danych osobowych uczestników spotkania z dnia 11 października 1996, w którym udział wzięli przedstawiciele Dyrekcji Generalnej ds. rynku wewnętrznego i usług finansowych Komisji, Ministerstwa Handlu i Przemysłu Zjednoczonego Królestwa oraz przedstawiciele związku piwowarów prowadzących działalność na wspólnym rynku. 27 sierpnia skarżąca (The Bavarian Lager Co Ltd., spółka, która chciała importować niemieckie piwo do angielskich pubów)zwróciła się o umożliwienie wzięcia jej udziału w tym spotkaniu, lecz Komisja odmówiła uwzględnienia jej żądania. Sąd stwierdził, że znajdujący się w protokole spotkania wykaz uczestników (o którego udostępnienie występowała strona skarżąca) zawiera dane osobowe w rozumieniu art. 2a lit.a) rozporządzenia nr 45/2001, ponieważ można w nim ustalić tożsamość uczestniczących w tym spotkaniu osób. Sama Komisja wcześniej zauważyła, że osoby obecne na spotkaniu, których nazwisk nie ujawniono, uczestniczyły w nim w charakterze przedstawicieli wcześniej wspomnianych organizacji, a nie z powodów osobistych. W związku z tym ujawnienie ich nazwisk nie może w konkretny i rzeczywisty sposób naruszyć prawa do ochrony prywatności i integralności fizycznej tych osób. Sąd uznał zatem, że Komisja naruszyła prawo, odmawiając ujawnienia danych.

Więcej: Wyrok Sądu Pierwszej Instancji z dnia 8 listopada 2007, T-194/04,

<http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=pl&newform=newform&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurtfp=jurtfp&alldocrec=alldocrec&docj=docj&docor=docor&docop=docop&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoj=docnoj&docnoor=docnoor&typeord=ALL&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&numaff=T-194%2F04&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=&domaine=&mots=&resmax=100&Submit=Szukaj>, dostęp: 30 czerwca 2014.

o otrzymanych środkach jest uzasadniona celem, jakim jest społeczna kontrola ich wydawania. Trybunał uznał, że nieważne są przepisy pozwalające na publikowanie informacji na temat beneficjentów środków pochodzących z EFRG i EFRROW w zakresie, w jakim, w odniesieniu do osób fizycznych będących beneficjentami pomocy z EFRG i EFRROW, przepisy te wymagają publikacji danych osobowych dotyczących każdego beneficjenta, bez wprowadzenia rozróżnienia według odpowiednich kryteriów, takich jak okresy, w których otrzymali tę pomoc, jej częstość czy też rodzaj i wysokość. Zatem wprawdzie w demokratycznym społeczeństwie podatnicy mają prawo do informacji o wykorzystaniu wydatków publicznych, niemniej odpowiednie wyważenie różnych podlegających uwzględnieniu interesów wymagało zweryfikowania przez odpowiednie instytucje, czy publikacja poprzez stronę internetową imiennych danych dotyczących wszystkich zainteresowanych beneficjentów i dokładnych kwot pochodzących z EFRG i EFRROW otrzymanych przez każdego z nich – bez rozróżnienia w zależności od okresu, częstości lub rodzaju i wysokości otrzymanej pomocy – nie jest nieproporcjonalne (nieadekwatne) do realizacji zasadnie zamierzonych celów (w tym przejrzystości wykorzystania środków). Nie można jednak automatycznie przyznać temu celowi pierwszeństwa przed prawem do ochrony danych osobowych, nawet jeżeli w grę wchodzą istotne interesy ekonomiczne[87].

W jednym z najnowszych orzeczeń TS UE musiał rozstrzygnąć konflikt między ochroną danych osobowych (użytkowników Internetu – ISP) a ochroną praw własności intelektualnej twórców (belgijskim stowarzyszeniem autorów, kompozytorów oraz wydawców – SABAM. Orzekł w tej sprawie, że ochrona praw własności intelektualnej nie ma charakteru absolutnego i jest ograniczona koniecznością ochrony innych praw jednostek (nie tylko twórców: autorów czy kompozytorów). System filtrowania nie może stanowić ogólnego nadzoru. W tym przypadku doszło do naruszenia praw użytkowników, tj. ochrony danych osobowych oraz prawa do swobodnego wysyłania oraz otrzymywania informacji w Internecie. System taki, w opinii TS UE, zagrażałaby także swobodzie działalności gospodarczej[88].

---

[87] Więcej: Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 9 listopada 2010, C-92/09 i C-93/09 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=PL&mode=doc&dir=&occ=first&part=1&cid=745649>, dostęp: 7 lipca 2014.

[88] SABAM zażądała przede wszystkim, aby stwierdzono istnienie naruszeń prawa autorskiego w odniesieniu do utworów muzycznych zawartych w jej repertorium – a w szczególności prawa do powielania i prawa do publicznego udostępniania – które to naruszenia wynikają z niedozwolonej wymiany, za pośrednictwem usług świadczonych przez Scarlet, elektronicznych plików muzycznych za pomocą programów „peer-to-peer". Następnie wniosła o nałożenie na Scarlet, pod groźbą okresowej kary pieniężnej, obowiązku doprowadzenia do zaprzestania tych naruszeń poprzez uniemożliwienie lub zablokowanie wszelkich form wysyłania lub otrzymywania przez jej klientów za

Ochrona danych osobowych w instytucjach Unii Europejskiej

Kwestia ochrony danych osobowych w instytucjach UE uregulowana jest w:

1) Rozporządzeniu 2001/45/WE Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych;

2) Decyzja Rady 2004/644/WE z dnia 13 września 2004 ustanawiająca reguły wykonawcze dotyczące rozporządzenia 2001/45/WE.

Rozporządzenie 2001/45/WE Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych. Stawia sobie za cel zapewnienie zarówno efektywnej zgodności z regułami rządzącymi ochroną podstawowych praw i wolności osób fizycznych oraz swobodnego przepływu danych osobowych między państwami członkowskimi a instytucjami i organami wspólnotowymi, jak i między instytucjami i organami wspólnotowymi do celów związanych z wykorzystaniem ich

---

pośrednictwem programów „peer-to-peer" plików zawierających utwory muzyczne bez zezwolenia podmiotów uprawnionych z tytułu praw autorskich. Wreszcie SABAM wystąpiła o przekazanie jej przez Scarlet, pod groźbą okresowej kary pieniężnej, opisu środków, jakie Scarlet podejmie celem wykonania przyszłego orzeczenia. Orzeczeniem z dnia 26 listopada 2004 r. prezes tribunal de premiere instance de Bruxelles stwierdził istnienie zgłoszonych przez SABAM naruszeń prawa autorskiego, jednakże przed wydaniem orzeczenia w przedmiocie wniosku o nakazanie zaprzestania naruszeń wyznaczył biegłego w celu zbadania, czy rozwiązania techniczne zaproponowane przez SABAM mogą być zrealizowane pod względem technicznym, czy umożliwiają filtrowanie wyłącznie bezprawnej wymiany plików elektronicznych i czy istnieją inne środki, za pomocą których można byłoby kontrolować używanie programów „peer-to-peer" oraz określać koszty rozpatrywanych środków. Ekspert stwierdził, że pomimo licznych trudności technicznych wprowadzenie filtrowania i blokady bezprawnej wymiany plików elektronicznych nie jest całkowicie wykluczone. W orzeczeniu z dnia 29 czerwca 2007 r. prezes tribunal de premiere instance de Bruxelles orzekł, że Scarlet ma doprowadzić, pod groźbą okresowej kary pieniężnej, do zaprzestania naruszeń praw autorskich, których istnienie zostało ustalone w orzeczeniu z dnia 26 listopada 2004 r., poprzez uniemożliwienie przesyłania lub odbierania przez jej klientów, w jakiejkolwiek formie, za pomocą programów „peer-to-peer", plików elektronicznych zawierających utwory muzyczne z repertorium SABAM. Od tego orzeczenia Scarlet wniosła apelację do sądu odsyłającego, utrzymując przede wszystkim, że zastosowanie się do tego nakazu jest niemożliwe, jako że skuteczność i trwałość systemów blokowania lub filtrowania nie została dowiedziona, oraz że wdrożenie takich rozwiązań napotyka na wiele praktycznych przeszkód, takich jak problemy przepustowości sieci i wpływ na sieć. Ponadto w jej opinii wszelkie próby blokowania takich plików są bardzo szybko skazane na porażkę, gdyż istnieje obecnie szereg programów „peer-to-peer" uniemożliwiających sprawdzenie ich zawartości przez osoby trzecie. Wreszcie dostawca usług internetowych stwierdził, że wdrożenie systemu filtrowania narusza przepisy prawa Unii dotyczące ochrony danych osobowych i tajemnicy połączeń w zakresie, w jakim filtrowanie pociąga za sobą przetwarzanie adresów IP, stanowiących dane osobowe. Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 24 listopada 2011, C-70/10, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=PL&mode=doc&dir=&occ=first&part=1&cid=745691>, dostęp: 7 lipca 2014.

kompetencji. Stosuje się do przetwarzania danych osobowych przez wszystkie instytucje i organy wspólnotowe, o ile takie przetwarzanie jest przeprowadzane podczas wykonywania czynności całkowicie lub częściowo podlegających prawu wspólnotowemu. Rozporządzenie reguluje ogólne zasady: dotyczące jakości danych, legalności ich przetwarzania[89], prawa osoby, której dane dotyczą[90] oraz powołuje urząd Europejskiego Rzecznika Ochrony Danych. Określa obowiązki administratora danych w przypadku, gdy pobiera dane od osób, których one dotyczą, jak również gdy pobiera dane z innych źródeł niż podmiot danych oraz zasady zapewniające poufność i bezpieczeństwo przetwarzania danych. Rozdział IV rozporządzenia dotyczy kwestii zapewnienia ochrony danych osobowych i prywatności w kontekście wewnętrznych sieci telekomunikacyjnych[91].

Decyzja Rady 2004/644/WE z dnia 13 września 2004 ustanawia reguły wykonawcze dotyczące ww. rozporządzenia[92]. Określa sposób powołania i kompetencje EIOD. Precyzuje zadania administratorów danych i kompetencje tzw. osób kontaktowych. Zobowiązuje administratora danych m.in. do powiadamiania inspektora ochrony danych (który zobowiązany jest do prowadzenia stosow-

---

[89] Zabrania przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych i danych dotyczących zdrowia lub życia seksualnego. Wyjątki dopuszczające przetwarzanie tych danych określone są w art. 10. Rozporządzenie Parlamentu Europejskiego i Rady 2001/45/WE z dnia 18 grudnia 2000, Dz. Urz. WE L 8 z dnia 12 stycznia 2001, s. 1.

[90] Czyli prawo: dostępu do danych w odpowiednim terminie (nie dłuższym niż 3 miesiące) i bez wnoszenia opłat; żądania wprowadzenia poprawek niedokładnych lub niekompletnych danych osobowych, zablokowania danych lub ich usunięcia; żądania powiadomienia stron, którym dane zostały ujawnione, o wszelkich poprawkach, zablokowaniu ich lub usunięciu; wniesienia sprzeciwu. Sekcja 4 Przekazywanie informacji podmiotowi danych, art. 11-19. Rozporządzenie Parlamentu Europejskiego i Rady 2001/45/WE z dnia 18 grudnia 2000, Dz. Urz. WE L 8 z dnia 12 stycznia 2001, s. 1.

[91] Przepisy tego rozdziału stosuje się do przetwarzania danych osobowych w połączeniu z użyciem sieci telekomunikacyjnych lub urządzeń końcowych, działających pod kontrolą instytucji lub organu Wspólnoty. Zarówno rozporządzenie 45/2001 (ochrona danych) jak i rozporządzenie 1049/2001 (publiczny dostęp) są gwarantowane przez instytucje. Odnośnie art. 29 grupa robocza ds. ochrony danych podkreśliła dnia 17 maja 2001, że „dane osobowe zawarte w oficjalnym dokumencie lub będące w posiadaniu administracji publicznej są nadal danymi osobowymi i muszą być w związku z tym chronione". W orzecznictwie Europejskiego Trybunału Praw Człowieka ochrona danych jest szeroko interpretowana, a w dokumencie informacyjnym z lipca 2005 w sprawie publicznego dostępu i ochrony danych Europejski Inspektor Ochrony Danych zwraca uwagę na kluczowe elementy takie jak „ochrona przed ujawnieniem informacji przekazanych lub otrzymanych w zaufaniu przez indywidualną osobę".
<http://www.europarl.europa.eu/meetdocs/2004_2009/documents/am/595/595119/595119pl.pdf>, dostęp: 4 grudnia 2014.

[92] Przepisy wykonawcze do rozporządzenia stosuje się bez uszczerbku dla rozporządzenia (WE) nr 1049/2001(2), decyzji 2004/338/WE, Euratom (3), w szczególności jej załącznika II, decyzji 2001/264/WE(4), w szczególności części II sekcji VI jej załącznika, jak również decyzji Sekretarza Generalnego Rady/Wysokiego Przedstawiciela ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa z dnia 25 czerwca 2001 Dz. Urz. WE L 296 z dnia 21 września 2004, s. 16.

nego rejestru) o każdej operacji przetwarzania danych. Decyzja rady określa też, w jakim trybie osoby uprawnione mogą skorzystać z przysługujących im praw np. dostępu do danych, wnoszenia poprawek lub żądania ich usunięcia, blokowania danych, wnoszenia sprzeciwu i o możliwych zwolnieniach i ograniczeniach tych praw.

Istotną rolę w kwestii ochrony danych osobowych spełnia niezależny organ nadzorczy, czyli EIOD. Do jego zadań należy monitorowanie i zapewnienie stosowania wspólnotowych przepisów o ochronie danych osobowych, doradzanie instytucjom i organom wspólnotowym oraz osobom, których dane dotyczą, w sprawach związanych z przetwarzaniem danych, a także współpraca z krajowymi organami ochrony danych i instytucjami nadzorczymi (z III filara UE). Doradza wszystkim instytucjom i organom wspólnotowym, albo z własnej inicjatywy, albo w odpowiedzi na konsultacje, we wszystkich kwestiach dotyczących przetwarzania danych osobowych (przed ich przyjęciem). Monitoruje rozwój w odpowiednich dziedzinach, o ile ma on wpływ na ochronę danych osobowych, w szczególności rozwój technologii informatycznych i telekomunikacyjnych. Współpracuje z krajowymi organami nadzoru oraz z organami nadzoru w dziedzinie ochrony danych ustanowionymi przez tytuł VI Traktatu o Unii Europejskiej, w szczególności mając na względzie poprawę spójności i zastosowania reguł i procedur, za zapewnienie zgodności z którymi są odpowiednio odpowiedzialne. Bierze udział w działalności grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, o którym mówi art. 29 dyrektywy 95/46/WE[93].

[93] Stanowisko Europejskiego Inspektora Ochrony Danych (EDPS) ustanowiono w 2001 na podstawie Rozporządzenia 2001/45/WE Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz. U. WE L 8 z dnia 12 stycznia 2001, s. 1. W 2004 Europejskim Inspektorem Ochrony Danych został Peter Johan Hustinx, zaś jego zastępcą – Joaquín Bayo Delgado. 23 grudnia 2008 Europejskim Inspektorem Ochrony Danych ponowanie został wybrany Peter Johan Hustinx, zaś jego zastępcą Giovanni Buttarelli. 27 listopada 2014 został wybrany Giovanni Buttarelli, a jego zastępcą dotychczasowy Generalny Inspektor Ochrony Danych Osobowych w Polsce, dr Wojciech Rafał Wiewiórowski. <https://secure.edps.europa.eu/EDPSWEB/edps/lang/pl/EDPS>, dostęp: 4 grudnia 2014.

Rozdział 3. Prawo do informacji a prawo do ochrony danych – konstytucyjny dylemat

Zarówno prawo do informacji (określone zarówno w art. 61 Konstytucji – czyli prawo dostępu do informacji publicznej, jak i w art. 54 Konstytucji – jako wolność posiadania i wyrażania poglądów), jak i prawo do ochrony danych osobowych (określone w art. 51 Konstytucji) są równorzędnymi zasadami prawnymi, które mają wiążący charakter, cechują się szczególną rolą oraz nadrzędnością w stosunku do innych norm prawnych. Umieszczenie tych zasad w Konstytucji (najwyższym w hierarchii akcie prawnym) jest wyrazem ich doniosłości oraz elementem demokratycznego państwa prawnego (określonego w art. 2 Konstytucji), ponieważ wyznaczają kierunek działań prawodawcy, ograniczając swobodę ingerencji państwa w prawa (wolności) jednostki.

Celem ochrony danych osobowych jest zagwarantowanie jednostce prawa do decydowania o sobie w sferze informacji i możliwość korzystania z prawa do ochrony prywatności i intymności. Marie-Theres Tinnefeld uważa, że „przestrzeganie prawa jednostki do informacji implikuje również istnienie prawa do niewiedzy, zwłaszcza gdy możliwe jest wejrzenie w genetyczną kulę kryształową”[1].

Prawo do ochrony danych osobowych (jako jedno z wolności i praw osobistych) uzyskało konstytucyjną gwarancję dopiero w Konstytucji z dnia 2 kwietnia 1997. Prawo to ma swoje źródło w przyrodzonej i niezbywalnej godności człowieka. Jakiekolwiek działania władzy publicznej w zakresie dotyczącym ochrony danych osobowych muszą uwzględniać istotę godności człowieka. Egzekwowanie tego prawa zapewnia zasada bezpośredniego stosowania przepisów Konstytucji, bez konieczności dodatkowych regulacji na poziomie ustawowym. Ponadto Konstytucja zapewnia ochronę prywatności jednostki nie tylko na linii państwo – jednostka, ale także chroni przed nadmiernym zainteresowaniem ze strony innych jednostek lub mediów[2]. Piotr Winczorek uważa, że w pewnych przypadkach przepis ten zapewnia ochronę danych i informacji także np. przedsiębiorcom[3].

Konstytucyjna gwarancja zapewnia jednostce prawo do anonimowości oraz możność kontrolowania przepływu informacji, które jej dotyczą. Brak takiej kontroli może pozbawić jednostkę swobody decydowania o własnym losie. Tak więc każda informacja, którą dana osoba uzna za prywatną lub intymną, może

---

[1] M. T. Tinnefeld, *Ochrona danych – kamień węgielny budowy Europy*, [w:] *Ochrona danych osobowych*, pod red. M. Wyrzykowskiego, Warszawa 1999, s. 37–38.

[2] Więcej : M. Safjan, *Prawo do ochrony życia prywatnego*, „Szkoła Praw Człowieka. Tematy wykładów” 1998, z. 4, s. 71–89.

[3] P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997*, Warszawa 2000, s. 69–70.

być przez nią zachowana w tajemnicy. Autonomię informacyjną jednostki gwarantuje przede wszystkim art. 51 Konstytucji, niezależnie od gwarancji ochrony prywatności zawartej w art. 47 Konstytucji. W myśl art. 51 ust. 1, nikt (nikt = = każdy, czyli mamy tu do czynienia z prawem człowieka, a nie wyłącznie obywatela) nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. W praktyce żądanie ujawnienia informacji w zakresie szerszym niż dopuszczalny ustawowo może prowadzić do dyskryminacji (np. ze względu na płeć)[4].

Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym (art. 51 ust. 2). Ograniczenie ma więc charakter podwójny: po pierwsze muszą być niezbędne, a po drugie konieczne w demokratycznym państwie prawnym. A contrario osoby prywatne i/lub osoby prawne mogą pozyskiwać dane osobowe bez szczególnych ograniczeń, pod warunkiem poszanowania prawa innych osób do prywatności[5]. Dziennikarz zatem może pozyskiwać informacje o osobach (np. swoich rozmówcach) na podstawie art. 51 ust. 2 Konstytucji, jak i na podstawie art. 54 Konstytucji, który to zapewnia wolność pozyskiwania i rozpowszechniania informacji. Ponadto, jak wynika z orzeczenie Naczelnego Sądu Administracyjnego w Warszawie z dnia 29 stycznia 2001, treść i umiejscowienie art. 51 Konstytucji wskazuje, że podstawa do przetwarzania danych (czyli również i zbierania) musi mieć charakter wyraźny i przy przetwarzaniu danych powinno stosować się wykładnię ścieśniającą[6]. Oznacza to, że przesłanki legalizujące zbieranie (przetwarzanie) danych osobowych muszą być precyzyjne i konkretne oraz wynikać wprost z przepisów prawa.

Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa (ust. 5). Zgodnie z ust. 3, każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Zapoznanie się ze zgromadzonymi

---

[4] Sąd Najwyższy (Izba Pracy) w wyroku z dnia 17 kwietnia 2007 uznał, że art. 22 kodeksu pracy określa granice uprawnienia pracodawcy do pozyskiwania od kandydatów ubiegających się o pracę informacji o ich sytuacji życiowej, relewantnej z punktu widzenia podjęcia zatrudnienia. Norma prawna zawarta w tym przepisie pozwala na podzielenie wszelkich okoliczności dotyczących życia pracownika (wcześniej kandydata na pracownika) na cztery sfery: 1. sferę identyfikacji personalnej, 2. sferę pracy, 3. sferę tajemnicy osobistej i 4. tajemnicy prywatnej. Zasadą jest udostępnianie pracodawcy informacji z zakresu dwóch pierwszych sfer. Pozostałe informacje o pracowniku i kandydacie na pracownika (informacje sfery osobistej) ustawodawca uznał generalnie za niedostępne pracodawcy, z jednym wyjątkiem. Pracodawca ma prawo żądania informacji stanowiących tajemnicę osobistą, w sytuacji gdy przepis szczególny na to zezwala. Pracownica podejmująca zatrudnienie nie ma obowiązku ujawniania faktu pozostawania w ciąży, jeżeli praca, jaką zamierza podjąć, nie jest niedozwolona dla kobiet z uwagi na ochronę macierzyństwa.

Wyrok SN (Izby Pracy) z dnia 17 kwietnia 2007, I UK 324/06, Legalis nr 89217.

[5] Zob. P. Sarnecki, *uwaga 7 do art. 51 Konstytucji RP* , [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, pod red. L. Garlickiego, Warszawa 2003, s. 4–5.

[6] Wyrok NSA w Warszawie z dnia 29 stycznia 2003, II SA 3085/01, LEX nr 156396.

dokumentami może wykazać, że dane te zostały zebrane w sposób sprzeczny z ustawą lub są nieprawdziwe czy niepełne. Ograniczenie tego prawa może określić ustawa. Zasada wyrażona w art. 51 ust. 3 Konstytucji musi być uwzględniana przy interpretacji art. 73 § 1 k.p.a., bowiem postępowanie administracyjne winno być prowadzone nie tylko zgodnie z zasadami: jawności postępowania, czynnego udziału stron, prawdy obiektywnej czy zaufania obywateli do organów państwa lecz również prawa dostępu każdego do dotyczących go urzędowo dokumentów i zbiorów danych[7].

Z kolei art. 51 ust. 4 stanowi, że każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Prawo to dotyczy wyłącznie informacji obejmujących dane osobowe. Za dane osobowe nie mogą być uznane np. ustalenia faktyczne zawarte w orzeczeniach prokuratury. Pogląd taki wyraził SN rozpatrując skargę Jacka B. (sygn. V CKN 1119/00). Skarżący zarzucił postanowieniu SA naruszenie Konstytucji. Istotą skargi było twierdzenie powoda o możliwości bezpośredniego stosowania Konstytucji (w tym art. 51 ust. 4) i dopuszczalność żądania sprostowania lub usunięcia informacji nieprawdziwych, niepełnych i zebranych w sposób sprzeczny z ustawą nie tylko informacji dotyczących osoby (danych osobowych), lecz wszystkich informacji. Zdaniem skarżącego, właściwa do ochrony tego prawa jest droga sądowa przed sądami powszechnymi[8] .W ten sposób bowiem każdy może wpływać na prawidłowość i kompletność dotyczących go informacji.

Artykuł 51 ust. 1 Konstytucji potwierdza prawo jednostki (każdego) do samodzielnego decydowania o ujawnianiu informacji o sobie (prawo do milczenia). Jedynie te informacje, których ujawnienie jest konieczne wobec organów władzy publicznej, wyjęte są spod ochrony. Obowiązek ujawnienia informacji o sobie

---

[7] Wyrok WSA w Łodzi z dnia 15 marca 2013, II SA/Łd 1193/12, LEX nr 1303070.

[8] Postanowienie SN z dnia 14 czerwca 2000, V CKN 1119/00, „OSNC" 2002, nr 4, poz. 49.

Jacek B. w pozwie z dnia 18 stycznia 1999 skierowanym przeciwko Skarbowi Państwa – Prokuratorowi Okręgowemu w W., powołując się na art. 51 ust. 4 Konstytucji, wniósł o wydanie wyroku nakazującego sprostowanie i usunięcie informacji nieprawdziwej i niepełnej, zawartej w postanowieniu Prokuratora Wojewódzkiego z dnia 20 sierpnia 1998 w brzmieniu „w toku postępowania Komisja Dyscyplinarna podjęła na posiedzeniu niejawnym decyzję odmawiającą dopuszczenia do postępowania dyscyplinarnego zawodowego adwokata jako obrońcy obwinionych studentów. Decyzję tę, ze względu na istniejące wątpliwości interpretacyjne odpowiednich przepisów ustawy o szkolnictwie wyższym dotyczących obrońców obwinionych, oparto na opinii Kierownika Katedry Postępowania Karnego Wydziału Prawa i Administracji Uniwersytetu W." Sąd Okręgowy we Wrocławiu, postanowieniem z dnia 14 kwietnia 1999 odrzucił pozew, uznając jednocześnie, że w powyższej sprawie niedopuszczalna jest droga sądowa (gdyż nie jest to sprawa cywilna). Sąd Apelacyjny(postanowieniem z dnia 21 listopada 1999) oddalił zażalenie powoda i podtrzymał stanowisko Sądu pierwszej instancji o niedopuszczalności drogi sądowej. Również Sąd Najwyższy uznał, że skarga kasacyjna nie ma uzasadnionych podstaw.

stanowi ograniczenie autonomii informacyjnej. Z drugiej jednak strony, jak wielokrotnie podkreślał TK, żaden obywatel nie jest zobowiązany do ubiegania się o funkcje publiczne, ani do pełnienia funkcji publicznej. Znając następstwa tego faktu w postaci upublicznienia pewnego zakresu informacji, należących do sfery prywatności, podejmuje on samodzielną i świadomą decyzję, opartą na rachunku pozytywnych i negatywnych konsekwencji, wkalkulowując określone ograniczenia oraz dyskomfort związany z ingerencją w życie prywatne[9].

Również w sprawie dotyczącej kwestii lustracji TK musiał rozstrzygnąć, czy można dopatrzyć się naruszenia przez art. 11 ust. 1 ustawy lustracyjnej normy art. 51 ust. 2 Konstytucji, która stanowi, że władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Trybunał Konstytucyjny uznał wówczas, że informacje odnoszące się do kwestii zaistnienia lub niezaistnienia faktu pracy, służby albo współpracy z organami bezpieczeństwa państwa są przekazywane przez osobę pełniącą funkcję publiczną i od jej woli zależy, czy taką funkcję chce pełnić. W demokratycznym państwie prawnym wiedza na ten temat jest konieczna dla urzeczywistnienia zasady jawności życia publicznego oraz ochrony interesu państwa związanego z prawidłowym wykonywaniem najważniejszych funkcji publicznych przez osoby, które muszą być wolne od wszelkich nacisków, presji czy prób szantażu związanego z pracą lub służbą oraz aktywnością realizowaną w przeszłości[10].

Ograniczenie takie może zostać wprowadzone tylko w drodze ustawy. Nałożenie takiego obowiązku musi mieścić się w granicach ingerencji państwa w sferę konstytucyjnych wolności i praw człowieka i obywatela, wyznaczonych przez art. 31 ust. 3 Konstytucji[11].

Pierwszy warunek dopuszczalnych ograniczeń to wymóg aby ograniczenia były ustanawiane w ustawie. Oznacza to, że ograniczenia wolności i praw nie mogą wynikać z rozporządzenia, nie ma natomiast przeszkód, aby były ustanawiane np. w samej konstytucji lub umowie międzynarodowej ratyfikowanej za

---

[9] Zob. wyrok TK z dnia 5 marca 2003, K 7/01, OTK-A 2003, nr 3, poz. 19.

[10] Wyrok TK z dnia 11 maja 2007, K 2/07, OTK-A 2007, nr 5, poz. 48.

[11] Art. 31 ust.3 Konstytucji stanowi, że „ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw." Dz. U. 1997, nr 78, poz. 483. Niedopuszczalne jest zatem dokonanie subdelegacji, czyli przekazanie kompetencji normodawczej innemu organowi, analogicznie do wykluczenia takiej możliwości w odniesieniu do rozporządzeń wykonawczych względem ustaw.

Andrzej Sakowicz uważa, że regulacja art. 31 ust. 3 Konstytucji nie stanowi samodzielnej podstawy prawnej ograniczania praw człowieka, lecz formułuje tylko warunki, jakie muszą spełniać ograniczenia. A. Sakowicz, *Prawnokarne gwarancje prywatności*, Warszawa 2006, s. 99.

uprzednią zgodą wyrażoną w ustawie, czy w prawie międzynarodowym stanowionym przez organizację międzynarodową[12]. Jak wynika też z orzeczenia TK z dnia 19 maja 1998 w odniesieniu do sfery wolności i praw człowieka zastrzeżenie wyłącznie ustawowej rangi unormowania ich ograniczeń należy pojmować dosłownie, z wykluczeniem dopuszczalności subdelegacji, tj. przekazania kompetencji normodawczej innemu organowi, analogicznie do wykluczenia takiej możliwości w odniesieniu do rozporządzeń wykonawczych względem ustaw. Trybunał Konstytucyjny uznał, iż w sytuacji sporu pomiędzy jednostką a organem władzy publicznej o zakres czy sposób korzystania z wolności i praw, podstawa prawna rozstrzygnięcia tego sporu nie może być oderwana od unormowania konstytucyjnego, ani mieć rangi niższej od ustawy[13]. Bogusław Banaszak uważa, że sformułowanie „»ingerencja w prawa i wolności może być przewidziana tylko w ustawie«, rozumiane być powinno jako obejmujące nie tylko przypadki, w których ustawa stanowi jedyne źródło ograniczeń, ale także i takie sytuacje, w których ustawodawca formułuje jedynie podstawowe elementy ograniczeń, zaś ich rozwinięcie, uzupełnienie może być już dokonane w innym akcie (podstawowym) – np. w uchwale rady gminy – miejscowym planie zagospodarowania przestrzennego, gdy w ustawie nie da się w precyzyjny sposób określić jakie ograniczenia mają być ustanowione”[14]. Zdaniem TK absolutnie niedopuszczalne jest jednak przyjmowanie w ustawie uregulowań blankietowych, pozostawiających organom władzy wykonawczej czy organom samorządu lokalnego swobodę wyznaczania tych ograniczeń[15].

Drugi warunek to kryterium konieczności. Ograniczenia wolności i praw dopuszczalne są tylko wtedy, gdy są konieczne w demokratycznym państwie w celu ochrony wartości określonych w art. 31 ust. 3 Konstytucji. Za konieczność uznaje się brak innych możliwości osiągnięcia zamierzonego celu. Wprowadzenie ustawowych ograniczeń praw i wolności ma wynikać nie z subiektywnego

---

[12] Umowa międzynarodowa ratyfikowana za uprzednią zgodą wyrażoną w ustawie ma pierwszeństwo przed ustawą, jeżeli ustawy tej nie da się pogodzić z umową. Ratyfikacja przez Rzeczpospolitą Polską umowy międzynarodowej i jej wypowiedzenie wymaga uprzedniej zgody wyrażonej w ustawie, jeżeli umowa dotyczy:

1) pokoju, sojuszy, układów politycznych lub układów wojskowych;

2) wolności, praw lub obowiązków obywatelskich określonych w Konstytucji;

3) członkostwa Rzeczypospolitej Polskiej w organizacji międzynarodowej;

4) znacznego obciążenia państwa pod względem finansowym,

spraw uregulowanych w ustawie lub w których Konstytucja wymaga ustawy (art. 91 w zw. z art. 89 Konstytucji) Dz. U. 1997, nr 78, poz. 483 z póź. zm.

Patrz także: Wyrok TK z dnia 29 kwietnia 2003, SK 24/02, OTK-A 2003, nr 4, poz. 33; Orzeczenie TK z dnia 22 września 1997, K 25/97, OTK 1997, nr 3–4, poz. 35; Orzeczenie TK z dnia 26 września 1995, U 4/95, OTK 1995, mr 1, poz. 4; Orzeczenie TK z dnia 28 maja 1986, U 1/86, OTK 1986, nr 1, poz. 2.

[13] Wyrok TK z dnia 19 maja 1998, U 5/97, OTK 1998, nr 4, poz. 46.

[14] B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012, s. 219.

[15] Wyrok TK z dnia 12 stycznia 2000, P 11/98, OTK 2000, nr 1, poz. 3.

przekonania o takiej potrzebie, ale z obiektywnej ich niezbędności[16]. Ustawodawca każdorazowo musi stwierdzić rzeczywistą potrzebę ingerencji w prawa lub wolności jednostki. Nie wystarczy, aby stosowane środki sprzyjały zamierzonym celom, albo były wygodne dla władzy. Niezbędność oznacza obowiązek korzystania ze środków najmniej uciążliwych dla jednostki, czyli ingerencja musi być racjonalna i w odpowiednich proporcjach do zamierzonych celów, a użyte środki godne demokratycznego i prawnego państwa[17]. Granice ingerencji władzy publicznej w sferę danych osobowych są więc zawężone i pozyskiwanie, gromadzenie oraz udostępnianie danych ma charakter wyjątku od zasady niepozyskiwania, niegromadzenia i nieudostępniania informacji o obywatelach.

Trzeci warunek zakazuje naruszania istoty wolności i praw w toku ustanawiania ograniczeń w ustawie. Potwierdzenie tego zakazu znaleźć możemy m.in. w wyroku TK z dnia 25 maja 1999, w którym stwierdził, że „koncepcja istoty praw i wolności opiera się na założeniu, że w ramach każdego konkretnego prawa i wolności można wyodrębnić pewne elementy podstawowe (rdzeń, jądro), bez których takie prawo czy wolność w ogóle nie będzie mogła istnieć, oraz pewne elementy dodatkowe (otoczkę), które mogą być ujmowane i modyfikowane w różny sposób bez zniszczenia tożsamości danego prawa czy wolności"[18]. W doktrynie można spotkać pogląd, że istota praw i wolności zostanie naruszona także wtedy, gdy państwo co prawda nie zniosło tego prawa (wolności), lecz w praktyce uniemożliwiło korzystanie z niego[19]. Kryteria konieczności,

---

[16] „W orzecznictwie Trybunału Konstytucyjnego wielokrotnie podkreślano, że do oceny racjonalności i współmierności wprowadzanych ograniczeń w pierwszym rzędzie jest powołany ustawodawca, a ingerencja Trybunału dopuszczalna jest dopiero wtedy, gdy „ustawodawca przekroczy zakres swej swobody regulacyjnej w sposób na tyle drastyczny, że naruszenie klauzul konstytucyjnych stanie się ewidentne" (orzeczenia z: dnia 26 kwietnia 1995, sygn. K. 11/94, OTK w 1995, cz. I, s. 134, z dnia 23 kwietnia 1996, sygn. K. 29/95, OTK ZU, nr 1996, nr 2, s. 109).„Wyrok TK z dnia 8 października 2001, K 11/01, OTK 2001, nr 7, poz. 210.

[17] „Nie wystarczy zatem sama celowość, pożyteczność, taniość czy łatwość posługiwania się przez władzę – w odniesieniu do użytego środka. Bez znaczenia jest też argument porównawczy, że podobne środki w ogóle bywają stosowane w innych państwach." Wyrok TK z dnia 12 grudnia 2005r, K 32/04, OTK-A 2005, nr 11, poz. 132.

[18] Wyrok TK z dnia 25 maja 1999, SK 9/98, OTK 1999, nr 4, poz. 78.

„W ocenie Trybunału Konstytucyjnego interpretacja zakazu naruszania istoty ograniczanego prawa lub wolności nie powinna sprowadzać się jedynie do płaszczyzny negatywnej, akcentującej odpowiednie miarkowanie dokonywanych ograniczeń. Należy widzieć w nim również stronę pozytywną, związaną z dążeniem do wskazania – choćby przykładowo – pewnego nienaruszalnego rdzenia danego prawa lub wolności, który pozostawać winien wolny od ingerencji prawodawcy nawet w sytuacji, gdy działa on w celu ochrony wartości wskazanych w art. 31 ust. 3 konstytucji. Wskazanie istoty prawa lub wolności powinno uwzględniać przy tym kontekst sytuacji, w której dochodzi do ograniczenia danego uprawnienia". Wyrok TK z dnia 12 stycznia 1999, P 2/98, OTK 1999, nr 1, poz. 2.

[19] Jak wskazuje Bogusław Banaszak nie ma jednolitości w rozumieniu „istoty wolności i praw". Zaznaczają się dwa stanowiska: 1. teoria istoty absolutnej, która zakłada, że istota prawa lub wolności jest niezmienna, absolutna, niezależnie od sytuacji; 2. teoria istoty względnej – która

niezbędności i proporcjonalności muszą respektować zarówno prawodawcy krajowi, jak też UE[20].

Przepis art. 51 mieści się w rozdziale II Konstytucji „Wolności, prawa i obowiązki człowieka i obywatela". Oznacza to, że zarówno po stronie władz publicznych, jak i każdej innej osoby ciąży obowiązek powstrzymania się od jakiejkolwiek ingerencji w sferę tych wolności. Pogląd taki wyraził TK w wyroku z dnia 19 lutego 2002, w którym stwierdził, że prawodawca konstytucyjny w art. 51 ustawy zasadniczej kładzie nacisk przede wszystkim na ochronę jednostki wobec władz publicznych. W ustępie 2 jako podmiot zobowiązany do realizacji prawa, o którym mowa w tym przepisie, wskazane zostały władze publiczne. Artykuł 51 ust. 1 Konstytucji nie określa w sposób jednoznaczny podmiotu zobowiązanego do realizacji prawa zagwarantowanego w tym przepisie. Oznacza to, że wymieniony przepis konstytucyjny dotyczy wszelkich przypadków, w których jednostka zobowiązana zostaje do ujawniania informacji o sobie innym podmiotom, a więc także podmiotom prywatnym. […]. W świetle art. 47 Konstytucji nie ulega jednak wątpliwości, że ustawodawca ma konstytucyjny obowiązek zapewnić jednostce odpowiednią ochronę sfery prywatności nie tylko przed ingerencją ze strony podmiotów publicznych, ale również przed ingerencją ze strony innych jednostek i podmiotów prywatnych[21].

Co więcej, po stronie władz publicznych istnieje obowiązek ochrony tych wolności i zapewnienia możliwości swobodnego z nich korzystania, bez przeszkód ze strony nieuprawnionych podmiotów. Należy zatem zagwarantować w konkretnych aktach prawnych, aby konstytucyjne prawa (w tym autonomii informacyjnej) nie były realizowane z naruszeniem czy chociażby narażeniem na jakąkolwiek szkodę prawa do prywatności innych osób. Taki pogląd wyraził także TK m.in. w wyroku z dnia 18 lutego 2004, w którym stwierdził, że aspekt pozytywny „wolności jednostki" polega na tym, że jednostka może swobodnie kształtować swoje zachowania w danej sferze, np. wybierając takie formy aktywności, które jej samej najbardziej odpowiadają lub powstrzymywać się od podejmowania jakiejkolwiek działalności, zaś aspekt negatywny „wolności jednostki" polega na prawnym obowiązku powstrzymania się – kogokolwiek – od ingerencji w sferę zastrzeżoną dla jednostki. Funkcja prawodawcy przy regulowaniu wolności jednostki („praw wolnościowych") nie polega bowiem na ustanowieniu normy zezwalającej na określone zachowania lecz na wprowadzeniu

---

zakłada, że pojęcie istoty prawa lub wolności powinno być określane w zależności od konkretnej sytuacji, z uwzględnieniem wszystkich okoliczności. B. Banaszak, *Prawa człowieka i obywatela w nowej Konstytucji Rzeczypospolitej Polskiej*, „Przegląd Sejmowy" 1997, nr 5, s. 57.

[20] Więcej: L. Wiśniewski, *Zakres ochrony prawnej wolności człowieka i warunki jej dopuszczalnych ograniczeń w praktyce*, [w:] *Wolności i prawa jednostki oraz ich gwarancje w praktyce*, pod red. L. Wiśniewskiego, Warszawa 2006, s. 21–34.

[21] Wyrok TK z dnia 19 lutego 2002, U 3/01, OTK-A 2002, nr 1, poz. 3.

zakazu podejmowania działań, które utrudniałyby podmiotowi danego prawa kształtowanie swojego zachowania w określonej sferze zgodnie z dokonanym przez siebie wyborem[22]. Również NSA w wyroku z dnia 29 stycznia 2003 stwierdził, że treść i umiejscowienie art. 51 Konstytucji wskazuje, że podstawa do przetwarzania danych musi mieć charakter wyraźny i powinno się do niej stosować wykładnię ścieśniającą[23].

[22] Wyrok TK z dnia 18 lutego 2004, P 21/02, OTK-A 2004, nr 2, poz. 9.
[23] Wyrok NSA z dnia 29 stycznia 2003, II SA 3085/01, LEX nr 156396.

Rozdział 4. Ochrona danych osobowych w orzecznictwie Trybunału Konstytucyjnego

Prawo do ochrony danych osobowych (określone w art. 51 Konstytucji) jest wyspecjalizowanym środkiem ochrony konstytucyjnych wartości określonych w art. 47 (i pośrednio art. 49) Konstytucji. Realizację gwarancji konstytucyjnej określonej w art. 51 zapewnia z kolei ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997. Trybunał Konstytucyjny musiał wielokrotnie definiować zakres autonomii informacyjnej jednostki i dopuszczalność ingerencji w sferę prywatności.

W orzeczeniu z dnia 20 czerwca 2005 TK rozstrzygał kwestię dopuszczalności wkroczenia w prywatność obywateli ze względu na ochronę interesów i praw majątkowych Skarbu Państwa oraz zapewnienia skuteczności wykonywania zobowiązań podatkowych (i innych należności) stanowiących dochód Skarbu Państwa. Trybunał Konstytucyjny stwierdził, że ustawodawca zbyt szeroko określił zakres uprawnień wywiadu skarbowego, ponieważ wkracza on w sferę życia prywatnego jednostki. Jednocześnie uregulowania nie zawierają dostatecznych zabezpieczeń proceduralnych. Trybunał Konstytucyjny nie zakwestionował natomiast funkcjonowania Wojewódzkich Kolegiów Skarbowych oraz utworzenia urzędów skarbowych właściwych dla pewnych kategorii podatników. Kolegia bowiem nie kształtują i nie prowadzą polityki wewnętrznej i zagranicznej państwa, ale uzgadniają działania w zakresie realizacji polityki celnej, podatkowej i kontrolnej. Cele państwa można natomiast realizować bez konieczności ingerencji w prywatność jednostki[1].

Trybunał Konstytucyjny w wyroku z dnia 20 listopada 2002 w sprawie abolicji podatkowej i deklaracji majątkowych w zakresie obowiązku składania

---

[1] Więcej: Wyrok TK z dnia 20 czerwca 2005, K 4/04, OTK-A 2005, nr 6, poz. 56.

Przed zmianą wynikającą z zaskarżonej nowelizacji wywiad skarbowy mógł gromadzić, przetwarzać i wykorzystywać informacje o dochodach, obrotach, rzeczach i prawach majątkowych tylko podlegających kontroli. Po wejściu w życie zaskarżonych przepisów wywiad skarbowy może gromadzić, przetwarzać i wykorzystywać więcej informacji o osobach. Drastyczność tych przepisów, zdaniem wnioskodawców, polega na tym, że wywiad skarbowy będzie mógł zdobywać i gromadzić wszelkie informacje na temat obywateli nie tylko w trakcie czynności operacyjno-rozpoznawczych podejmowanych w związku z obowiązkami finansowymi podatników. Dane mogą dotyczyć rozmaitych dziedzin życia i bardzo dużej liczby osób. Będzie można, według wnioskodawców, bez przeszkód obserwować i rejestrować na filmie ludzi spacerujących po parku, rozmawiających w kawiarni, w gmachu parlamentu, sądu, w zakładzie pracy a nawet przebywających w miejscach kultu religijnego. W kościele będzie można ustalić np., kto i jakie kwoty przeznaczył na tacę i w ten sposób sprawdzać, czy osoba posiada dochody nie znajdujące pokrycia w ujawnionych źródłach przychodów. Zaskarżone przepisy nie zawierają żadnych zasad ograniczających działanie wywiadu skarbowego. Czynności mogą być podjęte zarówno wobec podatnika jak inkasenta podatków czy osoby trzeciej odpowiadającej za cudzy dług.

deklaracji majątkowych stwierdził m.in. naruszenie prawa do prywatności (art. 47 Konstytucji oraz pośrednio art. 51 Konstytucji)[2]. Ochrona życia prywatnego, zagwarantowana w art. 47, obejmuje także tzw. autonomię informacyjną (określoną w art. 51), która oznacza prawo do samodzielnego decydowania o ujawnianiu innych informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów[3]. Informacje dotyczące majątku niewątpliwie należą do sfery prywatności jednostki (autonomii informacyjnej). Obowiązek wyjawienia całego majątku zgromadzonego w ciągu całego życia (z drobiazgowym wyliczeniem jego składników i ich wartości) głęboko wkracza w sferę życia prywatnego.

Ochrona prywatności nie ma charakteru absolutnego, jednak obowiązek ujawnienia informacji o sobie musi wynikać z ustawy i tylko w granicach określonych przez ustawę zgodnie z konstytucyjną zasadą proporcjonalności. Przepis o deklaracjach majątkowych jest wadliwy ze względu na niezachowanie przesłanek wymaganych przez art. 31 ust. 3 Konstytucji. Prawo do prywatności (art. 47 Konstytucji) – zgodnie z art. 233 ust. 1 Konstytucji – jest nienaruszalne nawet w ustawach ograniczających inne prawa, wydawanych w stanie wojennym i wyjątkowym. Zatem nie jest możliwe złagodzenie przesłanek, po spełnieniu których można wkroczyć w sferę życia prywatnego, nie narażając się na zarzut niekonstytucyjnej arbitralności.

Wzajemna relacja między tymi dwoma przepisami Konstytucji polega bowiem na tym, że autonomia informacyjna (art. 51 Konstytucji) jest jednym z elementów prawa do prywatności (w szerokim tego słowa znaczeniu). Istnienie w art. 51 ust. 2 Konstytucji odrębnej regulacji dotyczącej proporcjonalności wkraczania w prywatność jednostki wynika z faktu, że naruszenia prywatności poprzez żądanie niekoniecznych, lecz wygodnych dla władzy publicznej informacji o jednostce jest coraz częstsze. Naruszenie prywatności (autonomii informacyjnej) może nastąpić tylko wtedy, jeżeli jest to „konieczne w demokratycznym państwie prawnym". Ograny państwa muszą zatem udowodnić, że złamanie autonomii informacyjnej było konieczne (niezbędne) w demokratycznym państwie prawnym[4].

---

[2] Wyrok TK z dnia 20 listopada 2002, K 41/02, OTK-A 2002, nr 6, poz.83. „Deklaracje majątkowe, o szczegółowej treści (co do przedmiotu, szacunku i czasu w jakim majątek zgromadzono), z inkorporowanym w nich ryzykiem nierzetelności, ocenianym przez aparat administracyjny (co tworzy groźbę odpowiedzialności już za sam fakt nierzetelności, a nie za zatajenie dochodu) – zostały uznane we wniosku za rodzące wątpliwości (m.in.) co do: zachowania proporcjonalności (art. 31 ust. 3 Konstytucji), jako nakładające na zobowiązanego uciążliwości nie uzasadnione celem, który spodziewano się dzięki niej osiągnąć przez wkroczenie w prywatność. Tę zaś chronią przepisy Konstytucji: art. 47 (co do zasady) i art. 51 (co do pozyskiwania informacji o obywatelach) [...]".

[3] Również: wyrok TK z dnia 19 lutego 2002, U 3/01, OTK-A 2002 nr 1, poz. 3.

[4] Więcej: J. Oniszczuk, *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie TK na początku XXI wieku*, Kraków 2004, s. 461–471.

Na istotny związek prawa do prywatności oraz do ochrony danych osobowych wskazał także TK m.in. już w orzeczeniu z 24 czerwca 1997 w sprawie K 21/96. W orzeczeniu tym TK uznał również, że prawo do prywatności może podlegać ograniczeniom. Konieczne jest jednak, aby za tym ograniczeniem przemawiała inna norma, zasada lub wartość konstytucyjna, a stopień tego ograniczenia musi być proporcjonalny do rangi interesu, któremu ograniczenie to ma służyć[5]. Sędzia TK Zbigniew Czeszejko-Sochacki nie podzielił (i złożył zdanie odrębne) poglądu zawartego w orzeczeniu TK, stwierdzającego zgodność art. 1 pkt 1 ustawy z 31 maja 1996 o zmianie ustawy o zobowiązaniach podatkowych oraz o zmianie niektórych innych ustaw w zakresie jakim przyznał naczelnikowi urzędu skarbowego kompetencje żądania informacji objętych tajemnicą bankową, bez jakiejkolwiek kontroli sądu. Uznał, że narusza to prawo do ochrony prywatności i prawo do sądu. Nie można bowiem, w dążeniu do słusznych celów, pominąć zasad i procedur obowiązujących w demokratycznym państwie prawnym, zaś przewidziana w art. 34b kompetencja naczelnika urzędu skarbowego ma charakter prewencyjny (bo nie ma jeszcze podstaw do wszczęcia postępowania karno-skarbowego) i stanowi ingerencję w prywatność.

W innym wyroku z dnia 11 kwietnia 2000, TK orzekł, choć niejednomyślnie, o zgodności przepisów art. 182 i 183 ustawy z dnia 29 sierpnia 1997– Ordynacja podatkowa z Konstytucją (m.in. art. 47, 31 ust. 3 oraz art. 51). Zdanie odrębne złożyli sędziowie: Andrzej Mączyński i Jadwiga Skórzewska-Łosiak. Ordynacja podatkowa (w art. 183) dała naczelnikowi urzędu skarbowego kompetencje do żądania ujawnienia przez podatnika informacji chronionych tajemnicą bankową. Rzecznik Praw Obywatelskich stwierdził, że taki zapis w ustawie jest przejawem „hipokryzji prawa". Jeśli bowiem podatnik w wyznaczonym terminie nie udzieli żądanej informacji ani nie upoważni urzędu skarbowego do wystąpienia do instytucji finansowej o przekazanie informacji lub odmówi jej udzielenia, pozostaje to bez znaczenia dla dalszych czynności naczelnika urzędu skarbowego. Ponadto czynności naczelnika urzędu skarbowego nie podlegają zaskarżeniu przez podatnika (jest to naruszenie art. 78 oraz 77 ust. 2 Konstytucji). Sędzia

[5] Istnienie prawa do prywatności w polskim porządku prawnym znalazło już potwierdzenie w orzecznictwie Sądu Najwyższego, który (wyrok z dnia 8 kwietnia 1994, III ARN 18/94) odniósł koncepcję ochrony dóbr osobistych (art. 23 i 24 k.c) do sfery życia prywatnego i sfery intymności, wskazując m.in., iż : ochrona w tym zakresie może odnosić się do wypadków ujawniania faktów z życia osobistego i rodzinnego czy nadużywania uzyskanych informacji. Sąd Najwyższy uznał, że styl życia, przejawy kultury w najrozmaitszych zakresach należą do prywatnej sfery życia człowieka. Orzeczenie Sądu Najwyższego – Izby Pracy, Ubezpieczeń i Spraw Publicznych, OSNP 1994, nr 4, poz. 55.

Na tym tle Trybunał Konstytucyjny rozważył, czy prawu do prywatności można *de lege lata* przyznać rangę konstytucyjną. W dotychczasowym orzecznictwie Trybunału Konstytucyjnego ustabilizowało się przeświadczenie, że zasada demokratycznego państwa prawnego obejmuje swym zakresem także pewne treści materialne powiązane z prawami i wolnościami jednostki. Orzeczenie TK z dnia 24 czerwca 1997, K 21/96, OTK 1997 nr 2, poz. 23.

Andrzej Mączyński uznał, że tak sformułowane przepisy umożliwiają organowi władzy publicznej ingerencję w życie prywatne (w tym również w stan majątkowy). Jadwiga Skórzewska-Łosiak zauważyła, że precyzyjne określenie zakresu sfery prywatności może co prawda być trudne, nie ulega jednak wątpliwości, że prawna ochrona życia prywatnego obejmuje informacje dotyczące sytuacji majątkowej. Podstawowym celem tajemnicy bankowej jest zapewnienie jednostce ochrony przed możliwością zapoznania się podmiotów zewnętrznych z danymi stanowiącymi przedmiot tej tajemnicy. Ustawodawca, chcąc ingerować w prawa i wolności, musi określić precyzyjnie przesłanki tej ingerencji tak, aby ograniczyć „luz decyzyjny" oraz stworzyć odpowiednie mechanizmy kontroli działania tych organów. Ponadto, art. 182 i 183 ordynacji podatkowej nie spełniają wymogu konieczności ochrony porządku publicznego ani proporcjonalności[6].

W innej sprawie dotyczącej uprawnień organów kontroli skarbowej TK musiał odnieść się do wniosku Rzecznika Praw Obywatelskich, który uznał, że ustanowienie w ustawie o kontroli skarbowej szerszych możliwości pozyskiwania danych osobowych w postępowaniu nieprocesowym (inaczej niż ma to miejsce w k.p.k. czy k.k.s.), narusza konstytucyjnie chronione prawa i wolności (w tym zakaz pozyskiwania i gromadzenia informacji o obywatelach, innych niż niezbędne w demokratycznym państwie prawa). Organy kontroli skarbowej zostały uprawnione do uzyskiwania danych chronionych tajemnicą zawodową (których to wcale organy te nie potrzebują). Rzecznik Praw Obywatelskich wyraził również obawę co do potencjalnie niewłaściwego wykorzystania uzyskanych informacji. Trybunał Konstytucyjny uznał zaś, że upoważnienie organów kontroli skarbowej do zbierania i przetwarzania danych osobowych w „celu realizacji ustawowych zadań" sformułowane w taki sposób, obarczone jest kilkoma poważnymi wadami. Ogólne tylko odesłanie do zadań ustawowych organów kontroli skarbowej nie spełnia przesłanki precyzyjności, wymaganej w sytuacji ingerencji organów państwa w sferę prywatności człowieka. Drugie zastrzeżenie, to brak określenia związku, jaki ma zachodzić między konkretnym typem danych, które mają być zbierane a konkretnym celem czynności organów kontroli skarbowej. Ponadto kwestionowany przepis ustawy o kontroli skarbowej zobowiązywał administratorów danych do udostępnienia uprawnionemu kontrolerowi wszystkich danych, o jakie zawnioskuje, bez jakichkolwiek gwarancji prawidłowego wykorzystania danych przez kontrolera. Trybunał Konstytucyjny uznał, że wobec braku jakichkolwiek gwarancji proceduralnych, nawet bardzo ogólny wymóg „celowości" ma znaczenie wyłącznie dla oceny prawidłowości działania samego organu; nie stwarza natomiast podstaw do odmowy udzielenia określonych informacji administratorowi danych. Wymóg powyższy w żadnej mierze

[6] Wyrok TK z dnia 11 kwietnia 2000, K 15/98, OTK 2000 nr 3, poz. 86.

nie spełnia zatem roli gwarancyjnej z punktu widzenia dostępności do danych osobowych kontrolowanych podmiotów[7].

Inaczej wygląda ochrona prywatności osób pełniących funkcje publiczne. W wyroku z dnia 6 grudnia 2005 TK zauważył, że ustawodawca ma swobodę w ustalaniu zakresu ograniczeń dotyczących osób pełniących funkcje publiczne, z uwagi na nasilenie zjawisk korupcji i negatywną reakcję społeczną. Pozostawać one powinny w racjonalnym związku z interesem publicznym, któremu mają służyć, a ich zakres powinien być współmierny do rangi tego interesu. Trybunał Konstytucyjny stwierdził, że wymóg informowania przez radnego o dochodach osiąganych z tytułu zatrudnienia lub innej działalności zarobkowej, z podaniem kwot uzyskiwanych z każdego tytułu, nie wykracza poza granice wynikające z art. 31 ust. 3 Konstytucji. Prawo do prywatności nie ma bowiem charakteru absolutnego, a ograniczenie ochrony prawa do prywatności należy w tym przypadku rozpatrywać w kontekście prawa do uzyskiwania informacji (art. 61 Konstytucji). W odniesieniu do osób pełniących funkcje publiczne, ingerencja w sferę życia prywatnego może być znacznie głębsza, niż to ma miejsce w stosunku do innych osób. Składanie oświadczeń majątkowych pełni funkcję antykorupcyjną. Każdy z wyborców może sprawdzić, czy majątek radnego wzrósł (od poprzedniego roku) i czy odpowiada osiąganym dochodom[8]. Prawo do ochrony danych osobowych jako element prawa do prywatności, nie może również służyć ochronie danych dłużnika. Powodowałoby to nieuzasadnione uprzywilejowanie dłużnika. Ochrona dóbr osobistych jednych nie może odbywać się kosztem naruszania praw innych[9].

W innym orzeczeniu TK stwierdził, że udostępnianie danych osobowych jest dopuszczalne, gdy gwarantuje poszanowanie życia prywatnego osób, których dane te dotyczą, a wolność dostępu do informacji i ochrona danych osobowych nie muszą pozostawać ze sobą w sprzeczności. Rozwiązanie kolizji prawa do informacji z jednej strony i prawa do prywatności z drugiej strony powinno, według TK, opierać się na dwóch założeniach. Po pierwsze, nie może dojść do całkowitej eliminacji jednego z praw (np. prawa do prywatności), ale konieczne jest znalezienie równowagi. Po drugie, w takich przypadkach mają istotne znaczenie istniejące preferencje aksjologiczne wyrażone w zasadach naczelnych Konstytucji (tj. dobro wspólne, godność każdego człowieka)[10].

---

[7] Wyrok TK z dnia 17 czerwca 2008, K 8/04, OTK-A 2008 nr 5, poz. 81.

[8] Wyrok TK z dnia 6 grudnia 2005, SK 7/05, OTK-A 2005 nr 11, poz. 129.

[9] Wojewódzki Sąd Administracyjny w Warszawie uznał, że prawo do ochrony danych osobowych, jako jeden z elementów prawa do ochrony własnej prywatności, ma swoje źródło w przepisach art. 47, art. 49, art. 50 i art. 51 Konstytucji RP.

Wyrok WSA w Warszawie z dnia 21 września 2005, II SA/Wa 1443/05, LEX nr 204649.

[10] Wyrok TK z dnia 20 marca 2006, K 17/05, OTK-A 2006 nr 3, poz. 30.

W wyroku z dnia 26 października 2005 TK uznał za niezgodne z konstytucją przepisy ustawy o IPN ograniczające dostęp do dokumentów Instytutu (art. 30 ust. 1 oraz art. 31 ust. 1 i 2, art. 33 ust. 1 oraz art. 35 ust. 2 ustawy o IPN są niezgodne z art. 47 oraz 51 ust. 3 i 4 Konstytucji) poprzez uzależnienie prawa dostępu do dokumentów IPN od uzyskania statusu pokrzywdzonego[11]. Stwierdził, że ograniczenie prawa dostępu do tajnego (zastrzeżonego) zbioru dokumentów jest podyktowane dobrem wszystkich obywateli (ich bezpieczeństwem) i ze względu na zapewnienie prawidłowego funkcjonowania państwa i jego organów – musi być respektowane. Osoba, która została zaliczona do kategorii pokrzywdzonych ma prawo do:

– ochrony danych osobowych na zasadach określonych w tej ustawie (art. 1 pkt 3);

– prawo do uzyskania informacji o posiadanych i dostępnych, dotyczących jej dokumentach (art. 30 ust. 1);

– prawo do uzyskania w nie wglądu oraz do wydania jej kopii tych dokumentów (art. 31 ust. 1 i 2);

– prawo do ujawnienia nazwisk oraz dalszych danych osobowych funkcjonariuszy, pracowników i współpracowników organów bezpieczeństwa (którzy zbierali i oceniali dane o pokrzywdzonym) – (art. 32 ust. 1);

– prawo do załączania do zbioru dotyczących jej dokumentów, uzupełnień, sprostowań, uaktualnień czy wyjaśnień (art. 33 ust. 1);

– prawo do żądania zwrotu przedmiotów, które w momencie utraty stanowiły jej własność lub były w jej posiadaniu (art. 33 ust. 4);

– prawo do anonimizacji dotyczących jej danych (art. 34 ust. 1);

– prawo do zastrzeżenia, że dotyczące jej dane osobowe niepodlegające anonimizacji nie będą udostępniane w celach badawczych przez określony czas, jednak nie dłużej niż przez 90 lat od daty ich wytworzenia (art. 37 ust. 1).

Nie doszło jednak do zrównania osób o statusie pokrzywdzonego z pozostałymi osobami zainteresowanymi dostępem do dokumentów gromadzonych przez IPN, chociaż dostęp mają funkcjonariusze Służby Bezpieczeństwa i osoby, którym IPN nie przyznał statusu pokrzywdzonego[12].

Konstytucyjne prawo dostępu do dokumentów urzędowych i zbiorów danych, na gruncie ustawy o IPN, stosuje się do dokumentów i zbiorów danych, zawierających informacje na podstawie celowo gromadzonych danych o tej osobie, a nie do wszystkich dokumentów związanych z tą osobą w jakikolwiek

---

[11] Więcej: A. Mościcka, *Dostęp tylko dla wybranych*, „Gazeta Prawna" 2005, nr 210.

[12] „Sędzia Jerzy Stępień, sprawozdawca w tej sprawie, podkreślił, że wyrok nie oznacza likwidacji statusu pokrzywdzonego ani zrównania prawa osoby pokrzywdzonej z wszystkimi innymi zainteresowanymi osobami. Chodzi w szczególności o tych, którzy wytwarzali dokumenty znajdujące się w archiwach IPN-u, czyli tajnych współpracowników służb bezpieczeństwa".

K. Rychter, *Nie zrównano agentów z pokrzywdzonymi*, „Gazeta Prawna" 2005, nr 232.

sposób. Prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób niezgodny z prawem nie może być ograniczone jedynie do osób tzw. pokrzywdzonych, gdyż wszelkie ograniczenia w korzystaniu z tych praw muszą być ściśle określone i zgodne z art. 31 ust. 3 Konstytucji. Żaden interes państwa nie może sankcjonować i usprawiedliwiać zachowywania w dokumentach urzędowych i zbiorach danych informacji nieprawdziwych. Ze względu na podwójny charakter danych (informacje osobiste i o charakterze historycznym), nie może wchodzić w grę ich usunięcie[13].

W wyroku z dnia 27 czerwca 2008 TK orzekł, że art. 70a ustawy – przepisy wprowadzające ustawę o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego w zakresie, w jakim nie pozwala osobom objętym badaniem Komisji Weryfikacyjnej na dostęp do informacji ich dotyczących gromadzonych przez organ administracji rządowej ani nie pozwala na sprostowanie lub usunięcie nieprawdziwych danych jest niezgodny z art. 51 ust. 3 i 4 Konstytucji. Przepis art. 70a formułuje generalne prawo dostępu do dokumentów urzędowych i zbiorów danych oraz prawo do żądania sprostowania oraz usunięcia informacji, bez względu na to, czy wobec zainteresowanego toczy się jakieś postępowanie prowadzone przez organy władzy publicznej. Dostęp do akt sprawy przez strony postępowań oraz prawo żądania sprostowania lub usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą, zamieszczonych w aktach sprawy, w celu wydania indywidualnego rozstrzygnięcia, jest jednym ze standardów sprawiedliwego postępowania administracyjnego. Prawo dostępu do dokumentów oraz prawo strony do wysłuchania w zakresie informacji zbieranych przez organ prowadzący postępowanie w jego

---

[13] Niegodne z Konstytucją artykuły ustawy o IPN:

Art. 30 ust. 1. Pokrzywdzonemu należy, na jego wniosek, udzielić informacji o posiadanych i dostępnych, dotyczących go dokumentach.

Art. 31 ust. 1.Pokrzywdzonego albo osobę mu najbliższą Instytut Pamięci informuje o istnieniu w archiwum Instytutu Pamięci dotyczących go dokumentów oraz o sposobie uzyskania w nie wglądu.

2. Na wniosek pokrzywdzonego wydaje się mu kopie dotyczących go dokumentów.

Art. 33 ust. 1. Pokrzywdzony ma prawo załączać do zbioru dotyczących go dokumentów własne uzupełnienia, sprostowania, uaktualniania, wyjaśnienia oraz dokumenty lub ich kopie. Dane już zawarte w dokumentach nie ulegają jednak zmianie.

Art. 35 ust. 2. Funkcjonariusza, pracownika lub współpracownika organów bezpieczeństwa państwa, po uprzednim złożeniu przez niego oświadczenia Instytutu Pamięci o fakcie jego służby, pracy lub współpracy z tymi organami, informuje się, na jego wniosek o dotyczących go dokumentach znajdujących się w archiwum Instytutu Pamięci."

Wyrok TK z dnia 26 października 2005, K 31/04, OTK-A 2005 nr 9, poz. 103.

Po publikacji tego orzeczenia w prasie ukazały się artykuły, w których zastanawiano się nad potrzebą nowelizacji ustawy o IPN – m.in. A. Mościcka, *Czy trzeba zmienić ustawę o IPN*, „Gazeta Prawna" 2005, nr 212; A. Stankiewicz, J. Kroner, *Agenci zajrzą do teczek*, „Rzeczpospolita" 2005 nr 252; J. Kroner, *Teczki nie będą pułapką na kłamców*, „Rzeczpospolita" 2005, nr 284.

sprawie, wynika nie tylko z treści art. 51 Konstytucji, ale również z art. 2 Konstytucji. Kwestionowany przepis ustawy nie gwarantował zainteresowanym tych praw, dlatego też, został uznany za niekonstytucyjny[14].

Również w wyroku z dnia 12 grudnia 2005 TK wypowiedział się na temat zbierania (przetwarzania) danych osobowych przez Policję. Przyznał, że wobec zagrożeń istniejących we współczesnym świecie działania operacyjne policji są nieodzowne, ale często dochodzi do kolizji między obowiązkiem ochrony obywateli a ich prawem do prywatności. Zabronił Policji zbierać danych niemających związku z prowadzonym śledztwem. Niekonstytucyjny okazał się brak precyzji w określeniu, jakie informacje o przestępcach można gromadzić (nie powinna o tym decydować sama Policja)[15]. Następcza zgoda sądu na zachowanie materiałów operacyjnych zdobytych w sposób nielegalny (które powinny ulec zniszczeniu) nie może ograniczać konstytucyjnego prawa określonego w art. 51 ust. 4 (sprostowania informacji zebranych w sposób niezgodny z ustawą)[16]. Potencjalna celowość gromadzenia przez Policję informacji nie może być utożsamiana z niezbędnością w demokratycznym państwie prawnym. Zatem art. 20 ust. 2 ustawy o Policji, który nie określa warunków kiedy można zbierać informacje, a kiedy należy od tego odstąpić, narusza art. 51 ust. 5 Konstytucji (który wymaga, aby możliwie szczegółowo uregulować zasady i tryb gromadzenia informacji o jednostce).

Za niekonstytucyjny został uznany także przepis, który nie przewidywał usuwania ze zbiorów danych zebranych o osobach podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, które zostały prawomocnie uniewinnione, bądź wobec których postępowanie karne zostało prawomocnie bezwarunkowo umorzone, niezwłocznie po uprawomocnieniu się stosownego orzeczenia, ponieważ dalsze gromadzenie danych osoby podejrzanej w tej sytuacji traci cechę niezbędności. Możliwość zachowania danych nie dotyczy danych wrażliwych, ponieważ zebrane dane nie mogą szkodzić osobie prawomocnie uniewinnionej oraz jest to sprzeczne z art. 20 ust. 18 ustawy.

Niedopuszczalne jest także by zgoda jednej osoby przesądzała o ograniczeniu praw obywatelskich innej osoby. Zakwestionowany przez TK przepis ustawy

---

[14] Wyrok TK z dnia 27 czerwca 2008, K 51/07, OTK-A 2008 nr 5, poz. 87.

[15] Wyrok TK z dnia 12 grudnia 2005, K 32/04, OTK-A 2005 nr 11, poz. 132.

W sprawie K 32/04 Trybunał Konstytucyjny wydał postanowienie o umorzeniu postępowania w zakresie badania zgodności art. 20 ust. 19 ustawy z dnia 6 kwietnia 1990 o Policji, Dz. U. 2002 nr 7, poz. 58 z póź. zm. z art. 51 ust. 5 Konstytucji ze względu na cofnięcie wniosku przez RPO. Postanowienie TK z dnia 23 listopada 2005, K 32/04, OTK-A 2005 nr 10, poz. 126.

J. Kroner, *Funkcjonariuszom wolno zbyt wiele*, „Rzeczpospolita" 2005, nr 290.

[16] Trybunał Konstytucyjny musiał między innymi rozstrzygnąć dopuszczalność wykorzystania w procesie karnym „owoców zatrutego drzewa". Następcza zgoda sądu na zachowanie materiałów zebranych w ciągu pięciu dni (tymczasowego prowadzenia kontroli) legitymizuje możliwość dalszego, już legalnego, wykorzystania tych informacji w postępowaniu karnym.

o Policji pozwalał na inwigilację bez zgody sądu. Wystarczyła sama zgoda informatora na bycie inwigilowanym, a osoba utrzymująca kontakt z informatorem była podsłuchiwana „przy okazji". Taka zgoda nic nie kosztuje wyrażającego ją, ale także niczego nie gwarantuje drugiej stronie, w której sferę prywatności wkracza kontrola operacyjna. Dlatego też TK uznał, że alternatywne traktowanie zgody sądu i pisemnej zgody jednego z uczestników przekazu informacyjnego jest nieproporcjonalne i niezgodne z Konstytucją.

Trybunał Konstytucyjny orzekł również nielegalność zarządzenia nr 6[17] Komendanta Głównego Policji w sprawie uzyskiwania, przetwarzania i wykorzystywania informacji dotyczących m.in. fotografowania, daktyloskopowania[18] ponieważ zasady i tryb gromadzenia oraz udostępniania informacji o obywatelach może określać tylko ustawa. W zarządzeniu Komendant Główny Policji określił samodzielnie sytuacje, w których Policja pobiera np. odciski linii papilarnych lub sytuacji w których Policja może nie ingerować w konstytucyjne prawa obywateli.

W kolejnej sprawie dotyczącej Policji, Trybunał Konstytucyjny musiał rozstrzygnąć, czy jest zgodny z art. 51 ust. 2 Konstytucji, 47 Konstytucji w zw. z art. 31 ust. 3 Konstytucji zapis art. 62a ustawy o Policji, który zobowiązywał policjanta do poinformowania przełożonego (właściwego do spraw osobowych) o podjęciu przez małżonka lub osoby pozostające z nim we wspólnym gospodarstwie domowym zatrudnienia lub innych czynności zarobkowych w podmiotach świadczących usługi detektywistyczne lub ochrony osób i mienia oraz o objęciu w nich akcji lub udziałów, a także o fakcie bycia wykonawcą (zgodnie z prawem zamówień publicznych) na rzecz organów i jednostek nadzorowanych i podległych ministrowi właściwemu do spraw wewnętrznych, w terminie 14 dni od dnia powzięcia informacji o tym zdarzeniu. Rzecznik Praw Obywatelskich (wnioskodawca) nie negując tego, że przepis ten pełni rolę normy antykorupcyjnej, jednocześnie uznał, iż art. 62a ustawy o Policji jest sprzeczny z zasadą zaufania obywateli do państwa i stanowionego przez nie prawa. Kontrolowanej regulacji prawnej nie można bowiem uznać za służącą osiągnięciu założonego

---

[17] Art. 19 ust. 4, 18 oraz Art. 20 ust. 2 ustawy o Policji z dnia 6 kwietnia 1990, Dz. U. 2002 nr 7, poz. 58 z póź. zm., oraz zarządzenie Nr 6 Komendanta Głównego Policji z dnia 16 maja 2002 w sprawie uzyskiwania, przetwarzania i wykorzystywania przez Policję informacji oraz sposobów i prowadzenia zbiorów tych informacji, Dz. Urz. KGP Nr 8 poz. 44 oraz Nr 9 poz. 47 są niezgodne z Konstytucją.

[18] Trybunał uznał, że normy dotyczące np. daktyloskopowania nie mogą być regulowane w rozporządzeniu i powinny być zamieszczane w ustawie. W lipcu 2006 znowelizowano ustawę o policji. Doprecyzowano kataog sytuacji, w których policja może gromadzić i przetwarzać informacje o osobach, tj. dane osobowe, odciski linii papilarnych, zdjęcia, znaki szczególne, pseudonimy.

WIK, *Zaostrzenie zasad kontroli operacyjnej*, „Rzeczpospolita" 2006 nr 170; A. Wyszomirska, *Informacje muszą być niszczone*, „Gazeta Prawna" 2005 nr 241; M. Marczuk, *Trudne rozstanie z niekonstytucyjnym podsłuchem*, „Gazeta Prawna" 2006 nr 16.

przez ustawodawcę celu. Wnioskodawca stwierdził ponadto, że kwestionowane unormowanie prawne zbyt drastycznie ingeruje w sferę prywatności osób trzecich pozostających z policjantem we wspólnym gospodarstwie domowym. Ustawodawca nie wskazał przy tym wartości konstytucyjnych, które uzasadniałyby wprowadzenie takiej regulacji. Trybunał Konstytucyjny w swoim orzeczeniu zaprezentował zupełnie inny pogląd. Uznał bowiem, że kwestionowana regulacja prawna jest niezbędna i przydatna do osiągnięcia założonego przez ustawodawcę celu, a stopień i zakres ograniczenia m.in. autonomii informacyjnej policjanta i jego bliskich odpowiada wymogom proporcjonalności określonym w art. 31 ust. 3 Konstytucji. Obowiązek nałożony na funkcjonariusza ma wyłącznie charakter informacyjny, a zbierane informacje dotyczą tylko niektórych policjantów i nie są udostępniane publicznie[19].

Trybunał Konstytucyjny rozpatrując połączone skargi Agnieszki Gargas-Litwińskiej, Doroty Mroczek, Roberta Wąsowicza i Krzysztofa Buczka[20] musiał rozstrzygnąć czy art. 180 § 2 k.p.k., w zakresie w jakim dopuszcza zwolnienie dziennikarza z tajemnicy zawodowej, jest zgodny m.in. z art. 51 ust. 2 Konstytucji. Sąd na podstawie zaskarżonego przepisu zwolnił ich z obowiązku zachowania tajemnicy. Radcowie zaskarżyli to postanowienie, lecz sąd II instancji utrzymał je w mocy. Zdaniem wnioskodawców, zaskarżony art. 180 §. 2 k.p.k. niweczy instytucję tajemnicy zawodowej, ponieważ obowiązek zachowania tajemnicy zawodowej jest koniecznym warunkiem wykonywania tego zawodu. Pole do nadużyć stwarzają również mało precyzyjne zwroty (np. dobro wymiaru sprawiedliwości). Trybunał Konstytucyjny stwierdził jednak, że teoretycznie na naruszenie wolności wskazanych w art. 49 i art. 51 ust. 2, mogliby się raczej powoływać klienci radców prawnych, a nie sami radcowie. Obowiązek zachowania tajemnicy zawodowej ma chronić klientów, a nie radców. Zachowanie tajemnicy służbowej nie jest konstytucyjnym prawem radców prawnych. Nie można zatem uznać, że zwolnienie z obowiązku jej zachowania wówczas, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości i nie istnieją inne możliwości ustalenia prawdy, narusza Konstytucję[21].

W innym orzeczeniu tajemnicy statystycznej TK orzekł, że art. 180 § 1 k.p.k., w zakresie w jakim zwalnia z tajemnicy statystycznej, jest niezgodny z art. 51

---

[19] Wyrok TK z dnia 23 lutego 2010, K 1/08, OTK-A 2010 nr 2, poz. 14.

[20] Skarżący, w momencie wnoszenia skargi byli radcami prawnymi, którzy świadczyli pomoc prawną na rzecz spółki „Optimus" S.A. W toku postępowania karnego, toczącego się przeciwko byłemu Prezesowi Zarządu Spółki i innym kierującym nią osobom, Prokuratura Apelacyjna w Krakowie uznała za konieczne przesłuchanie ich w charakterze świadka (przy czym przesłuchanie miało dotyczyć informacji objętych tajemnicą zawodową radcy prawnego).

[21] Wyrok TK z dnia 22 listopada 2004, SK 64/03, OTK-A 2004 nr 10, poz. 107.

A. Wyszomirska, *Gwarancje poufności dla klienta, a nie dla radcy*, „Gazeta Prawna" 2004, nr 228; J.K., *Radcę może przesłuchać*, „Rzeczpospolita" 2004, nr 274.

ust. 2 oraz art. 47 i 31 ust. 3 Konstytucji. Niekonstytucyjna nie była sama dopuszczalność zwolnienia z obowiązku zachowania tajemnicy statystycznej, co brak wyraźnych przesłanek takiego zwolnienia przez prokuratora lub sąd oraz brak procedury umożliwiającej weryfikację o zwolnieniu z tego obowiązku. Zwłaszcza, gdy objęte tajemnicą są dane osobiste dotyczące życia prywatnego. W takim przypadku ochrona danych statystycznych powinna być zaostrzona, chociaż nie absolutna. Obowiązek statystyczny został wprowadzony w celu realizacji głównie interesu publicznego i w przeciwieństwie do innych tajemnic nie obejmuje informacji udzielanych dobrowolnie przez jednostki i w żadnym stopniu nie przysparza korzyści udzielającemu informacji. Zatem zwolnienie z tajemnicy statystycznej może doprowadzić do samooskarżania udzielającego tych informacji[22].

W sprawie SK 40/01 TK stwierdził, że księgi stanu cywilnego to rejestry szczególne, służące gromadzeniu przez właściwe organy państwowe składających się na stan cywilny informacji o obywatelach. Informacje te pozwalają następnie na ustalenie zaistnienia określonych zdarzeń i powstanie oznaczonych skutków prawnych[23]. Na gruncie tej sprawy TK stwierdził, że istota autonomii informacyjnej (z art. 51 Konstytucji) każdego człowieka sprowadza się do pozostawienia każdej osobie swobody w określeniu dostępności dla innych wiedzy o sobie. Informacja odnosząca się do zaprzeczenia ojcostwa dziecka, później uznanego przez skarżącego, należy do sfery prywatności zarówno ojca, jak i dziecka. Osoby zainteresowane (np. rodzice) nie mogą żądać wykreślenia ani usunięcia danych godzących w ich prywatność kreujących stan cywilnych i które są wymagane przepisami ustawy (o aktach stanu cywilnego). Naruszenia konstytucyjnego prawa do ochrony danych osobowych można ewentualnie doszukiwać się nie w samym ustawowym obowiązku rejestrowania określonych zdarzeń, ale w nałożeniu tego obowiązku z naruszeniem konstytucyjnej przesłanki niezbędności w demokratycznym państwie prawnym. Skarżący wskazuje, że utrzymywanie w treści aktu stanu cywilnego informacji o zaprzeczeniu ojcostwa narusza wyżej wspomniane kryterium. Z drugiej jednak strony na rzecz spełnienia przesłanki „niezbędności" przemawia fakt, że nie istnieje żaden inny sposób gromadzenia tych danych. W związku z tym prawo do ochrony danych osobowych określone w art. 51 ust. 2 Konstytucji nie podlega naruszeniu ze względu na sam fakt gromadzenia i rejestrowania danych mających znaczenia dla ustalenia stanu

[22] Wyrok TK z dnia 13 grudnia 2011, K 33/08, OTK-A 2011 nr 10, poz. 116.

[23] Skarżący uznał Szymona M. za swoje dziecko, po tym jak zostało obalone domniemanie jego pochodzenia z małżeństwa matki ze Szczepanem M. W akcie urodzenia dziecka została uwzględniona wzmianka dodatkowa o uznaniu dziecka, jednak w rubryce „ojciec" pozostawiono dane Szczepana M.. Krzysztof Toboła (skarżący) wystąpił z wnioskiem o sprostowanie aktu urodzenia syna i wykreślenie danych Szczepana M.

Wyrok TK z dnia 12 listopada 2002, SK 40/01, OTK-A 2002 nr 6, poz. 81.

cywilnego. Odnośnie prawa do sprostowania lub usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą TK stwierdził, że w momencie dokonywania odpowiedniego wpisu w aktach urodzenia dziecka domniemanie to istniało i stanowiło podstawę kształtowania stanu cywilnego dziecka, a dane składające się na stan cywilny jednej osoby mogą wpływać na skuteczność praw innych osób. Z analizy przepisów ustawy o aktach stanu cywilnego wynika, że definitywne usunięcie informacji z aktu urodzenia nie następuje nawet w przypadku przysposobienia całkowitego. W takich przypadkach dochodzi – albo może dojść – do sporządzenia nowego aktu urodzenia, a dotychczasowy akt urodzenia ze stosowną wzmianką jest nadal zachowywany i może być udostępniany przysposobionemu po osiągnięciu pełnoletności.

W innej sprawie Mariusz Kaźmierczyk skargą konstytucyjną z dnia 27 marca 2006 wniósł o stwierdzenie, że art. 76 k.r.o., w zakresie, w jakim uniemożliwia uznanie dziecka po jego śmierci, o ile nie pozostawia ono zstępnych, jest niezgodny z art. 51 ust. 4 Konstytucji. Zgodność ze stanem faktycznym informacji gromadzonych przez organy władzy publicznej jest jednym z warunków wykonywania zadań przez te organy i służy prawidłowości rozstrzygnięć indywidualnych wydawanych przez te organy. Trybunał Konstytucyjny podzielił pogląd, że sam akt uznania dziecka nie dotyczy jednak sfery autonomii informacyjnej i nie może być uważany za środek prostowania informacji zgromadzonych przez organy władzy publicznej. Niemożność uznania dziecka zmarłego bezpotomnie nie dotyka bezpośrednio prawa do sprostowania informacji nieprawdziwych (z art. 51 ust. 4 Konstytucji). Nie ma zatem podstaw do stwierdzenia niezgodności z nim art. 76 k.r.o.[24].

Trybunał Konstytucyjny w sprawie U 5/97 orzekł niezgodność z Konstytucją zakwestionowanego przepisu § 5 ust. 1 rozporządzenia Ministra Zdrowia

---

[24] Wyrok TK z dnia 16 lipca 2007, SK 61/06, OTK-A 2007 nr 7, poz. 77.

W tej sprawie również Marszałek Sejmu jak i Prokurator Generalny uznali, że nie można żądać sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych czy też zebranych w sposób sprzeczny z ustawą, ponieważ akt stanu cywilnego zmarłej córki skarżącego został sporządzony prawidłowo, zgodnie z wymogami ustawy. Nieadekwatnym wzorcem kontroli konstytucyjności w tej sprawie jest powołanie się zatem na ten artykuł Konstytucji. Trybunał Konstytucyjny stwierdził, że konstytucyjna ochrona musi przewidywać odpowiednie rozwiązania prawodawcze także na wypadek śmierci dziecka. Powinna szanować uczucia rodziców i uwzględniać ich potrzebę ustalenia rodzicielstwa dziecka, w sytuacji gdy nie było to możliwe przed jego śmiercią. Prawo rodziców do ustalenia rodzicielstwa obejmuje również dziecko zmarłe, pomimo że ustalenie nie doprowadzi do ukształtowania się więzi rodzinnej z dzieckiem. Tymczasem zaskarżony przepis uniemożliwia ustalenie rodzicielstwa w tej sytuacji. Zdaniem Trybunału nie tylko narusza przez to sferę osobistych i emocjonalnych odczuć rodziców, ale przede wszystkim konstytucyjne prawo do ochrony rodzicielstwa. W związku z tym Trybunał uznał, że art. 76 ustawy z dnia 25 lutego 1964 – kodeks rodzinny i opiekuńczy, Dz. U. nr 9, poz. 59 z póź. zm., jest niezgodny z art. 47 Konstytucji w związku z art. 31 ust. 3 oraz w związku z art. 18 Konstytucji.

J. Kroner, *Ojciec może uznać zmarłe dziecko*, „Rzeczpospolita" 2007, nr 165.

i Opieki Społecznej[25]. Miał na uwadze postanowienia ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych, która gwarantuje każdemu prawo do ochrony dotyczących go danych osobowych, oraz że przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą. Zgodnie z art. 27 ust. 1 i 2 w zw. z art. 7 pkt 2 tej ustawy zabrania się zbierania, utrwalania, przechowywania, udostępniania danych o stanie zdrowia bez zgody osoby, której dotyczą, chyba że przepis szczególny ustawy na to zezwala i stwarza pełne gwarancje ich ochrony. Zaskarżony przepis nakazywał zaś uwidocznienie numeru statystycznego choroby w orzeczeniu lekarskim, a znajomość tego numeru nie jest niezbędna pracodawcy (do ustaleniu prawa do zasiłku) i nie ma gwarancji zachowania poufnego charakteru informacji o rodzajach chorób pracowników[26].

We wniosku skierowanym do TK[27], grupa posłów uznała, że art. 22 ustawy o CBA ogranicza prawa do prywatności oraz pozbawia prawa do żądania sprostowania oraz usunięcia nieprawdziwych informacji. Artykuł 22 pozwala CBA gromadzić wszelkie dane osobowe, jeśli jest to uzasadnione charakterem realizo-

---

[25] Rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 17 maja 1996 w sprawie orzekania o czasowej niezdolności do pracy Dz. U. Nr 63, poz. 202, § 5 ust. 1. Orzeczenie lekarskie oraz orzeczenie o czasowej niezdolności do pracy z powodu konieczności osobistego sprawowania przez pracownika opieki nad chorym członkiem rodziny jest wydawane na formularzu zaświadczenia o czasowej niezdolności do pracy, według wzoru stanowiącego załącznik nr 2 do rozporządzenia.

[26] Trybunał Konstytucyjny postanowił, że utrata mocy obowiązującej §5 ust.1 rozporządzenia nastąpi do 19 maja 1999 ze względu na potrzeby prawodawcze, stosowny czas na rozważenie argumentów podniesionych w uzasadnieniu wyroku oraz potrzebę uchwalenie ustawy. Ponadto Trybunał orzekł, że kwestionowany przepis rozporządzenia poza konstytucją, narusza również art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności oraz art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych. Wyrok TK z dnia 19 maja 1998, U 5/97, OTK 1998, nr 4, poz. 46.

Również Sąd Najwyższy rozstrzygał kwestię czy pracodawca może żądać od pracownika zaświadczenia o zarobkach u innego pracodawcy. W wyroku z dnia 8 maja 2002, SN stwierdził, że pracodawca może żądać od pracownika złożenia zaświadczenia o zarobkach uzyskiwanych u drugiego pracodawcy. Powód twierdził natomiast, że naruszono jego dobro osobiste w postaci prawa do nieujawniania drugiego miejsca pracy (a wynika to z prawa do „autonomii informacyjnej) oraz prawa do prywatności. Sąd Najwyższy uznał jednak, że zobowiązanie powoda do przedstawienia zaświadczenia, które pozwoliłoby ustalić jego rzeczywistą sytuację materialną, nie nosi cech działania bezprawnego. Jest bowiem zgodne z postanowieniami ustawy o zakładowym funduszu świadczeń socjalnych oraz postanowieniami regulaminu przyznawania zapomóg i zapomóg losowych z zakładowego funduszu świadczeń socjalnych obowiązującego u strony pozwanej. Więcej: Wyrok SN z dnia 8 maja 2002, I PKN 267/01, OSNP 2004, nr 6, poz. 99.

[27] Grupa posłów wystąpiła 17 lipca 2006 z wnioskiem o stwierdzenie niezgodności niektórych przepisów ustawy o CBA z Konstytucją RP oraz EKPC. Trybunał postanowieniem z dnia 21 listopada 2007 umorzył postępowanie ze względu na niedopuszczalność wydania wyroku ze względu na utratę przez wnioskodawcę legitymacji czynnej, z powodu wcześniejszego rozwiązania Sejmu i zarządzenia przez Prezydenta nowych wyborów do Sejmu i Senatu na 21 października 2007, K 23/06, OTK-A 2007 nr 10, poz. 141.

wanych zadań. Wnioskodawcy uważają, że takie uprawnienie ingeruje w prawo do prywatności i autonomię informacyjną (tym bardziej, że dopuszcza się zbieranie danych wrażliwych, czyli np.: o stanie zdrowia, życiu seksualnym), a ponadto nie została zachowana zasada proporcjonalności; brakuje też kontroli sądowej legalności gromadzenia i przetwarzania danych osobowych przez CBA. W efekcie nie jest możliwa obiektywna kontrola działań CBA. Z treści art. 22 ustawy wynika też, że możliwe jest ograniczenie prawa do prywatności (autonomii informacyjnej) bez skonkretyzowania celów tego ograniczenia. Oznacza to, że ingerencja nie spełnia wymogów ustawowej konieczności i określoności działania władz publicznych oraz wykracza poza wymóg ograniczania prawa do prywatności jedynie w celach, dla których je wprowadzono[28]. Przyłączyłabym się do opinii, że w demokratycznym państwie prawnym, konieczne i dopuszczalne jest przetwarzanie danych osobowych tylko ze względu na ich potencjalną przydatność w przyszłości. Brak jasnych i precyzyjnych przepisów dotyczących możliwości zbierania i wykorzystywania danych osobowych przez CBA nie gwarantuje poszanowania praw jednostki[29].

Prokurator Generalny uznał jednak, że zwalczanie korupcji jest ważnym obowiązkiem państwa i jest konieczne w demokratycznym państwie prawnym (spełnia wymóg z art. 31 ust. 3 Konstytucji). Zatem gromadzenie danych (także wrażliwych), ich sprawdzanie oraz przetwarzanie stanowi uprawnione ograniczenie praw i wolności jednostki. Gwarancje dla osób, których dane te dotyczą, przewiduje procedura protokolarnego i komisyjnego zniszczenia. Następuje to niezwłocznie po uprawomocnieniu się uniewinniającego orzeczenia. Zgodnie z art. 13 ust. 4 ustawy o CBA zobowiązuje funkcjonariuszy CBA do poszanowania godności ludzkiej oraz przestrzegania i ochrony praw człowieka niezależnie od jego narodowości, pochodzenia, wyznania, przekonań politycznych, religijnych albo światopoglądowych. Także w opinii Sejmu art. 22 nie narusza przepisów Konstytucji i nie sprzeniewierza się zasadzie proporcjonalności, a sama już instytucja kontroli jest formą ingerencji w prawa i wolności[30]. Do kwestii kon-

---

[28] Negatywną opinię na temat m.in. art. 22 ustawy o CBA wyraził również: W. Gontarski, *Czy godzi się naruszać prawo do godnego życia*, „Rzeczpospolita" 2006, nr 160.

[29] Andrzej Sakowicz uważa, że art. 22 ustawy o CBA narusza zasadę określoności ustawowej ingerencji w sferę konstytucyjnych wolności i praw jednostki i może stać się samoistną przesłanką do stwierdzenia niekonstytucyjności. A. Sakowicz, *Ingerencja w prywatność musi być usprawiedliwiona*, „Rzeczpospolita" 2006, nr 201.

[30] Kwestionowany we wniosku posłów do TK o zbadanie zgodności z Konstytucją art. 22. Ustawy o CBA stanowił, że:

1. W zakresie swojej właściwości CBA może uzyskiwać informacje, w tym także niejawnie, gromadzić je, sprawdzać i przetwarzać.

2. CBA w celu zapobieżenia lub wykrycia przestępstw, określonych w art. 2 ust. 1 pkt 1, oraz identyfikacji osób może przetwarzać informacje, w tym również dane osobowe ze zbiorów prowadzonych na

stytucyjności art. 22 ustawy o CBA z Konstytucją wrócił TK w sprawie K 54/07[31]. Wówczas uznał, że CBA nie może bez zgody i wiedzy osoby przetwarzać jej danych osobowych, jeśli tylko jest to uzasadnione charakterem zadań realizowanych przez CBA. Za niezgodne z Konstytucją zostało uznane także: zobowiązanie administratora zbioru danych do udostępnienia danych na podstawie imiennego upoważnienia wydanego przez Szefa CBA okazanego przez

---

podstawie odrębnych przepisów przez organy władzy publicznej i państwowe jednostki organizacyjne, a w szczególności z Ewidencji Działalności Gospodarczej, Krajowej Ewidencji Podatników, Krajowego Rejestru Karnego, Krajowego Rejestru Sądowego, Powszechnego Elektronicznego Systemu Ewidencji Ludności, Rejestru Podmiotów Gospodarki Narodowej, Centralnego Rejestru Ubezpieczonych i Centralnego Rejestru Płatników Składek, Centralnej Ewidencji Pojazdów i Kierowców, Krajowego Centrum Informacji Kryminalnych. Administratorzy danych gromadzonych w tych rejestrach są obowiązani do nieodpłatnego ich udostępniania.

3. Dane ze zbiorów, o których mowa w ust. 2, przekazuje się w szczególności na nośniku optycznym, magnetycznym lub w drodze teletransmisji.

4. W zakresie swojej właściwości CBA może zbierać także wszelkie niezbędne dane osobowe, w tym również, jeżeli jest to uzasadnione charakterem realizowanych zadań, dane wskazane w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych (Dz. U. z 2002 nr 101, poz. 926 i nr 153, poz. 1271 oraz z 2004 nr 25, poz. 219 i nr 33, poz. 285), a także korzystać z danych osobowych i innych informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez uprawnione do tego organy, służby i instytucje państwowe oraz przetwarzać je, w rozumieniu ustawy o ochronie danych osobowych, bez wiedzy i zgody osoby, której te dane dotyczą.

5. Administrator zbioru danych jest obowiązany udostępnić określone w upoważnieniu dane osobowe, o których mowa w ust. 4, na podstawie imiennego upoważnienia wydanego przez Szefa CBA okazanego przez funkcjonariusza wraz z legitymacją służbową.

6. Dane osobowe zebrane w celu wykrycia przestępstwa przechowuje się przez okres, w którym są one niezbędne dla realizacji ustawowych zadań wykonywanych przez CBA. Funkcjonariusze CBA dokonują weryfikacji tych danych nie rzadziej niż co 10 lat od dnia uzyskania informacji, usuwając dane zbędne.

7. Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową oraz dane o stanie zdrowia, nałogach lub życiu seksualnym osób podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, które nie zostały skazane za te przestępstwa, podlegają komisyjnemu i protokolarnemu zniszczeniu niezwłocznie po uprawomocnieniu się stosownego orzeczenia.

8. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór upoważnienia, o którym mowa w ust. 5, zakres i tryb jego wydawania oraz zakres przedmiotowy upoważnienia mając na uwadze zapewnienie prawidłowego wykonania czynności przez funkcjonariusza CBA.

9. Prezes Rady Ministrów określi, w drodze rozporządzenia, zakres, warunki i tryb przekazywania CBA informacji przez organy, służby i instytucje państwowe, o których mowa w ust. 2 i 4, z uwzględnieniem sposobu dokumentowania tych informacji oraz podmiotów upoważnionych do ich przekazywania.

10. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposoby przetwarzania danych osobowych, o których mowa w ust. 2 i 4, w zbiorach danych, rodzaje jednostek organizacyjnych CBA uprawnionych do korzystania z tych zbiorów oraz wzory dokumentów obowiązujących przy przetwarzaniu danych, uwzględniając potrzebę ochrony danych przed nieuprawnionym dostępem.

Ustawa o Centralnym Biurze Antykorupcyjnym z dnia 9 czerwca 2006, Dz. U. 2014, poz. 1411 z póź. zm.

[31] Wyrok TK z dnia 23 czerwca 2009, K 54/07, OTK-A 2009 nr 8, poz. 86.

funkcjonariusza wraz legitymacją służbową, nieokreślony precyzyjnie okres weryfikacji prawdziwości i przydatności zbieranych danych osobowych (nie rzadziej niż co 10 lat) oraz procedura postępowania z danymi wrażliwymi (o nałogach, stanie zdrowia, życiu seksualnym)[32]. Trudno było uznać za legalne korzystanie przez CBA z danych wrażliwych (oraz informacji uzyskanych w toku czynności operacyjno-rozpoznawczych) bez wiedzy i zgody osoby, której dane dotyczą, bez jednoczesnego zagwarantowania instrumentów kontroli sposobów przechowywania i weryfikacji tych danych oraz sposobu usuwania danych zbędnych z punktu widzenia realizacji ustawowych zadań CBA[33].

[32] Przepisy art. 22 ust. 2-7 przestały obowiązywać od dnia 2 września 2010, Dz. U. Nr 151, poz. 1014.

[33] Wyrok Trybunału Konstytucyjnego z dnia 23 czerwca 2009 doczekał się licznych komentarzy prasowych. Ewa Siedlecka proponuje, aby kontrolować czy służby (CBA) „zbierają tylko to, co im wolno, i niszczą to, co nie służy ściganiu przestępstw". E. Siedlecka, *Trybunał kończy podsłuchowisko*, „Rzeczpospolita" z dnia 24 czerwca 2009, <http://wyborcza.pl/1,76842,6750534,Trybunal_konczy_podsluchowisko.html>, dostęp: 5 grudnia 2014.

Rozdział 5. Prawo do ochrony danych osobowych a wolność wypowiedzi w świetle orzecznictwa Europejskiego Trybunału Praw Człowieka

Europejski Trybunał Praw Człowieka w swoich orzeczeniach często wytyczał granice prywatności i stwierdzał, że ochrona życia prywatnego (określona w art. 8 Konwencji) nie ma charakteru absolutnego i musi być równoważona np. wolnością słowa (określoną w art. 10 tejże Konwencji). Wielokrotnie podkreślał też, że obowiązkiem prasy (a nie tylko przywilejem) jest rozpowszechnianie informacji i opinii w sprawach dotyczących interesu publicznego, ale równocześnie rozgraniczał kontrowersyjny nawet w formie ale rzetelny, obiektywny i prawdziwy głos mediów w dyskusji publicznej od ingerencji prasy w sferę życia prywatnego jedynie w celu wywołania sensacji. Jak wskazuje ETPC media nie pełnią roli „strażnika" demokracji, gdy ingerują w prywatność osób, które nie pełnią żadnej publicznej funkcji. Przypomniał także, że ochrona życia prywatnego (i danych osobowych) ma szczególne znaczenie dla prawidłowego rozwoju osobowości człowieka[1].

W sprawie von Hannover v. Niemcy ETPC wyraził pogląd, że choć opinia publiczna ma prawo do informacji, która to jest podstawowym prawem w demokratycznym społeczeństwie, oraz że w pewnych szczególnych okolicznościach może nawet obejmować aspekty życia prywatnego osób publicznych, (zwłaszcza gdy dotyczy polityków), to każdy ma prawo do ochrony prywatności. W tym przypadku publikacja zdjęć z wakacji Księżny Karoliny von Hannover i jej męża Księcia Ernsta Augusta von Hannover nie służyła jakiejkolwiek debacie publicznej, a wyłącznie ujawnieniu i komentowaniu szczegółów z życia prywatnego skarżącej[2]. Strasburscy sędziowie w toku procedowania weryfikowali bowiem dwie okoliczności: czy ujawnianie tożsamości, wizerunku oraz faktów dotyczących jednostki, a zwłaszcza jej życia prywatnego, dotykało osobę publiczną i łączyło się ze sprawowaną przez nią publiczną rolą oraz czy publikacja stanowiła wkład w debatę publiczną[3].

---

[1] Zob: teza 39, Judgment in the case of Armoniene v. Lithuania, (Application no. 36919/02), 25 listopada 2008
<http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89823>, dostęp: 28 lutego 2014.

[2] Zob. teza 63 i 64 Judgment in the case of von Hannover v. Germany, (Application no. 59320/00). 24 czerwca 2004
<http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61853>, dostęp: 4 marca 2014.

[3] Więcej: I. C. Kamiński, *Determinanty działalności dziennikarskiej. Uprawnienia i obowiązki dziennikarskie w orzecznictwie Europejskiego Trybunału Praw Człowieka*, [w:] *Status prawny dziennikarza*, pod red. W. Lisa, Warszawa 2014, LEX nr 198161.

Europejski Trybunał Praw Człowieka w sprawie Węgrzynowski i Smolczewski przeciwko Polsce musiał rozstrzygać konflikt między ochroną danych osobowych a prawem do informacji w Internecie. Prawnicy, Tadeusz Smolczewski i Szymon Węgrzynowski, (wspólnicy kancelarii prawnej „Iurator") wnieśli sprawę do ETPC, gdyż sądy polskie nie uwzględniły ich roszczenia i nie nakazały wydawcy „Rzeczpospolitej" usunięcia z archiwum gazety artykułów, w których Anna Marszałek i Bertold Kittel zarzucili im nieuzasadnione czerpanie korzyści z likwidacji upadających przedsiębiorstw państwowych (których likwidatorem był Smolczewski) oraz odzyskiwania w imieniu spółki Argon pieniędzy od Skarbu Państwa (czym zajmował się Węgrzynowski). Sprawa o naruszenie dóbr osobistych Węgrzynowskiego i Smolczewskiego, spowodowana była m.in. publikacją ww. dziennikarzy: *Wojewoda w sieci*. Prawnicy wnieśli powództwo przeciwko: dziennikarzom, ówczesnemu redaktorowi naczelnemu (Maciejowi Łukaszewiczowi) oraz wydawcy „Rzeczpospolitej" („Presspublica Sp. z o.o."). Sprawa zakończyła się zasądzeniem od dziennikarzy i redaktora naczelnego zadośćuczynienia i nakazaniem publikacji przeprosin[4]. Wyrok – choć korzystny – nie przyniósł satysfakcji Węgrzynowskiemu i Smolczewskiemu. W kolejnym powództwie przeciwko naczelnemu i wydawcy „Rzeczpospolitej" domagali się usunięcia inkryminowanego artykułu z internetowego archiwum gazety. „Rzeczpospolita" odmówiła usunięcia artykułu z archiwum i podniosła, że w bibliotekach i tak istnieją papierowe wersje tegoż artykułu. Dlatego żądanie prawników uznała za absurdalne. Sąd Okręgowy w Warszawie powództwo Węgrzynowskiego i Smolczewskiego oddalił, uznał że zmuszanie gazety do usunięcia artykułu z Internetu mijałoby się z celem i byłoby przejawem cenzury. Ponadto prawnicy zostali już za ten artykuł publicznie przeproszeni. Węgrzynowski i Smolczewski odwołali się od tego wyroku, ale Sąd Apelacyjny w Warszawie oddalił apelację jednego z nich, a apelacji drugiego w ogóle nie wziął pod uwagę, bo nie została opłacona w terminie. Uznał bowiem, że istnienie wersji elektronicznej (on-line) artykułu nie jest „okolicznością nieujawnianą" nieznaną w pierwszym procesie. Gdy SN odmówił przyjęcia sprawy do rozpoznania, prawnicy złożyli skargę do ETPC w Strasburgu. Twierdzili, że naruszone zostało ich prawo do poszanowania

[4] Sąd Okręgowy w Warszawie (jako sąd pierwszej instancji) zobowiązał Annę Marszałek, Bertolda Kittela i Macieja Łukaszewicza do opublikowania oświadczenia: „Zarząd Spółki Presspublica oraz Maciej Łukaszewicz Redaktor Naczelny dziennika „Rzeczpospolita" przepraszają Panów Tadeusza Smolczewskiego i Szymona Węgrzynowskiego za opublikowanie artykułu p.t. *Wojewoda w sieci*, zamieszczonego w „Rzeczpospolitej" w dniu 2/3 grudnia 2000 r., zawierającego treści dotyczące ich działalności zawodowej, naruszające ich dobra osobiste" w „Rzeczpospolitej", „Gazecie Wyborczej", „Palestrze" i „Radcy Prawnym" oraz do 30 tys. zadośćuczynienia na rzecz Stowarzyszenia „Wspólnota Amazonek Nadzieja" w Chorzowie. Sąd Apelacyjny w Warszawie oddalił apelację pozwanych utrzymując w mocy wyrok sądu okręgowego.

Więcej: <http://naszeblogi.pl/14280-kittel-i-marszalek-bez-prawa-do-zawodu>, dostęp: 28 lutego 2014.

życia prywatnego i dobrego imienia, ponieważ zniesławiający ich artykuł wciąż można przeczytać w Internecie.

Europejski Trybunał Praw Człowieka uznał, że Internet jest narzędziem informacji i komunikacji w znacznym stopniu różniącym się od tradycyjnych mediów drukowanych, zwłaszcza jeśli chodzi o zdolność do przechowywania i przekazywania informacji. Z tego powodu ryzyko naruszenia prawa do poszanowania życia prywatnego oraz rodzinnego jest w tym przypadku wyższe niż w przypadku mediów drukowanych (teza 58). Zauważył również, że skarżący, kierując po raz pierwszy powództwo przeciwko wydawcy dziennika „Rzeczpospolita", nie domagali się podjęcia odpowiednich kroków celem usunięcia lub sprostowania dotyczącego ich artykułu, pomimo faktu, iż ukazał się on jednocześnie zarówno w wersji drukowanej, jak i elektronicznej. To właśnie z tego powodu sądy krajowe nie mogły orzekać w tej sprawie po raz drugi. Trybunał Konstytucyjny podkreślił także, że organy sądowe nie mają obowiązku podejmowania działań, których celem jest usunięcie z domeny publicznej wszelkich śladów publikacji, co do których w przeszłości zapadło prawomocne orzeczenie stwierdzające, iż taka publikacja narusza prawa osób prywatnych. Archiwa internetowe służą interesowi publicznemu i podlegają gwarancjom wynikającym z ochrony swobody wypowiedzi. Jednym z istotnych zadań prasy, zwłaszcza w dobie rozwoju Internetu, poza sprawowaniem funkcji kontrolnej, jest właśnie dokumentowanie rzeczywistości i udostępnianie społeczeństwu informacji z przeszłości (teza 59). Dlatego też ETPC nie dopatrzył się w działaniu organów państwa względem skarżących naruszenia art. 8 konwencji[5].

[5] Judgment in the case of Węgrzynowski and Smolczewski v. Poland, (Application no. 33846/07), 16.07.2013, <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-122365>, dostęp: 28 lutego 2014.

Rozdział 6. Prawo do informacji w świetle ustawy o dostępie do informacji publicznej

Brak oddzielnej ustawy o dostępie do informacji publicznej przed 6 września 2001 (a faktycznie 1 stycznia 2002) powodował, że jedno z kluczowych praw politycznych określonych w Konstytucji nie mogło być w pełni realizowane. Doszło do kuriozalnej sytuacji, w której wcześniej określono wyjątki od zasady (dostępu do informacji), niż same zasady. W uzasadnieniu do projektu ustawy wskazywano, że proponowane rozwiązanie ma „rozwijać i precyzować konstytucyjną zasadę, że informacja publiczna jest jawna (a więc i dostępna poza sytuacjami ograniczenia jawności w drodze ustaw lub w związku z ochroną prywatności), wyznacza zakres jawności informacji publicznej oraz prawo dostępu do tej informacji w porządku prawnym RP.

Podczas tworzenia ustawy o ochronie danych osobowych zastanawiano się, czy oczywiście słuszna idea ochrony prywatności (interesów) jednostki nie niesie przypadkiem zagrożeń dla wolności obywatelskich, tj. prawa do informacji, wolności nauki, wolności prasy czy wolności gospodarczej. W praktyce okazało się, że wprowadzenie ustawy o ochronie danych osobowych miało negatywne konsekwencje przede wszystkim dla dziennikarzy. Uchwalenie bowiem ustawy o ochronie danych osobowych z dnia 29 października 1997 oraz ustawy o ochronie informacji niejawnych z dnia 22 stycznia 1999 spowodowało konieczność uchwalenia ustawy, która określałaby zakres, formy i tryb udostępniania informacji w celu zrównoważenia zasady ochrony informacji z konstytucyjnym prawem dostępu do informacji publicznej[1]. Myślą przewodnią pracy nad projektem tej ustawy, były słowa wypowiedziane kiedyś przez wicemarszałka Sejmu pierwszej kadencji profesora socjologii Jacka Kurczewskiego […], który powiedział, że „władza powinna być czysta i przezroczysta", a także słowa profesor Ewy Łętowskiej, która stwierdziła, że „korupcja jest przykładem zjawiska, które rozkwita w ciemności. Więcej może uczynić jasne światło wokół niej niż najsurowsze sankcje karne". Ustawa ta ma właśnie pomóc w tym „oświetleniu" procedur decyzyjnych, zapewnić dostęp do informacji zwykłym obywatelom, przede wszystkim obywatelom oraz organizowanym przez nich stowarzyszeniom, związkom, porozumieniom, grupom nacisku i tak dalej. Jak się wyraził Henryk Wujec: „Chodzi o to, żeby obywatele byli aktywni w procesie stanowienia prawa, żeby nie było w ten sposób, że raz na cztery lata wybiera się parlament i wtedy uczestniczy tylko w kampanii wyborczej. Chodzi o to, żeby obywatele

[1] Uzasadnienie do projektu ustawy o dostępie do informacji publicznej, druk nr 2094 <http://orka.sejm.gov.pl/Rejestrd.nsf?OpenDatabase>, dostęp: 9 lipca 2013.

mieli stały dostęp do tego, co jest stanowione zarówno w parlamencie, jak w innych organach władzy”[2].

Wejście w życie ustawy o ochronie danych osobowych przy jednoczesnym braku kompleksowej regulacji dotyczącej dostępu do informacji publicznej spowodowało całkowitą blokadę dostępu do jakichkolwiek informacji z urzędów publicznych. Nie tylko zresztą z urzędów publicznych. Ustawa o ochronie danych osobowych została potraktowana jako „parasol” dla każdej instytucji, która nie chciała udzielić żadnej informacji, np. Ministerstwo Sprawiedliwości odmówiło podania nazwisk prezesów sądów, a odmowę uzasadniło ustawą o ochronie danych osobowych[3].

Ustawa o dostępie do informacji publicznej, już na etapie projektu, nie przewidywała uprzywilejowanej pozycji dziennikarzy[4]. Od jej wejścia w życie, czyli od dnia 1 stycznia 2002 przestało obowiązywać rozporządzenie w sprawie trybu udostępniania prasie informacji oraz organizacji i zadań rzeczników prasowych w urzędach organów administracji rządowej. Na mocy tego rozporządzenia Rady Ministrów wyłącznie dziennikarze lub redakcje byli uprawnieni do żądania informacji o działalności naczelnych, centralnych, terenowych organów administracji rządowej, przedsiębiorstw państwowych, spółek Skarbu Państwa i innych państwowych jednostek organizacyjnych. Organy te musiały udzielić informacji w terminie nie dłuższym niż 24 godziny od zwrócenia się dziennikarza lub redakcji o informację. Ponadto organy administracji państwowej, zobowiązane

---

[2] Henryk Wujec na 86. posiedzeniu Sejmu III kadencji, dnia 13 września 2000 <http://orka2.sejm.gov.pl/Debata3.nsf/main/21D32B95>, dostęp: 08 lipca 2013.

[3] Pogląd taki wyraziła prof. dr hab. Ewa Kulesza na posiedzeniu Komisji Nadzwyczajnej do rozpatrzenia projektów ustaw dotyczących prawa obywateli do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne, a także dotyczących jawności procedur decyzyjnych i grup interesów w dniu 19 grudnia 2000
<http://orka.sejm.gov.pl/Biuletyn.nsf/0/BC0551F090B08A04C1256B73003D21D8?OpenDocument>, dostęp: 8 lipca 2013.

[4] Ekspertka Komisji, dr hab. Teresa Górzyńska, mówiąc o tym dla kogo jest ta ustawa, stwierdziła, że: „przede wszystkim dla obywateli, dla każdego – to jest ustawa o prawie obywateli do informacji. Dla obywatela, urzędnika, prasy i dla innych podmiotów. Chcę tu jeszcze wspomnieć, że jeśli chodzi o prasę, to w trakcie prac nad projektem przyjęto zasadę, że prasa nie będzie w żaden sposób faworyzowana, że każdy będzie miał taki sam dostęp do informacji”.
<http://orka.sejm.gov.pl/Biuletyn.nsf/0/E115DE844AAB0BAAC1256B73003DCF28?OpenDocument>, dostęp: 12 lipca 2013.

Podobny pogląd wyraziła Anna Grzymisławska, sekretarz stanu w Kancelarii Prezesa Rady Ministrów. Stwierdziła bowiem, komentując zawiłość definicji majątku publicznego, proponowanych w ustawie o dostępie do informacji publicznej, że: „naprawdę, projekt ustawy, nad którym pracujemy, nie jest przeznaczony dla urzędników i dziennikarzy. Mam nieodparte wrażenie, że my piszemy ustawy dla dziennikarzy, a ja bym chciała, rządowi na tym bardzo zależy, żeby była to ustawa również dla środowiska dziennikarskiego, ale także dla wszystkich – o to chodzi przy dostępie do informacji. Wydaje mi się, że „czynnik dziennikarski” jest tu decydujący”.
<http://orka.sejm.gov.pl/Biuletyn.nsf/0/E115DE844AAB0BAAC1256B73003DCF28?OpenDocument>, dostęp: 12 lipca 2013.

były do działania nie tylko na wniosek, ale z własnej inicjatywy nawiązywać i rozwijać kontakty z prasą oraz udostępniać informacje mogące zainteresować opinię publiczną. Odmowa udzielenia informacji możliwa była tylko ze względu na ochronę tajemnicy państwowej, służbowej lub innych tajemnic prawnie chronionych[5].

Obecnie obowiązująca ustawa o dostępie do informacji publicznej nie przewiduje szczególnych uprawnień dla prasy w zakresie dostępu do informacji publicznej. Korzysta ona z dostępu do informacji publicznej na zasadach ogólnych. Podczas debaty nad projektem ustawy o dostępie do informacji pojawiło się pytanie o głównego adresata ustawy. Poseł AWS, Jan Chmielewski „pytał o to, czy ten projekt jest bardziej dla obywateli, czy bardziej dla dziennikarzy. W naszym projekcie staraliśmy się kłaść nacisk – w ogóle tu się słowo dziennikarze nie pojawia – na to, że to jest projekt dla obywateli, że to jest realizacja prawa obywateli do informacji, do udziału w procesach decyzyjnych, poprzez wyrażanie swojej opinii. Tak więc staraliśmy się nadać charakter obywatelski, zgodnie z definicją społeczeństwa obywatelskiego.[6]"

Także NSA w wyroku z dnia 29 lipca 2004 potwierdził, że ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, samodzielnie i kompleksowo reguluje problematykę dostępu do informacji publicznej. Dlatego też, art. 22 ust. 1[7] ustawy z dnia 6 września 2001 o dostępie do informacji publicznej, w zakresie w jakim przysługuje podmiotowi prawo do wniesienia powództwa do sądu powszechnego o udostępnienie informacji publicznej, stosuje się także w odniesieniu do prasy[8].

W obecnym brzmieniu art. 5 ustawy o dostępie do informacji publicznej[9] nie wprowadza wprost, jako przesłanki ograniczenia prawa do informacji, ochrony

---

[5] Rozporządzenie Rady Ministrów w sprawie udostępniania prasie informacji oraz organizacji i zadań rzeczników prasowych w urzędach organów administracji rządowej z dnia 7 listopada 1995, Dz. U. nr 132, poz. 642 uchylone 1 stycznia 2002 r. na mocy art. 24 ust. 3 ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r., Dz. U. 2014, poz. 782.

[6] Wystąpienie posła Henryka Wujca na 86. posiedzeniu Sejmu III kadencji, dnia 13 września 2000 <http://orka2.sejm.gov.pl/Debata3.nsf/9a905bcb5531f478c125745f0037938e/08d7ebab5f438704c125749d00354499?OpenDocument>, dostęp: 8 lipca 2013.

[7] Art. 22 1.Podmiotowi, któremu odmówiono prawa dostępu do informacji publicznej ze względu na wyłączenie jej jawności z powołaniem się na ochronę danych osobowych, prawo do prywatności oraz tajemnicę inną niż informacja niejawna, tajemnica skarbowa lub tajemnica statystyczna, przysługuje prawo wniesienia powództwa do sądu powszechnego o udostępnienie takiej informacji." Przepis ten został uchylony ustawą (nowelizacją), która weszła w życie 29 grudnia 2011.

[8] Wyrok NSA z dnia 29 lipca 2004, OSK 693/04, LEX nr 164847.

[9] Art. 5 ust. 2 ustawy o dostępie do informacji publicznej stanowi, że prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Ustawa o dostępie do informacji publicznej z dnia 6 września 2001, Dz. U. 2014, poz. 782.

danych osobowych. Nie oznacza to jednak, że na gruncie ustawy o dostępie do informacji publicznej relacje między dostępem do informacji oraz ochroną danych osobowych nie występują. Należy je wyprowadzić z prawa do prywatności, o którym mowa w art. 5 ust. 2 ww. ustawy, a dopiero następnie to rozwiązanie odnieść do przepisów ustawy o ochronie danych osobowych[10]. Ograniczenie prawa dostępu do informacji należy traktować jako wyjątek od zasady dostępu do informacji publicznej. W świetle art. 61 Konstytucji prawo do informacji jest publicznym prawem obywatela, które odbywa się na zasadach skonkretyzowanych w ustawie o dostępie do informacji publicznej. Stąd prawo do informacji jest zasadą, a wyjątki od niego powinny być interpretowane ściśle. O ile ochrona informacji niejawnych wymaga wyodrębnienia określonych materiałów poprzez nadanie im określonej klauzuli, pozostałe tajemnice (w tym ochrona danych osobowych) nie wymagają nadania dokumentom specjalnej formy, mają bowiem charakter materialny. Nie oznacza to jednak, iż w przypadku odmowy w uzasadnieniu nie należy wskazać, jakie konkretnie fragmenty akt zostały wyłączone z uwagi na określoną tajemnicę[11].

Jak wynika z orzeczenia SN z dnia 8 listopada 2012 „reżim ochrony prawa do prywatności i reżim ochrony danych osobowych są wobec siebie niezależne. Niewątpliwie dochodzi przy tym do wzajemnych relacji i oddziaływania tych reżimów, bowiem w określonych sytuacjach faktycznych przetworzenie danych osobowych może spowodować naruszenie dobra osobistego w postaci prawa do prywatności, bądź ochrona prawa do prywatności będzie wymagała sprzeciwienia się wykorzystaniu danych osobowych". W dalszej kolejności SN rozważał, czy udostępnienie imienia i nazwiska osoby fizycznej przez jednostkę samorządu terytorialnego, w określonym stanie faktycznym, narusza jej prawo do prywatności. Sąd Najwyższy przyjął, że wyjątki zawarte w art. 5 ust. 2 zd. 2 ustawy o dostępie do informacji publicznej nie mają charakteru wyczerpującego dla ustalenia granic prawa do prywatności. Zakres tego prawa, czy też ochrony wywodzącej się z prawa do prywatności, winien być ustalony przy uwzględnieniu okoliczności faktycznych konkretnej sprawy. Jednak prawo do prywatności nie obejmuje informacji o imieniu i nazwisku osoby, która zawierała umowę cywilnoprawną z jednostką samorządu terytorialnego lub Skarbem Państwa i korzysta z przywileju czerpania z zasobów publicznych[12]". W innej sprawie, również dotyczącej kwestii ujawniania danych osobowych, NSA w Warszawie

---

W praktyce przepis ten stanowi nawiązanie do art. 47 Konstytucji RP, gwarantującego każdemu prawną ochronę życia prywatnego. Więcej: M. Bidziński, *Komentarz do art. 5*, [w:] *Ustawa o dostępie do informacji publicznej. Komentarz*, M. Bidziński, M. Chmaj, P. Szustakiewicz, Warszawa 2010, teza 3 <https://sip.legalis.pl/document-view.seam?documentId=mjxw62zog4ydanbugi4tmltqmfyc4mrygezdsnjtgi>, dostęp: 9 grudnia 2014.

[10] Zob. wyrok WSA w Krakowie z dnia 30 lipca 2013, II SA/Kr 395/13, LEX nr 1447479.

[11] Zob. wyrok NSA z dnia 7 marca 2003, II SA 3572/02, LEX nr 144641.

[12] Zob. wyrok SN z dnia 8 listopada 2012, I CSK 190/12, LEX nr 1286307.

orzekł, że imię i nazwisko mogą być informacją publiczną tylko wówczas, gdy dotyczą osób pełniących funkcje publiczne. Nie można tego interpretować rozszerzająco. Zgodnie z art. 5 ust. 2 ustawy o dostępie do informacji publicznej, prawo do takiej informacji podlega ograniczeniom ze względu m.in. na prywatność osoby fizycznej[13]. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne czy mających związek z pełnieniem tych funkcji. Autorów ekspertyz nie da się tak potraktować, ażeby tak ich zakwalifikować, musieliby uczestniczyć w podejmowaniu decyzji[14].

---

[13] W praktyce różnie (rozbieżnie) rozumiana jest prywatność. Prezes Sądu Rejonowego w C. odmówił udzielenia żądanej przez M. J. informacji o wynagrodzeniu (wraz z dodatkami) sędziego C.R., stwierdzając, że informacja ta nie jest informacją publiczną, podlegającą udostępnieniu w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Wynagrodzenie otrzymywane indywidualnie przez każdego pracownika. w tym również i sędziego, nie jest informacją mającą związek z pełnieniem tych funkcji, w tym informacją o warunkach powierzenia i wykonywania funkcji i dlatego też ujawnienie wysokości wynagrodzenia stanowiłoby naruszenie prywatności, o którym mowa w art. 5 ust. 2 ustawy. Konstytucyjne prawo do prywatności, wyrażone w art. 47 Konstytucji RP, przysługuje zaś każdemu. a zatem również osobie wykonującej funkcje publiczne, z pewnymi ograniczeniami, które jednak w tej sprawie nie zachodzą. Prezes Sądu Okręgowego podtrzymał decyzję sądu I instancji, również uznając, że informacją publiczną jest jedynie informacja o sprawach publicznych, celem ustawy o dostępie do informacji publicznej jest informowanie obywateli o sposobie i zasadach funkcjonowania podmiotów lub osób realizujących zadania publiczne lub gospodarujących mieniem publicznym. Trudno dopatrzyć się takiego celu w informowaniu każdego obywatela o wynagrodzeniu konkretnego sędziego, gdyż brak jest związku między działalnością Sądu Rejonowego w C. a wynagrodzeniem konkretnego sędziego. Zupełnie inny pogląd wyraził jednak Wojewódzki Sąd Administracyjny w Gdańsku, który uznał, że do warunków powierzenia i wykonywania funkcji należą zarówno obowiązki, jak i prawa osoby piastującej daną funkcję, w tym prawo do wynagrodzenia. Osoby podejmujące się sprawowania funkcji publicznej muszą mieć świadomość, że sfera ich prywatności będzie w tym zakresie ograniczona. Sędzia jest osobą pełniącą funkcję publiczną, a informacja o wysokości jego wynagrodzenia ma związek z pełnieniem tej funkcji, dotyczy bowiem warunków powierzenia i wykonywania funkcji. Zob. wyrok WSA w Gdańsku z dnia 22 maja 2013, II SA/Gd 190/13, LEX nr 1368693. Zob. także wyrok WSA w Bydgoszczy z dnia 21 maja 2013, II SAB/Bd 68/13, LEX nr 1352011.

[14] W przedmiotowej sprawie M. D. zwrócił się do Kancelarii Prezydenta Rzeczypospolitej Polskiej o udostępnienie informacji publicznej w postaci: kserokopii (skanu) umów, ewentualnie także aneksów do tych umów, faktur lub rachunków wystawionych do tych umów, na podstawie których Kancelaria Prezydenta zamówiła wykonanie następujących opinii i ekspertyz prawnych:

1) ekspertyzy naukowej (opinii) w zakresie: projektu ustawy o zmianie niektórych ustaw związanych z funkcjonowaniem systemu ubezpieczeń społecznych;

2) opinii do projektu „ustawy o zmianie niektórych ustaw związanych z funkcjonowaniem systemu ubezpieczeń społecznych" w zakresie dotyczącym zgodności z Konstytucją Rzeczypospolitej Polskiej z 2 kwietnia 1997 r.;

3) opinii prawnej dotyczącej projektu ustawy o zmianie niektórych ustaw związanych z funkcjonowaniem systemu ubezpieczeń społecznych;

4) opinii o projekcie ustawy o zmianie niektórych ustaw związanych z funkcjonowaniem systemu ubezpieczeń społecznych.

Kancelaria Prezydenta RP przekazała skarżącemu żądane dokumenty wraz z rachunkami, informując ponadto, że do przedmiotowych umów nie zawierano aneksów. Jednocześnie Szef Kancelarii Prezydenta Rzeczypospolitej Polskiej odmówił skarżącemu udostępnienia informacji publicznej w zakresie udostępnienia danych osobowych wykonawców umowy o dzieło. Wyrok NSA w Warszawie z dnia 25 kwietnia 2014, I OSK 2499/13, LEX nr 1453974.

Zgodne z ustawą o dostępie do informacji publicznej prawo do informacji publicznej nie podlega ograniczeniu ze względu na prywatność osoby fizycznej w przypadku informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji. Nie wyklucza to, co do zasady, możliwości przypisania wypowiedzi realizującej prawo do informacji publicznej cech kwalifikujących ją jako naruszającą dobra osobiste osoby, której dotyczy[15].

W sytuacji, gdy w treści informacji publicznej zawarte są dane osobowe, prawo do informacji podlega ograniczeniu ze względu na ustawę o ochronie danych osobowych, która stanowi *lex specialis* w stosunku do ustawy o dostępie do informacji publicznej. Konieczność ochrony danych osobowych nie zwalnia organu z udostępnienia informacji publicznej. Organ powinien dane osobowe (PESEL, adres zamieszkania) zanonimizować[16]. Czasami jednak nawet zanonimizowanie imienia i nazwiska będzie niewystarczające, bowiem daną osobę da się konkretnie wskazać na podstawie np. charakteru popełnionego czynu czy okoliczności i czasu jego popełnienia[17]. Ustawa o dostępie do informacji nie może jednak naruszać przepisów innych ustaw odrębnie regulujących zasady udostępniania danych osobowych. Nie jest bowiem konieczne podanie (ujawnienie) danych umożliwiających identyfikację poszczególnych osób (tu; imienia, nazwiska oraz nazwy sołectwa) do kontroli ważności podejmowanych uchwał (przez zebranie wiejskie). Wystarczy informacja o ogólnej liczbie osób biorących udział w zebraniu[18]. Podobnie nie jest niezbędne udostępnienie np. na stronie internetowej BIP urzędu gminy danych osoby (dalej: S.U.), która złożyła skargę na działalność wójta. S.U. wniósł skargę na działalność Wójta Gminy W. Następnie Rada Gminy W. wydała uchwałę w sprawie rozpatrzenia skargi S. U.,

---

[15] Zob. wyrok SN z dnia 28 listopada 2013, IV CSK 155/13, LEX nr 1415128.

[16] Zob. wyrok WSA w Poznaniu z dnia 7 marca 2013, II SA/Po 37/13, LEX nr 1293515.

[17] Zob. wyrok WSA w Białymstoku z dnia 14 lutego 2013, II SA/Bk 967/12, LEX nr 1334226.

[18] Stowarzyszenie A. złożyło (drogą elektroniczną) wniosek do Urzędu Gminy K. o udostępnienie danych dotyczących realizacji i sposobu wydatkowania funduszu sołeckiego oraz zebrań wiejskich przeprowadzonych w każdym sołectwie. W odpowiedzi na wniosek Wójt Gminy K. nie udzielił części informacji, a w pozostałej części – odesłał do BIP-u. Odmówił podania imiennej listy uczestników zebrań sołeckich, powołując się na art. 5 ust. 1 i art. 16 ustawy o dostępie do informacji publicznej (które to artykuły pozwalają na nieujawnianie informacji ze względu na ochronę wynikająca z innych ustaw) oraz art. 6 ust. 1 i 2 i art. 23 ust. 1 ustawy o ochronie danych osobowych. Powołał się przy tym na orzeczenie NSA z dnia 28 stycznia 2008, z którego wynika, że nawet dane w zakresie imienia i nazwiska mogą w niektórych przypadkach stanowić podstawę identyfikacji danej osoby, a tym samym stanowią dane osobowe. W tym przypadku zestawienie imienia, nazwiska i sołectwa umożliwia identyfikację bezpośrednią. Stowarzyszenie od tej decyzji wniosło odwołanie, powołując się na konstytucyjne prawo dostępu do informacji publicznej i prawo do kontroli społecznej działania organów władzy publicznej. Samorządowe Kolegium Odwoławcze utrzymało w mocy decyzję będącą przedmiotem odwołania, a Wojewódzki Sąd Administracyjny w Olsztynie uznał, że skarga nie zasługuje na uwzględnienie. Wyrok WSA w Olsztynie z dnia 30 kwietnia 2012, II SA/Ol 194/12, LEX nr 1287138.

w której zawarte zostały dane osobowe skarżącego w zakresie imienia i nazwiska. Przedmiotowa uchwała została opublikowana w BIP Wójta Gminy W. GIODO, po przeprowadzeniu postępowania administracyjnego w sprawie skargi S.U. na przetwarzanie przez Wójta Gminy W. jego danych osobowych w uchwale Rady Gminy W., nakazał wójtowi gminy W. wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych ww., poprzez usunięcie z powyższej uchwały, znajdującej się na stronie internetowej BIP Urzędu Gminy W., jego danych osobowych w zakresie imienia i nazwiska. Następnie Wójt Gminy W. złożył wniosek o ponowne rozpatrzenie sprawy zakończonej ww. decyzją. Zarówno jednak ponowne rozpatrzenie sprawy przez GIODO, jak i późniejszy wyrok WSA w Warszawie nie zmieniły rozstrzygnięcia[19].

Rozstrzygając konflikt między prawem do informacji a np. ochroną prywatności czy danych osobowych, WSA w Poznaniu wyraził pogląd, że prawo do informacji publicznej obejmuje uprawnienia do uzyskania informacji publicznej, w tym uzyskania informacji przetworzonej w takim zakresie, w jakim jest to szczególnie istotne dla interesu publicznego, wglądu do dokumentów urzędowych, dostępu do posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, a także uprawnienie do niezwłocznego uzyskania informacji publicznej zawierającej aktualną wiedzę o sprawach publicznych. Udostępnienie informacji publicznej, należy zatem interpretować jako przekazanie przez organ władzy pewnych stwierdzeń odnośnie faktów w takim zakresie, w jakim nie dotyczy to dokumentów prywatnych. Równocześnie dostęp do informacji publicznej nie ma charakteru absolutnego. Zgodnie z art. 5 ust. 1 ustawy o udostępnianiu informacji publicznej, prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych. Omawiany przepis ustanawia tym samym zasadę, że przepisy ustaw o ochronie danych osobowych stanowią *legi speciali* w stosunku do ustawy o dostępie do informacji publicznej i muszą być stosowane na zasadzie pierwszeństwa. W konsekwencji, w sytuacji, gdy wnioskowana informacja stanowi informację ustawowo chronioną (np. na podstawie ustawy o ochronie danych osobowych), wyłączona jest możliwość jej uzyskania na podstawie ustawy o dostępie do informacji publicznej[20].

W praktyce stosowania wyjątków ograniczających dostęp do informacji publicznej wielokrotnie pojawiała się wątpliwość, czy ustawę o ochronie danych osobowych (jako podstawę odmowy udzielenia informacji) można stosować

---

[19] Wyrok WSA w Warszawie z dnia 24 listopada 2011, II SA/Wa 1828/11, LEX nr 1153548.

[20] Wyrok WSA w Poznaniu z dnia 23 lutego 2011, II SA/Po 804/10, LEX nr 1086575.

także, i ewentualnie w jakim zakresie, do osób będących przedsiębiorcami. Naczelny Sąd Administracyjny w Warszawie w wyroku z dnia 13 stycznia 2011 uznał, że błędna jest taka interpretacja art. 2 ust. 1 ustawy o ochronie danych osobowych[21], według której wyłącza ona ochronę przewidzianą w ustawie w stosunku do osób będących przedsiębiorcami. Zasady postępowania przy przetwarzaniu danych przedsiębiorcy (w tym danych osobowych) rzeczywiście nie podlegają regułom ustawy o ochronie danych osobowych, ale jeśli osoba fizyczna będąca przedsiębiorcą staje się uczestnikiem obrotu prawnego już jako osoba fizyczna, wówczas korzysta z ochrony tej ustawy.

Zupełnie odmienny pogląd w tej sprawie wyrazili WSA oraz GIODO. Wojewódzki Sąd Administracyjny w Warszawie uznał, że kolizja prawa do prywatności z prawem do informacji nie może prowadzić do wyeliminowania jednego z chronionych konstytucyjnie praw, ale zmusza do wyważenia, które wartości powinny ustąpić dla dobra wspólnego. Przyjął, że ustawa o ochronie danych osobowych będzie miała ograniczone zastosowanie. Po pierwsze, z powodu wyłączeń stosowania ustawy o ochronie danych osobowych w stosunku do przedsiębiorców i włączeniu ustaw chroniących tajemnicę przedsiębiorcy, a także z powodu częściowego wyłączenia stosowania ustawy o ochronie danych osobowych do działalności dziennikarskiej i jednocześnie włączeniu ochrony *lex specialis*, tj. prawa prasowego i ustawy o dostępie do informacji publicznej. Sąd ustalił, że postępowanie karne toczyło się w stosunku do podmiotu gospodarczego – przedsiębiorcy J. P. świadczącego usługi jako radca prawny. Ma to, według sądu, decydujące znaczenie, bowiem art. 2 ust. 1 ustawy o ochronie danych osobowych stanowi, że ustawa ta ochroną obejmuje tylko osoby fizyczne. Samodzielnym przepisem przesądzającym o tym, że ustawa o ochronie danych osobowych nie ma zastosowania w stosunku do osób prowadzących działalność gospodarczą, był przepis art. 7a ust. 2 ustawy – Prawo działalności gospodarczej. Zgodnie z tym przepisem, obowiązującym w dacie udostępnienia akt dziennikarzowi, dane osobowe zawarte w ewidencji nie podlegały przepisom ustawy o ochronie danych osobowych. Mogły być chronione w trybie ustawy o zwalczaniu nieuczciwej konkurencji oraz w trybie karnym. Według sądu I instancji nawet gdyby J. P. nie był przedsiębiorcą, to i tak ustawa o ochronie danych osobowych miałaby ograniczone zastosowanie, z uwagi na przepis art. 3a ust. 1 tej ustawy. Zgodnie z tym przepisem ustawy, z wyjątkiem art. 14–19 i art. 36 ust. 1, nie stosuje się do prasowej działalności dziennikarskiej w rozumieniu prawa prasowego, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą. Zdaniem sądu, ustawodawca wyłączył działalność dziennikarską spod ochrony

[21] Art. 2 ust. 1 Ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Ustawa z dnia 29 sierpnia 1997, Dz. U. 2014, poz. 1182 z późn. zm.

ustawy o ochronie danych osobowych, nakładając na tę grupę zawodową ograniczenia w przetwarzaniu danych osobowych wynikające z prawa prasowego i z ustawy o dostępie do informacji publicznej. Do prawa prasowego dodany został art. 3a, który stanowi, że w zakresie prawa prasy do dostępu do informacji publicznej stosuje się przepisy ustawy o dostępie do informacji publicznej. Sąd I instancji uznał, że wykładnia art. 3a ustawy o ochronie danych osobowych w zestawieniu z art. 3a prawa prasowego prowadzi do wniosku, że uprawnienia GIODO ograniczone zostały tylko do tej działalności dziennikarskiej, która istotnie narusza prawa i wolności osoby, której dotyczą. Wojewódzki Sąd Administracyjny w Warszawie przyjął, iż akta zakończonego postępowania przygotowawczego stanowią informację publiczną i w odniesieniu do takich akt znajduje zastosowanie ustawa o dostępie do informacji publicznej. Prokuratura była zobowiązana do udostępnienia informacji dziennikarzowi na zasadzie art. 5 ust. 2 ustawy o dostępie do informacji publicznej. Według sądu, sankcje z tytułu naruszenia ww. przepisu ustawy o dostępie do informacji publicznej ustawa ta pozostawia innym regulacjom prawnym, tj. przepisom prawa cywilnego, prawu prasowemu i karnemu. Zdaniem sądu, GIODO zachowuje kompetencję tylko w stosunku do osoby fizycznej. Dziennikarzy zaś uznał sąd (na podstawie art. 3a prawa prasowego w związku z art. 5 ust. 2 ustawy o dostępie do informacji publicznej), za depozytariuszy wiedzy prywatnej pozyskiwanej z akt zakończonego postępowania. Sąd zauważył, że prokuratura miała świadomość ciążących na dziennikarzu ograniczeń, wiedziała też o jego wyjątkowych uprawnieniach. Na decyzje należało także spojrzeć przez pryzmat art. 1 Konstytucji, dobra wspólnego, dobra publicznego i ustawy o ochronie danych osobowych. Należało wziąć pod uwagę historyczne tło udostępnienia akt postępowania dotyczącego nielegalnego importu alkoholu (afera alkoholowa, o której media szeroko informowały opinię publiczną). Według sądu, nie można tracić z pola uwagi tego, że zainteresowanie mediów było tym większe, iż J. P. wykonuje zawód publicznego zaufania (radcy prawnego). Dopuszczalna jest bowiem szersza ingerencja w sferę prywatną w stosunku do zawodów szczególnego zaufania. Wojewódzki Sąd Administracyjny podzielił ocenę GIODO, że prokuratura zobowiązana była do udzielenia informacji dziennikarzowi dla dobra publicznego. W dalszej części wywodu WSA stwierdził, że nawet przyjęcie, iż informacja dotyczyła praw i wolności osoby, której te dane dotyczą, to i tak uznać należało, że w sprawie wystąpiły przesłanki legalizujące to udostępnienie, o których mowa w art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych. Ponadto, udostępnienie uzasadniał przepis art. 27 ust. 2 pkt 2 tej ustawy (przepis innej ustawy – art. 4 ust. 1, art. 1 ust. 1 ustawy o dostępie do informacji publicznej i art. 7a ustawy o działalności gospodarczej – na to udostępnienie zezwalał). Nawiązując do art. 153 p.p.s.a., WSA stwierdził, że „prywatność osoby fizycznej" nie dotyczy przedsiębiorcy. Zdaniem sądu, działania dziennikarza w niniejszej sprawie,

zakwalifikować należy do kategorii „usprawiedliwionego zainteresowania". Przypomniał, że doszło do udostępnienia imienia i nazwiska skarżącego, daty i miejsca jego urodzenia, treści wyroku jaki zapadł w I i II instancji, postanowienia o zabezpieczeniu dowodów oraz postanowienia o umorzeniu postępowania. W zakres informacji publicznej weszły więc zarówno elementy życia prywatnego, jak i informacje dotyczące działalności przedsiębiorcy. Część informacji pokrywała się z danymi w ewidencjach gospodarczych, które to dane były wyłączone z ochrony ustawy o ochronie danych osobowych. Nie można zatem uznać, że ingerencja w prywatność przedsiębiorcy J. P., wykonującego zawód zaufania publicznego, była nadmiernie głęboka. Sąd podkreślił, że zgoda prokuratury na udostępnienie akt dziennikarzowi nie była tożsama z zezwoleniem na publikowanie wszelkich informacji uzyskanych z tych akt. Prokuratura nie miała też prawa badać, w jaki sposób dziennikarz zamierza wykorzystać posiadane przez siebie informacje.

Niezależnie jednak, czy uznamy za słuszne poglądy wyrażone w tej sprawie przez GIODO i WSA, nie ma dobra publicznego w ujawnianiu, bez zgody osoby, której dane dotyczą, danych osobowych osoby, która była oskarżona o popełnienie przestępstwa, ale postępowanie wobec niej zostało umorzone[22]. W interesie publicznym jest, aby osoba, której organy państwa postawiły zarzuty, ale nie wykazały ich zasadności, nie ponosiła w związku z tym żadnych dodatkowych dolegliwości. Ujawnienie danych osobowych skarżącego nie służyło walce z przestępczością, tj. odstraszaniu, zapobieganiu, nie doszło też do skazania skarżącego[23].

[22] We wcześniejszym orzeczeniu WSA w Warszawie orzekł, że brzmienie art. 2 ustawy o ochronie danych osobowych jednoznacznie wskazuje, że działaniem ustawy objęte są tylko przypadki przetwarzania danych osób fizycznych i nie ma podstaw do jej stosowania nawet *per analogiam* do osób prawnych lub jednostek organizacyjnych nieposiadających osobowości prawnej. O prywatności można mówić wyłącznie w kontekście osób fizycznych. Gdy osoba fizyczna prowadzi działalność gospodarczą pod firmą swojego nazwiska, w pierwszej kolejności korzysta z ochrony, jaką ustawodawca zapewnia przedsiębiorcy. Podejmując działalność gospodarczą w takiej formie (a nie np. w formie spółki kapitałowej) musi się liczyć z utratą prywatności. Wyrok WSA w Warszawie z dnia 24 listopada 2009, II SA/Wa 1584/09, LEX nr 589249.

[23] Wyrok NSA z dnia 13 stycznia 2011, I OSK 440/10, LEX nr 952041.

Rozdział 7. Ustawa o ochronie danych osobowych a działalność dziennikarska

Relacja ustawy o ochronie danych osobowych do prawa prasowego

Ustawę o ochronie danych osobowych w pewnym ograniczonym zakresie stosuje się także do działalności prasowej (określonej w ustawie – prawo prasowe z dnia 26 stycznia 1984). Zgodnie z art. 3a ust. 2 tejże ustawy do prasy stosuje się wyłącznie art. 14-19 i art. 36 ust. 1. Wprowadzenie tego art. (3a ust. 2) wynikało przede wszystkim z konieczności realizacji zaleceń Komisji Europejskiej, która zwracała uwagę stronie polskiej na brak w polskiej ustawie odpowiednika art. 9 dyrektywy[1], statuującego zwolnienie w pewnym zakresie spod rygorów ustawy o ochronie danych osobowych m.in. działalności dziennikarskiej. Wyłączenie to nie ma jednak charakteru bezwzględnego. Nie obejmuje swoim zakresem sytuacji, w której poprzez korzystanie z wolności wypowiedzi dochodzi do istotnego naruszenia prawa i wolności osoby, której dane dotyczą[2]. Klauzula prasowa do ustawy o ochronie danych osobowych zaczęła obowiązywać dopiero z dniem uzyskania przez Rzeczypospolitą Polską członkowstwa w UE (1 maja 2004), czyli ponad 6 lat od uchwalenia samej ustawy. W okresie, między wejściem w życie ustawy o ochronie danych osobowych a obowiązywaniem klauzuli prasowej, działalność dziennikarska była paraliżowana przez konieczność stosowania całej ustawy o ochronie danych osobowych. Ustawa o ochronie danych osobowych (po wejściu w życie art. 3a ust. 2) nie będzie miała zastosowania do zbierania i przygotowywania materiału prasowego. Nie oznacza to jednak, że dziennikarz nie będzie zobowiązany do ochrony danych osobowych. Zgodnie bowiem z art. 12 prawa prasowego dziennikarz powinien

[1] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady WE z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych w art. 9 stanowi: Przetwarzanie danych osobowych i wolność wypowiedzi. Państwa Członkowskie wprowadzają możliwość wyłączenia lub odstąpienia od przepisów niniejszego rozdziału, rozdziału IV [dotyczącego przekazywania danych osobowych do państw trzecich] i VI [dotyczącego organu nadzoru i grupy roboczej ds. ochrony osób w zakresie przetwarzania danych osobowych] w przypadku przetwarzania danych osobowych wyłącznie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego jedynie wówczas, gdy jest to konieczne dla pogodzenia prawa do zachowania prywatności z przepisami dotyczącymi wolności wypowiedzi. Dz. Urz. WE 1995 L 281/31, s. 365.

[2] Zob. uzasadnienie do projektu ustawy o zmianie ustawy o ochronie danych osobowych, druk sejmowy nr 2120 <http://orka.sejm.gov.pl/Druki4ka.nsf/($vAllByUnid)/2B081C58BD0702DFC1256DC8003EE5AA/$file/2120.pdf>, dostęp: 4 sierpnia 2013.

zachować szczególną (czyli ponadprzeciętną) rzetelność i staranność w zbieraniu i wykorzystaniu materiałów prasowych, a ponadto chronić dobra osobiste działających w dobrej wierze informatorów.

Jak już wcześniej wspomniano, ustawy o ochronie danych – z wyjątkiem pewnych przepisów – nie stosuje się do prasowej działalności dziennikarskiej (w rozumieniu prawa prasowego). Powstaje więc konieczność precyzyjnego określenia, na czym polega prasowa działalność dziennikarska i czy do niej zalicza się również prasową działalność wydawniczą. Jak wynika z wyroku NSA z dnia 28 czerwca 2011 wyłączenie, o którym mowa w art. 3a ust. 2 ustawy o ochronie danych osobowych, dotyczy jedynie „prasowej działalności dziennikarskiej" a nie dziennikarzy w ogólności, rozumianych jako grupa zawodowa. W niniejszej sprawie sąd musiał odnieść się do kwestii możliwości żądania udostępnienia adresów zamieszkania redaktora naczelnego gazety – R. K. oraz jej dziennikarzy, którzy opublikowali artykuły naruszające dobra osobiste wnioskodawcy. Wniosek motywowano faktem, że powyższe dane są niezbędne do pozwania przed sądem redaktora i autorów artykułów. Wydawca odmówił wnioskodawcy ujawnienia powyższych danych. Takie zachowanie wydawcy może wywoływać wrażenie, jakoby osoby wykonujące zawód dziennikarza stanowiły szczególną grupę osób, cieszącą się specjalną ochroną prawną, odnoszącą się do ich danych osobowych[3]. Jak wynika zatem z tego orzeczenia, należy odróżnić dwie sfery: dziennikarską, literacką (w rozumieniu prawa prasowego) – bo tylko ta sfera podlega wyłączeniu z ustawy o ochronie danych osobowych – od sfery, kiedy ta działalność narusza prawa i wolności osoby, której dane dotyczą[4]. Zgodnie z art. 7 ust. 2 pkt 1 prasa to „publikacje periodyczne, które nie tworzą zamkniętej, jednorodnej całości, ukazujące się nie rzadziej niż raz do roku, opatrzone stałym tytułem albo nazwą, numerem bieżącym i datą, a w szczególności: dzienniki i czasopisma, serwisy agencyjne, stałe przekazy teleksowe, biuletyny, programy radiowe i telewizyjne oraz kroniki filmowe; prasą są także wszelkie istniejące i powstające w wyniku postępu technicznego środki masowego przekazywania, w tym także rozgłośnie oraz telewizja i radiowęzły zakładowe, upowszechniające publikacje periodyczne za pomocą druku, wizji, fonii lub innej techniki rozpowszechniania; prasa obejmuje również zespoły ludzi i poszczególne osoby zajmujące się działalnością dziennikarską".[5]

W praktyce definicja ta, mimo iż jest obszerna, nastręcza wiele wątpliwości interpretacyjnych. Brak precyzyjnej definicji może w praktyce skutkować utratą zaufania obywatela do państwa na płaszczyźnie stanowienia prawa. Tym bardziej jeśli SN będzie dokonywał wyłącznie literalnej wykładni art. 7 ust. 2 pkt 1-3

[3] Wyrok NSA z dnia 28 czerwca 2011, I OSK 1217/10, Legalis nr 368982.

[4] Zob.: Wyrok WSA w Warszawie z dnia 8 kwietnia 2010, II SA/Wa 1488/09, Legalis nr 235004.

[5] Prawo prasowe – ustawa z dnia 26 stycznia 1984, Dz.U. nr 5, poz. 24 z póź. zm.

prawa prasowego. Sąd Najwyższy w postanowieniu z dnia 26 lipca 2007 wyraził pogląd (który potem został powtórzony w innych orzeczeniach), że ustawodawca wyraźnie i jednoznacznie stwierdza, że prasą są zarówno dzienniki i czasopisma, jak i „wszelkie istniejące i powstające w wyniku postępu technicznego środki masowego przekazywania [...] upowszechniające publikacje periodyczne za pomocą druku, wizji, fonii lub innej techniki rozpowszechniania" – art. 7 ust. 2 pkt 1 *in fine* prawa prasowego. W tej sytuacji jest rzeczą bezsporną, że dzienniki i czasopisma przez to że ukazują się w formie przekazu internetowego, nie tracą znamion tytułu prasowego, i to zarówno wówczas gdy przekaz internetowy towarzyszy przekazowi utrwalonemu na papierze, drukowanemu, stanowiąc inną, elektroniczną jego postać w systemie *on-line*, jak i wówczas, gdy przekaz istnieje tylko w formie elektronicznej w Internecie, ale ukazuje się tylko periodycznie, spełniając wymogi, o których mowa w art. 7 ust. 2 prawa prasowego. Konsekwencją takiego założenia jest bezwzględny obowiązek rejestracji prasy internetowej. Jakkolwiek korzystne dla dziennikarzy postanowienie SN spotkało się z krytyką m.in. Wojciecha Górowskiego. Stwierdził on, że „wyłączając odpowiedzialność karną oskarżonych, SN posłużył się okolicznością, która nie ma odzwierciedlenia normatywnego w kodeksie karnym. Na gruncie omawianej sprawy powinny znaleźć zastosowanie instytucje kodeksowe, co w konsekwencji mogło doprowadzić SN do rozstrzygnięcia nawet tożsamego z wydanym, ale na podstawie innych przesłanek. Oparcie postanowienia na pozakodeksowej okoliczności wyłączającej odpowiedzialność karną naraża organ orzekający na zarzut niemożności stwierdzenia, który element struktury przestępstwa został „zdekompletowany" w przypadku zachowania oskarżonych. Czy był to czyn bezprawny, ale niezawiniony; czy wyłączona została jego bezprawność; czy też był wprawdzie bezprawny i zawiniony, lecz jego społeczna szkodliwość była znikoma? Brak takiego wskazania powoduje trudne do zaakceptowania konsekwencje. Po pierwsze, nie pozwala na wskazanie ewentualnego środka obrony przed naruszeniem dobra (czy można np. zamknąć witrynę internetową, powołując się na naruszenie prawa?). Po drugie, wywołuje stan niepewności co do granicy między zachowaniami karalnymi a bezkarnymi, co jest nie do pogodzenia z funkcją gwarancyjną prawa karnego. Po trzecie zaś, nie spełnia procesowego wymogu dokładnego opisania czynu. Ponadto, wskazanie takiej ogólnej okoliczności wyłączającej odpowiedzialność karną nie daje podstawy do wymierzania środków związanych z zachowaniem bezprawnym niezawinionym (np. przepadek przedmiotów – tytułem środka zabezpieczającego czy też na podstawie art. 100 k.k.). Warto zwrócić tu uwagę na spór dotyczący możliwości wyłączenia odpowiedzialności karnej w oparciu o pozakodeksowe kontratypy czy też okoliczności wyłączające winę"[6]. Czy można uznać stronę internetową

[6] W. Górowski, *Glosa do postanowienia SN z dnia 26 lipca 2007r., IV KK 174/07*, „Państwo i Prawo" 2008, nr 6, s. 127–128.

lub bloga za prasę (tzn. czy jest to środek masowego przekazywania powstający w wyniku postępu technicznego?) lub czy gazetka reklamowa z produktami jakiegoś sklepu (która ma kolejny numer i ukazuje się cyklicznie) jest także prasą?

Prasą są także zespoły ludzkie – więc czy każdy, kto chociaż raz opublikuje materiał prasowy np. w dzienniku jest dziennikarzem? Kogo zatem, w myśl prawa prasowego, można uznać za dziennikarza?

Tego, czy blog jest prasą, nie rozstrzygają nawet najnowsze orzeczenia sądowe. W postanowieniu z dnia 18 stycznia 2013 SA w Łodzi orzekł, że „blog nie jest formą publikacji na tyle zamkniętą i jednorodną, by można było *a priori* zakładać, że jako przekaz internetowy nigdy nie wypełnia ustawowych znamion definicji prasy”[7]. Oznacza to, że niektóre serwisy internetowe (w tym blogi) mogą być uznane za prasę, jeśli: ukazują się w regularnych odstępach czasu, ale nie rzadziej niż raz do roku, opatrzone są stałym tytułem albo nazwą, numerem bieżącym i datą, nie tworzą zamkniętej, jednorodnej całości (związanej fabułą, postaciami) i mają ogólnoinformacyjny charakter. W innym postanowieniu z tego samego dnia SA w Łodzi podkreślił, że skoro rolą i zadaniem prasy jest rozpowszechnianie informacji, to periodyczność przekazu, czyli cyklicznego informowania opinii publicznej o określonych faktach społecznych, ekonomicznych, gospodarczych, politycznych, oświatowych, kulturalnych, pod oznaczonym tytułem, nazwą, adresem czy nawet linkiem, wskazywać będzie na cel, jaki realizuje redakcja, wydawca czy autor danej publikacji elektronicznej, na stworzonej specjalnie w tym celu stronie internetowej[8]. Innymi słowy podkreślił rolę periodyczności przekazu (a nie formy) jako niezbędnej cechy prasy.

Rozstrzygnięcie kwestii, czy blog jest prasą, ma istotne znaczenie praktyczne. Zgodnie bowiem z art. 38 prawa prasowego odpowiedzialność cywilną za naruszenie prawa spowodowane opublikowaniem materiału prasowego lub za samo ujawnienie materiału prasowego przed publikacją ponoszą: autor, redaktor lub inna osoba odpowiedzialna za publikację, może nią być także wydawca. Dziennikarz może również swoim działaniem wypełnić dyspozycję przestępstwa prasowego (karnego), albo poprzez samą zawartość materiału (np. przestępstwo zniesławienia) albo poprzez naruszenie norm porządkowych zawartych w przepisach prasowych (np. wydawanie prasy drukowanej bez rejestracji). W przypadku bloga odpowiedzialność za treści znajdujące się na stronach internetowych mogą ponieść:

a) dostawcy treści (Internet Content Provider, ICP) lub użytkownicy końcowi, którzy dodadzą komentarz do materiału , tzw. autorzy treści,

---

[7] Postanowienie SA w Łodzi z dnia 18 stycznia 2013, I ACa 1031/12, LEX nr 1280424.

[8] Postanowienie SA w Łodzi z dnia 18 stycznia 2013, I ACa 1032/12, LEX nr 1280426.

b) dostawcy usług internetowych (Internet Service Provider) lub dostawcy dostępu do Internetu (Internet Access Provider, IAP), tzw. administratorzy domen[9].

Aby jednak pokrzywdzony mógł skorzystać z drogi prawnej w celu ochrony swoich danych osobowych, czci lub dobrego imienia, musi skorzystać z art. 12-14 ustawy o świadczeniu usług drogą elektroniczną[10]. Prawo krajowe powinno umożliwić pociągnięcie do odpowiedzialności bezpośrednio autora treści naruszającej prawa pokrzywdzonego. Nie ma większego problemu, jeżeli treści te

---

[9] J. Kulesza, *Ius internet*, Warszawa 2012, s. 193–194.

[10] Art. 12.1. Usługodawca, który świadczy drogą elektroniczną usługi obejmujące transmisję w sieci telekomunikacyjnej danych przekazywanych przez odbiorcę usługi lub zapewnienie dostępu do sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, nie ponosi odpowiedzialności za treść tych danych, jeżeli:

1) nie jest inicjatorem przekazu danych;

2) nie wybiera odbiorcy przekazu danych;

3) nie wybiera oraz nie modyfikuje informacji zawartych w przekazie.

2. Wyłączenie odpowiedzialności, o którym mowa w ust. 1, obejmuje także automatyczne i krótkotrwałe pośrednie przechowywanie transmitowanych danych, jeżeli działanie to ma wyłącznie na celu przeprowadzenie transmisji, a dane nie są przechowywane dłużej, niż jest to w zwykłych warunkach konieczne dla zrealizowania transmisji.

Art. 13.1. Nie ponosi odpowiedzialności za przechowywane dane ten, kto transmitując dane oraz zapewniając automatyczne i krótkotrwałe pośrednie przechowywanie tych danych w celu przyspieszenia ponownego dostępu do nich na żądanie innego podmiotu:

1) nie modyfikuje danych;

2) posługuje się uznanymi i stosowanymi zwykle w tego rodzaju działalności technikami informatycznymi określającymi parametry techniczne dostępu do danych i ich aktualizowania oraz

3) nie zakłóca posługiwania się technikami informatycznymi uznanymi i stosowanymi zwykle w tego rodzaju działalności w zakresie zbierania informacji o korzystaniu ze zgromadzonych danych.

2. Nie ponosi odpowiedzialności za przechowywane dane ten, kto przy zachowaniu warunków, o których mowa w ust. 1, niezwłocznie usunie dane albo uniemożliwi dostęp do przechowywanych danych, gdy uzyska wiadomość, że dane zostały usunięte z początkowego źródła transmisji lub dostęp do nich został uniemożliwiony, albo gdy sąd lub inny właściwy organ nakazał usunięcie danych lub uniemożliwienie do nich dostępu.

Art. 14.1. Nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych.

2. Usługodawca, który otrzymał urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie ponosi odpowiedzialności względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych.

3. Usługodawca, który uzyskał wiarygodną wiadomość o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie odpowiada względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych, jeżeli niezwłocznie zawiadomił usługobiorcę o zamiarze uniemożliwienia do nich dostępu.

4. Przepisów ust. 1-3 nie stosuje się, jeżeli usługodawca przejął kontrolę nad usługobiorcą w rozumieniu przepisów o ochronie konkurencji i konsumentów.

Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002, Dz.U. 2013, poz. 1422.

będą umieszczone na witrynie pod adresem domenowym zarządzanym przez polskie podmioty. Sytuacja komplikuje się jednak, kiedy tymi adresami (domenami) zarządzają podmioty zagraniczne. Uzyskanie danych administratora witryny będzie trudne lub czasami nawet niemożliwe.

Sąd Najwyższy w jednym z orzeczeń stwierdził, że dzienniki i czasopisma przez to, że ukazują się w formie przekazu internetowego nie tracą znamion tytułu prasowego, i to zarówno wówczas, gdy przekaz internetowy towarzyszy przekazowi utrwalonemu na papierze, drukowanemu, stanowiąc inną, elektroniczną jego postać w systemie *on-line*, jak i wówczas, gdy przekaz istnieje tylko w formie elektronicznej w Internecie, ale ukazuje się tylko periodycznie, spełniając wymogi, o których mowa w art. 7 ust. 2 prawa prasowego. Prasy ukazującej się w Internecie nie wolno utożsamiać z witryną internetową. Ustawodawca nie nałożył obowiązku rejestracji na strony czy witryny internetowe, a objął tym obowiązkiem jedynie prasę, a ściślej rzecz biorąc dzienniki i czasopisma[11]. Również WSA w Warszawie w orzeczeniu z dnia 30 października 2008 stwierdził, że periodyki internetowe, by mogły być uznane za wydawnictwa prasowe, wcale nie muszą mieć postaci typowych „gazet" elektronicznych, których wydawcami są tylko wielkie koncerny prasowe, firmujące jedynie znane tytuły publikatorów w systemie *on-line*. O tym, czy publikacja internetowa ma charakter prasowy, decydować powinien cel, jakiemu ma służyć[12].

Definicji prasy nie precyzuje także wyrok SN – Izby Cywilnej z dnia 19 lipca 2006, z którego wynika, że za prasę nie powinien być uznawany każdy publikator o cechach wymienionych w art. 7 ust. 2 pkt 1 prawa prasowego, ale taki, który również „organizacyjnie" może być wiązany z działalnością prasy. W sprawie tej sądy musiały rozstrzygnąć m.in. czy dodatek do gazety (tzw. wkładka) jest także prasą, czy tylko dodatkiem do prasy. Nawet w razie uznania, że dodatek sam jest prasą (a nie łącznie z pismem, do którego jest dodawany), to i tak nie miałyby zastosowania przepisy, które mają zapewnić przyspieszone i uproszczone dochodzenie prostowania informacji podawanych w tym piśmie. Gdyby bowiem dodatek miał mieć status prasy, to pozwanym powinien być redaktor naczelny tego dodatku, nie zaś np. redaktor naczelny pisma, do którego dodatek jest dołączany. Dodatek nie ma jednak redaktora naczelnego, wobec czego nie ma osoby, którą można byłoby pozwać. Jest to istotny argument przemawiający za przyjęciem szerszej interpretacji pojęcia „prasa"[13]. Przy rozstrzyganiu czy dana gazetka, czy blog jest prasą, powinno się brać pod uwagę nie tylko wymogi z art. 7 ust. 2 pkt 1, czyli to, czy publikacja ukazuje się nie rzadziej niż 1 do roku, ma tytuł, numer i datę, i przybiera formę jakiegokolwiek

[11] Postanowienie SN z dnia 15 grudnia 2010, III KK 250/10, LEX nr 784329.

[12] Postanowienie WSA w Warszawie z dnia 30 października 2010, II SA/Wa 1885/07, LEX nr 521930.

[13] Wyrok SN – Izby Cywilnej z dnia 19 lipca 2006, I CSK 147/06, Legalis nr 304551.

środka masowej komunikacji, ale także (zgodnie z wymogami rejestracji tytułu z art. 20 prawa prasowego[14]) czy posiada dane umożliwiające identyfikację redaktora naczelnego i wydawcy, dokładny adres redakcji i wydawcy oraz częstotliwość ukazywania się. Brak dokładnych danych wydawcy (imienia i nazwiska oraz adresu zamieszkania) uniemożliwia skuteczne wniesienie pozwu przeciwko naczelnemu, a brak konkretnie oznaczonego naczelnego uniemożliwia żądanie publikacji sprostowania[15]. Tylko bowiem zarejestrowana prasa, działająca legalnie, korzysta z ochrony prawnej, a dziennikarz tam pracujący może powoływać się na chociażby prawo do anonimatu czy ochronę tajemnicę zawodowej.

Dla uznania jakiegoś środka masowego komunikowania za prasę nie ma też znaczenia do kogo jest skierowana i jaki poziom prezentuje. Jak wynika bowiem z wyroku SN z dnia 29 maja 2008, prasą są także „tytuły przeznaczone dla masowego, nie wyrobionego odbiorcy, schlebiające najprymitywniejszym gustom, zaspokajające prostacką żądzę sensacji. […] Ani kodeks karny ani prawo prasowe określając prawa i obowiązki dziennikarzy (art. 10-12 prawo prasowe) ani żaden inny akt prawny nie czyni dystynkcji między standardami, jakie muszą spełniać poważne tytuły prasowe, adresowane do wyrobionego, wykształconego czytelnika a tymi wymogami, którym muszą odpowiadać pisma popularne, szukające sensacji, w tym także tabloidy. Nie różnicuje także według tego kryterium praw i obowiązków dziennikarzy w swoich judykatach ETPC w Strasburgu[16]".

Prawo prasowe określa, że prasą są również zespoły ludzi i poszczególne osoby zajmujące się działalnością dziennikarską. Konieczne jest zatem precyzyjne ustalenie kim jest sam dziennikarz? Lakoniczne sformułowanie art. 7 ust. 2 pkt 5, że dziennikarz to osoba zajmująca się redagowaniem, tworzeniem lub przygotowaniem materiałów prasowych, pozostająca w stosunku pracy z redakcją lub zajmująca się taką działalnością na rzecz i z upoważnienia redakcji, też budzi wiele wątpliwości[17]. Choć nie jest to wskazane wprost, ustawodawca

---

[14] Z obowiązku rejestracji prasy, zgodnie z art. 24 prawa prasowego, wyłączona jest działalność radiowa i telewizyjna („rejestracja" uregulowana jest w ustawie o radiofonii i telewizji z dnia 29 grudnia 1992, Dz.U. 2011 nr 43, poz. 226 z póź. zm.) oraz działalność Polskiej Agencji Prasowej (ta uregulowana jest w ustawie z dnia 31 lipca 1997 o Polskiej Agencji Prasowej Dz.U. nr 107, poz. 687 z póź. zm). Prawo prasowe z dnia 26 stycznia 1984, Dz.U. nr 5, poz. 24 z póź. zm.

[15] Od dnia 2 listopada 2012 wyłączono (w odniesieniu do spraw o publikację sprostowania) wymóg wskazania w pozwie adresu pozwanego. Jak bowiem pokazała praktyka – obowiązek oznaczania w piśmie inicjującym postępowanie miejsca zamieszkania redaktora naczelnego (tzn. podania danych, które nie są powszechnie dostępne, np. jawne ze stopki redakcyjnej), niejednokrotnie przekreśla możliwość skutecznego poszukiwania ochrony prawnej na drodze sądowej. Dz.U. 2012 nr 1136, art. 1.

[16] Wyrok SN z dnia 29 maja 2008, II KK 12/08, LEX nr 448953.

[17] Ewa Ferenc-Szydełko w komentarzu do prawa prasowego twierdzi, że „zdefiniowanie zawodu dziennikarza staje się ważną potrzebą. Ujawnia się ona w dyskusji nad sprawą lustracji, ale także współczesne realia życia społecznego wymagają dokładnego wskazania, kto jest dziennikarzem i w związku z tym może powoływać się na prerogatywy związane z tym zawodem, na przykład

tworząc prawo prasowe preferuje zatrudnienie dziennikarza na podstawie umowy o pracę. Jak wynika z wyroku SN z dnia 24 października 2006, rozdzielenie czynności dziennikarza służących przygotowaniu i przedstawieniu audycji radiowej na antenie, pomiędzy umowę o pracę (za minimalnym wynagrodzeniem) i umowę prawa cywilnego (za wynagrodzeniem, które nie obciążało pracodawcy dodatkowymi kosztami pracy) może świadczyć o zamiarze obejścia prawa (nie tylko prawa pracy, ale także prawa ubezpieczeń społecznych i prawa podatkowego)[18].

Ponadto obowiązek zatrudniania dziennikarzy na podstawie umowy o pracę wynika z treści art. 10 ust. 2 i 3 prawa prasowego. Dziennikarz w ramach stosunku pracy[19] ma obowiązek realizowania ustalonej w statucie lub regulaminie redakcji, w której jest zatrudniony, jej ogólnej linii programowej[20]. Działalność sprzeczna z tym obowiązkiem stanowi naruszenie obowiązku pracowniczego, nie stanowi jednak podstawy wystarczającej do rozwiązania bez wypowiedzenia umowy o pracę z winy dziennikarza[21].

Dziennikarz zatem to osoba, która zajmuje się opracowaniem tekstu, nanoszeniem poprawek, a wcześniej zbieraniem materiałów do tekstu, ale pod warunkiem, że jest zatrudniony w redakcji lub działa na rzecz redakcji i z jej upoważ-

---

prawo do tajemnicy dziennikarskiej (art. 15 pr. pras.). Problem ten zauważono w piśmiennictwie. Definicja zawodu powinna być jasno i konkretnie wyrażona. Wydaje się niezbędne ustalenie kryteriów uzyskania statusu dziennikarza. Są nimi: 1) ściśle określona sytuacja prawna do redakcji, 2) twórczy charakter pracy, 3) odpowiednie wykształcenie. Przynależność do korporacji dziennikarskiej nie powinna być obligatoryjna. Konieczny natomiast wydaje się rejestr dziennikarzy, zgodnie z polską (kod: 245101) i europejską klasyfikacją zawodów". E. Ferenc-Szydełko, *Prawo prasowe. Komentarz*, Warszawa 2013, s. 93–94.

[18] Wyrok SN – Izby Pracy z dnia 24 października 2006, I PK 80/06, Legalis nr 77013.

[19] Stosunek pracy, zgodnie z postanowieniami kodeksu pracy, tworzy się na podstawie: umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę. W praktyce istnieją także niepracownicze stosunki zatrudnienia o charakterze: cywilnoprawnym, administracyjnoprawnym, penalnoprawnym, ustrojowoprawnym, gospodarczoprawnym, handlowoprawnym, społeczno-prawnym, socjalnoprawnym, naukowoprawnym, sportowoprawnym, agralnoprawnym. K.W. Baran, *Komentarz do art. 2*, [w:] *Kodeks pracy. Komentarz*, pod red. K. W. Baran, Warszawa 2012, LEX nr 8681, dostęp: 8 grudnia 2014.

[20] Grzegorz J. Pacek uważa, że co prawda nie ma wprawdzie obowiązku podania linii programowej w formie pisemnej, to absurdalne jest twierdzenie, że statut lub regulamin mogą być podawane w formie ustnej. Forma pisemna jest wskazana z kilku powodów: łatwo jest pociągnąć dziennikarza do odpowiedzialności na naruszenie obowiązku nierealizowania linii programowej redakcji oraz można swobodniej odmawiać publikacji reklam (niezgodnych z założeniami programowymi pisma). G.J. Pacek, *Możliwość odmowy publikowania płatnych ogłoszeń i reklam przez wydawcę*, „Glosa" 2007, nr 4, s. 90–91.

[21] Nie ma tutaj zastosowania art. 52 kodeksu pracy, który pozwala w przypadku ciężkiego naruszenia przez pracownika podstawowych obowiązków pracowniczych rozwiązać umowę o pracę bez wypowiedzenia z winy pracownika. Ciężkie naruszenie to działanie charakteryzujące się znacznym stopniem winy pracownika, np. wykorzystywanie zwolnienia lekarskiego niezgodnie z przeznaczeniem.

Wyrok SN z dnia 21 października 1999, I PKN 308/99, LEX nr 45507.

nienia. Poza tą definicją pozostają jednak autorzy blogów spełniających definicję prasy (zarejestrowanych w sądzie okręgowym). Jeśli blog jest prowadzony jednoosobowo – wówczas dana osoba jest równocześnie dziennikarzem i redaktorem naczelnym. Tymczasem prawo prasowe szczególne kompetencje przewiduje w odniesieniu do redaktora naczelnego (inne niż w przypadku dziennikarza). Zgodnie bowiem z art. 7 ust. 2 pkt 7 jest to osoba, która posiada uprawnienia do decydowania o całokształcie działalności redakcji. Z jednej strony zawsze może wpłynąć na ukazanie się i kształt każdej publikacji, decydować o podjęciu jakiegoś tematu, kreować linię programową redakcji czy podejmować decyzje w sprawach personalnych. Z drugiej jednak strony redaktor naczelny powinien wprowadzić w redakcji takie standardy, procedury i system kontroli, aby nie dochodziło do bezprawnych publikacji (lub chociażby naruszających zasady etyki zawodowej). Uchybiając tym ogólnym i szczególnym obowiązkom, musi się liczyć z odpowiedzialnością prawną[22].

Precyzyjne określenie kto jest dziennikarzem lub redaktorem naczelnym ma znaczenie także przy określaniu zdolności sądowej. Wojewódzki Sąd Administracyjny w Gdańsku rozpatrywał sprawę dotyczącą legitymacji procesowej prasy i formy odmowy udzielenia informacji niejawnych. Uznał, że ustawodawca nadał prasie istotne uprawnienia, stwierdzając w art. 1 ust. 1 prawa prasowego, że prasa korzysta z wolności wypowiedzi i urzeczywistnia prawo obywateli do ich rzetelnego informowania, jawności życia publicznego oraz kontroli i krytyki społecznej, odsyłając w art. 3a prawa prasowego do ustawy o dostępie do informacji publicznej w zakresie prawa do informacji publicznej. W tej sytuacji stwierdzić należy, że prasa ma zdolność sądową przed sądem administracyjnym nawet wtedy, gdy w konkretnej sprawie jest to jednostka organizacyjna nieposiadająca osobowości prawnej. Zgodnie bowiem z art. 25 § 3 ustawy z dnia 30 sierpnia 2002 – prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2012, poz. 270 ze zm.) zdolność sądową mają także inne jednostki organizacyjne nieposiadające osobowości prawnej, jeżeli przepisy prawa dopuszczają możliwość przyznania im uprawnień lub stwierdzenia albo uznania uprawnienia wynikającego z przepisów prawa. Zatem skoro prasa ma zdolność sądową w postępowaniu przed sądem administracyjnym, to w przypadku, gdy jest to jednostka organizacyjna nieposiadająca osobowości prawnej, musi być określona osoba fizyczna lub osoby fizyczne, które będą za tę jednostkę organizacyjną działały. Z art. 7 ust. 2 pkt 8 prawa prasowego wynika, że jednostką organizującą proces przygotowywania materiałów do publikacji w prasie jest redakcja. Redakcja jest zatem podstawową jednostką organizacyjną prasy. Z kolei redakcją, zgodnie z art. art. 25 ust. 1 prawa prasowego, kieruje redaktor naczelny. Redaktor naczelny redakcji jest zatem uprawniony do występowania

[22] Wyrok SA w Warszawie z dnia 10 kwietnia 2013, VI ACa 1347/12, Legalis nr 722850.

w postępowaniu przed sądem administracyjnym za określoną redakcję. W rozstrzyganej sprawie strona skarżąca w skardze oraz późniejszych pismach była oznaczana jako „B. K. redaktor naczelny A", przy czym w treści skargi B. K. wskazywał, że działa w imieniu A, a zatem nie wniósł on skargi w imieniu własnym. Także z przytoczonych w skardze okoliczności faktycznych wynikało, iż żądanie nie jest związane z prywatną działalnością B. K., lecz z pełnioną przez niego funkcją redaktora naczelnego A. Do Burmistrza o udostępnienie informacji publicznej zwracał się nie B. K., lecz dziennikarz Redakcji A B. G. Z okoliczności faktycznych sprawy wynikało jednocześnie, że B. G. nie występował do Burmistrza we własnym imieniu, lecz w imieniu A. Wskazuje na to jednoznacznie nagłówek oraz stopka wiadomości elektronicznej skierowanej do organu i zawierającej wniosek o udzielenie żądanej informacji. Sąd uznał zatem, że skarżącym w niniejszej sprawie jest Redakcja A, w którego imieniu działa jej redaktor naczelny B. K., a skarga dotyczy bezczynności Burmistrza w zakresie żądania skierowanego do tego organu przez Redakcję A w osobie jednego z jej dziennikarzy, B. G. Skarga redakcji A. mogła zatem zostać poddana merytorycznemu rozpoznaniu[23].

Uprawnienia kontrolne GIODO względem prasy

W celu wykonania zadań GIODO, jego zastępca lub upoważnieni przez niego pracownicy (dalej: inspektorzy[24]) mają prawo wstępu, w godzinach od 6.00 do 22.00, do pomieszczenia, w którym zlokalizowany jest zbiór danych oraz pomieszczenia, w którym przetwarzane są dane osobowe poza zbiorem, po wcześniejszym okazaniu imiennego upoważnienia do kontroli i legitymacji służbowej[25]. Mogą żądać złożenia pisemnych lub ustnych wyjaśnień, wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego

[23] Zob. wyrok WSA w Gdańsku z dnia 5 grudnia 2012, II SAB/Gd 79/12, LEX nr 1234516.

[24] Ustawa (ani rozporządzenie) nie określa żadnych wymagań wobec pracowników – kontrolerów Biura GIODO. Każdy zatem pracownik Biura GIODO, niezależnie od stosunku pracy czy służbowego, wykształcenia, stażu pracy i kwalifikacji, jeśli ma stosowne upoważnienie, może wykonywać czynności kontrolne. P. Szustakiewicz, *Kontrole Generalnego Inspektora Ochrony Danych Osobowych*, „Kontrola Państwowa" 2007, nr 6, s. 57.

[25] Na podstawie art. 22a ustawy o ochronie danych osobowych Minister Spraw Wewnętrznych i Administracji wydał 22 kwietnia 2004 rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych, Dz. U. nr 94, poz. 923 z póź. zm. Po nowelizacji rozporządzenia od 20 maja 2011 upoważnienie kontrolera musi zawierać informacje: dane kontrolera, jego stanowisko służbowe, numer legitymacji służbowej, określenie podmiotu kontroli, czyli informacja na temat kontrolowanego zbioru danych osobowych, miejsca kontroli oraz zakres przedmiotowy kontroli i datę rozpoczęcia oraz przewidywany termin zakończenia kontroli. Upoważnienie imienne ważne jest tylko razem z legitymacją służbową. Nie ma już natomiast wymienionych uprawnień kontrolera (określonych w art. 14 uodo).

oraz zlecać sporządzanie ekspertyz i opinii. Mają prawo wglądu do wszelkich dokumentów i danych, mających bezpośredni związek z przedmiotem kontroli (oraz sporządzania ich kopii), przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych, służących do przetwarzania danych[26]. W praktyce przesłuchanie osób w charakterze świadka stosowane jest w sytuacji, gdy inne środki dowodowe okazały się niewystarczające do ustalenia stanu faktycznego[27]. Kontrolerom nie przysługuje jednak uprawnienie do zatrzymania dokumentów objętych kontrolą. Wszelkie uprawnienia kontrolne mogą być wykonywane tylko w celu realizacji zadań określonych w art. 12 ust. 1 i 2, czyli kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz wydawania decyzji administracyjnych i rozpatrywania skarg w sprawach wykonania tych przepisów. Od 7 marca 2011 utrudnianie pracy kontrolerom jest karalne. Każdy, kto udaremnia lub utrudnia kontrolerowi wykonanie czynności kontrolnej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 54a). Wprowadzenie tego przepisu było spowodowane m.in. wcześniejszą praktyką stosowania ustawy i tym, że art. 225 k.k. zawęża katalog osób podlegających ochronie prawnej ze względu na prowadzoną kontrolę[28]. Z drugiej jednak strony kontrolerzy nie są uprawnieni do nieograniczone-

---

[26] W odniesieniu do zbiorów danych: zawierających informacje niejawne, dotyczących osób należących do kościoła lub związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego a uzyskanych w wyniku czynności operacyjno-rozpoznawczych przez uprawnionych funkcjonariuszy, i przetwarzanych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Centralne Biuro Antykorupcyjne – GIODO nie przysługują uprawnienia określone w art. 12 pkt 2, art. 14 pkt 1 i 3-5 oraz art. 15-18 – art. 43 ust. 2 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997, Dz. U. 2014, poz.1182 z póź. zm. Zatem kontrolerowi przysługuje w odniesieniu do tego rodzaju zbiorów przysługuje wyłącznie żądanie złożenia pisemnych lub ustnych wyjaśnień oraz wzywanie i przesłuchiwanie osób w zakresie niezbędnym do ustalenia stanu faktycznego.

[27] B. Pilc, *Rola administratora bezpieczeństwa informacji podczas inspekcji prowadzonej przez Generalnego Inspektora Ochrona Danych Osobowych*, dodatek „Monitora Prawniczego" 2012, nr 7, s. 1046.

[28] Art. 225 kodeksu karnego stanowi, że „§ 1. Kto osobie uprawnionej do przeprowadzania kontroli w zakresie ochrony środowiska lub osobie przybranej jej do pomocy udaremnia lub utrudnia wykonanie czynności służbowej, podlega karze pozbawienia wolności do lat 3.

§ 2. Tej samej karze podlega, kto osobie uprawnionej do kontroli w zakresie inspekcji pracy lub osobie przybranej jej do pomocy udaremnia lub utrudnia wykonanie czynności służbowej.

§ 3. (uchylony).

§ 4. Tej samej karze podlega, kto osobie upoważnionej do przeprowadzania czynności w zakresie nadzoru i kontroli w jednostkach organizacyjnych pomocy społecznej lub w placówkach zapewniających całodobową opiekę osobom niepełnosprawnym, przewlekle chorym lub osobom w podeszłym wieku udaremnia lub utrudnia wykonanie czynności służbowych." Oznacza to, że przedmiotem ochrony jest tu wyłącznie prawidłowość służbowych czynności kontrolnych w zakresie ochrony środowiska, inspekcji pracy oraz w zakresie nadzoru i kontroli w jednostkach pomocy społecznej i w placówkach zapewniających całodobową opiekę osobom niepełnosprawnym, przewlekle chorym lub w podeszłym wieku. Ochronie nie podlegają kontrolerzy biura Generalnego Inspektora Ochrony Danych Osobowych.

go poruszania się po kontrolowanej jednostce. Nadużyciem z ich strony byłoby żądanie dostępu do gabinetu kierownika kontrolowanej jednostki, jeśli nie ma w nim dokumentów objętych przedmiotem kontroli[29].

Kierownik jednostki kontrolowanej oraz kontrolowana osoba fizyczna, będąca administratorem danych osobowych[30], zobowiązani są umożliwić kontrolerowi przeprowadzenie kontroli oraz spełnić żądania, o których mowa w art. 14 pkt 1-4 (wstępu do lokalu, żądania pisemnych lub ustnych wyjaśnień, wglądu do dokumentów, przeprowadzania oględzin urządzeń). Przepis art. 15 ust. 1 koresponduje z przepisem art. 14 i zapewnia inspektorowi odpowiednie warunki do przeprowadzenia kontroli. Przepis ten stosuje się również (zgodnie z art. 31 ust. 5) do kontroli zgodności przetwarzania danych przez podmiot, któremu na podstawie umowy zawartej na piśmie powierzono przetwarzanie danych.

Podczas kontroli inspektor zwraca szczególną uwagę na :

1) przesłanki legalności przetwarzania danych (i danych wrażliwych, czyli szczególne chronionych), np. poprzez zweryfikowanie treści oświadczenia upoważniającego do przetwarzania danych lub treści umowy;

2) zakres i cel przetwarzania danych – czyli jakie kategorie danych i o jakich podmiotach są przetwarzane;

3) merytoryczną poprawność danych i ich adekwatność w odniesieniu do celu przetwarzania, czyli podmiot kontrolowany musi uzasadnić potrzebę przetwarzania danych osobowych i ich poprawność;

4) obowiązek informacyjny, czyli czy administrator danych w sposób właściwy poinformował osoby, których dane dotyczą o przysługujących im prawach;

5) zgłoszenie zbioru do rejestracji, czyli czy prowadzone przez podmiot kontrolowany zbiory podlegają obowiązkowi rejestracji u GIODO;

6) przekazywanie danych do państwa trzeciego, czyli czy podmiot kontrolowany przekazuje dane do państwa trzeciego, a jeśli tak, czy robi to legalnie i z poszanowaniem wymogów technicznych;

7) powierzenie przetwarzania danych, czyli komu administrator danych powierzył faktyczne administrowanie nimi (czy umowa została sporządzona na piśmie, precyzyjność jej uregulowań);

8) zabezpieczenie danych, czyli zgodność przetwarzania danych z przepisami ustawy o ochronie danych osobowych[31].

---

[29] Więcej: P. Szustakiewicz, *Kontrole Generalnego Inspektora Ochrony Danych Osobowych*, „Kontrola Państwowa" 2007, nr 6, s. 52–59.

[30] Środki przewidziane w art. 14 pkt 1-4, mogą być zgodnie z art. 15 kierowane jedynie do administratora danych. Tylko administrator jest bowiem zobowiązany umożliwić te czynności. Wyrok NSA z dnia 30 stycznia 2002, II SA 1098/01, „Wokanda" 2002, nr 7/8, s. 70 i Legalis nr 54272.

[31] Zob. więcej: B. Pilc, *Ochrona danych osobowych – zaganienia wybrane*, [w:] *Ochrona informacji niejawnych i danych osobowych. Wymiar praktyczny i teoretyczny*, pod red. S. Topolewskiego i P. Żarkowskiego, Siedlce 2014, s. 233–275.

W przypadku kontroli danych osobowych, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów państwa uprawnionych do tych czynności, inspektor ma prawo wglądu do zbioru jedynie za pośrednictwem upoważnionego przedstawiciela jednostki kontrolowanej.

Problem może powstać co do rozumienia warunku „pośrednictwa". Kolejną wątpliwość może budzić relacja od art. 15 ust. 2 do art. 43 ust. 2 , który wyłącza całkowicie stosowanie przepisu art. 15 w odniesieniu do zbiorów danych, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych dokonywanych przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz CBA. Przyjmuje się, że pierwszeństwo mają normy art. 43 ust. 2 i GIODO, jego zastępca i upoważnieni inspektorzy mają prawo jedynie żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego[32].

Z czynności kontrolnych inspektor sporządza protokół pokontrolny. Wszystkie czynności istotne dla sprawy muszą być utrwalone w formie protokołu (a nie np. adnotacji), ponieważ protokół ma umożliwić później odtworzenie przebiegu kontroli[33]. Protokół czynności kontrolnych powinien zawierać: pełną nazwę i adres podmiotu kontrolowanego, dane inspektora (kontrolera), tj. imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia, dane osoby reprezentującej podmiot kontrolowany, datę rozpoczęcia i zakończenia kontroli, określenie przedmiotu i zakresu kontroli, opis stanu faktycznego i informacje mające znaczenie dla oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, wyszczególnienie załączników stanowiących część składową protokołu[34], omówienie i parafowanie wszelkich

---

[32] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 416–417.

Autorzy zastanawiają się, czy takie rozróżnienie jest uzasadnione i czy nie lepszym rozwiązaniem byłoby ujednolicenie norm w tym zakresie.

[33] „Nie można uznać odręcznych notatek pracowników organu za dowody w sprawie. Możliwość sporządzenia adnotacji z czynności organu, przewidziana w art. 72 k.p.a., nie może dotyczyć ustaleń istotnych dla sprawy. Mogą to być bieżące adnotacje, pomocne wprawdzie przy rozpatrywaniu sprawy, jednakże nie obejmujące ustaleń, od których jej rozstrzygnięcie zależy lub może zależeć. Ustalenia istotne dla sprawy powinny więc spełniać warunki określone w art. 67 i nast. k.p.a." Wyrok NSA z dnia 4 czerwca 1982, I SA 258/82, LEX nr 9685.

[34] Załącznik do protokołu stanowią protokoły z poszczególnych czynności oraz inne dowody związane z kontrolą. Zgodnie bowiem z art. 70 k.p.a. organ administracji publicznej może zezwolić na dołączenie do protokołu zeznania na piśmie. Możliwe jest także dołączenie do protokołu innych dokumentów mających znaczenie dla sprawy. Określenie „może zezwolić" oznacza, że możliwość dołączenia załączników do protokołu pozostawiono uznaniu organu. Uznanie musi przybrać formę procesową. Odmowa takiego zezwolenia musi przybrać formę postanowienia w rozumieniu art. 123 k.p.a – wyrok WSA w Warszawie z dnia 30 maja 2006 r., II SA/WA 1894/05, LEX nr 232206. Na odmowę zezwolenia, nawet jeśli jest w formie postanowienia, nie przysługuje zażalenie. Więcej: B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2012, Legalis.

poprawek, wzmiankę o doręczeniu egzemplarza protokołu osobie reprezentującej podmiot kontrolowany oraz wzmiankę o wniesieniu lub niewniesieniu zastrzeżeń i uwag do protokołu. Ponadto protokół zawiera informację o dacie i miejscu podpisania protokołu przez kontrolera i osobę uprawnioną, czyli kontrolowanego administratora danych. Do postępowania w sprawach uregulowanych w ustawie o ochronie danych osobowych, w tym do protokołów sporządzonych przez inspektora, zgodnie z art. 22, stosuje się przepisy k.p.a.[35]. Tak lakoniczne stwierdzenie może być – i jak wskazuje praktyka staje się – źródłem niepewności prawnej[36].

Artykuł 16 ustawy o ochronie danych osobowych przyznaje więcej uprawnień kontrolowanemu administratorowi danych niż k.p.a. Kontrolowany podmiot ma bowiem prawo, poza podpisaniem protokołu, wnosić również umotywowane zastrzeżenia i uwagi, otrzymać jeden egzemplarz protokołu, a w razie odmowy podpisania – przedstawić swoje stanowisko GIODO w terminie 7 dni (liczonego od dnia odmowy podpisania protokołu). Wzmiankę o odmowie podpisania protokołu sporządza się wyłącznie w sytuacji odmowy podpisania protokołu przez kontrolowanego administratora danych osobowych, a nie przez osobę upoważnioną jedynie do jego odbioru[37]. Żaden przepis nie określa, jakie konsekwencje prawne wywołuje takie zachowanie kierownika jednostki kontrolowanej. Inspektor nie może utrudniać podmiotowi kontrolowanemu korzystania z tych uprawnień. Umotywowane zastrzeżenia mogą odnosić się zarówno do ustaleń zawartych w protokole, jak i do sposobu przeprowadzenia kontroli. Treść protokołu ma wpływ na późniejsze działania GIODO[38]. Na podstawie bowiem wyników

---

[35] Kodeks postępowania administracyjnego – ustawa z dnia 14 czerwca 1960, Dz. U. 2000 nr 98, poz. 1071 z póź. zm. (Dział II, Rozdział 2 Protokoły i adnotacje, art. 67-72).

Zgodnie z wyrokiem NSA z dnia 11 kwietnia 2003 uprawnienia GIODO przewidziane w ustawie o ochronie danych osobowych są realizowane według przepisów k.p.a. (co wynika z art. 22). Łączą się z trybem przetwarzania danych osobowych (art. 7 pkt 2) jako wszelkich operacji na danych osobowych, i uprawnieniami osób, których dane dotyczą, do różnych form ochrony ich interesów (art. 24 i 25 oraz rozdział 4). Nie zależą one od określonych w art. 23 przesłanek dopuszczalności przetwarzania danych.

Wyrok NSA z dnia 11 kwietnia 2003, II SA 1449/02, LEX nr 148969.

[36] M. Kempa, *Stosowanie przepisów kodeksu postępowania administracyjnego w postępowaniu w sprawach ochrony danych osobowych*, [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X-lecie polskiej ustawy o ochronie danych osobowych*, pod red., G. Goździewicza, M. Szabłowskiej, Toruń 2008, s. 280–291.

[37] Wyrok WSA w Warszawie z dnia 30 maja 2006, II SA/Wa 1894/05, LEX nr 232206.

[38] Stanisław Sagan uważa, że każdemu przysługuje prawo do dobrej administracji, która obejmuje m.in.: rzetelność, bezstronność, rozpatrywanie sprawy w rozsądnym terminie, prawo każdej osoby do osobistego przedstawienia sprawy, prawo dostępu każdej osoby do akt sprawy, prawo do dochodzenia naprawienia szkody spowodowanej bezprawną czy niecelową decyzją czy w końcu sądową kontrolę administracji. Więcej: S. Sagan, *Prawo do dobrej administracji (aspekty konstytucyjno-prawne)*, [w:] *Jakość administracji publicznej. Międzynarodowa konferencja naukowa*, Rzeszów 2004, s. 370–372.

kontroli następuje wszczęcie postępowania administracyjnego. O wszczęciu postępowania należy powiadomić wszystkie osoby będące stronami sprawy (zgodnie z art. 61 § 4 k.p.a.). W zawiadomieniu wymienione są przepisy o ochronie danych osobowych, które zostały naruszone oraz opis stanu faktycznego ze wskazaniem dowodów, na podstawie których został on ustalony, czyli zawiera uzasadnienie prawne i faktyczne. Ponadto kontrolowany administrator danych osobowych jest informowany o prawie złożenia w określonym terminie dodatkowych wyjaśnień i o prawie przesłania uzupełniających dowodów, np. dokumentów lub wydruków z systemu informatycznego, które mogą potwierdzić usunięcie stwierdzonych uchybień. Jeśli kontrolowany nie skorzysta z przysługującego mu uprawnienia, decyzja kończąca postępowanie zostanie wydana na podstawie materiału dowodowego zebranego w toku kontroli, o czym również kontrolowany podmiot jest informowany. W wyniku przeprowadzonej kontroli GIODO wydaje decyzje: nakazujące przywrócenie stanu zgodnego z prawem, jeżeli zostały naruszone przepisy o ochronie danych osobowych (zgodnie z art. 18 uodo); umarzające postępowanie jako bezprzedmiotowe, jeżeli postępowanie administracyjne zostało wszczęte w wyniku stwierdzonych w toku kontroli uchybień, a w trakcie postępowania kontrolowany podmiot je usunął i przywrócił stan zgodny z prawem. Jeżeli kontrolowany podmiot kwestionuje skierowaną do niego decyzję, może zwrócić się do GIODO z wnioskiem o ponowne rozpatrzenie sprawy (art. 21 ust. 1 uodo). Na decyzję GIODO wydaną w przedmiocie wniosku o ponowne rozpatrzenie sprawy przysługuje kontrolowanemu skarga do sądu administracyjnego. W pozostałym zakresie obowiązują przepisy k.p.a. Na podstawie ustaleń kontroli inspektor może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień. Kontrolowany podmiot jest obowiązany do poinformowania GIODO w określonym terminie o wynikach tego postępowania i podjętych działaniach (art. 17 ust. 2 uodo).

Jeśli w wyniku kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych (a nie „ustawy o ochronie danych osobowych”[39]), zobowiązany jest wystąpić do GIODO o zastosowanie środków określonych w art. 18[40].

---

[39] Mariusz Swora zwraca uwagę, że ustawodawca w art. 18 ust. 1 u.o o.d.o. mówi o naruszeniu „przepisów o ochronie danych osobowych” nie o „ustawie o ochronie danych osobowych”, z czego należy wnosić, że naruszenie może dotyczyć również innych niż zawarte w tej ustawie przepisów chroniących dane osobowe. M. Swora, *Glosa do wyroku NSA z dnia 4 kwietnia 2003 r., II SA 2935/02*, „Państwo i Prawo” 2004, nr 1, s. 124.

[40] Art. 18 był już kilka razy nowelizowany. 3 października 2001 dodano ust. 2a, następnie 1 marca 2004 poszerzono katalog podmiotów wobec których GIODO nie posiada uprawnień. Ostatnią zmianą z 1 maja 2004 usunięto z artykułu określenie „administratorowi danych”. Zatem adresatem decyzji GIODO, o której mowa w art. 18 ust. 1, może być nie tylko administrator danych, ale także inny podmiot przetwarzający dane osobowe, której administrator powierzył w drodze umowy przetwarzanie danych.

Może również żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień[41] i poinformowania GIODO w określonym terminie o wynikach tego postępowania i podjętych działaniach[42].

Protokoły czynności kontrolnych (i załączniki do nich, np. ekspertyzy biegłych, opinie) uzyskane podczas kontroli są dowodami w już toczącym się postępowaniu administracyjnym. W przypadku naruszenia przepisów o ochronie danych osobowych[43] GIODO z urzędu lub na wniosek osoby zainteresowanej (postępowanie nie może być wszczęte jednocześnie z urzędu i na wniosek[44]) w drodze decyzji administracyjnej nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

1) usunięcie uchybień;

2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych[45];

3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;

4) wstrzymanie przekazywania danych osobowych do państwa trzeciego;

---

[41] Tadeusz Kuczyński wskazuje, że „w związku z tym, że ustawa o ochronie danych osobowych nie zawiera odrębnej, swoistej dlań definicji zwrotu „postępowanie dyscyplinarne", należy przyjąć, iż termin ten powinien być interpretowany w sposób zgodny z regułą znaczeniową przyjętą w prawie pracy. Odpowiedzialność dyscyplinarna jest tam rozumiana jako odpowiedzialność szczególna, której podlegają mianowani pracownicy służby publicznej z powodu naruszenia obowiązków pracowniczych. Ma ona swój odpowiednik na gruncie niepracowniczych stosunków zatrudnienia typu administracyjnoprawnego (służby mundurowe) jako odpowiedzialność funkcjonariuszy z tytułu naruszenia obowiązków służbowych. [...] Na gruncie umownych stosunków pracy będzie to odpowiedzialność porządkowa pracownika." T. Kuczyński, *Ochrona danych osobowych w stosunkach zatrudnienia*, „Przegląd Sądowy" 1998, nr 11–12, s. 128–131.

[42] Grzegorz Sibiga uważa, że czynności kontrolne spełniają dwie funkcje:

„1)środka pozwalającego stwierdzić, czy istnieją podstawy do wszczęcia postępowania administracyjnego i stanowiącego jednocześnie przesłankę wszczęcia tego postępowania w trybie art. 17 ustawy o ochronie danych osobowych,

2) środka dowodowego w już toczącym się postępowaniu administracyjnym.

G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003, s. 149–150.

[43] Konieczne jest stwierdzenie naruszenia przepisów ustawy o ochronie danych osobowych. Uprawnienie do żądania udostępnienia pracownikowi dokumentów (ksero) złożonych w jego aktach osobowych nie mieści się w zakresie praw, które przysługują osobie w związku z przetwarzaniem jej danych osobowych. Uprawnienia tego należy poszukiwać w treści praw i obowiązków wynikających ze stosunku pracy.

Wyrok WSA w Warszawie z dnia 6 września 2005, II SA/Wa 825/05, I. Kamińska, *Ochrona danych osobowych*, Warszawa 2007, s. 69-70 i LEX nr 192892.

[44] Wyrok NSA z dnia 12 lipca 2005, OSK 1365/04. LEX nr 190725.

[45] GIODO jest jedynym organem upoważnionym do rozstrzygnięć w sprawach dotyczących udostępnienia danych osobowych. Żaden z przepisów ustawy o ochronie danych osobowych nie upoważnia administratora danych do prowadzenia postępowania i orzekania w sprawach dotyczących danych osobowych w trybie k.p.a.

Postanowienia SKO w Olsztynie z dnia 24 czerwca 1999, SKO 511/27/99, „OSS" 2000 nr 3 poz. 74.

5) zabezpieczenie danych lub przekazanie ich innym podmiotom;

6) usunięcie danych osobowych[46].

Decyzje GIODO powinny spełniać wszystkie wymogi decyzji administracyjnej określone w art. 107 k.p.a. GIODO nie ma pełnej swobody w wyborze wcześniej wymienionych środków. Wybór powinien być proporcjonalny do zagrożeń prywatności osób, których dane dotyczą. Naruszenie przepisów ustawy o ochronie danych osobowych może stanowić źródło odpowiedzialności administracyjnej oraz odpowiedzialności karnej (określonej w rozdziale 8)[47].

Aby mogło dojść do wydania decyzji merytorycznej na podstawie art. 18 ust. 1 uodo, dane osobowe osoby zainteresowanej – która złożyła do organu wniosek dotyczący przetwarzania jej danych osobowych – muszą znajdować się w posiadaniu podmiotu, którego wniosek ten dotyczy. Decyzja nakazująca przywrócenie stanu zgodnego z prawem nie może bowiem zostać wydana w sytuacji, gdy organ stwierdzi dokonanie w przeszłości naruszeń ustawy o ochronie danych osobowych, jeśli dane te zostały następnie usunięte. W przypadku kolizji ustawy o ochronie danych osobowych z prawem prasowym przepis art. 15 ust. 1 pr. pras. wyłącza obowiązek ujawnienia danych osobowych dziennikarza – autora artykułu prasowego w takiej sytuacji, gdy zastrzegł on anonimowość swojego nazwiska (podpisał artykuł pseudonimem). W takiej sytuacji administrator danych powinien kategorycznie odmówić ujawnienia danych osobowych takiego dziennikarza, wskazując, iż posługiwał się on pseudonimem. Odmowa taka będzie mieściła się w ramach art. 29 ust. 2 i 3 w związku z art. 5 ustawy o ochronie danych osobowych[48]. Istotne, z punktu widzenia obowiązków dziennikarza w zakresie ochrony danych osobowych jest orzeczenie NSA w Warszawie z dnia 28 czerwca 2011. W orzeczeniu tym sąd stwierdził, że prawo prasowe w art. 15 (stanowiącym o prawie do anonimatu) chroni źródło informacji, a nie osobę dziennikarza, którą z kolei obciąża realizacją tego obowiązku.

Wykonywanie przez GIODO funkcji kontrolnych podlega ograniczeniom w okresie poprzedzającym wybory (od dnia zarządzenia wyborów do dnia głosowania) na urząd Prezydenta, do Sejmu, do Senatu, organów samorządu terytorialnego i wyborów do Parlamentu Europejskiego. Jest to celowe działanie prawodawcy. W innym przypadku przepisy ustawy o ochronie danych osobowych mogłyby stać się środkiem w walce wyborczej, utrudniającym zgłaszanie i umieszczanie kandydatów na listach wyborczych.

---

[46] Wyrok NSA z dnia 13 lutego 2003, II SA 1620/01, „Palestra" 2004, nr 1, poz. 231.

[47] GIODO nie może zastosować innych niż określone w art. 18 ust. 1 sankcji nawet względem podmiotu, który wprawdzie od naruszenia ustawy odstąpił, ale wcześniej przetwarzał dane niezgodnie z przepisami.

Wyrok NSA z dnia 19 listopada 2001, II SA 2707/00, I. Kamińska, *Ochrona danych osobowych*, Warszawa 2007, s. 62–63.

[48] Wyrok WSA w Warszawie z dnia 13 lutego 2009, II SA/Wa 1570/08, LEX nr 519829.

Zgodnie z postanowieniami art. 18 ust. 2a GIODO nie jest upoważniony do wydawania decyzji nakazujących usunięcie danych osobowym podmiotom, które zebrały te dane w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa. Możliwe jest nakazanie zachowań innych niż usunięcie ze zbioru, jeśli zbiór prowadzony jest przez podmioty inne niż: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, CBA, Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego.

Przy ustalaniu kompetencji GIODO, wynikających z art. 18, należy wziąć pod uwagę przepisy szczególne regulujące odrębnie wykonywanie czynności określone w art. 18 ust. 1, w razie naruszenia przepisów o ochronie danych osobowych. Przepisy takie znajdują się w: k.p.k (w tym przetwarzanie danych przez komorników), k.p.k., ustawie o Prokuraturze i ustawie o Policji[49], prawie o ustroju sądów powszechnych[50]. Jak wynika z wyroku WSA w Warszawie z dnia 13 czerwca 2006 treść art. 18 ust. 3 ustawy o ochronie danych osobowych nie przesądza ani o właściwości, ani też o braku właściwości organu. Przepis ten nie może stanowić podstawy do zwolnienia GIODO od oceny i rozstrzygania, czy w konkretnie rozpoznawanej sprawie nie doszło do naruszenia ustawy o ochronie danych osobowych. Nie stanowi podstawy do stwierdzenia braku właściwości rzeczowej. Przyznaje jedynie prawo do uwzględnienia przy wydawaniu nakazu, o którym mowa w art. 18 ust. 1, odrębnych przepisów[51].

W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby będącej administratorem danych nosi znamiona przestępstwa określonego w art. 49-54a, GIODO jest zobowiązany skierować zawiadomienie o popełnieniu przestępstwa do organu powołanego do ścigania przestępstw[52], dołączając do zawiadomienia dowody potwierdzające to podejrzenie[53]. Po złożeniu zawiadomienia uprawnienia GIODO ograniczają

---

[49] Więcej: Sprawozdanie z działalności GIODO za okres 01.01.1999– 31.12.1999, s. 77–78.

[50] Więcej: Sprawozdanie z działalności GIODO za okres 01.01.2000– 31.12.2000, s. 56.

[51] Wyrok WSA w Warszawie z dnia 13 czerwca 2006, II SA/Wa 2016/05, LEX nr 219349.

[52] Liczba zawiadomień o podejrzeniu popełnieniu przestępstwa kierowanych przez GIODO:
W 2006 – 15 – brak dokładnych danych
W 2007 – 18 – brak dokładnych danych
W 2008 – 31 – w tym tylko 1 w związku z przeprowadzonymi kontrolami
W 2009 – 27 – w tym tylko 7 w związku z przeprowadzonymi kontrolami
W 2010 – 23 – w tym tylko 5 w związku z przeprowadzonymi kontrolami
W 2011 – 10 – w tym tylko 1 w związku z przeprowadzonymi kontrolami
Zdecydowaną podstawą większości zawiadomień o podejrzeniu popełnieniu przestępstwa stanowią skargi wniesione do GIODO.
Sprawozdanie z działalności GIODO za rok 2011, 2010, 2009, 2008, 2007 i 2006, <http://www.giodo.gov.pl/138/id_art/2685/j/pl/>, dostęp: 30 lipca 2013.

[53] Od 7 marca 2011 obowiązuje art. 19a. 1. W celu realizacji zadań, o których mowa w art. 12 pkt 6 Generalny Inspektor może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących

się wyłącznie do możliwości zaskarżenia postanowienia o odmowie wszczęcia postępowania. Nie ma on możliwości prawnych korzystania ze środków przysługujących pokrzywdzonemu po wszczęciu postępowania karnego (np. składania wniosków dowodowych, zaskarżenia postanowienia o umorzeniu postępowania)[54]. Nie może również wypowiadać się w kwestii popełnienia lub niepopełnienia przestępstwa (np. z art. 49 ustawy o ochronie danych osobowych), ponieważ przekroczyłby swoje kompetencje, a jedynymi organami właściwymi do oceny, czy w danej sprawie zostało popełnione przestępstwo, jest sąd[55].

Zgodnie z art. 36 ust. 1 uodo administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich:

1) udostępnieniem osobom nieupoważnionym (art. 51),
2) zabraniem przez osobę nieuprawnioną (art. 52),
3) przetwarzaniem z naruszeniem ustawy oraz (art. 49, 53 i 54)
4) zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 52).

Ustawodawca nie przesądził jednak, jakie mają być to środki. Mogą być to zatem środki architektoniczno-budowlane, systemy alarmowe, służby ochrony, czy karty chipowe, kody dostępu lub systemy kodujące. Zastosowane środki powinny być stosowne nie tylko do stopnia zagrożenia, ale przede wszystkim do

---

osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych.

2. Generalny Inspektor może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

3. Podmiot, do którego zostało skierowane wystąpienie lub wniosek, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania."

Zmiana ta została na etapie projektu pozytywnie zaopiniowana gdyż dawała GIODO uprawnienia podobne do Rzecznika Praw Obywatelskich, Rzecznika Praw Dziecka czy Rzecznika Ubezpieczonych, a miała w praktyce zapewnić skuteczniejszą ochronę danych osobowych poprzez występowanie z wnioskami o podjęcie inicjatywy ustawodawczej, bądź zmianę aktów prawnych dotyczących ochrony danych osobowych.

Zob. <http://orka.sejm.gov.pl/Druki6ka.nsf/0/1C375B9EBAEAA9EAC12574420044A07F/$file/488.pdf> dostęp: 29 lipca 2013.

[54] GIODO w piśmie do Ministra Sprawiedliwości postulował wprowadzenie takich zmian w postępowaniu karnym, które umożliwiłyby mu uczestniczenie w postępowaniu w charakterze pokrzywdzonego. Kodeks postępowania karnego dopuszcza bowiem możliwość korzystania z praw pokrzywdzonego także innym podmiotom, niż osoby fizyczne lub prawne, których dobro prawne zostało bezpośrednio naruszone lub zagrożone przez przestępstwo (np. zakładowi ubezpieczeń, organom kontroli).

Więcej: Sprawozdanie z działalności GIODO za okres 01.01.2000 – 31.12.2000, s. 317–318.

Obowiązek wynikający z art. 19 nie powstaje wówczas, gdy popełnione przestępstwo nie jest stypizowane w ustawie o ochronie danych osobowych. Nie wyklucza to możliwości złożenia przez GIODO zawiadomienia o przestępstwie (na podstawie k.p.k. o wszczęciu śledztwa).

[55] Więcej: Wyrok WSA w Warszawie z dnia 7 marca 2007, II SA/Wa 2260/06, LEX nr 322805

kategorii chronionych danych osobowych. Ustawa o ochronie danych osobowych nie klasyfikuje wszystkich kategorii danych. Wskazuje tylko, że tzw. dane wrażliwe (czyli np. informacja o karalności, stanie zdrowia...) powinny być szczególnie, ponadprzeciętnie chronione. Zatem to do administratora należy określenie kategorii danych i ich potencjalnych zagrożeń. Powinien on rozważyć, jakie skutki mogą nastąpić w związku z nieuprawnionym dostępem do danych oraz koszty zainstalowania odpowiedniej ochrony.

Przepisy ustawy o ochronie danych osobowych zawierają przepisy karne, uznając większość działań niezgodnych z ustawą za przestępstwa, które podlegają karze grzywny, ograniczenia wolności a nawet pozbawienia wolności. Sankcjom karnym podlega, m.in. przetwarzanie w zbiorze danych osobowych, w sytuacji kiedy ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest się uprawnionym (art. 49). Za przestępstwo uznawany jest czyn popełniony wyłącznie z winy umyślnej. Kwalifikowaną postać czynu zabronionego określonego w tym artykule stanowi przetwarzanie danych wrażliwych (ale nie wszystkich, chodzi bowiem tylko o dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym). Przestępstwo zagrożone jest karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat 2, a w postaci kwalifikowanej do lat 3. Aby jednak działanie sprawcy zostało uznane za przestępstwo, dane osobowe muszą stać się elementem zbioru danych osobowych (zgodnie z treścią art. 7[56]). Ponadto trzeba sprawdzić czy sprawca przetwarzający dane (których przetwarzanie nie było możliwe lub do których nie miał uprawnień) nie może się powołać na jakąkolwiek z przesłanek legalizujących przetwarzanie danych osobowych[57]. Odpowiedzialność karną w przypadku przestępstwa

---

[56] Zgodnie z artykułem 7 pkt. 1 zbiorem danych jest każdy mający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, przy założeniu, że wszystkie kryteria spełnione są łącznie.

Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997, Dz. U 2014, poz. 1182 z póź. zm.

Z orzeczenia NSA z dnia 7 maja 2008 nie wynika, że dane osobowe mają być w definiowanym „zbiorze danych" danymi podstawowymi. Nie wynika również, że kryterium dostępu do tych danych mają być dane identyfikacyjne (inne nazwisko, adres „PESEL"). Byłoby sprzeczne z intencją ustawodawcy i gwarancjami konstytucyjnymi przyjęcie, że dane osobowe prowadzone i przechowywane w zbiorach tworzonych dla realizowania celów gospodarczych czy ochrony bezpieczeństwa, mają nie podlegać ochronie tylko dlatego, że nie są w tych zbiorach danymi podstawowymi. Wyrok NSA z dnia 7 maja 2008, I OSK 983/07, Legalis nr 139618.

[57] Przesłanki legalizujące zostały wymienione w art. 23 uodo. Przetwarzanie danych jest możliwe tylko wtedy, gdy:

Osoba, której dane dotyczą, wyrazi na to zgodę (chyba, że chodzi o usunięcie dotyczących jej danych);

Jest to niezbędne dla zrealizowania uprawnienia lub obowiązku wynikającego z przepisu prawa;

określonego w art. 49 może ponieść każdy (a nie wyłącznie administrator danych osobowych), kto faktycznie decydował o przetwarzaniu danych z naruszeniem ustawy[58].

Kolejnym przestępstwem jest udostępnianie przez administrującego zbiorem danych lub obowiązanego do ochrony danych osobowych dostępu do zbioru osobom nieupoważnionym (art. 51). Trudno jednak uznać, że żądanie udostępnienia przez administratora danych osobowych, np. informacji o wieku sędziego, stanowi nakłanianie do popełnienia przestępstwa (określonego w art. 51 uodo). Informacja o wieku sędziego jest bowiem informacją nierozerwalnie związaną z pełnioną funkcją publiczną i jako taka również stanowi informację publiczną. Nie stosuje się w tym przypadku przesłanki odmowy ujawnienia informacji ze względu na prawo do prywatności[59].

Jest to konieczne dla realizacji umowy, gdy osoba, której dane dotyczą, jest stroną tej umowy, lub gdy jest to konieczne dla podjęcia działań poprzedzających zawarcie umowy;

Jest to konieczne dla wykonania określonych prawem zadań realizowanych dla dobra publicznego;

Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

W odniesieniu do tzw. danych wrażliwych przetwarzanie danych jest dopuszczalne (zgodnie z art. 27), jeżeli:

Osoba, której dane dotyczą wyrazi na to zgodę na piśmie;

Przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i jednocześnie gwarantuje pełną ochronę danych;

Przetwarzanie tych danych jest niezbędne dla ochrony żywotnych interesów tej osoby, a gdy osoba sama nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;

Jest niezbędne do wykonania zadań statutowych kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji, organizacji non-profit lub innych instytucji pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub stałych współpracowników i zapewnione są pełne gwarancje ochrony danych osobowych;

Przetwarzanie danych jest konieczne do dochodzenia praw przed sądem;

Przetwarzanie danych jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia;

Przetwarzanie jest prowadzone w celu ochrony stanu zdrowia (i świadczenia usług medycznych) przy zapewnieniu pełnych gwarancji ochrony danych osobowych;

Przetwarzanie dotyczy danych, które zostały wcześniej podane do wiadomości publicznej przez osobę, której dane dotyczą;

Jest to niezbędne do prowadzenia badań naukowych, publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;

Przetwarzanie danych jest prowadzone przez stronę w celu realizacji prawa i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Art. 23 ust. 1 pkt. 1-5 oraz art. 27 ust. 2 pkt 1-10 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997, Dz. U. 2014, poz. 1182 z póź. zm.

[58] Czynu zabronionego nie popełnia osoba, która pozostaje w błędzie co do okoliczności stanowiącej jego znamię np. gdy administrujący danymi osobowymi jest przekonany, że: zbierane dane nie stanowią danych osobowych w rozumieniu ustawy, sposób przetwarzania danych nie wpisuje się w definicje zbioru, ma prawo przetwarzać dane na podstawie przepisów innej ustawy. Zob. L. Kępa, *Ochrona danych osobowych w praktyce*, Warszawa 2014, s. 313–318.

[59] Wyrok NSA z dnia 5 marca 2013, I OSK 2872/12, Legalis nr 661544.

Przestępstwo z art. 51 uodo, jest przestępstwem indywidualnym i może być popełnione wyłącznie przez administrującego zbiorem danych osobowych lub osobę obowiązaną do ochrony danych osobowych[60] (np. ABI[61]) czy pracownika zatrudnionego do ochrony fizycznej obszaru danych osobowych). Obowiązek ochrony danych osobowych wynikać musi jednoznacznie z przepisów prawa, a nie tylko woli podmiotów zaangażowanych w proces przetwarzania danych[62]. W przypadku podmiotów przetwarzających dane osobowe na zlecenie lub osób upoważnionych do przetwarzania danych obowiązek ochrony danych osobowych nie musi być zawarty w stosownej umowie, ale musi wynikać wprost z przepisów ustawy. W umowie mogą zaś zostać określone dodatkowe (szersze) obowiązki. Przestępstwo to można popełnić umyślnie jak i nieumyślnie zarówno poprzez działanie, jak i zaniechanie. Forma udostępnienia danych jest obojętna. Może to nastąpić poprzez przekazanie nośnika z danymi, wydruku, transmisji danych. Przestępstwem będzie także dopuszczenie osoby nieuprawnionej do przetwarzania danych przez administratora danych. Jak wynika jednak z postanowienia SN z dnia 21 listopada 2007 udostępnienie danych lub umożliwienie dostępu do nich jednej osobie nie wyczerpuje znamion omawianego przestępstwa[63]. Takie stanowisko SN spotkało się z krytyką Aleksandra Herzoga. Przywołał on w swojej krytycznej glosie orzeczenie SN z 21 listopada 2001, z którego wynika, że „samo tylko użycie liczby mnogiej dla określenia

---

[60] Zob. art. 37 uodo stanowi, że „do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych". Ustawa nie określa kwalifikacji ani żadnych wymagań w odniesieniu do osób zatrudnionych przy przetwarzaniu danych osobowych. Dla celów dowodowych upoważnienie powinno: mieć formę pisemną, być sporządzone odrębnie (a nie być wywodzone z treści umowy o pracę), mieć charakter imienny i określać dozwolony zakres przetwarzania danych. W praktyce nadanie upoważnienia powinno być związane ze złożeniem oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych i obowiązkiem zachowania tajemnicy.

Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997, Dz. U 2014, poz. 1182 z póź. zm.

[61] Wacław Zimny kategorycznie wyłącza możliwość stosowania art. 51 do AB1. Więcej: W. Zimny, *Legalność ustanowienia, relacja do administratora danych, odpowiedzialność i rola administratora bezpieczeństwa informacji*, „Ochrona danych osobowych. Biuletyn Administratorów Bezpieczeństwa Informacji" 2000, nr 1, s. 7.

[62] Kodeks pracy przewiduje bowiem (w art. 100§ 2 pkt 4 i 5 kodeksu pracy), że pracownik ma obowiązek zachowania w tajemnicy informacji, które mogłyby narazić pracodawcę na szkodę. Adwokat Monika Brzozowska uważa, że zarówno w stosunku do pracownika, który miał uprawnienia do przeglądania bazy danych, jak i w odniesieniu do pracownika, który takich uprawnień nie miał – stosuje się przepis art. 266§1 kodeksu karnego. M. Brzozowska, *Kradzież danych osobowych*, „Marketing w praktyce" 2012, nr 10, s. 89.

[63] Sąd Najwyższy uznał bowiem, że literalna wykładnia omawianego przepisu skłania do negatywnej odpowiedzi na pytanie, czy w przypadku udostępnienia danych osobowych tylko jednej osobie nieupoważnionej można uznać za wyczerpujące znamiona czynu z art. 51 ustawy. (Art. 51. 1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2).

przedmiotu bezpośredniej ochrony, przedmiotu czynności sprawczej lub środka służącego do popełnienia przestępstwa nie oznacza, że ustawodawca używa jej w znaczeniu zwrotu: „co najmniej dwa”[64]. Ponadto zauważył, że SN w swoim orzeczeniu zupełnie nie rozważał kwestii, że podmiot, który był zobowiązany do ochrony danych osobowych, a który to umożliwił osobie nieuprawnionej dostęp do danych osobowych, musiał liczyć się z tym, że dane te staną się dostępne większej liczbie osób. Nie ma już bowiem kontroli nad tymi danymi. Zatem argument, że udostępnienie danych osobowych tylko jednej nieuprawnionej osobie jest niewłaściwy i stanowi wyraz „niechlujstwa językowego”. Powinno się raczej w każdym przypadku, gdy ustawodawca posługuje się liczbą mnogą, każdorazowo ustalać zakres i znaczenie tejże liczby mnogiej[65].

Gdy sprawca działał umyślnie, podlega karze grzywny, ograniczenia wolności lub pozbawienia wolności do lat 2, a gdy działał nieumyślnie – karze grzywny, ograniczenia wolności albo pozbawienia wolności tylko do roku. Nie wyczerpuje znamion przestępstwa ujawnienie przez administratora danych ogólnie dostępnych[66].

W odniesieniu do prasy – odpowiedzialność karną na podstawie art. 51 ustawy o ochronie danych osobowych – za opublikowanie w materiale prasowym danych osobowych (np. adresu), wbrew zakazowi określonemu w art. 14 ust. 6 prawa prasowego[67], ponosi redaktor naczelny jako osoba ustawowo obowiązana do ochrony tych danych[68]. Nie ponosi jej redaktor (dziennikarz), który przygotował materiał prasowy do publikacji, gdyż ani z przepisów u.o.d.o. nie wynika, że na nim spoczywa obowiązek zabezpieczenia danych osobowych przed udostępnieniem osobom nieupoważnionym (art. 36 ust. 1), ani też prawo prasowe nie czyni go odpowiedzialnym karnie za opublikowanie materiału

---

[64] Uchwała SN z dnia 21 listopada 2001, I KZP 26/01, OSNKW 2002 Nr 1–2, poz. 4.

[65] A. Herzog, Glosa *do orzeczenia Sądu Najwyższego z dnia 21 listopada 2007r., sygn. IV KK 376/07*, „Prokuratura i Prawo” 2008, nr 11, s. 166–167.

[66] H. Dwulat, *Odpowiedzialność karna administratora danych z art. 51 ustawy o ochronie danych osobowych*, „Radca Prawny” 2003, nr 5, s. 51–57.

[67] Art. 14 ust. 6 prawa prasowego stanowi, że „nie wolno bez zgody osoby zainteresowanej publikować informacji oraz danych dotyczących prywatnej sfery życia, chyba że wiąże się to bezpośrednio z działalnością publiczną danej osoby”.

Prawo prasowe – ustawa z dnia 26 stycznia 1984, Dz. U. Nr 5, poz. 24.

[68] Jak wynika z orzeczenia NSA w Warszawie z dnia 25 kwietnia 2014 roku obowiązek zachowania w tajemnicy danych osobowych ciążący na „osobach, które zostały upoważnione do przetwarzania danych” jest unormowaniem, które nie określa charakteru prawnego danych osobowych jako danych objętych tajemnicą ustawową, a ma walor regulacji dotyczącej sposobu zachowania się osób, które „technicznie” dokonują przetwarzania tych danych z upoważnienia administratora danych osobowych. Tajemnica ta nie została powiązana z wykonywaniem określonych zawodów, a upoważnienie do przetwarzania danych może zostać nadane nie tylko pracownikom administratora, ale także innym osobom podlegającym administratorowi. Nie można zatem kwalifikować jej jako tajemnicy zawodowej. Wyrok NSA z dnia 25 kwietnia 2014, I OSK 2499/13, LEX nr 1463584.

prasowego z naruszeniem art. 14 ust. 6, skoro odpowiedzialność za treść materiałów prasowych spoczywa na redaktorze naczelnym (art. 25 ust. 4)[69]. Krytycznie do tego orzeczenia odniosły się Anna Młynarska-Sobaczewska oraz Marlena Sakowska-Baryła, które uważają, że terminu „administrator danych" nie można odnosić wprost do działalności prasowej. Za bardziej adekwatne uważają inne sformułowanie użyte w art. 51: „będąc obowiązany do ochrony danych osobowych". Jeśli zatem pojęcia „administrator danych osobowych" nie stosować w odniesieniu do działalności prasowej, to aktualne zostaje pytanie, kto może być sprawcą przestępstwa z art. 51 ustawy o ochronie danych osobowych. Z treści samego prawa prasowego wynika, że co prawda to redaktor naczelny jest osobą posiadająca uprawnienia do decydowania o całokształcie działalności redakcji, ale nie oznacza to, iż ma on wyłączne prawo do decydowania o publikacji materiału. Prawo do współdecydowania o publikacjach ma również redaktor (dziennikarz). Z analizy art. 49 prawa prasowego wynika również, że odpowiedzialność prawną za naruszenie niektórych przepisów prawa prasowego ponosi każdy (a nie tylko sam redaktor naczelny). Zgodnie z art. 36 ust. 1 ustawy o ochronie danych osobowych to administrator danych jest obowiązany zapewnić środki techniczne i organizacyjne adekwatne do zagrożeń i kategorii danych objętych ochroną. Jeśli zatem, jak twierdzi SN w swoim orzeczeniu, instytucji administratora danych nie można wprost odnieść do działalności dziennikarskiej, to nie sposób stwierdzić czy rzeczywiście na redaktorze naczelnym ciąży obowiązek z art. 36 ust. 1 ustawy o ochronie danych osobowych. Sąd Najwyższy z jednej strony uznał, że redaktor naczelny nie jest administratorem danych, ale z drugiej, zarzucił mu uchybienie obowiązkom administratora danych. Ponadto z treści art. 3a ust. 2 ustawy o ochronie danych osobowych nie wynika wprost, że do działalności prasowej stosuje się także przepisy karne (w tym art. 51). Autorki glosy do orzeczenia SN z dnia 2 października 2006 uważają, że „w działalności prasowej norma może być zrekonstruowana w ten sposób, że popełnia przestępstwo ten, kto w ramach wykonywanej prasowej działalności dziennikarskiej, administrując zbiorem danych lub będąc obowiązany do ich ochrony, udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, o ile doszło przez to do istotnego naruszenia praw i wolności"[70].

Kolejnym występkiem jest naruszenie przez administrującego choćby nieumyślnie obowiązku zabezpieczenia danych przed zabraniem ich przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem (art. 52). Przestępstwo to może popełnić każda osoba, na której ciąży taki obowiązek. Zachowanie sprawcy polega na samym naruszeniu obowiązku zabezpieczenia danych bez względu na to,

---

[69] Wyrok SN z dnia 2 października 2006, V KK 243/06, Legalis nr 79183.

[70] A. Młynarska-Sobaczewska, M. Sakowska-Baryła, *Glosa do wyroku Sądu Najwyższego z dnia 2 X 2006, V KK 243/06*, „Państwo i Prawo" 2007, nr 6, s. 141.

czy dane osobowe zostały zabrane przez osobę nieuprawnioną, zniszczone czy uszkodzone. W praktyce nie ma żadnego znaczenia czy osoba nieuprawniona faktycznie te dane zabrała. Istotne jest w przypadku tego czynu – jak mówi postanowienie SN z dnia 11 grudnia 2000, z którego wynika, że dane osobowe korzystają z ochrony przewidzianej ustawą już wówczas, kiedy tylko istnieje potencjalna możliwość ich znalezienia się w zbiorze danych osobowych, bez względu na to, czy się w nim ostatecznie znalazły, a ustawa w odniesieniu do różnych etapów i rodzajów przetwarzania danych określa jeszcze dodatkowe uprawnienia osób, których dane te dotyczą. Każdy ma bowiem prawo do ochrony dotyczących go danych osobowych, a nie jedynie ten, czyje dane znalazły się już w zbiorze[71]. Obowiązek zabezpieczenia danych osobowych nie jest tożsamy z obowiązkiem nadzorowania przestrzegania zasad ochrony danych osobowych. Pojęcie osoby administrującej danymi osobowymi należy odróżnić od osoby administrującej zbiorem danych osobowych. Zatem, jak wynika z treści art. 52 uodo, przestępstwo może popełnić każda osoba, która zarządza danymi osobowymi (w procesie ich przetwarzania), a nie tylko administrator danych osobowych czy podmioty przetwarzające dane osobowe na zlecenie administratora. Jest to przestępstwo formalne, czyli do jego popełnienia nie jest konieczny jakikolwiek skutek naruszenia obowiązku zabezpieczenia danych. Można je popełnić zarówno umyślnie, jak i nieumyślnie, a sprawca podlega karze grzywny, ograniczenia wolności albo pozbawienia wolności do roku[72].

Niezgłoszenie zbioru danych do rejestracji (art. 53), to kolejne przestępstwo. Może je popełnić każdy, na kim ciąży obowiązek rejestracji zbioru danych, czyli zarówno administrator danych osobowych, jak i osoba działająca w imieniu administratora. Przy czym według interpretacji Pawła Barty i Pawła Litwińskiego czynu określonego w art. 53 nie może popełnić osoba, w przypadku której obowiązek zgłoszenia zbioru danych osobowych do rejestracji nie wynika z przepisów uodo, lecz z czynności prawnej[73]. Nie wypełnia znamion czynu zabronionego niezgłoszenie do rejestracji zbioru ewidencyjnego albo niekompletne zgłoszenie zbioru danych. Czyn może być popełniony tylko umyślnie poprzez zaniechanie, a sprawca podlega karze grzywny, ograniczenia wolności albo pozbawienia wolności do roku.

Ustawa o ochronie danych osobowych wielokrotnie nakłada na administrujących zbiorami danych osobowych obowiązki informacyjne. Niewykonanie obowiązku informacyjnego (określonego w art. 54) może dotyczyć zarówno

---

[71] Postanowienie SN z dnia 11 grudnia 2000, II KKN 438/00, LEX nr 45466.

[72] Więcej: M. Organiściak, R. Zakrzewski, *Ochrona danych osobowych – przepisy karne*, „Przegląd Ustawodawstwa Gospodarczego" 2002, nr 8, s. 16–22.

[73] P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2013, <https://sip.legalis.pl/document-view.seam?documentId=mjxw62zoge3tambvgu3tgnjoobqxalrsha3tmmztha3q>, dostęp: 9 grudnia 2014.

sytuacji zbierania danych osobowych, jak i podczas dalszego przetwarzania danych. W praktyce chodzi tu o przestępstwo niepoinformowania o:

a) prawie dostępu do treści danych;

b) prawie poprawiania danych;

c) nazwie i adresie administratora danych;

d) celu zbierania danych i odbiorcach danych oraz o

e) dobrowolności albo obowiązku podania danych;

f) przysługujących danej osobie (o której zbierane są dane osobowe) prawach.

Przestępstwo popełnić może tylko przez zaniechanie, z winy umyślnej podmiot administrujący zbiorem danych[74]. Znamiona przestępstwa zostaną wypełnione także wtedy, gdy obowiązki określone w art. 24, 25, 32 i 33[75] zostaną spełnione jedynie częściowo[76].

Wszystkie te przestępstwa są ścigane z oskarżenia publicznego. W literaturze można spotkać pogląd, z którym trzeba się zgodzić, że rangę właściwego stosowania i przestrzegania przepisów dotyczących ochrony danych osobowych określa m.in. liczna przestępstw określonych w ustawie oraz fakt, że ustawodawca przewidział za te przestępstwa m.in. karę pozbawienia wolności[77].

Niezależnie od postępowania karnego czy administracyjnego spowodowanego naruszeniem przepisów o ochronie danych osobowych, osoba której prawa naruszono może wszcząć postępowanie cywilne i dochodzić swoich roszczeń na podstawie art. 23 i 24 k.c.

Oprócz zadośćuczynienia możliwe jest też żądanie odszkodowania na podstawie art. 415 k.c., jeśli ujawnienie danych osobowych przyczyniło się do powstania szkody. Osoba żądająca odszkodowania musi jednak wykazać po pierwsze zaistnienie szkody, a po drugie związek między szkodą a brakiem zabezpieczenia danych (czyli winę sprawcy).

---

[74] Paweł Barta i Paweł Fajgielski uważają, że przestępstwo niedopełnienia obowiązku poinformowania może popełnić wyłącznie administrator danych osobowych, gdyż inne podmioty nie zostały, zgodnie z ustawą o ochronie danych osobowych, zobowiązane do wykonywania obowiązku informacyjnego. P. Barta, P. Fajgielski, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2013 <https://sip.legalis.pl/document-view.seam?documentId=mjxw62zoge3tambvgu3tgnjoobqxalrsha3tmmztha4a>, dostęp: 9 grudnia 2014.

[75] Problematyczne może być ustalenie konkretnego terminu wykonania tych obowiązków. Przepisy ustawy nie wyznaczają ścisłych terminów. Obowiązek wynikający z art. 24 powinien być spełniony przed rozpoczęciem zbierania danych, obowiązek ustalony w art. 25 – bezpośrednio po utrwaleniu danych, natomiast obowiązek z art. 32 w zw. z art. 33 administrator musi wykonać w terminie 30 dni od dnia złożenia wniosku.

[76] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 678.

[77] B. Sadowski, *Odpowiedzialność za przetwarzanie danych osobowych niezgodnie z prawem*, „Służba Pracownicza" 2004, nr 10, s. 35–36.

Współpraca GIODO z prasą

Generalny Inspektor Ochrony Danych Osobowych wielokrotnie wskazywał, że kwestia ujawnienia danych osobowych w prasie powinna być rozpatrywana głównie na gruncie przepisów ustawy prawo prasowe. Stosownie do przepisu art. 1 prawa prasowego prasa, zgodnie z Konstytucją, korzysta z wolności wypowiedzi i urzeczywistnia prawo obywateli do ich rzetelnego informowania, jawności życia publicznego oraz kontroli i krytyki społecznej. Tym bardziej, jeśli na przykład prasa informuje o wydatkach poniesionych przez gminę, ponieważ wiąże się to z konstytucyjnym prawem do informacji o działalności władzy publicznej oraz zasadą jawności finansów publicznych. Zgodnie z art. 61 ust. 1 Konstytucji „obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne [...] w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa". Zgodnie z aktualnie obowiązującą Konstytucją ograniczenie prawa do informacji może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa (art. 61 ust. 3 Konstytucji). Generalny Inspektor Ochrony Danych Osobowych już w sprawozdaniu z działalności za 2001 rok uznał także, iż zgodnie z brzmieniem art. 11 ust. 1 ustawy z dnia 26 listopada 1998 o finansach publicznych „finanse publiczne są jawne", zaś jawność tę wyłącza się jedynie w stosunku do tych środków publicznych, których pochodzenie lub przeznaczenie zostało uznane za tajemnicę państwową na podstawie odrębnych przepisów lub jeżeli wynika to z umów międzynarodowych[78]. Analogiczna jest treść art. 61 ustawy z dnia 8 marca 1990 o samorządzie gminnym, zgodnie z którym „gospodarka finansowa gminy jest jawna", a zarząd jest obowiązany m.in. do informowania mieszkańców gminy o wykorzystywaniu środków budżetowych. Biorąc powyższe pod uwagę GIODO stwierdził, iż ujawnienie w prasie wydatków poniesionych przez gminę, na przykład w związku z organizacją imprezy, uzasadnione jest konstytucyjnym prawem obywateli do informacji o działalności organów władzy publicznej oraz zasadą jawności finansów publicznych[79].

Sam GIODO – mimo iż wielokrotnie podkreślał rolę mediów i konieczność publikowania w prasie informacji sprawdzonych i rzetelnych – stał się ich

[78] Obecnie obowiązująca ustawa o finansach publicznych została uchwalona 27 sierpnia 2009, Dz. U. nr 152, poz. 1240 z póź. zm (obecnie Dz. U. 2013, poz. 885 z póź.zm.) Ówczesny art. 11 to obecnie art. 33 ust 1. „gospodarka środkami publicznymi jest jawna", a ograniczenie jawności wynika z treści art. 33 ust. 2 „ Przepisu ust. 1 nie stosuje się do środków publicznych, których pochodzenie lub przeznaczenie zostało uznane za informację niejawną na podstawie odrębnych przepisów lub jeżeli wynika to z umów międzynarodowych."

[79] Sprawozdanie z działalności GIODO za 2001 rok, s. 236 <http://www.giodo.gov.pl/138/id_art/2685/j/pl/>, dostęp: 5 sierpnia 2013.

„ofiarą". O nierzetelności prasy GIODO miał okazję przekonać się przy okazji publikacji artykułu na temat ustawy o ochronie danych osobowych, zamieszczonego w tygodniku „Polityka"[80]. Wzmiankowany tekst okazał się nie tylko nierzetelny, ale też w jego treści pojawiły się informacje nieprawdziwe, wprowadzające czytelnika w błąd. Tytułem przykładu wskazać można, że zdaniem autorki artykułu: ustawa o ochronie danych osobowych weszła w życie w 1997. W rzeczywistości zaś obowiązuje ona od 30 kwietnia 1998; dalej – ustawa o ochronie danych osobowych obejmuje ochroną informacje o osobach zmarłych, co też rozmija się z prawdą. Ponadto treść artykułu, w miejscach w których nie znajdowały się oczywiste przekłamania, przedstawiała zjawiska w sposób wypaczający sens i istotę ustawy. Wobec wątpliwości przedstawianych GIODO przez czytelników „Polityki", którzy wykazali się lepszą niż autorka publikacji wiedzą na jej temat, Generalny Inspektor podjął próby przekonania tygodnika „Polityka" do opublikowania artykułu na temat ochrony danych osobowych, uwzględniającego rzeczywisty stan prawny. Ponieważ starania GIODO w tym zakresie nie zostały przez redakcję uwzględnione, wobec czego skierował on sprawę na drogę postępowania sądowego[81].

Niezależnie jednak od efektów współpracy, GIODO od samego początku swojej działalności starał się o dobry kontakt z mediami. Jak wynika ze sprawozdania GIODO: „Pierwsza konferencja prasowa została zorganizowana w dniu 3 listopada 1998 r. Do udziału zostały zaproszone wszystkie ośrodki telewizji publicznej i komercyjnej, stacje radiowe, dziennikarze prasy codziennej i periodycznej oraz agencje informacyjne. Tematem konferencji było – *Pierwsze półrocze działalności Biura Generalnego Inspektora Ochrony Danych Osobowych*. Generalny Inspektor Ochrony Danych Osobowych przekazał dziennikarzom informacje o pierwszych miesiącach swej działalności (organizacja Biura, struktura zatrudnienia, ilość oraz tematyka skarg i zapytań)"[82]. Wykorzystywał również media o największym zasięgu („Rzeczpospolitą", „Życie", „Gazetę Wyborczą", „Trybunę") do informowania administratorów baz danych o ciążących na nich obowiązkach. Obecnie GIODO przekazuje do publikacji w prasie materiały informacyjno-edukacyjne (w tym decyzje, wystąpienia, sygnalizacje, gotowe opracowania konkretnych zagadnień z zakresu ochrony danych osobowych). Współpracuje z:

- prasą codzienną („Rzeczpospolitą", „Dziennikiem. Gazetą Prawną", „Pulsem Biznesu");

[80] Artykuł autorstwa Martyny Bundy, *Oj dana, dana*, „Polityka" 2004, nr 43, s. 32–34.

[81] Sprawozdanie z działalności GIODO za 2004, s. 57–58 <http://www.giodo.gov.pl/138/id_art/2685/j/pl/> dostęp: 5 sierpnia 2014.

[82] Sprawozdanie z działalności GIODO za okres 23.04.1998– 30.04.1999, s. 29 <http://www.giodo.gov.pl/541/id_art/2685/j/pl/>, dostęp: 5 sierpnia 2014.

- ogólnopolskimi pismami branżowymi („Serwisem Pracowniczym", „Przeglądem Komunalnym", „Computerworldem", „IT w Administracji");
- portalami internetowymi („Dziennikiem Internautów" , „lex.pl");
- czasopismami „kobiecymi" („Twoim Imperium", „Światem Kobiety");
- stacjami radiowymi i telewizyjnymi (IAR, Polskim Radiem Jedynką, Polskim Radiem 24, Radiem TOK FM, Radiem dla Ciebie, TVP INFO, Telewizją Polsat, Superstacją czy TVN 24);
- agencjami informacyjnymi (PAP, KAI, Newserią, która w maju 2013 uruchomiła specjalny kanał informacyjny GIODO).

Sądząc z lektury dotychczasowych sprawozdań z działalności GIODO, najbardziej intensywna współpraca z prasą miała miejsce w 2013. Wyemitowano/ /opublikowano wówczas ponad 170 materiałów prasowych o tematyce ochrony danych osobowych, a GIODO udzielił (pisemnie lub telefonicznie) ponad 320 odpowiedzi. Z roku na rok zwiększał się zakres problemów, z którymi do GIODO zwracali się dziennikarze.

Współpraca z mediami jest tylko jedną z form przekazywania maksymalnie szerokiemu gronu odbiorców najistotniejszych informacji z zakresu danych osobowych. Poza prasą, do działalności informacyjnej wykorzystuje GIODO także:
- stronę internetową (Biuletyn Informacji Publicznej);
- Infolinię;
- Newsletter;
- konferencje i seminaria naukowe;
- szkolenia, kampanie informacyjne i edukacyjne (np: Dni Otwarte GIODO, Dzień Ochrony Danych Osobowych), debaty;
- publikacje książkowe.

Jak wynika z treści sprawozdań – mimo funkcjonowania wielu dostępnych i wykorzystywanych kanałów informacji GIODO ciągle poszerza swoje kontakty z mediami, a dziennikarze mają coraz więcej pytań dotyczących ochrony danych osobowych.

Rozdział 8. Ochrona danych osobowych w innych ustawach a praktyka prasowa

Dane osobowe, które pozyskała nieuprawniona osoba w wyniku braku działania lub nienależytego działania np. administratora danych osobowych, mogą być podstawą do popełnienia innych przestępstw określonych w kodeksie karnym.

Polski kodeks karny z dnia 6 czerwca 1997[1] przewiduje m.in. przestępstwo „podszywania się pod inną osobę" (art. 190a § 2 obowiązuje od 6 czerwca 2011)[2]. Dobrem chronionym są tutaj wizerunek i inne dane osobowe pokrzywdzonego[3]. Przestępstwo to polega na fałszywym podawaniu się za inną osobę

---

[1] W literaturze przedmiotu można znaleźć pogląd, iż dziennikarz może swoim działaniem wypełnić znamiona innych przestępstw określonych w kodeksie karnym, tj.: Do przestępstw popełnionych w treści materiału prasowego (tzw. przestępstw prasowych niewłaściwych) można zaliczyć m.in.: 1) zniesławienie (pomówienie) oraz znieważenie za pomocą środków masowego komunikowania (art. 212 § 2 k.k., art. 216 § 2 k.k.); 2) nawoływanie do wszczęcia wojny napastniczej (art. 117 § 3 k.k.); 3) publiczne znieważanie Narodu lub Rzeczypospolitej Polskiej (art. 133 k.k.); 4) publiczne znieważenie Prezydenta RP (art. 135 § 2 k.k.); 5) publiczne znieważenie głowy państwa obcego lub członka personelu dyplomatycznego bądź urzędnika konsularnego państwa obcego (art. 136 § 2 i 3 k.k.); 6) publiczne znieważenie symboli państwowych Rzeczypospolitej Polskiej (art. 137 § 1 k.k.) lub państwa obcego (art. 138 § 2 k.k.); 7) obrazę uczuć religijnych (art. 196 k.k.); 8) publiczne pochwalanie lub propagowanie pedofilii (art. 200b k.k.); 9) prezentowanie treści pornograficznych (art. 202 § 1 k.k.); 10) znieważenie funkcjonariusza publicznego, a także organu konstytucyjnego RP (art. 226 k.k.); 11) publiczne rozpowszechnianie informacji z postępowania przygotowawczego (art. 241 § 1 k.k.), a także informacji z rozprawy sądowej prowadzonej z wyłączeniem jawności (art. 241 § 2 k.k.); 12) publiczne nawoływanie do popełnienia przestępstwa (art. 255 § 1–2 k.k.) lub pochwalanie popełnienia przestępstwa (art. 255 § 3 k.k.); 13) publiczne znieważanie ze względu na przynależność etniczną, narodową, rasową, wyznaniową itp. (art. 257 k.k.); 14) ujawnienie tajemnicy państwowej, służbowej, zawodowej (art. 265–266 k.k.).

Więcej: M. Bartnik, *Granice wolności dziennikarza. Odpowiedzialność karna dziennikarza*, [w:] *Status prawny dziennikarza*, pod red. W. Lisa, Warszawa 2014, LEX nr 198161.

[2] Art. 190a §2 kodeksu karnego przewiduje karę pozbawienia wolności do lat 3 za podszywanie się pod inną osobę, wykorzystywanie jej wizerunku lub danych osobowych w celu wyrządzenia tej osobie szkody majątkowej lub osobistej.

Kodeks karny – ustawa z dnia 6 czerwca 1997, Dz. U. Nr 88, poz. 553 z póź. zm.

[3] Sformułowanie „wizerunek lub inne [jej] dane osobowe" użyty w art. 190a § 2 jest pewną niezręcznością językową. Wizerunek jest jednym z elementów danych osobowych, podobnie jak PESEL, czy imię i nazwisko, adres zamieszkania, stan cywilny, informacja o zadłużeniu. Pogląd taki wyraził np. Naczelny Sąd Administracyjny w wyroku z dnia 18 listopada 2009. Uznał, że wizerunek jest jednym z bardzo osobistych dóbr człowieka i brak zgody na jego publikowanie, jeśli nie chodzi o osoby publiczne, jest wystarczającym powodem do uznania, że działają przepisy ustawy o ochronie danych osobowych, jeśli tylko spełnione zostały przesłanki z art. 6 ust. 2 ustawy o ochronie danych osobowych. Zatem zdjęcia osoby fizycznej, chociażby wykonane w przeszłości, umożliwiające jej identyfikację, w sytuacji gdy zdjęcie takie jest umieszczone wraz z imieniem i nazwiskiem osoby na

(z wykorzystaniem jej danych osobowych) w celu wyrządzenia jej szkody majątkowej lub osobistej. Czyn ten jest elementem uzupełniającym przestępstwo „stalkingu”[4], czyli uporczywego nękania. W literaturze przedmiotu można znaleźć pogląd, że „przede wszystkim poza zakresem penalizacji art. 190a § 2 k.k. pozostaje sytuacja, kiedy sprawca działa jedynie w celu ukrycia własnej tożsamości lub w celu wyrządzenia szkody innej osobie niż tej, której danymi się posługuje”[5].

Przestępstwo ma charakter formalny, bo dochodzi do niego już w momencie podania się za inną osobę (pokrzywdzonego). W przypadku tego przestępstwa stosuje się art. 6 ustawy o ochronie danych osobowych, który definiuje pojęcie danych osobowych, zgodnie z którym za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej w celu ustalenia jej tożsamości. W praktyce popełniający to przestępstwo nie musi faktycznie wyrządzić szkody majątkowej lub osobistej pokrzywdzonemu. Wystarczy aby sprawca tego chciał (i dążył do tego)[6]. Powodem uzasadniającym konieczność wprowadzenia tego rodzaju regulacji do kodeksu karnego był brak przepisu, który obejmowałby zarówno uporczywe nękanie, jak i równoczesne wykorzystywanie danych osobowych. Ryszard Stefański i Jacek Kosonoga uważają, że gdyby w art. 190a § 2 chodziło wyłącznie o nielegalne posługiwanie się danymi osobowymi, to lepszym rozwiązaniem byłoby umieszczenie tego przepisu w ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997. Mimo dylematów umieszczono jednak ten przepis w kodeksie karnym, ponieważ przestępstwo to może popełnić każdy (jest to „przestępstwo powszechne”) – a nie tak jak w większości przypadków w ustawie o ochronie danych osobowych – administrator danych osobowych (lub inny podmiot działający z upoważnienia administratora). Ponadto przepisów ustawy o ochronie danych osobowych nie stosuje się do osób fizycznych przetwarzających dane w celach

---

nim występującej w miejscu dostępnym dla nieograniczonej liczby podmiotów, należy uznać, iż stanowi ono dane osobowe podlegające ochronie na podstawie ustawy o ochronie danych osobowych. Wyrok NSA z dnia 18 listopada 2009, I OSK 667/09, Legalis nr 240487.

[4] Najczęstszą postacią przestępstwa podszywania się pod inną osobę, wykorzystywania jej wizerunku lub innych danych osobowych jest „cyberstalking”. Stalking polega na wywołaniu uczucia strachu i zagrożenia poprzez świadome i zamierzone naruszenie sfery prywatności poszkodowanego. Zazwyczaj polega na: przejęciu władztwa nad komputerem, publikowaniu nieprawdziwych informacji na temat poszkodowanego, prześladowaniu i obserwowaniu poszkodowanego. Cyberstalking można zaś podzielić na: *e-mail stalking*, *Internet stalking* i *Computer stalking*. Więcej: M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 275.

[5] Więcej: M. Romańczuk-Grącka, *Korzystanie z cudzych dowodów tożsamości a kradzież tożsamości – od Rozporządzenia Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. po aktualne rozwiązania prawne*, [w:] *Idee nowelizacji kodeksu karnego*, pod red. M. Lubelskiego, R. Pawlika, A. Strzelca, Kraków 2014, s. 207–219.

[6] S. Hypś, *Kodeks karny. Komentarz (art. 1-363)*, pod red. A. Grześkowiak, K. Wiaka, Warszawa 2013, s. 860.

„osobistych i domowych" (art. 3a ust. 1 pkt 1)[7]. Poza ochroną art. 190a § 2 pozostają podmioty inne niż osoby fizyczne oraz osoby zmarłe. Przedmiotem ochrony są bowiem „dobra osobiste", a te mogą posiadać wyłącznie osoby żyjące. Kodeks karny używa pojęcia „osoba" – a zmarły już nią nie jest, a ustawa o ochronie danych osobowych wyraźnie stanowi, że dane osobowe charakteryzują wyłącznie osoby żyjące.

Innym przestępstwem stypizowanym w k.k. jest naruszenie tajemnicy służbowej. Zgodnie z art. 266 § 1 „kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2."[8] W praktyce przepis art. 266 § 1 stosuje się w przypadku bezprawnego ujawnienia tajemnicy informatora przez jakąkolwiek osobę (ale nie samego dziennikarza). W przypadku dziennikarza nie ma zastosowania art. 266 § 1 k.k., ponieważ prawo prasowe posiada przepisy karne (regulujące kwestie ochrony danych informatora), a zatem stanowią one *lex specialis* w stosunku do kodeksu karnego. W literaturze przedmiotu można znaleźć twierdzenie, że „niebędący dziennikarzem autor materiału prasowego, który narusza zastrzeżoną tajemnicę swojego informatora, popełnia przestępstwo z art. 266 § 1 k.k., a współdziałający z nim dziennikarz czy redaktor odpowie jako pomocnik lub podżegacz"[9]. Za wykluczeniem odpowiedzialności dziennikarza z tytułu ujawnienia tajemnicy służbowej (ale nie dziennikarskiej) przemawia fakt, że sprawca musi sam zapoznać się z informacją objętą ochroną, a nie dzięki informatorowi. Zgodnie z postanowieniami art. 49 prawa prasowego dziennikarzowi za naruszenie tajemnicy dziennikarskiej lub redakcyjnej oraz za publikacje danych prywatnych bez zgody uprawnionego grozi kara grzywny lub ograniczenia wolności.

Uznanie, że do działalności dziennikarskiej nie stosuje się niektórych przepisów ustawy o ochronie danych osobowych, w tym przepisów dotyczących administratora danych, wywołuje określone konsekwencje. Jak wynika bowiem z wyroku WSA w Warszawie wszczęcie postępowania w przedmiocie stwierdzenia bezprawności działania, przetwarzania danych osobowych, zebranych w ramach „śledztwa dziennikarskiego" na potrzeby publikacji prasowej, w stosunku do wydawcy, zamiast w stosunku do redaktora naczelnego, skutkuje umorzeniem postępowania w stosunku do wydawcy. Skoro materiał prasowy został udostępniony sądowi przez dziennikarza i skoro spółka – wydawca nie była administra-

---

[7] *Kodeks karny. Komentarz (art. 1-358*), pod red. R. Stefańskiego, Warszawa 2012, <https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogeztkmbvgeytenroobqxalrrgy2donjrg44a>, dostęp: 9 grudnia 2014.

[8] Kodeks karny – ustawa z dnia 6 czerwca 1997, Dz. U. Nr 88, poz. 553 z póź. zm.

[9] K. Gotkowicz, B. Komus, *Prawo prasowe. Komentarz*, pod. red. B. Komusa, G. Kuczyńskiego, Warszawa 2013, s. 291.

torem tych danych oraz nie opublikowała tego materiału, zasadne jest uznanie, iż przepisy ustawy o ochronie danych osobowych w stosunku do spółki w ogóle nie znajdą zastosowania[10]. To, że przepisy ustawy o ochronie danych osobowych (zgodnie z art. 3a ust. 2) nie mają zastosowania do przetwarzania danych osobowych w związku z prowadzoną działalnością dziennikarską nie oznacza, że dziennikarz nie poniesie odpowiedzialności prawnej za ujawnienie cudzych danych osobowych.

Zgodnie z wymogami prawa prasowego dziennikarz zbierając i wykorzystując materiały do publikacji musi dbać o to, aby nie naruszać przepisów prawa, np. chronionych prawem tajemnic, zwłaszcza jeśli prowadzi „śledztwa" dziennikarskie. Zdarza się także, że dziennikarz, aby lepiej poznać opisywany przez siebie problem, np. zatrudnia się u przedsiębiorcy. Jak pisze Bogusław Komus „nikt nie będzie przecież „wszczynał" dziennikarskiego śledztwa dla wyjawienia błahych, podrzędnych uchybień, a tym bardziej, by zaprezentować czytelnikom czy widzom przykład gospodarności, uczciwości"[11].

Prawo prasowe nakłada na dziennikarza, bez względu na jego specjalizację, obowiązki: dochowania szczególnej ostrożności i staranności w zbieraniu i wykorzystywaniu materiałów prasowych, maksymalnego obiektywizmu czy przedstawiania prawdy obiektywnej itd. Dziennikarze śledczy często jednak domagają się liberalizacji wymagań w odniesieniu do ich działalności, tłumacząc to pełnioną przez siebie misją, np. ochrony społeczeństwa przed patologiami. Nawet jednak tak szczytny cel nie może uświęcać środków. W odniesieniu do informacji stanowiącej tajemnicę przedsiębiorstwa (przedsiębiorcy)[12] ma zastosowanie art. 23 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji, który stanowi, że kto uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa ujawnia ją innej osobie […] podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2[13].

---

[10] Wyrok WSA w Warszawie z dnia 22 marca 2007, II SA/Wa 1933/06, Legalis nr 165044.

[11] B. Komus, *Dziennikarstwo śledcze w opinii prawników*, [w:] *O dziennikarstwie śledczym. Normy, Zagrożenia, Perspektywy*, pod red. M. Palczewskiego, M. Worsowicz, Łódź 2009, s. 88.

[12] Tajemnica przedsiębiorstwa to nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. Są to zatem informacje odnoszące się do sposobu wykonywania prac, procesu wytwarzania (przetwarzania) produktów, informacje handlowe, czyli listy kontrahentów, treść ofert handlowych, dane marketingowe, czy informacje organizacyjne, czyli np. struktura organizacyjna przedsiębiorstwa, co do których przedsiębiorca podjął działania, aby pozostały niejawne. Nie mogą być objęte tajemnicą takie informacje dotyczące działalności gospodarczej, które muszą być ujawnione przez przedsiębiorców na podstawie innych ustaw. Zob. *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, pod red. J. Szwaji, Warszawa 2013, s. 992–1015.

[13] Ustawa o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993, Dz. U. 2003 nr 153, poz. 1503 z póź. zm.

Przestępstwo to może popełnić osoba, którą nie łączy z przedsiębiorcą żaden stosunek prawny, ponieważ jest to przestępstwo powszechne. Dziennikarz może zatem odpowiadać na podstawie art. 23 ust. 2, jeśli jego działanie w jakikolwiek sposób zagroziło lub naruszyło interes przedsiębiorcy[14]. Swoim działaniem nie musi wywołać poważnej szkody. Powstanie szkody powoduje jednak zwiększenie stopnia karygodności czynu. Dziennikarz nie może uchylić się od odpowiedzialności prawnej ani powołując się na „dobrą wiarę" przy zdobywaniu informacji objętej tajemnicą przedsiębiorstwa (z powodu obowiązku zachowania szczególnej rzetelności i staranności przy zbieraniu i wykorzystywaniu materiałów prasowych), ani tym bardziej w sytuacji, w której nabycie takich informacji nastąpiło w niejasnych okolicznościach[15]. W przypadku, gdy upłynął już trzyletni okres (określony w art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji) lub inny okres określony w umowie od ustania stosunku pracy (lub innego), pracownik może już ujawnić np. dziennikarzowi lub w inny sposób wykorzystać informacje stanowiące tajemnicę przedsiębiorstwa. Dotyczy to jednak tylko takich informacji, w posiadanie których wszedł legalnie. Jeżeli zaś uzyskał informacje stanowiące tajemnicę przedsiębiorstwa w sposób nielegalny, to nawet po upływie wcześniej wspomnianego okresu takie zachowanie będzie bezprawne[16]. Zatem na podstawie art. 23 ust. 2 dziennikarz może odpowiadać za ujawnienie tajemnicy przedsiębiorstwa, gdy uzyskał informację bezprawnie[17].

Zgodnie z art. 116 k.k. przepisy części ogólnej kodeksu karnego mają zastosowanie do innych ustaw przewidujących odpowiedzialność karną, chyba że ustawy te wyraźnie wyłączają ich stosowanie. W przypadku art. 23 ustawy o zwalczaniu nieuczciwej konkurencji takiego wyłączenia nie ma, zatem będą miały zastosowanie przepisy kodeksu karnego. Zgodnie z art. 18 k.k. odpowiedzialność karną ponosi nie tylko sprawca (który ukradł informacje objęte tajemnicą), ale także współsprawca (jeśli dziennikarz popełnia przestępstwo wspólnie i w porozumieniu z inną osobą), podżegacz, czyli ten kto chce, aby inna osoba dokonała czynu zabronionego i nakłania ją do tego oraz pomocnik, czyli ten, kto w zamiarze aby inna osoba dokonała czynu zabronionego, swoim zachowaniem ułatwia jego popełnienie.

---

[14] Zob. np. E. Nowińska, M. du Vall, *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, Warszawa 2013, s. 470.

[15] Anna Golonka uważa, że „czynność sprawcza przestępstwa określonego w art. 23 u.z.n.k. obejmuje jedynie ujawnienie albo wykorzystanie we własnej działalności takich informacji. Przekazanie ich lub nabycie (!) pozostają więc poza zakresem regulacji prawnokarnej." A. Golonka, *Czyny zabronione a czyny nieuczciwej konkurencji*, „Prokuratura i Prawo" 2013, nr 1, s. 128–129.

[16] Będzie to bezprawie cywilne (art. 11 ust. 1 u.z.n.k), jak i kryminalne (art. 23 ust. 2 u.z.n.k). Zob: M. Mozgawa, *Prawnokarne aspekty zwalczania nieuczciwej konkurencji*, „Prokuratura i Prawo" 1996, nr 4, s. 31–47.

[17] Zob: M. Mozgawa, *Glosa do wyroku SN z dnia 3 kwietnia 2002 r., VKKN 223/2000*, „Prokuratura i Prawo" 2003, nr 11, s. 113–123.

Zgodnie z art. 12 ust. 1 pkt 2 prawa prasowego dziennikarz ma obowiązek chronić dobra osobiste, a ponadto interesy działających w dobrej wierze informatorów (i innych osób, które okazują mu zaufanie). W samym prawie prasowym (ani w k.c.) nie ma definicji pojęć „dobra wiara" czy „dobra osobiste". Samo pojęcie „dóbr osobistych" wywoływało spory w doktrynie. Obecnie, według Jacka Sobczaka, dominuje pogląd, że „są wartościami niemajątkowymi, wiążącymi się z osobowością człowieka, uznanymi powszechnie w danym społeczeństwie"[18]. Jeśli porównamy treść art. 12 ust. 1 pkt 2 prawa prasowego z treścią art. 24 k.c., to z porównania jasno wynika, że prawo prasowe przewiduje szerszą ochronę, nakazując dziennikarzowi chronić dobra osobiste informatora czy osoby, która okazała mu zaufanie. Z uznaniem, że dziennikarz ma obowiązek ochrony dóbr osobistych informatorów (i innych osób) polemizuje Ewa Nowińska. Uważa ona, że dziennikarz bardzo łatwo i w wielu sytuacjach narusza dobra osobiste publikacją materiałów prasowych i nie zawsze musi być to spowodowane pogonią za sensacją lecz częściej jest to po prostu związane z koniecznością ujawnienia wielu faktów, okoliczności czy opinii, które mogą naruszyć czyjeś dobra osobiste. Z tych względów proponuje, aby przepis art. 12 ust. 1 pkt 2 „odczytywać następująco: ustawodawca w każdym jego punkcie określił autonomicznie obowiązki dziennikarzy. I tak, w pkt 1 chodzi o obowiązek w postaci szczególnej staranności i rzetelności; w pkt 2 – o obowiązek ochrony interesów działających w dobrej wierze informatorów i osób, które dziennikarzowi okazują zaufanie oraz ich dóbr osobistych i wreszcie w punkcie 3 – o dbałość o poprawność języka polskiego. Z takiego ujęcia […] wynika, iż ustawodawca celowo połączył w jednym przepisie obowiązek ochrony dóbr osobistych i interesów wskazanych w pkt 2 art. 12 osób. Wskazuje na to zwrot „ponadto", który włącza do zakresu ochrony przewidzianej tym postanowieniem dobra osobiste skonkretyzowanej grupy osób. Nie było przecież żadnych przeszkód natury technicznej, aby w razie odmiennej woli ustawodawcy ustalić w sposób nie budzący wątpliwości zakres obowiązku, o którym mowa. Tak więc uważam, iż żaden szczególny obowiązek w odniesieniu do ochrony dóbr osobistych wszystkich osób, którymi interesuje się prasa, nie ciąży na dziennikarzach. Ich odpowiedzialność kształtuje się na zasadach podobnych, jak w odniesieniu do innych osób, z pewnymi prerogatywami dotyczącymi możliwości podawania informacji ze sfery prywatności (art. 14 ustawy) czy wynikającymi z prawa do krytyki (art. 41 ustawy). Ewentualny obowiązek ciążący na dziennikarzu widziałabym w wymogu rzetelności, którego immanentnym elementem jest przecież poszanowanie dóbr osobistych"[19]. Zupełnie inny pogląd ma w tej sprawie Jacek Sobczak, który uważa, że dziennikarz ma bezwzględny obowiązek chronić dobra osobiste, stąd

[18] J. Sobczak, *Dziennikarz – sprawozdawca sądowy. Prawa i obowiązki*, Warszawa 2000, s. 97.
[19] E. Nowińska, *Wolność wypowiedzi prasowej*, Warszawa–Kraków 2007, s. 77.

też nawet brak staranności w weryfikacji np. ogłoszeń prasowych, narusza dobro osobiste osoby. Nierzetelne i niestaranne zachowanie redakcji/ dziennikarza można uznać za umyślne naruszenie dobra osobistego, gdyż winą umyślną jest także zamiar ewentualny, z którym mamy do czynienia w sytuacji, gdy sprawca naruszenia ma świadomość szkodliwego skutku swojego działania i, przewidując jego nastąpienie, co najmniej nań się godzi – *dolus eventualis*[20].

Niezależnie od sporu o zakres obowiązków dziennikarskich brak ochrony dóbr osobistych informatorów (lub osób, które okazały dziennikarzowi zaufanie) może spowodować pociągnięcie dziennikarza do odpowiedzialności prawnej (cywilnej) zgodnie z art. 38 prawa prasowego. Dobra osobiste, przykładowo wymienione w kodeksie cywilnym, są ściśle związane z człowiekiem (i jego godnością). Mimo iż nie wymienione wprost w art. 23 k.c., dane osobowe są zaliczane do dóbr osobistych (samodzielnie lub jako element składowy prawa do prywatności)[21]. Osobie, której dobra osobiste zostały zagrożone (a nie wyłącznie naruszone) bezprawnym działaniem dziennikarza, przysługuje prawo żądania: zaniechania dalszego działania (naruszającego dobra osobiste), usunięcie skutków naruszenia oraz zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy na cel społeczny a także żądanie naprawienia szkody majątkowej.

Abstrahując od przysługujących danej osobie (której dobra osobiste zostały naruszone) żądań wobec dziennikarza, trudno rozstrzygnąć permanentnie pojawiający się konflikt między interesem ogólnym[22] a interesem jednostki. Pomoc-

---

[20] J. Sobczak, *Prawo prasowe. Komentarz*, Warszawa 2008, teza 18 do art. 12, LEX nr 7830.

[21] Do kategorii dóbr osobistych zalicza się: życie, zdrowie, nietykalność cielesną, integralność seksualną, wolność, swobodę sumienia i wyznania, cześć, nazwisko i pseudonim, wizerunek, głos, stan cywilny, przynależność do określonej płci, prywatność, wolność komunikowania się i tajemnicę korespondencji, nietykalność mieszkania, twórczość artystyczna, wynalazcza i racjonalizatorska, kult pamięci o zmarłej osobie, rodzina (więzi rodzinne) oraz rzadko zaliczane do dóbr osobistych jest korzystanie z wartości środowiska naturalnego. P. Machnikowski, A. Cisek, *Kodeks cywilny. Komentarz*, pod red. E. Gniewka, P. Machnikowskiego, Warszawa 2014, Legalis.

Ponadto do dóbr osobistych zalicza się prawo do herbu i innych znaków indywidualizujących, nazwę jednostki niemającej zdolności prawnej, poczucie tożsamości narodowej a sporadycznie zalicza się do kategorii dóbr osobistych: przywiązanie do zwierząt i rzeczy, tytuł zawodowy, udział w tworzeniu wartości kulturalnych oraz prawo do planowania rodziny (w tym prawo do aborcji). P. Księżak, *Kodeks cywilny. Komentarz. Część ogólna*, pod red. P. Księżaka, M. Pyziak-Szafnickiej, Warszawa 2014, LEX nr 170637.

[22] Jak zauważa Zofia Zawadzka, „w ustawodawstwie, orzecznictwie i piśmiennictwie najczęściej używane są pojęcia interesu publicznego i interesu społecznego. Powyższe terminy nie mają definicji legalnej. Nie są również definiowane w doktrynie. Istotne jest, że zarówno interes społeczny, jak i publiczny stanowią klauzule generalne, które wymagają konkretyzacji". Z. Zawadzka, *Wolność prasy a ochrona prywatności osób wykonujących działalność publiczną*, Warszawa 2013, s. 320–321.

O ile nie budzi wątpliwości, że te dwa pojęcia nie są synonimami, to w praktyce trudno dokonać konkretnego ich rozróżnienia. Abstrahując od kontekstu historycznego kształtowania się tych pojęć, za właściwsze (częściej używane) uznaje się pojęcie „interesu publicznego". Prawo prasowe częściej posługuje się terminem „interes społeczny" np. w art. 13 ust. 3 zgodnie z którym, właściwy

ne w rozstrzyganiu tego dylematu może być bogate orzecznictwo sądowe. Sąd Najwyższy w wyroku z dnia 18 stycznia 1984 podkreślił, że wolność prasy może usprawiedliwiać publikowanie informacji o charakterze osobistym, zaś wkroczenie w sferę prywatności (w tym danych osobowych) podjęte w obronie społecznie uzasadnionego interesu (czyli interesu wielu podmiotów, a nie tylko jednego) nie jest bezprawne. Dążenie prasy do osiągnięcia zamierzeń moralizatorskich nie pozwala nikogo przedstawiać w fałszywym świetle[23]. Prawidłowa relacja między interesem ogólnym a interesem społecznym środowiska (w sferze dóbr osobistych) nie może być naruszona w sposób krzywdzący jednostkę. Nawet bowiem prawdziwość i obiektywność relacji nie stanowią wystarczającego kryterium dla stwierdzenia, że podanie do wiadomości publicznej informacji identyfikujących postacie zaprezentowane w materiale prasowym jest dopuszczalne[24]. W innym orzeczeniu SN uznał, że bezprawne jest rozpowszechnianie przez dziennikarza w środkach masowego przekazu bez zgody osoby zainteresowanej informacji i danych dotyczących sfery jej życia prywatnego wyłącznie z powołaniem się na prawo do przedstawiania i krytyki wszelkich zjawisk realizowane w warunkach swobodnego doboru tematu i opracowania materiału prasowego[25]. Z drugiej strony, dominuje obecnie pogląd, że media publiczne przedstawiając wszelkie zjawiska patologiczne, mogą legalnie ujawniać wszystkie (zwłaszcza niekorzystne) fakty dotyczące osób pełniących funkcje publiczne lub tzw. celebrytów, nawet gdy wkraczają w sferę ich prywatności. Sąd Apelacyjny w Gdańsku w wyroku z dnia 24 czerwca 2014 uznał, że jeżeli interes obywatela rozumieć, nie jako prawo do posiadania wiedzy o życiu prywatnym i osobistym (tu: polityków) dla samej satysfakcji ingerowania w ten sposób w ich prywatność, lecz jako wiedzę pozwalającą na weryfikację ich wiarygodności, prawdomówności, konieczną przy dokonywaniu świadomej oceny działalności „osoby publicznej", zwłaszcza w kontekście konstytucyjnego prawa dostępu do informacji publicznej, to pewne informacje o życiu prywatnym takich osób, nie tylko mogą, ale powinny być publikowane[26].

---

sąd lub prokurator może zezwolić, ze względu na ważny interes społeczny, na ujawnienie danych osobowych i wizerunku osób, przeciwko którym toczy się postępowanie przygotowawcze lub sądowe; zaś zgodnie z art. 44 każdy, kto nadużywając swojego stanowiska lub funkcji działa na szkodę innej osoby z powodu krytyki prasowej, opublikowanej w społecznie uzasadnionym interesie, podlega grzywnie albo karze ograniczenia wolności.

Więcej na temat interesu społecznego zobacz: M. Wyrzykowski, *Pojęcie interesu społecznego w prawie administracyjnym*, Warszawa 1986.

[23] Wyrok SN z dnia 18 stycznia 1984, I CR 400/83, LEX nr 2997.

[24] Wyrok SA w Poznaniu z dnia 15 czerwca 2011, I ACa 477/11, LEX nr 898647.

[25] Wyrok SA w Poznaniu z dnia 15 czerwca 2011, I ACa 477/11, LEX nr 898647.

[26] Wyrok SA w Gdańsku z dnia 24 czerwca 2014, I ACa 206/14, LEX nr 1504361. Zob. także: Wyrok SA w Warszawie z dnia 8 lipca 2009, I ACa 316/09, LEX nr 1120112; Wyrok SA w Warszawie z dnia 10 czerwca 2008, VI ACa 1648/07, LEX nr 486304; Wyrok SA w Poznaniu z dnia 27 września 2005, I ACa 1443/03, LEX nr 177088.

Niewątpliwie ochrona dóbr osobistych informatora (i innych osób) nie może sięgać tak daleko, by skutecznie uniemożliwiać wszelką dyskusję (nawet na tematy bulwersujące) z drugiej jednak strony działanie prasy nawet w słusznym celu nie usprawiedliwia krzywdzenia jednostki[27].

[27] Zob. A. Patryk, *Granice prawa mediów publicznych do przedstawiania faktów z życia prywatnego osób*, LEX/ el. 2014, LEX nr 229397.

Zakończenie

Wprowadzeniu do polskiego porządku prawnego mocno spóźnionej ustawy o ochronie danych osobowych towarzyszyły obawy, że będzie ona stanowiła źródło utrudnień w sferze prowadzenia działalności gospodarczej (w tym prasowej). Stawiano też pytanie, czy oczywiście słuszna idea ochrony prywatności (interesów) jednostki nie niesie przypadkiem zagrożeń dla wolności obywatelskich, tj. prawa do informacji, wolności nauki, wolności prasy czy wolności gospodarczej[1]. Ponad szesnaście lat stosowania ustawy rozwiało te wątpliwości. Co nie znaczy, że nie pojawiają się opinie wskazujące na ujemne konsekwencje uchwalenia ustawy. Chodzi przede wszystkim o utrudnienia w pozyskiwanie niektórych informacji[2].

Niezależnie od zgłaszanych wątpliwości źródłem zagrożeń prawa do ochrony danych osobowych mogą być same przepisy ustawy o ochronie danych, jak też inne akty prawne. Zagrożenie może wynikać z braku przejrzystości przepisów (używania nieostrych pojęć) oraz z tendencji do wyłączania stosowania ustawy o ochronie danych osobowych na podstawie innych ustaw. Ustawa o ochronie danych osobowych ma bowiem charakter generalny, a jej dopełnienie stanowią przepisy innych ustaw[3].

---

[1] Poseł Krzysztof Dołowy w toku prac nad ustawą (na 94 posiedzeniu Sejmu II kadencji, 20 listopada 1996), stwierdził, że projekty (rządowy i poselski) są paradoksalnie i spóźnione i przedwczesne. „Spóźnione dlatego, że normy europejskie i światowe dawno regulują zasady dostępu do danych osobowych, a w Polsce o tyle wydają się być abstrakcyjne i przedwczesne, że w kraju, w którym nie są jeszcze powszechne telefony, to zagrożenie, przetwarzaniem i dostępem do danych osobowych przez osoby niepowołane, jest zdecydowanie mniejsze niż w krajach znajdujących się na wyższym poziomie telefonizacji."

<http://orka2.sejm.gov.pl/Debata2.nsf>, dostęp: 1 lutego 2014.

Jose Luis Piñar Mañas uważa, że „prawo do ochrony danych osobowych może stać w sprzeczności z:

1) wolnością wypowiedzi,
2) transparentnością (działań administracji) i dostępem do informacji,
3) interesami gospodarczymi i rozwojem rynku oraz
4) walką z terroryzmem i gwarancjami bezpieczeństwa publicznego."

Więcej: J. L. Piñar Mañas, *Fundamentalne prawo do ochrony danych osobowych, jego istota i wiążące się z nimi wyzwania*, [w:] *Ochrona danych osobowych wczoraj, dziś, jutro*, Warszawa 2006, s. 356–357.

[2] Autor uważa, że pod pozorem prywatności (ochrony danych osobowych) ograniczono prawo dostępu do informacji publicznej i sytuacji tej nie poprawiło znacząco uchwalenie ustawy o dostępie do informacji publicznej. Więcej: C. Martysz, *Informacja publiczna czy chronione dane osobowe*, [w:] *Ochrona danych osobowych wczoraj, dziś, jutro*, Warszawa 2006, s. 229–235.

[3] GIODO wskazuje, że nie tylko całkowite wyłączenie spod ustawy o ochronie danych osobowych, ale także jednostkowe zwolnienie od dopełnienia obowiązków określonych w jej przepisach wymaga szczegółowego uzasadnienia. Sprawozdanie z działalności GIODO za 2006 rok, s. 111–113 <http://www.giodo.gov.pl/156/>, dostęp: 1 lutego 2014.

Jak wynika z doświadczeń GIODO, pozytywnie nie może być oceniona kwestia stosowania przepisów karnych z ustawy o ochronie danych osobowych. Często bowiem organy ścigania albo nie miały świadomości istnienia takiej ustawy, albo bagatelizowały jej zasady (art. 49-54). Tylko w niewielu przypadkach zawiadomień o popełnieniu przestępstwa sprawy znalazły swój finał przed sądem. Najczęściej postępowania w tych sprawach były umarzane z powodu znikomej społecznie szkodliwości czynu, braku znamion czynu zabronionego, czy z powodu niemożności ustalenia sprawcy czynu[4]. Powoli następuje jednak zmiana podejścia Policji i prokuratury do kwestii przestępstw popełnianych na gruncie ustawy o ochronie danych osobowych. Pomimo jednak wzrostu poziomu zrozumienia wśród organów ścigania problematyki ochrony danych osobowych, wydawane orzeczenia wciąż są przykładem iluzoryczności ochrony prawnej osób, których dane dotyczą. Z drugiej jednak strony, jak wynika ze sprawozdań z działalności GIODO, z roku na rok maleje liczba zawiadomień o popełnieniu przestępstwa (np. z 82 w 2004 do 3 w 2014). Niewielka liczba zawiadomień złożonych do organów ścigania może wskazywać, iż wśród podmiotów przetwarzających dane osobowe wzrasta świadomość prawna w zakresie zasad przetwarzania danych osobowych.

Jednym z zadań GIODO jest propagowanie idei ochrony danych osobowych. Początkowo GIODO spotykał się z dziennikarzami na konferencjach prasowych oraz udzielał wywiadów. Później on i pracownicy Biura zaczęli prowadzić szkolenia, seminaria i wykłady odnośnie stosowania przepisów o ochronie danych w instytucjach państwowych, samorządowych i jednostkach wymiaru sprawiedliwości, szkołach wyższych i u innych podmiotów. Obecnie GIODO udziela informacji również poprzez Infolinię czy Newsletterię. Zwiększa się też z roku na rok liczba konferencji zarówno krajowych i zagranicznych, w których udział bierze GIODO. Współpracuje on także z Europejskim Inspektorem Ochrony Danych i innymi instytucjami i organizacjami międzynarodowymi.

Z roku na rok zwiększa się również świadomość ryzyka związanego z przekazywaniem danych osobowych przez Internet. Dzieje się tak m.in. dzięki działalności edukacyjnej GIODO, dokonywanej przy pomocy strony internetowej (www.giodo.gov.pl – gdzie znajduje się serwis „materiały informacyjne") oraz porad i wskazówek tam umieszczanych.

Ustawa o ochronie danych osobowych do chwili obecnej była wielokrotnie nowelizowana. Z punktu widzenia działalności dziennikarskiej największe znaczenia miała nowelizacja, która weszła w życie w 2004. Zawężono bowiem

[4] A. Lewiński, *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. 10-lecie polskiej Ustawy o ochronie danych osobowych*, [w:] *Prawna ochrona danych osobowych na tle europejskich standardów. X-lecie polskiej ustawy o ochronie danych osobowych*, pod red. G. Goździewicza, M. Szabłowskiej, Toruń 2008, s. 9–16.

stosowanie przepisów ustawy o ochronie danych do działalności prasowej oraz działalności literackiej lub artystycznej, z wyjątkiem sytuacji, w których wolność wyrażania poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą[5].

Na kształt ustawy o ochronie danych wpływ miały inne ustawy, m.in. ustawa o podpisie elektronicznym, ochronie informacji niejawnych, o świadczeniu usług drogą elektroniczną, o CBA, czy o dostępie do informacji publicznej. Słabą stroną polskiej ustawy o ochronie danych osobowych jest fakt, że GIODO nie ma możliwości np. wniesienia skargi konstytucyjnej czy bezpośrednio inicjatywy legislacyjnej lub nakładania wysokich kar finansowych na podmioty łamiące przepisy ustawy, co poważnie ogranicza skuteczność podejmowanych przez niego działań. Badania opinii publicznej prowadzone na zlecenie GIODO w latach 2004–2006 (po wprowadzeniu wielu nowelizacji) wskazało, że poczucie bezpieczeństwa obywateli w odniesieniu do dotyczących ich danych osobowych zgromadzonych w bazach danych różnych urzędów (firm, instytucji) nadal jest niskie. Aż 58% badanych uważało, że ich dane są źle chronione. Na taki stan rzeczy wpływ mogły mieć: złe doświadczenia własne badanych (lub ich bliskich), nagłaśniane przez media przypadki „wycieków danych", nieznajomość przepisów ustawy o ochronie danych osobowych czy nieufność obywateli wobec instytucji publicznych[6].

Ustawa o ochronie danych osobowych nie zawiera odesłania do prawa do prywatności czy ochrony dóbr osobistych. W pełni jednak odpowiada wymogom prawa wspólnotowego. Jak zauważa EIOD skuteczna ochrona danych osobowych, jako podstawowa wartość leżąca u podstaw unijnych polityk, powinna być postrzegana jako warunek ich powodzenia[7].

---

[5] Dz. U. 2002 nr 153, poz. 1271, 2004 nr 25, poz. 219, 2004 nr 33, poz. 285.

[6] Sprawozdanie z działalności GIODO za 2006 rok, s. 114–116 <http://www.giodo.gov.pl/156/>, dostęp: 1 lutego 2014.

[7] A. Szczerba, *Europejski Inspektor Ochrony Danych – niezależny organ nadzoru*, [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów,* pod red. G. Goździewicza, M. Szabłowskiej, Toruń 2008, s. 225.

Bibliografia

Publikacje zwarte:

Aarnio R. L. L. M, *Ochrona danych w życiu zawodowym (Data Protection in working life)*, [w:] *Ochrona danych osobowych wczoraj, dziś, jutro. Personal data protection yesterday, today, tomorrow*, Warszawa 2006.

Adamiak B., Borkowski J., *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2012, Legalis.

Amin S. M., Justyński J., *Instytucje i porządek prawny Unii Europejskiej na tle tekstów prawnych oraz orzecznictwa Europejskiego Trybunału Sprawiedliwości*, Toruń 1999.

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012.

Baran K. W., *Komentarz do art. 2, [w:] Kodeks pracy. Komentarz*, pod red. K.W.Baran, Warszawa 2012.

Barbasiewicz A., *Europejska Karta Praw Podstawowych w orzecznictwie polskiego Sądu Najwyższego*, [w:] *5 lat Karty Praw Podstawowych UE. Materiały pokonferencyjne*, pod red. A. Gubrynowicza, Warszawa 2006.

Barta J., Fajgielski P, Markiewicz R., *Ochrona danych osobowych. Komentarz*, Kraków 2007.

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2013.

Bartnik M., *Granice wolności dziennikarza. Odpowiedzialność karna dziennikarza*, [w:] *Status prawny dziennikarza*, pod red. W. Lisa, Warszawa 2014.

Bidziński M., *Komentarz do art. 5*, [w:] *Ustawa o dostępie do informacji publicznej. Komentarz*, M. Bidziński, M. Chmaj, P. Szustakiewicz, Warszawa 2010.

Bisztyga A., *Ochrona praw człowieka w systemie Rady Europy*, [w:] *System ochrony praw człowieka*, B. Banaszak, A. Bisztyga, K. Complak, M. Jabłoński, R. Wieruszewski, K. Wójtowicz, Kraków 2005.

Braciak J., *Prawo do prywatności*, Warszawa 2004.

Bygrave L. A., *Zapewnienie prywatności w Internecie*, [w:] *Prawo do prywatności-prawo do godności. Międzynarodowa Konferencja Ochrony Prywatności i Danych Osobowych 14–16 września 2004 Wrocław*, Warszawa 2006.

Den Boer M., *Międzynarodowe uprawnienia policyjne przyznane policji przez Układ z Schengen*, [w:]*Układ z Schengen. Współpraca policji i organów sprawiedliwości po Maastricht*, pod red. J. Beczały, Łódź 1998.

Dorobek Schengen, [w:]*Unia Europejska. Wspólnota Europejska. Zbiór dokumentów*, oprac. E. Wojtaszek-Mik, C. Mik, Kraków 2005.

Dybowski M., *Prawa fundamentalne w orzecznictwie ETS*, Warszawa 2007.

Ferenc-Szydełko E, *Prawo prasowe. Komentarz*, Warszawa 2013.

Garlicki L., *Komentarz do art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*, [w:] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom 1. Komentarz do artykułów 1–18*, pod red. L. Garlickiego, Warszawa 2010.

Gliszczyńska-Grabias A., Sękowska-Kozłowska K., *Komentarz do art. 17 Międzynarodowego paktu praw obywatelskich i politycznych*, [w:] *Międzynarodowy pakt praw obywatelskich (osobistych) i politycznych. Komentarz*, pod red. R. Wieruszewskiego, Warszawa 2012.

Gotkowicz K., Komus B., *Prawo prasowe. Komentarz*, pod. red. B. Komusa, G. Kuczyńskiego, Warszawa 2013.

Gromski W., Kolasa J., Kozłowski A., Wójtowicz K., *Europejskie i polskie prawo telekomunikacyjne*, Warszawa 2004.
Hypś S., *Kodeks karny. Komentarz (art. 1-363)*, pod red. A. Grześkowiak, K. Wiaka, Warszawa 2013.
Jackowski M., *Ochrona danych medycznych*, Warszawa 2002.
Jasiński F., *Zagadnienia biometrii w Unii Europejskiej. Materiały Robocze 4(8)/06*, Warszawa 2006.
Jaskiernia J. , *Karta Praw Podstawowych Unii Europejskiej a Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności – konflikt czy komplementarność?*, [w:] *Karta Praw Podstawowych w europejskim i krajowym porządku prawnym*, pod red. A. Wróbla, Warszawa 2009.
Justyński J*., Acquis communautaire a acquis Schengen*, [w:] *Unia Europejska – wyzwanie dla polskiej Policji*, pod red. W. Pływaczewskiego, G. Kędzierskiej, P. Bogdalskiego, Szczytno 2003.
Kamiński I. C., *Unia Europejska. Podstawowe akty prawne*, Warszawa 2005.
Kamiński I. C., *Determinanty działalności dziennikarskiej*.*Uprawnienia i obowiązki dziennikarskie w orzecznictwie Europejskiego Trybunału Praw Człowieka*, [w:] *Status prawny dziennikarza*, pod red. W. Lisa, Warszawa 2014.
Karta Praw Podstawowych Unii Europejskiej. *Komentarz*, pod red. A. Wróbla, Warszawa 2013.
Kempa M., *Stosowanie przepisów kodeksu postępowania administracyjnego w postępowaniu w sprawach ochrony danych osobowych*, [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X-lecie polskiej ustawy o ochronie danych osobowych*, pod red., G. Goździewicza, M. Szabłowskiej, Toruń 2008.
Kępa L., *Ochrona danych osobowych w praktyce*, Warszawa 2014.
Kodeks karny. Komentarz (art. 1-358), pod red. R. Stefańskiego, Warszawa 2012.
Komus B., *Dziennikarstwo śledcze w opinii prawników*, [w:] *O dziennikarstwie śledczym. Normy, Zagrożenia*, Perspektywy, pod red. M. Palczewskiego, M. Worsowicz, Łódź 2009.
Kornobis-Romanowska D., *Europejska Konwencja Praw Człowieka w systemie Prawa Wspólnot Europejskich*, Warszawa 2001.
Kotowski M., *Wstęp do ochrony danych. Materiały szkoleniowe*, Warszawa 1979.
Księżak P., *Kodeks cywilny. Komentarz. Część ogólna*, pod red. P. Księżaka, M. Pyziak-Szafnickiej, Warszawa 2014.
Kulesza J., *Ius internet*, Warszawa 2012.
Kuźniar R., *Prawa człowieka. Prawo, Instytucje, Stosunki międzynarodowe*, Warszawa 2008.
Lewiński A., *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. 10-lecie polskiej Ustawy o ochronie danych osobowych*, [w:] *Prawna ochrona danych osobowych na tle europejskich standardów. X-lecie polskiej ustawy o ochronie danych osobowych*, pod red. G. Goździewicza, M. Szabłowskiej, Toruń 2008.
Machnikowski P, Cisek A., *Kodeks cywilny. Komentarz*, pod red. E. Gniewka, P. Machnikowskiego, Warszawa 2014.
Martysz C., *Informacja publiczna czy chronione dane osobowe*, [w:] Ochrona danych osobowych wczoraj, dziś , jutro, Warszawa 2006.
Michalska A., *Komitet Praw Człowieka. Kompetencje, funkcjonowanie, orzecznictwo*, Warszawa 1994.
Mrózek A., *Ustawowe prawo ochrony danych. Analiza Prawnoporównawcza*, Toruń 1981.
Napierała K., *Prawne aspekty ochrony danych osobowych przetwarzanych w systemach informatycznych*, Warszawa 1997.
Nowicki M. A., *Europejski Trybunał Praw Człowieka. Orzecznictwo*, tom 2, Kraków 2002.
Nowińska E., *Wolność wypowiedzi prasowej*, Warszawa–Kraków 2007.
Nowińska E., du Vall M., *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz*, Warszawa 2013.

Ochrona danych. Standardy europejskie. Zbiór materiałów, pod red. T. Jasudowicza, Toruń 1998.
Oniszczuk J., *Konstytucja Rzeczypospolitej Polskiej w orzecznictwie TK na początku XXI wieku*, Kraków 2004.
Patryk A., *Granice prawa mediów publicznych do przedstawiania faktów z życia prywatnego osób*, LEX/ el. 2014.
Pietraś Z. J., *Prawo wspólnotowe i integracja europejska*, Lublin 2006.
Pilc B., *Ochrona danych osobowych – zaganienia wybrane*, [w:] *Ochrona informacji niejawnych i danych osobowych. Wymiar praktyczny i teoretyczny*, pod red. S. Topolewskiego i P. Żarkowskiego, Siedlce 2014.
Piňar Maňas J. L., *The fundamental right to personal data protection, essential content and current challanges (Fundamentalne prawo do ochrony danych osobowych, jego istota i wiążące się z nim wyzwania)*, [w:] Ochrona danych osobowych wczoraj, dziś, jutro, Warszawa 2006.
Plaňavová-Latanowicz J., *Trybunał Sprawiedliwości Wspólnot Europejskich i ochrona praw podstawowych*, Warszawa 2000.
Privacy Rights in the Digital Age, A Proposal for a New General Comment on the Right to Privacy under Article 17 on the International Covenant and Political Rights: A Draft Report and General Comment by the American Civil Liberties Union
Romańczuk-Grącka M., *Korzystanie z cudzych dowodów tożsamości a kradzież tożsamości – od Rozporządzenia Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. po aktualne rozwiązania prawna,* [w:] *Idee nowelizacji kodeksu karnego*, pod red. M. Lubelskiego, R. Pawlika, A. Strzelca, Kraków 2014, s. 207–219.
Safjan M., *Rozwój nauk biomedycznych a granice ochrony prawnej*, [w:] *Współczesne problemy bioetyki w obszarze regulacji prawnych. Materiały z konferencji zorganizowanej przez Komisję Nauki i Edukacji Narodowej pod patronatem Marszałek Sejmu prof. dr hab. Alicji Grześkowiak, 3 kwietnia 2001*, Warszawa 2001.
Sagan S., *Prawo do dobrej administracji (aspekty konstytucyjno-prawne)*, [w:] *Jakość administracji publicznej. Międzynarodowa konferencja naukowa*, Rzeszów 2004.
Sakowicz A., *Prawnokarne gwarancje prywatności*, Warszawa 2006.
Sarnecki P., *Komentarz do art. 51 Konstytucji RP*, [w:]*Konstytucja Rzeczypospolitej Polskiej. Komentarz*, pod red. L. Garlickiego, Warszawa 2003.
Sibiga G., *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003.
Siwicki M., *Cyberprzestępczość*, Warszawa 2013.
Sobczak J., *Dziennikarz – sprawozdawca sądowy. Prawa i obowiązki*, Warszawa 2000.
Sobczak J., *Prawo prasowe. Komentarz*, Warszawa 2008.
Szczerba A., *Europejski Inspektor Ochrony Danych – niezależny organ nadzoru*, [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów,* pod red. G. Goździewicza, M. Szabłowskiej, Toruń 2008.
Tinnefeld M-T., *Ochrona danych – kamień węgielny budowy Europy*, [w:] *Ochrona danych osobowych*, pod red. M. Wyrzykowskiego, Warszawa 1999.
Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz, pod red. J. Szwaji, Warszawa 2013.
Winczorek P., *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997*, Warszawa 2000.
Wiśniewski L., *Karta Praw Podstawowych Unii Europejskiej a konstytucyjny katalog praw człowieka*, [w:] *Sześć lat Konstytucji Rzeczypospolitej Polskiej. Doświadczenia i inspiracje*, Warszawa 2003.
Wiśniewski L., *Zakres ochrony prawnej wolności człowieka i warunki jej dopuszczalnych ograniczeń w praktyce*, [w:] *Wolności i prawa jednostki oraz ich gwarancje w praktyce*, pod red. L. Wiśniewskiego, Warszawa 2006.

Wójtowicz K., *Ochrona prawa człowieka w Unii Europejskiej*, [w:] *System ochrony praw człowieka*, B. Banaszak, A. Bisztyga, K. Complak, M. Jabłoński, R. Wieruszewski, K. Wójtowicz, Kraków 2005.
Wyrzykowski M., *Pojęcie interesu społecznego w prawie administracyjnym*, Warszawa 1986.
Zawadzka Z., *Wolność prasy a ochrona prywatności osób wykonujących działalność publiczną*, Warszawa 2013.

Czasopisma:

Banaszak B., *Prawa człowieka i obywatela w nowej Konstytucji Rzeczypospolitej Polskiej*, „Przegląd Sejmowy" 1997, nr 5.
Brzozowska M., *Kradzież danych osobowych*, „Marketing w praktyce" 2012, nr 10.
Bundy M., *Oj dana, dana*, „Polityka" 2004, nr 43.
Canadian protection of personal data found compliant with exacting EU standars, International Law Update Vol. 8, January 2002, p.15.
Dwulat H., *Odpowiedzialność karna administratora danych z art. 51 ustawy o ochronie danych osobowych*, „Radca Prawny" 2003, nr 5.
Glendon M. A., *Knowing the Universal Declaration of Human Rights*, 73 Notre Dame Law Review 1153 (1998).
Golonka A., *Czyny zabronione a czyny nieuczciwej konkurencji*, „Prokuratura i Prawo" 2013, nr 1.
Gontarski W., *Czy godzi się naruszać prawo do godnego życia*, „Rzeczpospolita" 2006, nr 160.
Górowski W., *Glosa do postanowienia SN z dnia 26 lipca 2007r., IV KK 174/07*, „Państwo i Prawo" 2008, nr 6.
Herzog A., *Glosa do orzeczenia Sądu Najwyższego z dnia 21 listopada 2007 r., sygn. IV KK 376/07*, „Prokuratura i Prawo" 2008, nr 11.
Hoc S., *Glosa do uchwały SN z dnia 22 stycznia 2003, I KZP 45/02*, „Przegląd Sądowy" 2003, nr 11–12.
Jackiewicz A., Karta *Praw Podstawowych Unii Europejskiej (uwagi konstytucyjnoprawne)*, „Państwo i Prawo" 2002, nr 1.
K J.., *Radcę może przesłuchać*, „Rzeczpospolita" 2004, nr 274.
Klosek J., *European Court establishes broad interpretation of data privacy law*, The Metropolitan Corporate Councel, 2004/03. http://www.goodwinprocter.com/getfile.aspx?filepath=/Files/publications/klosek_j_03_04.pdf
Kroner J., *Funkcjonariuszom wolno zbyt wiele*, „Rzeczpospolita" 2005, nr 290.
Kroner J., *Ojciec może uznać zmarłe dziecko*, „Rzeczpospolita" 2007, nr 165.
Kroner J., *Teczki nie będą pułapką na kłamców*, „Rzeczpospolita" 2005, nr 284.
Kuczyński T., *Ochrona danych osobowych w stosunkach zatrudnienia*, „Przegląd Sądowy" 1998, nr 11–12.
Marczuk M., *Trudne rozstanie z niekonstytucyjnym podsłuchem*, „Gazeta Prawna" 2006, nr 16.
Mednis A., *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej*, „Państwo i Prawo" 1997, nr 6.
Młynarska-Sobaczewska A., Sakowska-Baryła M., *Glosa do wyroku Sądu Najwyższego z dnia 2 X 2006*, V KK 243/06, „Państwo i Prawo" 2007, nr 6.
Mościcka A., *Dostęp tylko dla wybranych*, „Gazeta Prawna" 2005, nr 210.
Mościcka. A., *Czy trzeba zmienić ustawę o IPN*, „Gazeta Prawna" 2005, nr 212.
Mozgawa M., *Glosa do wyroku SN z dnia 3 kwietnia 2002r., VKKN 223/2000*, „Prokuratura i Prawo" 2003, nr 11.

Mozgawa M., *Prawnokarne aspekty zwalczania nieuczciwej konkurencji*, „Prokuratura i Prawo" 1996, nr 4.
Nowicki M.A., *Interes pacjenta kontra interes śledztwa*, „Prawo i Życie" 2000, nr 6.
Organiściak M., Zakrzewski R., *Ochrona danych osobowych - przepisy karne*, „Przegląd Ustawodawstwa Gospodarczego" 2002, nr 8.
Pacek G.J., *Możliwość odmowy publikowania płatnych ogłoszeń i reklam przez wydawcę*, „Glosa" 2007, nr 4.
Pilc B., *Rola administratora bezpieczeństwa informacji podczas inspekcji prowadzonej przez Generalnego Inspektora Ochrona Danych Osobowych*, dodatek „Monitora Prawniczego" 2012, nr 7.
Przegląd orzecznictwa Europejskiego Trybunału Sprawiedliwości i Sądu Pierwszej Instancji, nr 2 cz. I, 15 września–15 listopada 2003. http:/www2.ukie.gov.pl/HLP/files.nsf/a50f2d318bc65d9dc1256e7a003922ed/ffc5fb6686dc923dc1256e7b0045fc69?OpenDocument
Rychter K., *Nie zrównano agentów z pokrzywdzonymi*, „Gazeta Prawna" 2005, nr 232.
Sadowski B., *Odpowiedzialność za przetwarzanie danych osobowych niezgodnie z prawem*, „Służba Pracownicza" 2004, nr 10.
Safjan M., *Prawo do ochrony życia prywatnego*, „Szkoła Praw Człowieka" Zeszyt 4 (1998), s. 71–89.
Sakowicz A., *Ingerencja w prywatność musi być usprawiedliwiona*, „Rzeczpospolita" 2006, nr 201.
Siedlecka E., *Trybunał kończy podsłuchowisko*, „Rzeczpospolita" z dnia 24 czerwca 2009, http://wyborcza.pl/1,76842,6750534,Trybunal_konczy_podsluchowisko.html
Stankiewicz A., Kroner J., *Agenci zajrzą do teczek*, „Rzeczpospolita" 2005, nr 252.
Swora M., *Glosa do wyroku NSA z dnia 4 kwietnia 2003 r., II SA 2935/02*, „Państwo i Prawo" 2004, nr 1.
Szustakiewicz P., *Kontrole Generalnego Inspektora Ochrony Danych Osobowych*, „Kontrola Państwowa" 2007, nr 6.
WIK, *Zaostrzenie zasad kontroli operacyjnej*, „Rzeczpospolita" 2006, nr 170.
Wyszomirska A., *Gwarancje poufności dla klienta, a nie dla radcy*, „Gazeta Prawna" 2004, nr 228.
Wyszomirska A., *Informacje muszą być niszczone*, „Gazeta Prawna" 2005, nr 241.
Zimny W. , *Legalność ustanowienia, relacja do administratora danych, odpowiedzialność i rola administratora bezpieczeństwa informacji*, „Ochrona danych osobowych. Biuletyn Administratorów Bezpieczeństwa Informacji" 2000, nr 1.

Akty prawne:

Krajowe przepisy prawa:

Konstytucja RP z dnia 2 kwietnia 1997, Dz. U. nr 78, poz. 483
Kodeks karny – ustawa z dnia 6 czerwca 1997, Dz. U. nr 88, poz. 553 z późn. zm.
Prawo prasowe – ustawa z dnia 26 stycznia 1984, Dz. U. nr 5, poz. 24 z późn. zm.
Ustawa o Centralnym Biurze Antykorupcyjnym z dnia 9 czerwca 2006, Dz. U. 2014, poz. 1411 z późn. zm.
Ustawa o finansach publicznych z dnia 27 sierpnia 2009, Dz. U. 2013, poz. 885 z późn. zm.
Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997, Dz.U 2014, poz. 1182 z późn. zm.
Ustawa o dostępie do informacji publicznej z dnia 6 września 2001, Dz. U. 2014, poz. 782 z późn. zm.

Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002, Dz. U. 2013, poz. 1422.
Ustawa o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993, Dz. U. 2003, nr 153, poz. 1503 z późn. zm.
Rozporządzenie Rady Ministrów w sprawie udostępniania prasie informacji oraz organizacji i zadań rzeczników prasowych w urzędach organów administracji rządowej z dnia 7 listopada 1995, Dz. U. Nr 132, poz. 642 uchylone 1 stycznia 2002 na mocy art. 24 ust. 3 ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r., Dz. U. Nr 112, poz. 1198
Rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 17 maja 1996 w sprawie orzekania o czasowej niezdolności do pracy, Dz. U. Nr 63, poz. 302.
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych, Dz. U. Nr 94, poz. 923 z późn. zm.

Międzynarodowe przepisy prawa:

ONZ:

Guidelines for the Regulation of Computerized Personal Data Files adopted by General Assembly resolution 45/95 of 14 December 1990, http://www.un.org/documents/ga/res/45/a45r095.htm
Karta Narodów Zjednoczonych z dnia 26 czerwca 1945, Dz. U. 1947, nr 23, poz. 90.
Międzynarodowy Pakt Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966, Dz. U. 1977, nr 38, poz. 167.
Protokół Fakultatywny do Międzynarodowego Paktu Praw Obywatelskich i Politycznych z dnia 16 grudnia 1966, Dz. U. 1994, nr 23, poz. 80.
Powszechna Deklaracja Praw Człowieka z dnia 10 grudnia 1948 roku http://www.unic.un.org.pl/prawa_czlowieka/dok_powszechna_deklaracja.php
Powszechna Deklaracja o Genomie Ludzkim i Prawach Człowieka z dnia 11 listopada 1997, http://libr.sejm.gov.pl/tek01/txt/inne/1997.html.
Rezolucja Zgromadzenia Ogólnego ONZ z dnia 17 grudnia 1979 http://www.un.org/documents/ga/res/34/a34res169.pdf

OECD:

OECD Guidelineo of the Protection of Privacy and Transforder Flows of Persnol Data (23 September 1980) <www.oecd.org/sti/ieconomy/15590241.pdf>

Europejskie przepisy prawa:

Rada Europy:

Statut Rady Europy z dnia 5 maja 1949, Dz. U. 1994, nr 118, poz. 565.
Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950, Dz. U. 1993, nr 61, poz. 284.
Europejska Konwencja o Prawach Człowieka i Biomedycynie z dnia 4 kwietnia 1997 http://libr.sejm.gov.pl/tek01/txt/re/1997.html

Konwencja Rady Europy nr 108 z dnia 28 stycznia 1981 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, Dz. U. 2003, nr 2, poz. 25. Protokół Dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych z dnia 8 listopada 2001, Dz. U. 2001, nr 3, poz. 15.
Rezolucja Komitetu Ministrów RE 29 (78) dotyczącą pobierania i przeszczepiania ludzkich tkanek i organów
Rezolucja Komitetu Ministrów RE 3 (95) dotycząca karty oceny zawodowej osób niepełnosprawnych
Rekomendacja R (97) 3, z dnia 3 grudnia 1997, przyjęta przez Grupę Roboczą ds. Ochrony Danych „Anonimowość w Internecie"
Rekomendacja R (87) 23 w sprawie systemów informatycznych w szpitalach
Rekomendacja R (89) 14 w sprawie etycznych problemów zakażenia wirusem HIV w zakładach służby zdrowia i placówkach społecznych
Rekomendacja R (89) 4 w sprawie zbierania danych epidemiologicznych w podstawowej opiece medycznej
Rekomendacja R (90) 13 w sprawie prenatalnych genetycznych badań przesiewowych, prenatalnej diagnostyki genetycznej oraz związanego z tym poradnictwa
Rekomendacja R (90) 3 w sprawie badań medycznych na istotach ludzkich
Rekomendacja R (90) 8 w sprawie napływu nowych technologii do służby zdrowia
Rekomendacja R (91) 15 w sprawie współpracy europejskiej w ramach badań epidemiologicznych w dziedzinie zdrowia psychicznego
Rekomendacja R (92) 1 w sprawie wykorzystania kwasu dezoksyrybonukleinowego (DNA) w postępowaniu karnym
Rekomendacja R (92) 3 w sprawie genetycznych badań diagnostycznych i przesiewowych wykorzystywanych dla celów opieki zdrowotnej.

Unia Europejska:

Karta Praw Podstawowych Dz. Urz. UE C 2010/83, s. 19.
Rozporządzenie Parlamentu Europejskiego i Rady 2001/45/WE z dnia 18 grudnia 2000, Dz. U. WE L 8 z dnia 12 stycznia 2001, s. 1.
Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady WE z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych Dz. Urz. WE 1995 L 281/31, s. 365.
Dyrektywa 99/5/WE Parlamentu Europejskiego i Rady z dnia 9 marca 1999 w sprawie urządzeń radiowych i urządzeń końcowych łączności elektronicznej oraz wzajemnego rozpoznawania ich zgodności. Dz. Urz. WE L 1999/91, s. 10.
Dyrektywa 2002/58/WE z dnia 12 lipca 2002 w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej. Dz. Urz. WE L 2002/201, s. 37.
Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz. Urz. WE L 2006/105 s. 54.
Układ z Schengen z dnia 14 czerwca 1985, Dz. Urz. WE L 2000/239, s. 13.
Konwencja Wykonawcza do Układu z Schengen Dz. Urz. WE L 2000/239, s. 19.
Protokół między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia

Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, Dz. Urz. UE L 2011/ 160, s. 21.
Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji Rady w sprawie utworzenia, działania i wykorzystania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (COM(2005)230 wersja ostateczna); wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie utworzenia, eksploatacji i wykorzystania Systemu Informacyjnego Schengen (SIS II) drugiej generacji (COM(2005)236 wersja ostateczna), oraz wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie dostępu służb odpowiedzialnych w Państwach Członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II) (COM(2005)237 wersja ostateczna), Dz. Urz. WE C 2006/91, s. 38.

Inne:

Decyzja 2006/253/WE Komisji z dnia 6 września 2005 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Imiennym Rejestrze Pasażerów linii lotniczych, przekazanym do Agencji Służb Granicznych Kanady (notyfikowana jako dokument nr C(2005) 3248), Dz WE L 2006/91, s. 49.
Opinia Grupy roboczej ds. Ochrony Danych ustanowionej na mocy art. 29 nr 6/2005, przyjęta dnia 25 listopada 2005, 2067/05/PL.

Orzecznictwo:

Europejski Trybunał Sprawiedliwości:

Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 6 listopada 2003, C-101/01, http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=154144
Wyrok Europejskiego Trybunału sprawiedliwości z dnia 24 czerwca 2004, C-350/02, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-350/02
Wyrok Sądu Pierwszej Instancji z dnia 8 listopada 2007, T-194/04, http://curia.europa.eu/juris/liste.jsf?pro=&lgrec=en&nat=or&oqp=&dates=&lg=&language=pl&jur=C%2CT%2CF&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&num=T-194%252F04&td=%3BALL&pcs=Oor&avg=&page=1&mat=or&jge=&for=&cid=174889
Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 9 listopada 2010r., C-92/09 i C-93/09 http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=PL&mode=doc&dir=&occ=first&part=1&cid=745649
Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 24 listopada 2011, C-70/10, http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=PL&mode=doc&dir=&occ=first&part=1&cid=745691
Wyrok Europejskiego Trybunału Sprawiedliwości z dnia 8 kwietnia 2014, C-293/12 i C-594/12, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=PL

Trybunał Konstytucyjny:

Orzeczenie TK z dnia 28 maja 1986, U 1/86, OTK 1986 nr 1, poz. 2.
Orzeczenia TK z dnia 26 kwietnia 1995, sygn. K. 11/94, OTK w 1995, cz. I.
Orzeczenie TK z dnia 26 września 1995, U 4/95, OTK 1995 nr 1.
Orzeczenie TK z dnia 23 kwietnia 1996, sygn. K. 29/95, OTK ZU 1996 nr 2.
Orzeczenie TK z dnia 24 czerwca 1997, K 21/96, OTK 1997 nr 2.
Orzeczenie TK z dnia 22 września 1997, K 25/97, OTK 1997 nr 3-4.
Wyrok TK z dnia 19 maja 1998, U 5/97, OTK 1998 nr 4.
Wyrok TK z dnia 12 stycznia 1999, P 2/98, OTK 1999 nr 1.
Wyrok TK z dnia 25 maja 1999, SK 9/98, OTK 1999 nr 4, poz. 78.
Wyrok TK z dnia 12 stycznia 2000, P 11/98, OTK 2000 nr 1, poz. 3.
Wyrok TK z dnia 11 kwietnia 2000, K 15/98, OTK 2000 nr 3.
Wyrok TK z dnia 8 października 2001, K 11/01, OTK 2001 nr 7.
Wyrok TK z dnia 19 lutego 2002, U 3/01, OTK-A 2002 nr 1.
Wyrok TK z dnia 12 listopada 2002, SK 40/01, OTK-A 2002 nr 6.
Wyrok TK z dnia 20 listopada 2002, K 41/02, OTK-A 2002 nr 6.
Wyrok TK z dnia 5 marca 2003, K 7/01, OTK-A 2003 nr 3.
Wyrok TK z dnia 29 kwietnia 2003, SK 24/02, OTK-A 2003 nr 4.
Wyrok TK z dnia 18 lutego 2004, P 21/02, OTK-A 2004 nr 2.
Wyrok TK z dnia 22 listopada 2004, SK 64/03, OTK-A 2004 nr 10.
Wyrok TK z dnia 20 czerwca 2005, K 4/04, OTK-A 2005 nr 6.
Wyrok TK z dnia 26 października 2005, K 31/04, OTK-A 2005 nr 9.
Postanowienie TK z dnia 23 listopada 2005, K 32/04, OTK-A 2005 nr 10.
Wyrok TK z dnia 6 grudnia 2005, SK 7/05, OTK-A 2005 nr 11.
Wyrok TK z dnia 12 grudnia 2005, K 32/04, OTK-A 2005 nr 11.
Wyrok TK z dnia 20 marca 2006, K 17/05, OTK-A 2006 nr 3.
Wyrok TK z dnia 11 maja 2007, K 2/07, OTK-A 2007 nr 5.
Wyrok TK z dnia 16 lipca 2007, SK 61/06, OTK-A 2007 nr 7.
Postanowienie TK z dnia 21 listopada 2007, K 23/06, OTK-A 2007 nr 10, poz. 141.
Wyrok TK z dnia 17 czerwca 2008, K 8/04, OTK-A 2008 nr 5.
Wyrok TK z dnia 27 czerwca 2008, K 51/07, OTK-A 2008 nr 5.
Wyrok TK z dnia 23 czerwca 2009, K 54/07, OTK-A 2009 nr 8.
Wyrok TK z dnia 23 lutego 2010, K 1/08, OTK-A 2010 nr 2.
Wyrok TK z dnia 13 grudnia 2011, K 33/08, OTK-A 2011 nr 10.

Samorządowe Kolegium Odwoławcze:

Postanowienia SKO w Olsztynie z dnia 24 czerwca 1999, SKO 511/27/99, „OSS" 2000 nr 3.

Sądy Apelacyjne:

Wyrok SA w Krakowie z dnia 11 kwietnia 2001, I ACa 244/01, LEX nr 82416.
Wyrok SA w Poznaniu z dnia 15 czerwca 2011, I ACa 477/11, LEX nr 898647.
Wyrok SA w Poznaniu z dnia 27 września 2005, I ACa 1443/03, LEX nr 177088.
Wyrok SA w Warszawie z dnia 10 czerwca 2008, VI ACa 1648/07, LEX nr 486304;
Wyrok SA w Warszawie z dnia 8 lipca 2009, I ACa 316/09, LEX nr 1120112;
Wyrok SA w Poznaniu z dnia 15 czerwca 2011, I ACa 477/11, LEX nr 898647.

Postanowienie SA w Łodzi z dnia 18 stycznia 2013, I ACa 1031/12, LEX nr 1280424.
Postanowienie SA w Łodzi z dnia 18 stycznia 2013, I ACa 1032/12, LEX nr 1280426.
Wyrok SA w Warszawie z dnia 10 kwietnia 2013, VI ACa 1347/12, Legalis nr 722850.
Wyrok SA w Gdańsku z dnia 24 czerwca 2014, I ACa 206/14, LEX nr 1504361.

Sądy Administracyjne:

Wyrok WSA w Warszawie z dnia 6 września 2005, II SA/Wa 825/05, LEX nr 192892.
Wyrok WSA w Warszawie z dnia 21 września 2005, II SA/Wa 1443/05, LEX nr 204649.
Wyrok WSA w Warszawie z dnia 30 maja 2006, II SA/Wa 1894/05, LEX nr 232206.
Wyrok WSA w Warszawie z dnia 13 czerwca 2006, II SA/Wa 2016/05, LEX nr 219349.
Wyrok WSA w Warszawie z dnia 7 marca 2007, II SA/Wa 2260/06, LEX nr 322805.
Wyrok WSA w Warszawie z dnia 22 marca 2007, II SA/Wa 1933/06, Legalis nr 165044.Wyrok WSA w Warszawie z dnia 13 lutego 2009, II SA/Wa 1570/08, LEX nr 519829.
Wyrok WSA w Warszawie z dnia 24 listopada 2009, II SA/Wa 1584/09, LEX nr 589249.
Wyrok WSA w Warszawie z dnia 8 kwietnia 2010, II SA/Wa 1488/09, Legalis nr 235004.
Postanowienie WSA w Warszawie z dnia 30 października 2010, II SA/Wa 1885/07, LEX nr 521930.
Wyrok WSA w Poznaniu z dnia 23 lutego 2011, II SA/Po 804/10, LEX nr 1086575.
Wyrok WSA w Warszawie z dnia 24 listopada 2011, II SA/Wa 1828/11, LEX nr 1153548.
Wyrok WSA w Olsztynie z dnia 30 kwietnia 2012, II SA/Ol 194/12, LEX nr 1287138.
Wyrok WSA w Gdańsku z dnia 5 grudnia 2012, II SAB/Gd 79/12, LEX nr 1234516.
Wyrok WSA w Białymstoku z dnia 14 lutego 2013, II SA/Bk 967/12, LEX nr 1334226.
Wyrok WSA w Poznaniu z dnia 7 marca 2013, II SA/Po 37/13, LEX nr 1293515.
Wyrok WSA w Łodzi z dnia 15 marca 2013, II SA/Łd 1193/12, LEX nr 1303070.
Wyrok WSA w Gdańsku z dnia 22 maja 2013, II SA/Gd 190/13 LEX nr 1368693.
Wyrok WSA w Krakowie z dnia 30 lipca 2013, II SA/Kr 395/13, LEX nr 1447479.
Wyrok NSA z dnia 4 czerwca 1982, I SA 258/82, LEX nr 9685.
Wyrok NSA z dnia 19 listopada 2001, II SA 2707/00, I. Kamińska, *Ochrona danych osobowych*, Warszawa 2007.
Wyrok NSA z dnia 30 stycznia 2002, II SA 1098/01, Legalis nr 54272.
Wyrok NSA z dnia 29 stycznia 2003, II SA 3085/01, LEX nr 156396.
Wyrok NSA z dnia 13 lutego 2003, II SA 1620/01, „Palestra" 2004 nr 1.
Wyrok NSA z dnia 7 marca 2003, II SA 3572/02, LEX nr 144641
Wyrok NSA z dnia 11 kwietnia 2003, II SA 1449/02, LEX nr 148969.
Wyrok NSA z dnia 29 lipca 2004, OSK 693/04, LEX nr 164847.
Wyrok NSA z dnia 12 lipca 2005, OSK 1365/04. LEX nr 190725.
Wyrok NSA z dnia 7 maja 2008, I OSK 983/07, Legalis nr 139618.
Wyrok NSA z dnia 18 listopada 2009, I OSK 667/09, Legalis nr 240487.
Wyrok NSA z dnia 13 stycznia 2011, I OSK 440/10, LEX nr 952041.
Wyrok NSA z dnia 28 czerwca 2011, I OSK 1217/10, Legalis nr 368982.
Wyrok NSA z dnia 5 marca 2013, I OSK 2872/12, Legalis nr 661544.
Wyrok NSA z dnia 25 kwietnia 2014, I OSK 2499/13, LEX nr 1463584.

Sąd Najwyższy:

Wyrok SN z dnia 18 stycznia 1984, I CR 400/83, LEX nr 2997.
Wyrok SN z dnia 8 kwietnia 1994, III ARN 18/94, OSNP 1994 nr 4.
Wyrok SN z dnia 21 października 1999, I PKN 308/99, LEX nr 45507.

Postanowienie SN z dnia 14 czerwca 2000, V CKN 1119/00, „OSNC" 2002 nr 4, poz. 49.
Postanowienie SN z dnia 11 grudnia 2000r., II KKN 438/00, LEX nr 45466.
Uchwała SN z dnia 21 listopada 2001, I KZP 26/01, OSNKW 2002 nr 1-2, poz. 4.
Wyrok SN z dnia 8 maja 2002, I PKN 267/01, OSNP 2004 nr 6.
Wyrok SN- Izby Cywilnej z dnia 19 lipca 2006, I CSK 147/06, Legalis nr 304551.
Wyrok SN z dnia 2 października 2006, V KK 243/06, Legalis nr 79183.
Wyrok SN-Izby Pracy z dnia 24 października 2006, I PK 80/06, Legalis nr 77013.
Wyrok SN (Izby Pracy) z dnia 17 kwietnia 2007, I UK 324/06, Legalis nr 89217.
Wyrok SN z dnia 29 maja 2008, II KK 12/08, LEX nr 448953.
Postanowienie SN z dnia 15 grudnia 2010, III KK 250/10, LEX nr 784329.
Wyrok SN z dnia 8 listopada 2012, I CSK 190/12, LEX nr 1286307.
Wyrok SN z dnia 28 listopada 2013, IV CSK 155/13, LEX nr 1415128.

Strony internetowe:

http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta77/erec818.htm
http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta82/erec934.htm
http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?FileID=15215&lang=EN https://secure.edps.europa.eu/EDPSWEB/edps/lang/pl/EDPS
http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=pl&newform=newform&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurtfp=jurtfp&alldocrec=alldocrec&docj=docj&docor=docor&docop=docop&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoj=docnoj&docnoor=docnoor&typeord=ALL&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&numaff=T-194%2F04&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=&domaine=&mots=&resmax=100&Submit=Szukaj
http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm
http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61853
http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89823
http://naszeblogi.pl/14280-kittel-i-marszalek-bez-prawa-do-zawodu http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-122365
http://orka.sejm.gov.pl/Biuletyn.nsf/0/BC0551F090B08A04C1256B73003D21D8?OpenDocument http://orka.sejm.gov.pl/Biuletyn.nsf/0/E115DE844AAB0BAAC1256B73003DCF28?OpenDocument
http://orka.sejm.gov.pl/Biuletyn.nsf/0/E115DE844AAB0BAAC1256B73003DCF28?OpenDocument
http://orka.sejm.gov.pl/Druki4ka.nsf/($vAllByUnid)/2B081C58BD0702DFC1256DC8003EE5AA/$file/2120.pdf
http://orka.sejm.gov.pl/Druki6ka.nsf/0/1C375B9EBAEAA9EAC12574420044A07F/$file/488.pdf
http://orka.sejm.gov.pl/Rejestrd.nsf?OpenDatabase
http://orka2.sejm.gov.pl/Debata2.nsf
http://orka2.sejm.gov.pl/Debata3.nsf/9a905bcb5531f478c125745f0037938e/08d7ebab5f438704c125749d00354499?OpenDocument
http://orka2.sejm.gov.pl/Debata3.nsf/main/21D32B95
http://www.aip-bg.org/pdf/rec1037.pdf
http://www.coe.int./t/dg3/healthbioethic/texts_and_documents/ETS164Polish.pdf
http://www.europarl.europa.eu/meetdocs/2004_2009/documents/am/595/595119/595119pl.pdf
http://www.giodo.gov.pl/138/id_art/2685/j/pl/

http://www.giodo.gov.pl/138/id_art/2685/j/pl/
http://www.giodo.gov.pl/138/id_art/2685/j/pl/
http://www.giodo.gov.pl/230/id_art/640/j/pl/
http://www.giodo.gov.pl/230/od/0/j/pl
http://www.giodo.gov.pl/230j/od/12/j//
http://www.giodo.gov.pl/plik/id_p/1011/t/pdf/j/pl/
http://www.giodo.gov.pl/plik/id_p/1012/t/pdf/j/pl/
http://www.giodo.gov.pl/plik/id_p/347/t/pdf/j/pl/
http://www.giodo.gov.pl/plik/id_p/349/t/pdf/j/pl/
http://www.giodo.gov.pl/plik/id_p/351/t/pdf/j/pl/
http://www.giodo.gov.pl/plik/id_p/476/t/pdf/j/pl/
http://www.memex.pl/doc/rekomendacja_85_20.doc
http://www.memex.pl/doc/rekomendacja_banki_medyczne.doc
http://www.uke.gov.pl/uke/index.jsp?place=Lead01&news_cat_id=168&news_id=4850&layout=3&page=text
https://sip.legalis.pl/document-view.seam?documentId=mjxw62zog4ydanbugi4tmltqmfyc4mrygezdsnjtgi
https://sip.legalis.pl/document-view.seam?documentId=mjxw62zoge3tambvgu3tgnjoobqxalrsha3tmmztha3q
https://sip.legalis.pl/document-view.seam?documentId=mjxw62zoge3tambvgu3tgnjoobqxalrsha3tmmztha4a
https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogeztkmbvgeytenroobqxalrrgy2donjrg44a
https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf