Ochrona prywatności w cyberprzestrzeni w prawie polskim i międzynarodowym z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji

Rozprawa doktorska
napisana pod kierunkiem
dr. hab. Cezarego Banasińskiego

Warszawa 2018
„Starożytność była cywilizacją spektaklu:
Udostępniać wielkiej masie ludzi oglądanie niewielkiej liczby przedmiotów
– to zadanie rozwiązywała architektura świątyń, teatrów i cyrków. W widowisku
kulminowała życie publiczne, intensywność świąt, zmysłowa bliskość.
Epoka nowoczesna odwraca problem:
Dostarczyć niewielu osobom, a nawet jednemu człowiekowi, natychmiastowy wgląd w
wielką masę ludzi.
W społeczeństwie, którego konstytutywych elementów nie stanowi już wspólnota ani życie
na forum, ale prywatne jednostki z jednej, a państwo z drugiej strony, relacje może
regulować jedynie forma będąca dokładną odwrotnością widowiska:
Przeto współczesności, stałe rosnącemu wpływowi państwa, jego z każdym dniem
pogłębiającej się ingerencji we wszystkie szczegóły i wszystkie relacje życia społecznego,
przypadło w udziale, aby poszerzać i ulepszać jej oddziaływanie, a to przez
wykorzystywanie i wdrażanie do tego wielkiego celu budowy i dystrybucji gmachów
służących równoczesnemu nadzorowaniu wielkiej masy ludzi”.

Michel Foucault
Przedmowa


Zaprezentowane w niniejszej pracy poglądy są wyrazem moich przemysleń i opinii, a także głębokiego przekonania, że każda forma zinstytucjonalizowanego nadzoru i kontroli wypacza ideały, które stanowią podstawę naszego społeczeństwa. Nic w tym zakresie nie straciły na aktualności poglądy J. Milla, który wskazywał na wolność myśli jako jedną z fundamentalnych swobód człowieka: „żadne społeczeństwo, w którym swobody te nie są, na ogół biorąc, szanowane, nie jest wolne, bez względu na formę jego rządu; i żadne społeczeństwo nie jest całkowicie wolne, jeżeli nie są one w nim uznawane bez żadnych absolutnie zastrzeżeń”.

---

Spis treści

Przedmowa ........................................................................................................... 3
Spis treści ............................................................................................................. 5
Wykaz najważniejszych skrótów .......................................................................... 8
Wprowadzenie .................................................................................................... 9

CZĘŚĆ 1. OCHRONA PRYWATNOŚCI: HISTORIA, TERAŻNIEJSZOST I PRZYSZŁOŚĆ 18

Rozdział 1. Prywatność i cyberprzestrzeń – zagadnienia podstawowe ................. 18
1.1. Psychologiczne i socjologiczne rozumienie prywatności ............................ 18
1.2. Geneza prawnej ochrony prywatności ....................................................... 23
1.3. Prywatność a ochrona danych osobowych – związek pojęciowy ................. 28
1.4. Cyberprzestrzeń jako nowa płaszczyzna budowania relacji społecznych ......... 32
1.5. Prawne problemy regulacji cyberprzestrzeni ............................................. 40
1.6. Zagrożenia dla prywatności w cyberprzestrzeni ........................................ 48

Rozdział 2. Prawnomiedzynarodowe i konstytucyjne źródła norm w obszarze ochrony prywatności .......................................................... 51
2.1. Wprowadzenie .............................................................................................. 51
2.2. Dorobek prawny Organizacji Narodów Zjednoczonych ......................... 53
2.2.1. Powszechna Deklaracja Praw Człowieka ............................................ 54
2.2.2. Międzynarodowy Pakt Praw Obywatelskich i Politycznych .................. 55
2.2.3. Pozycja MPPOP w krajowym systemie prawnym .................................. 59
2.3. Europejska Konwencja Praw Człowieka .................................................. 62
2.3.1. Geneza traktatu i zakres ochrony prywatności ..................................... 62
2.3.2. Ewolucja i dorobek orzecznictwy ETPC .............................................. 63
2.3.3. Pozycja EKPC w krajowym systemie prawnym ..................................... 68
2.4. Karta Praw Podstawowych Unii Europejskiej ............................................. 70
2.4.1. Ewolucja ochrony praw podstawowych w prawie WE/UE .................... 70
2.4.2. Charakter prawny oraz zakres przedmiotowy i podmiotowy ................... 72
2.4.3. Dorobek orzecznictwy TSUE na tle KPP ............................................ 77
2.4.4. Relacja pomiędzy KPP a EKPC .......................................................... 80
2.4.5. Zakres stosowania KPP w prawie krajowym ....................................... 85
2.5. Przepisy konstytucyjne ............................................................................. 88
2.5.1. Ochrona prywatności w polskim porządku prawnym przed rokiem 1997 88
2.5.2. Konstytucja RP z 1997 roku ................................................................. 90
2.5.3. Limitacja i derogacja ............................................................................ 93
2.6. Podsumowanie ............................................................................................ 96

Rozdział 3. Ewolucja zasad ochrony danych osobowych .................................. 101
3.1. Wprowadzenie .......................................................................................... 101
3.2. Wczesne rozwiązania prawne .................................................................. 101
3.3. Wytyczne OECD ...................................................................................... 104
3.4. Konwencja nr 108 Rady Europy ................................................................ 107
3.5. Wytyczne ONZ .......................................................................................... 117
3.6. Międzynarodowe Standardy Ochrony Prywatności .................................. 118
3.7. Podsumowanie .......................................................................................... 122

Rozdział 4. Prawo UE jako narzędzie podnoszenia standardów w obszarze prywatności w cyberprzestrzeni .................................................. 128
4.1. Wprowadzenie i uwagi ogólne ................................................................. 128
4.2. Geneza i ewolucja przepisów wspólnotowych .......................................... 129
4.3. Terminologia ............................................................................................. 136
4.4. Zakres regulacji ......................................................................................... 138
4.4.1. Dyrektywa 95/46 .................................................................................. 138
4.4.2. Dyrektywa 2002/58 .............................................................................. 143
4.4.3. Rozporządzenie 2016/679 .................................................................. 144
4.5. Obszary regulacji ....................................................................................... 147
3. Charakterystyka zjawiska ................................................................. 255
   3.1. Definicja usług przetwarzania w chmurze ..................................... 255
   3.2. Podział ze względu na zasady współdziałaania (model implementacyjne) .................................................... 256
   3.3. Podział ze względu na udostępnione zasoby (model usługowe) .......... 258
   3.4. Odniesienie do modelu klient-serwer ........................................ 260
   3.5. Wirtualizacja .............................................................................. 261
4. Analiza prawna ................................................................................. 262
   4.1. Najważniejsze ryzyka związane z przetwarzaniem w chmurze obliczeniowej ................................................ 262
   4.2. Charakter prawny i definicja umowy przetwarzania w chmurze ............ 263
   4.3. Prawo właściwe i jurysdykcja dla umów przetwarzania w chmurze .... 266
   4.4. Chmura obliczeniowa z perspektywy przepisów europejskich ................ 278
   4.5. Chmura obliczeniowa z perspektywy prawa USA ................................ 284
5. Podsumowanie i wnioski ..................................................................... 291
6. Analizy dużych zbiorów danych (Big Data) ........................................ 294
7. Wprowadzenie .................................................................................. 294
7. Hipotezy badawcze ........................................................................... 298
8. Charakterystyka zjawiska ................................................................. 299
   8.1. Najważniejsze cechy Big Data ....................................................... 299
   8.2. Podstawowe źródła danych ............................................................ 303
   8.3. Ponowna identyfikacja podmiotów danych ...................................... 309
   8.4. Aspekty etyczne Big Data ............................................................... 311
9. Analiza prawna .................................................................................. 312
   9.1. Najważniejsze ryzyka związane z Big Data ....................................... 312
   9.2. Dane ujawniające Big Data ............................................................. 313
   9.3. Praktyczność zasady minimalizacji danych ...................................... 316
   9.4. Anonimizacja w regulacjach prawnych ............................................ 318
   9.5. Kontrola przetwarzania i prawa podmiotów danych ......................... 320
7.5. Podsumowanie i wnioski ................................................................. 322
Rozdział 8. Prywatność a bezpieczeństwo publiczne – podstawy prawne prowadzenia
programów masowej inwigilacji obywateli ........................................... 324
8.1. Wprowadzenie ........................................................................... 324
8.2. Hipotezy badawcze ................................................................. 327
8.3. Opis problemu ........................................................................ 328
  8.3.1. Kluczowe pojęcia ................................................................. 328
  8.3.2. Główne programy inwigilacyjne i związane z nimi możliwości techniczne .... 331
  8.3.3. Środki technicznej ochrony prywatności i anonimowości w Internecie ........ 336
8.4. Analiza prawna ......................................................................... 339
  8.4.1. Masowa inwigilacja w orzecznictwie ETPC .............................. 339
  8.4.2. Masowa inwigilacja w orzecznictwie TSUE ......................... 345
  8.4.3. Przepisy krajowe i ich zgodność z normami międzynarodowymi ............. 352
8.5. Podsumowanie i wnioski ........................................................... 362
Wnioski końcowe ............................................................................. 367
Bibliografia ...................................................................................... 378
Wykaz najważniejszych skrótów

<table>
<thead>
<tr>
<th>Skrót</th>
<th>Opis</th>
</tr>
</thead>
<tbody>
<tr>
<td>EKPC</td>
<td>Konwencja o ochronie praw człowieka i podstawowych wolności</td>
</tr>
<tr>
<td>EIOD</td>
<td>Europejski Inspektor Ochrony Danych</td>
</tr>
<tr>
<td>EOG</td>
<td>Europejski Obszar Gospodarczy</td>
</tr>
<tr>
<td>ETPC</td>
<td>Europejski Trybunał Praw Człowieka</td>
</tr>
<tr>
<td>EWG</td>
<td>Europejska Wspólnota Gospodarcza</td>
</tr>
<tr>
<td>FTK</td>
<td>Federalny Trybunał Konstytucyjny RFN</td>
</tr>
<tr>
<td>GCHQ</td>
<td>Centrala Łączności Rządowej (Government Communications Headquarters) – agencja wywiadowcza Wielkiej Brytanii</td>
</tr>
<tr>
<td>GIODO</td>
<td>Generalny Inspektor Ochrony Danych Osobowych</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet Rzeczy (ang. Internet of Things)</td>
</tr>
<tr>
<td>KE</td>
<td>Komisja Europejska</td>
</tr>
<tr>
<td>KPC</td>
<td>Komitet Praw Człowieka</td>
</tr>
<tr>
<td>KPP</td>
<td>Karta Praw Podstawowych UE</td>
</tr>
<tr>
<td>MC</td>
<td>Ministerstwo Cyfryzacji</td>
</tr>
<tr>
<td>MPPOP</td>
<td>Międzynarodowy Pakt Praw Obywatelskich i Politycznych</td>
</tr>
<tr>
<td>MSOP</td>
<td>Międzynarodowe Standardy Ochrony Prywatności</td>
</tr>
<tr>
<td>MSWiA</td>
<td>Ministerstwo Spraw Wewnętrznych i Administracji</td>
</tr>
<tr>
<td>NSA</td>
<td>Naczelny Sąd Administracyjny; również, w zależności od kontekstu (gł. w rozdz. 8.), Agencja Bezpieczeństwa Wewnętrznego (National Security Agency) – agencja wywiadowcza Stanów Zjednoczonych</td>
</tr>
<tr>
<td>PDPC</td>
<td>Powszechna Deklaracja Praw Człowieka</td>
</tr>
<tr>
<td>PNR</td>
<td>Dane dotyczące pasażera (ang. passenger name record)</td>
</tr>
<tr>
<td>RE</td>
<td>Rada Europy</td>
</tr>
<tr>
<td>RODO</td>
<td>Ogólne rozporządzenie o ochronie danych osobowych</td>
</tr>
<tr>
<td>SN</td>
<td>Sąd Najwyższy</td>
</tr>
<tr>
<td>TFUE</td>
<td>Traktat o funkcjonowaniu Unii Europejskiej</td>
</tr>
<tr>
<td>TK</td>
<td>Trybunał Konstytucyjny</td>
</tr>
<tr>
<td>TSUE</td>
<td>Trybunał Sprawiedliwości Unii Europejskiej</td>
</tr>
<tr>
<td>TUE</td>
<td>Traktat o Unii Europejskiej</td>
</tr>
</tbody>
</table>
Wprowadzenie

W uchwalonej w 1948 roku Powszechnej Deklaracji Praw Człowieka po raz pierwszy wyróżniono i nazwano potrzebę prawnej ochrony sfery prywatności jako jedno z podstawowych praw człowieka. Niemal siedemdziesiąt lat później, w 2018 roku, w nauce prawa nadal nie wypracowano uniwersalnej i powszechnie akceptowanej definicji prywatności, a także standardów jej ochrony. Pomimo przyjęcia licznych deklaracji, rezolucji i wytycznych gremiów międzynarodowych, nie wyłączając tak poważanych, jak Organizacja Narodów Zjednoczonych czy Rada Europy, nadal aktualny jest problem poszanowania prywatności zarówno w relacjach wertykalnych, jak i horyzontalnych. Problematyka ta zyskuje na znaczeniu wraz z coraz powszechniejszym wykorzystaniem nowoczesnych środków komunikacji i przetwarzania danych w kolejnych sferach życia. Fenomen cyberprzestrzeni i związany z nią brak terytorialności, pozorna anonimowość i łatwość w dystrybucji informacji skutkują potrzebą ponownej analizy, czy normy prawne ustanowione kilkadziesiąt lat wcześniej są wystarczające i adekwatne do ochrony prywatności w odniesieniu do nowych zagrożeń technologicznych.

Od połowy lat siedemdziesiątych dwudziestego wieku rośnie ponadto znaczenie legislacji międzynarodowej dotyczącej przetwarzania danych osobowych. Przepisy stanowione w tym obszarze miały przeciwdziałać potencjalnym nadużyciom związanym z przetwarzaniem dużej ilości danych osobowych w systemach informatycznych. Aby cel ten mógł być osiągnięty, funkcja ochronna przepisów została uzupełniona o rozwiązania publicznoprawne i nadanie szeregu nowych praw podmiotom danych, dzięki czemu możliwa była lepsza kontrola nad realizowanymi procesami przetwarzania. O ile w przypadku ochrony prywatności normy międzynarodowe miały prowadzić do ochrony przed arbitralnością władzy krajowej, to w przypadku ochrony danych osobowych miały zapewnić stosowanie tych samych standardów i reżimów przetwarzania na płaszczyźnie ponadnarodowej. W ten sposób przeniesienie wiążących zobowiązań na grunt prawnomiedzynarodowy miało z jednej strony usunąć bariery w międzynarodowym transferze danych, a z drugiej – stworzyć bezpieczną przestrzeń do przetwarzania danych. Niestety, cel ten nie został nigdy w pełni osiągnięty. Po części stało się tak z uwagi na odmienne rozumienie i definiowanie prywatności – różne w poszczególnych kręgach kulturowych. Ponadto, nawet uznając prywatność za uniwersalną potrzebę człowieka, pojawiała się trudność w zdefiniowaniu granic potrzebnej ochrony, a w konsekwencji i sytuacji uzasadniających_ix, a w konsekwencji i sytuacji uzasadniających możliweą ingerencję.
Odmienne spojrzenie na znaczenie prawa do prywatności skutkowało wprowadzaniem przepisów różnej rangi w poszczególnych systemach prawnych. Klasycznym przykładem może być odmienne spojrzenie na prywatność w amerykańskiej i europejskiej nauce prawa. W efekcie, skoro w gronie państw demokratycznych, zbudowanych w oparciu o te same wartości i podstawy ustrojowe, nie sposób było osiągnąć zgodności co do rozpoznania prawa do prywatności jako jednego z podstawowych praw człowieka, jest oczywiste, że różnice te tylko narastały w odniesieniu do państw niedemokratycznych.

Upowszechnienie Internetu oraz dynamiczny rozwój technik przetwarzania informacji, w tym pojawienie się zupełnie nowych modeli przetwarzania, takich jak chmura obliczeniowa czy analizy Big Data, zwiększyło potrzebę wprowadzenia skutecznych mechanizmów ochrony praw w cyberprzestrzeni. Możliwość gromadzenia i przetwarzania dużych zbiorów danych, pozyskanych z wielu rozproszonych baz danych i ich swobodne, globalne przetwarzanie doprowadziło do powstania rynku brokerów danych – przedsiębiorców, posiadających bazy danych na temat setek milionów osób, w których uwzględniono informacje na temat ich stanu zdrowia, indywidualnych preferencji, sytuacji finansowej czy przynależności do określonych mniejszości. Profilowanie – a więc budowanie w oparciu o informacje pozyskiwane z wielu elektronicznych baz danych opisu jednostki – stało się skuteczną techniką marketingu produktów i usług, ale również badania i przewidywania zachowań ludzi albo całych społeczności, a w variancie bardziej rozbudowanym – skutecznym narzędziem inwigilacji. W ten sposób już dzisiaj możliwe jest określenie, jaka część uczestników festiwalu muzycznego Open’er to kobiety starające się o dziecko, a jaka – przedstawiciele mniejszości seksualnych. Z kolei amerykańska sieć handlowa Target może określać zaawansowanie ciąży swoich klientów, a także precyzyjnie przewidywać planowany termin porodu – i w ten sposób odpowiednio reagować w zakresie promowanych produktów. Wszystko to w oparciu o dane pozyskane dzięki nowoczesnym środkom przetwarzania danych, bez pytania osób zainteresowanych o konkretne fakty i zdarzenia z ich życia. W efekcie normy prawne i możliwości techniczne coraz częściej postrzegane są w kategoriach dychotomii, pozostawiając jednocześnie nierozstrzygniętymi formułowane wątpliwości etyczne i moralne. Jest to błędna diagnoza, pomijająca znaczenie nowoczesnych form przetwarzania dla dalszej ewolucji w kierunku społeczeństwa opartego na wiedzy. Europejski Inspektor Ochrony Danych zauważył, że „nigdy wcześniej podstawowe prawa do prywatności

---

2 Szczegółowe analiza przypadku, wraz ze wskazaniem zastosowanych technologii oraz implikacji z punktu widzenia ochrony prywatności – zob. rozdział 7.1 (s. 291).
i ochrony danych osobowych nie były tak istotne dla ochrony godności człowieka. Dają one człowiekowi możliwość rozwijania własnej osobowości, prowadzenia niezależnego życia, wykazywania się innowacyjnością oraz korzystania z innych praw i wolności. Technologia nie powinna narzucać wartości i praw, jednak relacji tej nie należy również sprowadzać do błędnej dychotomii. Z rewolucją cyfrową wiążą się obietnice korzyści w takich obszarach jak zdrowie, środowisko, międzynarodowy rozwój i efektywność ekonomiczna. Te same technologie, które prywatni przedsiębiorcy wykorzystują do swoich działań komercyjnych, władze państwowe starają się wykorzystać w obszarze szeroko pojętego bezpieczeństwa narodowego. Analityka predykcyjna – termin określający możliwość typowania zdarzeń w oparciu o zaawansowane algorytmy i duże, wieloaspektowe zbiory danych – jest już dzisiaj wykorzystywana do wskazywania osób podejrzanych o najpoważniejsze przestępstwa. Ponieważ termin najpoważniejsze przestępstwa jest chętnie używany w deklaracjach i oświadczeniach politycznych, ale nie został zdefiniowany na gruncie norm prawnych w sposób powszechnie akceptowany, to w sposób oczywisty pojawia się poważne ryzyko nadużycia władzy. Ta sama technologia może zostać wykorzystana do gromadzenia informacji na temat przeciwników politycznych czy stworzenia stałego systemu nadzoru nad społeczeństwem. Stale rozbudowywane programy masowej inwigilacji, bazujące na gromadzeniu hurtowych i nieukierunkowanych informacji na temat wszystkich użytkowników sieci łączności elektronicznej każą ponownie zadać pytanie o skuteczność istniejących prawnych mechanizmów ochrony prywatności – krajowych, regionalnych oraz międzynarodowych. Problem ten został dostrzegony także przez Parlament Europejski, który w odniesieniu do istniejących mechanizmów ochrony prywatności stwierdził, że „traktaty międzynarodowe oraz prawodawstwo UE i Stanów Zjednoczonych, a także krajowe mechanizmy nadzoru, nie zdołały zagwarantować niezbędnych kontroli i równowagi ani demokratycznej rozliczalności”. W polskiej literaturze brakuje kompleksowego opracowania dotyczącego problematyki ochrony prywatności w cyberprzestrzeni. Dominują ujęcia ukierunkowane na przedstawienie prywatności jako elementu prawa międzynarodowego lub systemów ochrony

---

5 Rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188(INI), sygn. P7_TA(2014)0230, p. 9.
praw człowieka7. W ostatnich latach, na skutek większej atencji związanej z negatywnymi zjawiskami mającymi miejsce w cyberprzestrzeni, publikowane są opracowania dotyczące cyberprzestępczości8 oraz cyberbezpieczeństwa – rozumianego głównie w wymiarze zapewnienia ochrony infrastruktury systemów i sieci przed atakami9.

W krajowym prawodawstwie, z racji funkcjonowania Polski zarówno w systemie europejskiej konwencji, jak i członkostwa w Radzie Europy oraz Unii Europejskiej, funkcjonują trwałe i wielostopniowe mechanizmy prawnej ochrony prywatności. Powstaje jednak pytanie, na ile są to rozwiązania skuteczne i adekwatne do ryzyk obecnych w cyberprzestrzeni? Czy brak granic, swoboda dostępu i wymiany informacji – rozróżniająca cyberprzestrzeń od przestrzeni fizycznej – nie tworzy z praw i gwarancji wynikających z praw o krajowym lub regionalnym zakresie stosowania, norm tworzących z pewnymi ochrony prywatności?

Oddzielnym zagadnieniem jest ocena rozwiązań prawnomiedzynarodowych wprowadzanych przez organizacje o zasięgu regionalnym, takie jak UE czy RE. Przyczyną dla opracowania przez UE własnych regulacji związanych z ochroną prywatności oraz danych osobowych było przekonanie, że w przeciwnym przypadku nie powiedzie się projekt związany z budową nowoczesnego społeczeństwa opartego na informacji. Tylko zniesienie barier w swobodnej wymianie informacji może przyczynić się do nieskrępowanego rozwoju nowoczesnych usług świadczonych w sieciach takich jak Internet. O ile więc projekt budowy europejskiego modelu ochrony danych można z dzisiejszego punktu widzenia ocenić jako udany, to w szerzej perspektywie jego sukces unaczkł ryzyka i niedoskonałości wynikające z braku wspólnych, ponadregionalnych regulacji związanych z badaną problematyką. Internet nie ma granic, w przeciwieństwie do prawodawstwa, w tym także stanowionego przez organizację ponadnarodową, taką jak UE. Problem ten trafnie podsumowała Grupa Robocza Art. 29, wskazując, że „zgodnie z prawem UE, prawo do ochrony danych osobowych to prawo podstawowe, podlegające ochronie na mocy art. 8 Karty Praw Podstawowych UE. W innych częściach świata potrzeba ochrony danych jest uznawana, niekoniecznie jednak ma status prawa podstawowego. UE i jej państwa członkowskie winny zagwarantować to podstawowe prawo każdej osobie objętej ich jurysdykcją. W zaglobalizowanym świecie

8 M. Siwicki, Cyberprzestępczość, CH Beck 2013.
9 M. Górka (red.), Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Difin 2014.
oznacza to, że obywatele mogą również żądać ochrony, jeśli ich dane są przetwarzane poza terytorium UE”10.

Podstawową tezą niniejszej pracy jest stwierdzenie, że istniejące regulacje prawne – w szczególności prawnomiędzynarodowe – nie zapewniają skutecznej ochrony przed zagrożeniami dla prywatności wynikającymi z nowoczesnych technik przetwarzania danych.

Potrzeba dokonania analizy konsekwencji prawnych związanych z upowszechnieniem się nowych modeli przetwarzania danych nie powinna prowadzić do mylnego przekonania, że głównym zagrożeniem dla ochrony prywatności jest postęp techniki. Jeżeli przyjąć by bowiem taką tezę za prawdziwą, to w konsekwencji celem wprowadzanych norm prawnych powinno być przeciwdziałanie temu zjawisku, a więc de facto próba powstrzymania lub znacznego ograniczenia upowszechnienia się nowoczesnych technik przetwarzania informacji. To podejście błędne, wynikające zapewne z pozanaukowego przekonania, że technologia może mieć cechy przypisywane działaniom ludzi. W rzeczywistości technika jest narzędziem o konkretnych możliwościach i funkcjach, bardziej lub mniej doskonałych – ale cały czas nie stanowi samodzielnego bytu w przestrzeni społecznej. Ludzie kształtują sposób, w jaki nowoczesna technika jest wykorzystywana. Sposobem ograniczania lub kontrolowania jej zastosowań jest między innymi wprowadzanie skutecznych norm prawnych. Celem prawodawcy nie powinno być hamowanie postępu techniki poprzez wprowadzanie archaicznych, niedopasowanych przepisów, ale kształtowanie go we właściwy sposób, zgodny z wartościami stojącymi u podstaw funkcjonowania współczesnych społeczeństw. Wprowadzanie tego typu regulacji – i to nie czekając na pojawienie się negatywnych skutków związanych z ich brakiem – jest zadaniem trudnym, zwłaszcza że obszary zastosowań niektórych technologii (np. Big Data czy IoT) nie są jeszcze gruntownie rozpoznane. Nie zmienia to jednak faktu, że jak zauważyła KE, tylko synergie pomiędzy normami prawnymi oraz rozwiązaniach technologicznych może zaowocować pomyślną transformacją w kierunku społeczeństwa opartego na wiedzy i informacji11.

Zakreślony powyżej problem badawczy jest złożony i wieloaspektowy. Jego badanie wykracza poza przestrzeń nauki prawa, nie może bowiem pomijać aspektów technicznych związanych z funkcjonowaniem cyberprzestrzeni i zagrożeń w niej występujących.

Rozważania dotyczące skuteczności norm prawnych bez odniesienia i omówienia technologii, które normy te mają regulować, są obarczone ryzykiem, że przedstawione wnioski będą niepełne i wybiorcze. W efekcie duża część rozważań przedstawionych w niniejszej pracy służy omówieniu i wyjaśnieniu, dlaczoego istniejące lub proponowane przepisy prawne są i będą nieskuteczne w odniesieniu do technologii, którą mają regulować. Dyskutując tę kwestię, określono także brzegowe warunki, jakie powinny zostać spełnione i uwzględnione, aby będąca efektem prac umowa międzynarodowa prowadziła do skutecznej ochrony prywatności w cyberprzestrzeni.

Przestrzeń badawcza wyznaczona przez określoną powyżej temę wymagała dekompozycji, dzięki czemu możliwe stało się udzielenie odpowiedzi na kilka węzłowych – i powiązanych ze sobą – problemów:

- czy obecne normy prawnomiedzynarodowe – wynikające z systemów ochrony praw człowieka, ustanawiające przepisy ochronne w zakresie prawa do prywatności oraz ochrony danych osobowych – są wystarczające do regulowania zdarzeń oddziałujących na prywatność, a mających miejsce w cyberprzestrzeni?
- czy prawo unijne ma potencjał prowadzący do standaryzacji w zakresie ochrony prywatności, a w efekcie do stworzenia bezpiecznej przestrzeni przetwarzania danych, wykraczającej poza granice państw członkowskich UE?
- czy niedoskonałości prawa ponadnarodowego mogą być uzupełnione na płaszczyźnie prawa krajowego; w szerszym ujęciu – jaka jest rola prawodawcy krajowego w badanym obszarze i czy w ogóle krajowe normy ochronne mają praktyczne znaczenie z punktu widzenia sposobu funkcjonowania sieci Internet?
- wreszcie – czy biorąc pod uwagę techniczne aspekty związane z nowymi technikami przetwarzania informacji, klasyczne rozumienie „prywatności” jako wolności człowieka od ingerencji (zainteresowania) ze strony świata zewnętrznego jest nadal aktualne? W jaki sposób rozwiązać oczywiste niedopasowanie Internetu bez granic oraz terytorialności cechującej stanowione normy prawne?

Przygotowując dysertację, skorzystano z kilku metod badawczych. Podstawową była metoda formalno-dogmatyczna, związana z analizą krajowych oraz międzynarodowych (w tym unijnych) aktów prawnych odnoszących się do badanej problematyki. Zakres przepisów poddanych analizie objął normy krajowe (konstytucyjne oraz ustawowe), a także regulacje prawnomiedzynarodowe, które funkcjonują w krajowym porządku prawnym – czy to na
skutek ratyfikacji określonego traktatu, czy w następstwie ustanowienia norm prawnych przez organizację międzynarodową, której RP jest członkiem.

Metoda formalno-dogmatyczna została uzupełniona metodą prawno-porównawczą oraz historyczno-porównawczą. W efekcie możliwe stało się nie tylko zidentyfikowanie i analiza obowiązujących norm prawnych, ale również ocena ich skuteczności w odniesieniu do nowoczesnych technik przetwarzania informacji. Ponadto podejście takie pozwoliło na przedstawienie ewolucji badanych rozwiązań prawnych nie tylko na płaszczyźnie krajowej, ale również międzynarodowej.

W części drugiej pracy szerzej wykorzystano komparatystkę prawniczą, szczególnie do zobrazowania różnice pomiędzy modelem ochrony prywatności obowiązującym w nauce europejskiej oraz rozwiązań stosowanych w Stanach Zjednoczonych Ameryki.

Istotnym elementem pracy była także analiza orzecznictwa, w tym międzynarodowych organów sądowych i kontrolnych. Z uwagi na znaczenie norm prawno-międzynarodowych dla badanej problematyki szczególną uwagę poświęcono analizie orzecznictwa ETPC oraz TSUE. W pracy wykorzystano też informacje udostępnione przez krajowe organy władzy publicznej na podstawie przepisów ustawy o dostępie do informacji publicznej.

Rozprawę podzielono na osiem rozdziałów, zgrupowanych w dwóch częściach. Część pierwszą poświęcono omówieniu istniejących i planowanych norm prawnych w badanym obszarze, ze szczególnym zwróceniem uwagi na analizę ich adekwatności do różnych form elektronicznego przetwarzania informacji oraz możliwych negatywnych konsekwencji dla sfery prywatności jednostek. Z kolei w części drugiej rozważań formalno-dogmatyczne uzupełniono o analizę ich skuteczności w odniesieniu do konkretnych zastosowań technicznych, realizowanych w cyberprzestrzeni. Celem było zbadanie oraz zobrazowanie niedoskonałości obowiązujących norm prawnych – krajowych, unijnych i międzynarodowych. Jednocześnie możliwe stało się sformułowanie wniosków de lege ferenda na temat warunków brzegowych, jakie muszą być uwzględniane w przyszłych działaniach legislacyjnych, aby stanowione prawo w odpowiedni sposób rozwiązywało zidentyfikowane problemy.

Zdefiniowany powyżej problem badawczy wymagał w pierwszej kolejności wprowadzenia i wyjaśnienia podstawowych pojęć i terminów – takich jak prywatność i związane z nią prawo do prywatności, a także cyberprzestrzeń oraz wzajemna relacja pomiędzy ochroną danych osobowych a ochroną prywatności. Zagadnienia te zostały

---

12 Ustawa z 6.09.2001 o dostępie do informacji publicznej (t.j. Dz.U. z 2016 r. poz. 1764 ze zm.).
prowadzone w rozdziale pierwszym. Szczególną uwagę zwrócono na wyjaśnienie uniwersalnej roli prywatności jako potrzeby warunkującej prawidłowy rozwój osobowości człowieka. Jest to kwestia o fundamentalnym znaczeniu, nadal bowiem – również w dyskursie prawniczym – spotyka się opinie sugerujące, że prywatność stanowi wytwór współczesnej cywilizacji państw wysokorozwiniętych, a w efekcie próba przeniesienia mechanizmów jej prawnej ochrony na płaszczyznę ponadnarodową musi się spotkać z zarzutem narzucaenia innym własnych wartości.

W rozdziale drugim przedstawiono analizę i omówienie najważniejszych systemów ochrony praw człowieka, funkcjonujących w polskim porządku prawnym i wprowadzających normy ochronne związane z prawem do prywatności. Pokazano ewolucję postrzegania prywatności na gruncie prawodawstwa różnych organizacji międzynarodowych (w szczególności ONZ, RE i UE). Rozważania dotyczące prawa materialnego uzupełniono analizą skuteczności środków ochrony prawnej – w szczególności powołanych organów kontrolnych i sądowych, a także znaczenia wydawanych przez nich rozstrzygnięć dla sytuacji prawnej jednostek na gruncie przepisów krajowych. W rozdziale tym przedstawiono również analizę najważniejszych norm konstytucyjnych, mających wpływ na badaną problematykę, wraz z ich porównaniem ze standardami ochrony wynikającymi z traktatów międzynarodowych.

Rozdział trzeci poświęcono przedstawieniu najważniejszych aktów prawnomiedzynarodowych, w większości o charakterze niewiączącym, wprowadzających wytyczne dotyczące ochrony danych osobowych. Regulacje te miały znaczący wpływ na ukształtowanie norm prawa krajowego wielu państw, ale również norm ponadnarodowych – takich jak prawo UE. Chociaż cechują się one o wiele bardziej szczegółowym i technicznym charakterem – zwłaszcza w porównaniu z ogólną treścią norm wynikających z systemów ochrony praw człowieka – to de facto w dużej części wpłynęły na ukształtowanie dzisiejszego europejskiego modelu ochrony danych.

W kolejnym, czwartym rozdziale przedstawiono najważniejsze akty prawne oraz obszary regulacji związane z prawem UE. Prawodawstwo unijne jest powszechnie uznawane za modelowe w zakresie podnoszenia standardów ochrony prywatności w cyberprzestrzeni. Jest też często przytaczane w literaturze przedmiotu jako przejawienie podejścia funkcjonującego w systemie prawnym Stanów Zjednoczonych. Reforma unijnych przepisów o ochronie danych to doskonały moment nie tylko do oceny, na ile wprowadzane oraz dyskutowane regulacje mogą stanowić kompleksowe rozwiązanie problemu ochrony prywatności w cyberprzestrzeni, ale również na ile proponowany przez prawodawcę unijnego
sposób budowania bezpiecznej przestrzeni przetwarzania informacji w relacjach z państwami trzecimi (nienależącymi do UE/EOG) jest realny i możliwy do zastosowania.

W rozdziale piątym omówiono płaszczyznę przepisów krajowych oraz roli krajowego prawodawcy w obszarze ochrony prywatności w cyberprzestrzeni. Uwzględniając funkcjonowanie Polski w kilku systemach praw człowieka (MPPOP, EKPC, KPP) oraz pamiętając o istotnej roli przepisów stanowionych przez UE w zakresie ochrony prywatności, interesujące było zbadanie, czy i w jakim zakresie krajowy prawodawca dysponuje przestrzenią do stanowienia dodatkowych regulacji kształtujących prawne granice prywatności. W ten sposób, poza wskazaniem wniosków de lege lata i de lege ferenda, przeprowadzono ocenę istniejących rozwiązań prawnomiędzynarodowych, w szczególności ich skuteczności w przypadku, gdy władze publiczne nie realizują odpowiednio swoich pozytywnych lub negatywnych obowiązków wynikających z treści traktatów.

W kolejnych trzech rozdziałach omówiono wybrane zagadnienia dotyczące najważniejszych, zdaniem autora, problemów związanych z ochroną prywatności w cyberprzestrzeni. Każde z przedstawionych zagadnień nie tylko może posłużyć do zobrazowania różnych słabości istniejących modeli ochrony prywatności, ale także prowadzi do konieczności rozważenia, czy w ogóle przyjęte założenia doktrynalne leżące u podstaw prawnej ochrony prywatności i danych osobowych są prawidłowe i aktualne. W rozdziale szóstym omówiono przetwarzanie w modelu chmury obliczeniowej, w rozdziale siódmym – analizy dużych zbiorów danych (Big Data), a w rozdziale ósmym – obecne możliwości władzy publicznej związane z prowadzeniem masowych programów inwigilacji. Wszystkie rozdziały części drugiej przygotowano w podobny sposób, w szczególności określono w nich zestaw szczegółowych hipotez badawczych będących przedmiotem badania, a także dokonano analizy prawnej wraz z odwołaniem się w podsumowaniu i wnioskach do głównej tezy pracy. Jednocześnie w każdym z rozdziałów części drugiej przedstawiono analizowany problem z innej perspektywy, dając możliwość zrozumienia wieloaspektowości badanej problematyki.

Rozprawę kończy podsumowanie, w którym zebrano wnioski cząstkowe i na ich podstawie określono, czy i w jaki sposób normy prawnomiędzynarodowe powinny tworzyć ramy ochronne i regulacyjne w zakresie prawa do prywatności w cyberprzestrzeni.

CZĘŚĆ 1. OCHRONA Prywatności: historia, teraźniejszość i przyszłość

Rozdział 1. Prywatność i cyberprzestrzeń – zagadnienia podstawowe

1.1. Psychologiczne i socjologiczne rozumienie prywatności

Prywatność stosunkowo niedawno, bo w drugiej połowie dwudziestego wieku, stała się odrębnym przedmiotem badań nauk psychologicznych i socjologicznych. Wcześniej wiązano ją z innymi, lepiej poznanymi pojęciami – takimi, jak afiliacja, terytorializm, samotność czy izolacja. W rezultacie prywatność, chociaż będąca terminem powszechnie używanym dla różnych form opisu relacji między jednostką a otaczającą ją społecznością, na gruncie badań naukowych do dzisiaj pozostaje zjawiskiem stosunkowo słabo poznanym. Dlatego przed rozpoczęciem rozważań na temat celu i zakresu prawnej ochrony prywatności, a także odniesienia środków prawnych do nowej płaszczyzny budowania relacji społecznych, jaką stanowi cyberprzestrzeń, konieczne jest odpowiednie przedstawienie poglądów nauki na sam fenomen prywatności, w szczególności w odniesieniu do prawidłowego rozwoju osobowości i wpływu na kształtowanie społeczeństwa.

Podstawowe pytanie, jakie należy w tym miejscu sformułować, dotyczy charakteru prywatności. Czy jest to potrzeba człowieka, charakterystyczna dla wszystkich ludzi w sposób niezależny od wpływu środowiski i kręgu kulturowego? Czy raczej należy ją uznać za cechę osobowości, której nasilenie objawiające się potrzebą różnych form izolacji wyraża potrzebę określonej jednostki, ale nie jest wspólne dla ogółu ludzi. Odpowiedzi na te pytania, chociaż wykraczając poza sfery nauk prawnych, mają fundamentalne znaczenie dla określania konieczności i celowości wprowadzania norm prawnych chroniących ten aspekt życia. Także wskazanie istnienia oraz stopnia zależności występowania potrzeby prywatności (jeżeli uznać prywatność za potrzebę) od określonego kręgu kulturowego jest istotne dla rozważań związanych z uwzględnieniem jej ochrony w katalogu podstawowych praw człowieka. Jeżeli bowiem prywatność nie byłaby podobnie traktowana i interpretowana w różnych grupach społecznych czy kręgach kulturowych, wprowadzenie uniwersalnych rozwiązań prawnych

13 K. Jędruszczak, Prywatność jako potrzeba w ramach koncepcji siebie, Roczniki Psychologiczne 2005, nr 2, s. 112.
14 Por. np. rozważania K. Jędruszak w zakresie statusu prywatności, Prywatność..., op. cit., s. 116.
służących jej ochronie mogłoby spotkać się z uzasadnionym zarzutem próby narzucania innym własnych wartości i wizji funkcjonowania społeczeństwa.

Jako wskazuje się w literaturze przedmiotu, w dwudziestym wieku nastąpiła dynamiczna ekspansja fenomenu prywatności\(^\text{15}\). W efekcie tego sytuacje, które kilkadziesiąt lat wcześniej nie były interpretowane jako należące do sfery życia prywatnego, dzisiaj są już tak traktowane. Obserwowane jest jednak także zjawisko przeciwne – polegające na akceptowaniu ujawniania i wprowadzania do sfery publicznej informacji, które historycznie uznawane były za dotyczące sfery prywatności. Rozumienie prywatności jest zależne od kręgu kulturowego, ale i wieku osób badanych, ich osobistych preferencji w zakresie nawiązywania relacji społecznych, pozycji zawodowej czy społecznej. Co więcej, ta sama osoba może w tym samym czasie (będąc w tym samym wieku) oceniać tę samą sytuację jako naruszającą jej poczucie prywatności lub nie – w zależności od kontekstu sytuacyjnego.

Ciekawe wyniki badań przedstawił w tym zakresie A. Mednis, wskazując, że odpowiedzi ankietowanych dotyczące oceny sytuacji, w której byłiby podglądani podczas mycia, zmieniły się, jeżeli treść pytania została uzupełniona informacją, że osobą obserwującą jest 2-letnie dziecko\(^\text{16}\). Obserwacja ta prowadzi do wniosku, że oczekiwanie prywatności może się zmieniać w zależności od zrozumienia przez jednostkę całego kontekstu sytuacji. Wniosek ten ma szczególne znaczenie w odniesieniu do cyberprzestrzeni – która tworząc pozory anonimowości, ale jednocześnie dostarczając narzędzi nieskrępowanego wyrazu, może wpływać na zmianę granic prywatności jednostki, sprawiając, że te same sytuacje i zdarzenia będą przez nią inaczej interpretowane tylko dlatego, że nie zachodzą w przestrzeni fizycznej.

---

\(^{15}\) Kwestia rozumienia granic prywatności w różnych dziedzinach nauki oraz języku potocznym jest przedmiotem intensywnych badań. Interesujące wyniki w tym zakresie przedstawiła D. Kasper, która przeprowadziła analizę informacji publikowanych w amerykańskiej prasie w latach 1990-2003. Kwerenda dotyczyła tekstów, w których tytuł lub akapit wprowadzającym wymieniony został termin „naruszenie prywatności” (ang. invasion of privacy). W ten sposób wybrano ponad 3700 artykułów prasowych. Zakresem badań było przeanalizowanie częstotliwości publikowanych wiadomości z podziałem na typ ingerencji (w tym celu Kasper wprowadziła podział na trzy kategorie: pozyskanie informacji, obserwacja lub wkraczanie) oraz określenie strony, która jest sprawcą oraz ofiarą naruszenia prywatności. Celem badań było ustalenie, czy w badanym okresie nastąpiła ewolucja rozumienia terminu naruszenie prywatności oraz opisanie zakresu tej zmiany. W ten sposób autorka ustaliła, że niezmiennie najczęściej występującą formą naruszenia jest pozyskanie informacji (średnio 60% badanych przypadków), na drugim miejscu znajduje się wkraczanie (średnio 21%) a najmniej przypadków dotyczyło obserwacji (18%). Badaczka zaprezentowała także szereg wniosków szczegółowych związanym z poszczególnymi typami naruszeń oraz analizą stron naruszających prywatność. Badanie zasługuje na uwagę z powodu wyboru nietypowej metody badawczej (analiza prasy), pozwalającej na przesłedzenie trendów w dużej populacji (Stany Zjednoczone), a nie tylko w odniesieniu do ankietowanej, stosunkowo niewielkiej grupy osób. Szczegóły: D. Kasper, The Evolution (Or Devolution) of Privacy, Sociological Forum 2005, nr 1, s. 69-92.

\(^{16}\) Tak wyniki i wnioski opisuje A. Mednis: „Aż 80% ankietowanych uznalo podglądanie kogoś przy myciu za naruszenie prywatności. Jeśli podglądającym miałoby być dwuletnie dziecko, to tylko 43% uznalooby to za naruszenie, dla 47% nie jest to w tym wypadku ingerencja w prywatność. Poczucie naruszenia prywatności jest więc dla wielu osób silnie powiązane ze zdolnością rozumienia sytuacji przez podglądacza”, idem, Granice prywatności, [w:] Prawo do prywatności a interes publiczny, Zakamucze 2006.
Prywatność jest zatem zjawiskiem wieloaspektowym i złożonym, w badaniu którego istotna jest nie tylko jednostka (potrzeby, oczekiwania, światopogląd), ale również jej umiejscowienie w społeczeństwie. Stąd aspekt socjologiczny, obok psychologicznego, jest również istotny w zrozumieniu prywatności.

W literaturze przedmiotu wskazuje się dwie teorie jako najbardziej istotne z punktu widzenia psychologicznego zrozumienia fenomenu prywatności – regulacyjna teoria prywatności I. Altmana (Privacy Regulation Theory, PRT) oraz teoria A. Westina17.


Zgodnie z teorią PRT prywatność jest procesem dwukierunkowym, będącym efektem interakcji jednostki z otoczeniem. Kontrolując przepływ informacji, jednostka próbuje osiągnąć stan oczekiwany przez siebie, poruszając się przy tym przy dwóch skrajnych poziomach: pełnego otwarcia (afiliacji) oraz zamknięcia (izolacji).

Odmienne, krytyczne podejście do teorii PRT zaprezentowali S. O’Connor i L. Rosenblood w modelu społecznej afiliacji (Social Affiliation Model, SAM). Przyjęto w nim założenie, że każda osoba ma jeden, optymalny stan prywatności, do którego dąży. Podstawowa różnica pomiędzy obydwoma podejściami polega na sposobie osiągania

---

18 I. Altman, Privacy Regulation: Culturally Universal or Culturally Specific?, Journal of Social Issues 1977, nr 3, s. 67.
19 K. Jędruszczak, Prywatność..., op. cit., s. 113.
21 Por. także wnioski zaprezentowane przez I. Altmana w Privacy Regulation..., op. cit., s. 82.
oczekiwanego poziomu prywatności w czasie. Zgodnie z teorią PRT jednostka porusza się pomiędzy dwoma skrajnymi biegunami, podczas gdy według modelu SAM jednostka chce odbudowywać zachwiany poziom optymalnej afiliacji, dobierając względnie podobne środki do podejmowanych poprzednio.

R. Dopierala zauważa, że prywatność postrzegana jako regulacja lub kontrola dostępu nie ogranicza się wyłącznie do fizycznego, przestrzennego charakteru – mniej istotnego w przypadku relacji internetowych, ale dotyczy także – kluczowego w ich kontekście – aspektu informacyjnego22. Z pracy I. Altmana wynika, że prywatność jest potrzebą uniwersalną, chociaż może być realizowana w odmienny sposób w różnych kręgach kulturowych. W konsekwencji otoczenie nie warunkuje potrzeby prywatności, ale określa sposób, w jaki może ona być regulowana. Środowisko zatem wpływa nie na nasilenie potrzeby prywatności, ale na to, w jakim stopniu udaje się ją zaspokoić23.

Z kolei A. Westin jest prekursorem w badaniu prywatności za pomocą metody kwestionariuszy. W ten sposób wyróżnił cztery stany, w jakich przejawia się prywatność – są to: samotność (rozumiana też jako wolność od obserwacji dokonywanych przez innych), intymność (separacja w kręgu osób bliskich od zainteresowania zewnętrznego), anonimowość (wolność od identyfikacji i inwigilacji) oraz rezerwa (dotycząca tworzenia psychicznych barier przeciwkoingerencji w sferę prywatną, skutkującą ograniczeniem ujawniania informacji na swój temat). Wskazane przez A. Westina stany stały się podstawą dalszych badań, w których nie tylko postulowano wyróżnienie kolejnych kategorii, ale również prezentowano wzajemne interakcje i powiązania pomiędzy poszczególnymi stanami24. A. Westin wyróżnił także funkcje prywatności, a wśród nich zapewnienie warunków do kształtowania tożsamości. W tym znaczeniu pozostawanie w prywatności sprzyja przyswajaniu i twórczemu przetwarzaniu informacji, rozważaniu alternatyw i konsekwencji zachowań oraz działań25.

Prywatność jako wyraz potrzeb, prowadząca do kontroli przepływu informacji, nie może być w pełni zrozumiana i zbadana bez odniesienia do społeczności, w której jednostka funkcjonuje. W szczególności istniejące normy społeczne i wynikające z nich wzorce zachowania nie pozostają bez wpływu na zakres oraz rozumienie prywatności. Stąd

22 R. Dopierala, Internetowe manifestacje..., op. cit., s. 108.
23 K. Jędruszczak, Prywatność..., op. cit., s. 117.
24 Ibidem, s. 108.
25 R. Dopierala, Internetowe manifestacje..., op. cit., s. 108 (przypis 6).
też interesujące wydaje się spojrzenie socjologiczne, które, jak wskazała M. Ossowska, można podsumować w trzech perspektywach:

1) prywatność jako uprawnienie do okresowej samotności, której nie należy mylić z osamotnieniem; w takim rozumieniu prywatność prowadzi do czasowego wycofania się z określonych relacji społecznych i może być wskazana jako przeciwieństwo stadności;

2) prywatność jako środek zabezpieczający przed kontrolą lub ingerencją ze strony osób trzecich; w tej perspektywie prywatność daje przestrzeń bezpieczeństwa wobec obcych;

3) prywatność jako element godności człowieka – szanowanie granic określonych przez jednostkę prowadzi do zachowania jej indywidualności.

Jak zauważa J. Kopka, wskazane podejścia mogą się łączyć i przenikać, powodując, że faktyczne zrozumienie prywatności jest zmienne w czasie i zależne od uwarunkowań kulturowych. Z punktu widzenia przedmiotu badań niniejszej pracy szczególnie interesujące są również wyniki badań M. Peay i E. Peaya, którzy wykazali, że ludzie w dużych zbiorowościach wycofywali się i podejmowali mniej afiliacyjne działania niż te, które występowały w środowisku o małym zagęszczeniu.


W rezultacie uzasadnione wydaje się oczekiwanie, że podobnie jak inne wartości mające wpływ na kształtowanie koncepcji siebie (np. wolność, godność, bezpieczeństwo) prywatność znajduje się w kręgu wartości chronionych normami nie tylko moralnymi, ale również prawnymi. Co więcej, uniwersalność fenomenu prywatności wykazana przez I. Altmana prowadzi do konkluzji o zasadności ustanowienia mechanizmów jej ochrony w

---

28 Ibidem, s. 27.
sposób niezależny od uznania krajowej władzy publicznej, a więc za pośrednictwem międzynarodowych systemów ochrony praw człowieka.

1.2. Geneza prawnej ochrony prywatności

W nauce prawa współczesne rozumienie terminu prawo do prywatności łączy się z opublikowanym w 1890 roku artykułem S. Warrena i L. Brandeisa Right to privacy, w którym zdefiniowali oni prywatność jako uprawnienie do poszanowania odrębności i braku ingerencji w strefę osobistą jednostki (right to be let alone). A. Sakowicz zauważa, że znaczenie wskazanej publikacji związane jest z nadaniem prawu do prywatności charakteru prawa samoistnego, co w szczególności oznacza, że przesłanki ochrony nie muszą być warunkowane naruszeniem innego dobra chronionego.

Pogląd S. Warrena i L. Brandeisa nie od razu zyskał akceptację w doktrynie, jak i judykaturze. Jeszcze w 1902 roku w sprawie Roberson v. Rochester Folding Box Co. stanowy sąd apelacyjny w Nowym Jorku oddalił powództwo związane z ochroną wizerunku kobiety, której zdjęcie bez uprzedniej zgody zostało wykorzystane w kampanii reklamowej. W uzasadnieniu sąd stwierdził, że „tak zwane prawo do prywatności nie znalazło stałego miejsca w judykaturze i, jak uważamy, doktryna ta nie może zostać zastosowana bez naruszenia ugruntowanych zasad prawa”. Sąd wskazywał przede wszystkim na wyłącznie niematerialny charakter naruszenia, a także na ryzyko, że uznanie możliwości ochrony prawa do prywatności na drodze sądowej doprowadzi „nie tylko do ogromnej liczby spraw, ale także sporów graniczących z absurdem”.


31 A. Sakowicz, Prywatność jako samoistne dobro prawne, Państwo i Prawo 2006, nr 1, s. 18.
33 K. Motyka, Prawo do prywatności, Zeszyty Naukowe Akademii Podlaskiej w Siedlcach, Seria Administracja i Zarządzanie 2010, nr 85, s. 12.
prawo jednostki do ochrony swojej prywatności zostało uznane i potwierdzone przez Sąd Najwyższy USA w orzeczeniu wydanym w sprawie Griswold v. Connecticut

Odmienne od S. Warrena i L. Brandeisa podejście w zdefiniowaniu prawa do prywatności zaproponował W. Prosser. Zamiast próby wprowadzenia jednej, uniwersalnej definicji wskazał on różne obszary, w jakich wystąpić mogą naruszenia wiązane z ochroną prywatności:

1) wkroczenie w sferę życia prywatnego jednostki,
2) ujawnienie w domenie publicznej wstydliwych informacji z życia prywatnego,
3) przekazanie do domeny publicznej fałszywych informacji na temat jednostki,
4) przywłaszczenie sobie, w celu uzyskania korzyści, czyjegoś nazwiska lub wizerunku

Rozważania W. Prossera były prowadzone w roku 1960, a więc ich podstawą było już rozbudowane – i różnorodne – orzecznictwo sądów stanowych i federalnych w USA. Myśli jego nie powinno więc przypisywać się charakteru negacji wcześniejszych poglądów S. Warrena i L. Brandeisa, a raczej ich rozwinięcia i ewolucji uwzględniającej ówczesny dorobek nauki prawa.

W polskiej literaturze przedmiotu pierwszą próbę zdefiniowania pojęcia prawa do prywatności podjął A. Kopff w 1973 roku, określając je jako „prawo jednostki do życia swym własnym życiem, układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej”. Na tym tle A. Kopff zaproponował jednak ujęcie prywatności w modelu sferycznym, znanym z nauk socjologicznych. W rezultacie doszedł do wniosku, że w prawie do prywatności znanym z amerykańskiej nauki prawa (w kształcie postulowanym przez S. Warrena i L. Brandeisa), a nazywanym przez niego prawem do ochrony sfery życia prywatnego, należy wyróżnić dwie kategorie (sfer): prawa do intymności życia osobistego oraz prawa do prywatności życia osobistego. Pierwszej ze stref przyznaje A. Kopff absolutną ochronę prawną – „strefa życia intymnego zasługuje zawsze na ochronę prawną i nie ma żadnych okoliczności usprawiedliwiających jakiekolwiek wkroczenie w tę strefę”. W efekcie nie można jej skutecznie przeciwwstawić żadnego interesu społecznego, w tym także związanego z prawem do informacji. Z kolei definiując pojęcie strefy prywatności życia osobistego, autor wskazuje na przydatność kryterium

34 Wyrok Sądu Najwyższego USA z 7.06.1965 w sprawie Griswold v. Connecticut, 381 U.S. 479 (1965).
36 A. Kopff, Koncepcja praw do intymności i do prywatności życia osobistego, Studia Cywilistyczne t. XX, Państwowe Wydawnictwo Naukowe 1972, s. 30.
37 Ibidem, s. 33.
„usprawiedliwionego zainteresowania”. Granice tej strefy nie mogą być wyznaczone w oderwaniu od świata zewnętrznego, w szczególności od interakcji jednostki z otoczeniem i będącym efektem tej relacji – uzasadnionym zainteresowaniem, które może wiązać się ze sferą życia prywatnego. Jako nadrzędne dla obu przestawionych sfer (kategorii) wskazywane jest ogólne prawo do ochrony życia prywatnego – jednak w ocenie A. Kopffa termin ten jest mało przydatny z uwagi na jego pojemność, a co za tym idzie trudność w zdefiniowaniu zakresu oraz skutecznych środków ochrony.

Podsumowując wywody dotyczące stanu legislacji i orzecznictwa w różnych krajowych systemach prawnych, A. Kopff dochodzi do wniosku, że naruszenia prawa do prywatności można sklasifikować w następujący sposób:

- ingerencja w życie prywatne, rodzinne lub domowe,
- naruszenie integralności psychofizycznej jednostki,
- naruszenie wolności, przekonań lub obyczajów człowieka,
- naruszenie czci, honoru lub uzyskanej opinii,
- ukazanie innej osoby w niekorzystnym dla niej świetle,
- ujawnienie krępujących lub intymnych faktów odnoszących się do życia prywatnego,
- przywłaszczenie sobie cudzego nazwiska, pseudonimu lub osiągnięć,
- niepokojenie drugiej osoby przez jej śledzenie, narzucanie swojego towarzystwa lub w inny sposób,
- dopuszczenie się naruszenia korespondencji oraz rozpowszechniania cudzego wizerunku bez zezwolenia osoby portretoowanej,
- nadużywanie informacji uzyskanych prywatnie,
- ujawnienie informacji uzyskanych od zainteresowane lub udzielonych mu w warunkach poufności.

Katalog naruszeń przedstawionych przez A. Kopffa jest zatem znacznie bardziej pojemny, niż wynika to z klasyfikacji przedstawionej przez W. Prossera. W takim rozumieniu prawo do prywatności służy ochronie szeregu innych dóbr osobistych, takich jak wolność myśli, sumienia i wyznania czy prawo do bezpieczeństwa osobistego. Tak szerokie zakresienie terminu prywatności może tworzyć je trudnym w ochronie. Poszczególne dobra chronione – takie jak chociażby prawo do posiadania własnych poglądów oraz wolność sumienia – służą zapewnieniu nadrzędnej wartości, jaką jest godność człowieka, jest więc oczywiste, że często występują łącznie lub w pewnych sferach życia przenikają się
wzajemnie. W zakresie tym nie traci nic na aktualności pogląd Trybunału Konstytucyjnego o ścisłym związku między zagrożeniami dla godności człowieka, stanowiącej podstawę konstytucyjnych wolności i praw jednostki, a wszelkimi czynnościami, które wkraczą w prywatność jednostki

Jednak trwałe powiązanie naruszeń prywatności z innymi dobrami chronionymi może prowadzić do nietrafionego wniosku, że prawo do prywatności nie jest samodzielną wartością, co w szczególności mogłoby oznaczać, że nie można mówić o jego naruszeniu, jeżeli jednocześnie nie wykazano by innego dobra chronionego, z którym naruszenie to było związane. K. Kubiński zauważa, że takie podejście nie uwzględniałoby możliwości pojawienia się działań, które godzą wyłącznie w życie prywatne człowieka, nie naruszając przy tym żadnego ze znanych dóbr osobistych – co częstokroć ma miejsce.


Powyższe zastrzeżenia nie zmieniają faktu, że koncepcja przedstawiona przez A. Kopffa została przyjęta przyczynie w doktrynie i doprowadziła do ugruntowania poglądu o tym, że sfera życia prywatnego należy do dóbr osobistych objętych ochroną prawa cywilnego. Teoria sfer A. Kopffa – w praktycznie niezmienionej formie – znalazła także miejsce w orzecznictwie Trybunału Konstytucyjnego: „o ile sfera życia intymnego (w znaczeniu szerszym niż potocznie przyjęte) objęta jest pełną prawną ochroną, o tyle ochrona

38 Wyrok TK z 23.06.2009, sygn. K 54/07, OTK-A 2009, nr 6, poz. 86.
39 K. Kubiński, Ochrona życia prywatnego człowieka”, RPEiS 1993, nr 1, s. 64.
40 M. Wild, Ochrona prywatności w prawie cywilnym, Państwo i Prawo 2001, nr 4, s. 54.
41 Ibidem s. 65
42 B. Kordasiewicz, Cywilnoprawna ochrona prawa do prywatności, Kwartalnik Prawa Prywatnego 2000, nr 1, s. 24.
sfery życia prywatnego podlega pewnym ograniczeniom, uzasadnionym usprawiedliwionym zainteresowaniem⁴³.

Zestawiając definicje naruszenia prawa do prywatności, proponowaną w nauce amerykańskiej z europejską myślą prawniczą, S. Stromhölm wskazuje na następujące obszary wspólne:

- wkroczenie – fizyczne lub za pośrednictwem innych środków – w sferę, którą jednostka chce zachować dla siebie,
- zbieranie materiałów, w najszerszym możliwym rozumieniu, o osobie zarówno poprzez naruszenie, jak i za pomocą innych metod uważanych za niewłaściwe,
- czynienie użytku z materiałów, także zgromadzonych w sposób legalny, o danej osobie dla publikacji lub innych specjalnych celów, takich jak przedstawienie dowodu przeciwko danej osobie⁴⁴.

Przenosząc powyższe rozważania na grunt polskiej nauki prawa L. Kański dochodzi do wniosku, że szereg wyliczonych przez S. Stromhölsa działań prowadzi do naruszenia ukształtowanych w krajowym prawodawstwie gwarancji tajemnicy korespondencji i nienaruszalności mieszkania⁴⁵. W efekcie zastanawia się nad wzajemną relacją dóbr chronionych, w szczególności nad zasadnością uznania prawa do prywatności jako wartości nadrzędnej, obejmującej swoim zakresem tajemnicę korespondencji oraz nienaruszalność mieszkania. Dochodzi jednak do wniosku, że tak zakreślony problem nie ma praktycznego znaczenia z uwagi na możliwość potraktowania prywatności w sposób równoległy i równorzędny do innych, tradycyjnych dóbr osobistych.

Prywatność, jako odrębne dobro, podlega współcześnie ochronie w większości systemów prawnych. Jest to związane z jednej strony z dynamicznym rozwojem techniki, prowadzącym do wyraźniejszego uwypuklenia zagrożeń związanych z ochroną prywatności, z drugiej jednak strony z uznaniem prywatności jako jednego z podstawowych praw człowieka.

W nauce prawa brakuje jednolitej, kompletnej i powszechnie akceptowanej definicji praw człowieka⁴⁶. W doktrynie podkreśla się ich związek z godnością człowieka, z czego wywodzi się ich charakter:

- uniwersalny – przysługują każdemu człowiekowi, niezależnie od miejsca zamieszkania, przynależności etnicznej, płci, wyznawanej religii itp.;
- przyrodzony – co oznacza, że przysługują każdemu od chwili urodzenia, nie są związane ze statusem jednostki w społeczeństwie;
- niezbywalny – oznaczający, że jednostka nie może się ich skutecznie zbyć ani ograniczyć ich stosowania względem siebie;
- nienaruszalny – skutkujący brakiem prawnej możliwości pozbawienia jednostki przysługujących jej praw.

Powyższe zasady mają charakter ogólny i w praktyce są modyfikowane w poszczególnych systemach ochrony praw człowieka. Normą jest między innymi wprowadzanie mechanizmów limitacji (ograniczenia) lub derogacji (wyłączania stosowania) poszczególnych praw przez władzę publiczną w wyjątkowych i szczególnie uzasadnionych sytuacjach.

Prywatność w takim rozumieniu jest prawem o charakterze publiczno-prawnym, ponieważ jego głównym adresatem i podmiotem zobowiązującym jest państwo, na które nałożone zostają zarówno obowiązki negatywne (zakaz nieuzasadnionej ingerencji), jak i pozytywne (wdrożenie regulacji wewnętrznych prowadzących do poszanowania prawa do prywatności w relacjach horyzontalnych).

Umiejscowienie prawa do prywatności w katalogu podstawowych praw człowieka skutkowało także jego konstytucjonalizacją w krajowych systemach prawnych oraz internacjonalizacją w prawie międzynarodowym.

### 1.3. Prywatność a ochrona danych osobowych – związkek pojęciowy

Rozpatrując kwestię ochrony prywatności w związku z przetwarzaniem informacji w sieciach informatycznych, należy zastanowić się nad wzajemną relacją pomiędzy ochroną prywatności a ochroną danych osobowych. Pierwsze regulacje krajowe związane z obszarem ochrony danych osobowych zostały wprowadzone na początku lat siedemdziesiątych dwudziestego wieku, przy czym były to przepisy fragmentaryczne, w których ochrona danych

---

była jednym z elementów wprowadzanej regulacji. Z kolei pierwsze próby opracowania wytycznych międzynarodowych związanych z ochroną danych osobowych należy wiązać z pracami Komitetu Rady Ministrów Rady Europy, w szczególności z decyzjami dotyczącymi ochrony prywatności jednostek w obszarze stosowania elektronicznych banków danych.7

Genezy przepisów o ochronie danych należy upatrywać w dynamicznym rozwoju informatyki skutkujących rosnącymi możliwościami gromadzenia i przetwarzania dużych zbiorów danych. W rozwiązaniach tych upatrywano potencjalne zagrożenia dla prywatności. W rezultacie francuski prawodawca w art. 1 ustawy o informatyce, zbiorach danych i wolnościach zadeklarował, że „informatyka ma być w służbie każdego obywatela. Nie może stanowić zagrożenia ani dla tożsamości istoty ludzkiej, ani dla praw człowieka, ani dla życia prywatnego ani dla wolności indywidualnych i publicznych”.

Prawo do prywatności i prawo do ochrony danych osobowych – chociaż służące ochronie tej samej wartości, jaką jest sfera życia osobistego – różni zakres podmiotów zobowiązanych. O ile w przypadku ochrony prywatności na pierwszym planie zawsze były relacje wertykalne, podkreślające znaczenie zagrożeń związanych z ingerencjami ze strony władzy publicznej, to analizując historię legislacji związanej z ochroną danych osobowych, łatwo zauważyć, że tłem dla wprowadzenia pierwszych regulacji były obawy przed zagrożeniami horyzontalnymi, związanymi z brakiem nadzoru nad transferem, gromadzeniem i przetwarzaniem coraz większych zbiorów danych bez żadnego prawnego instrumentu kontroli.

Już w 1983 roku niemiecki Federalny Trybunał Konstytucyjny (FTK) wskazał, że ochrona jednostki przed nieograniczonym gromadzeniem, przetwarzaniem i wymianą danych osobowych może być zapewniona na podstawie ogólnego konstytucyjnego prawa osobistości (Persönlichkeitsrechte)49. W ten sposób FTK wywiązał z istniejących norm konstytucyjnych uprawnienie jednostki do ochrony swoich danych osobowych, przejawiającego się między innymi w decydowaniu o zakresie wykorzystania oraz ujawniania informacji o sobie. Obowiązkiem pracodawcy powinno być natomiast wprowadzenie środków organizacyjnych i proceduralnych, które będą przeciwdziaływały naruszeniu tego prawa. Chociaż niemiecka

---

47 Zagadnienie szerzej omówione w rozdziale 3.1.
konstytucja nie podejmowała zagadnienia ochrony danych osobowych, wyrok FTK podniósł rangę autonomii informacyjnej jednostki do rangi prawa podstawowego.

We wczesnych regulacjach ochronę danych traktowano więc jako szczególną formę ochrony prywatności, o czym świadczą nawet same tytuły przytoczonych dokumentów. Przy takim podejściu dane osobowe są traktowane jako komponent sfery prywatności, wobec czego środki podjęte w celu ich ochrony w naturalny sposób realizują także cele związane z ochroną prywatności. Pogłąd taki podziela J. Borecka\(^50\), zauważając jednocześnie, że celem ochrony danych osobowych jest pomoc jednostce w zabezpieczeniu jej interesów przed ryzykami, jakie mogą wiązać się z przetwarzaniem informacji, a z drugiej strony umożliwienie administratorom danych w korzystaniu z posiadanych zbiorów danych.

Z kolei zdaniem M. Poloka, jedną z podstawowych przyczyn zainteresowania się samymi danymi osobowymi przez prawodawcę jest fakt ich znaczącej digitalizacji, *de facto* skomputeryzowania procesu przetwarzania danych. Z tej obserwacji buduje on pogląd, że adaptacja do obszaru ochrony danych osobowych koncepcji prawa do prywatności jest niewystarczająca – ponieważ nie uwzględnia chociażby zjawiska coraz większej digitalizacji, a tym samym większej niż dotychczas liczby zagrożeń przetwarzanych danych\(^51\). Także J. Benett zwraca uwagę, że ochrona danych jest odnoszona zazwyczaj do informacji przetwarzanych w systemach informatycznych. Stanowi także realizację koncepcji autonomii informacyjnej, która zgodnie z klasyczną definicją A. Westina jest „oczekiwaniem jednostek, grup lub instytucji decydowania kiedy, gdzie i jakie dokładnie informacje ich dotyczące zostaną udostępnione innym”.

Błędem byłoby traktowanie ochrony danych osobowych wyłącznie jako doprecyzowania prawa do prywatności. O ile prawo do prywatności zorientowane jest na zachowanie poufności informacji, to już ochrona danych osobowych związana jest z kontrolowaniem zakresu wykorzystania informacji oraz nadzorowaniem administratorów danych, czego przejawem jest nadanie specyficznych praw dla podmiotów danych (np. prawo do informacji, prawo do poprawienia danych). W takim rozumieniu ochrona danych osobowych może być w niektórych przypadkach terminem obejmującym obszary niezwiązane z ochroną prywatności. Przykładem może być zasada zapewnienia jakości danych, której stosowanie nie wpływa na gwarancje jednostki związane z ochroną prywatności, a jednocześnie w większości systemów prawnych stanowi jeden z

---

\(^{50}\) J. Borecka, *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych*, Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie 2006, nr 4, s. 9

podstawowych obowiązków administratora danych wynikających z przepisów dotyczących ochrony danych osobowych.

Omówienia wymaga także sama definicja obu terminów. Przepisy krajowe oraz normy prawa międzynarodowego definiują prywatność poprzez wymienienie obszarów chronionych, tworzących razem sferę osobistą jednostki. Prywatność w takim rozumieniu może być terminem bardzo pojemnym, niemającym charakteru definicji zamkniętej. K. Motyka wskazuje, że „eksansywność pojęcia prawa do prywatności przynajmniej w części jest rezultatem braku jego wyraźniej definicji, która miałaby jakieś szersze uznanie”52. Na tym tle prawna definicja ochrony danych osobowych przyjmuje charakter bardziej szczegółowy i techniczny. Zakres ochrony wyznaczony jest kluczowymi terminami takimi, jak dane osobowe, przetwarzanie czy podmiot danych.

M. Safjan wskazuje na odmienny charakter prawny przepisów o ochronie danych osobowych – ukierunkowanych na prewencję i zapobieganie naruszeniom, podczas gdy mechanizmy ochrony prywatności zorientowane są na działanie post factum (sankcje cywilnoprawne i karne)53. Sposobem zwiększenia skuteczności przepisów dotyczących ochrony danych jest oparcie ich na reżimie publicznoprawnym (prawo administracyjne) zamiast na rozwiązaniach cywilistycznych.

W literaturze przedmiotu podkreśla się, że przepisy dotyczące ochrony danych osobowych służą realizacji dwóch podstawowych funkcji. Z jednej strony mają być instrumentem niezbędnym dla poszanowania podstawowych, uznanych powszechnie praw i wolności, zwłaszcza prawa do prywatności, z drugiej – ich zadaniem jest ochrona interesów użytkowników najnowszej technologii informatycznej i Internetu, w tym różnych instytucji publicznych oraz zapewnienie niezbędnego do ich działania zaufania i bezpieczeństwa54.

Podsumowując powyższe rozważania, konieczne jest udzielenie odpowiedzi na pytanie, czy problem ochrony prywatności w cyberprzestrzeni można sprowadzić do zagadnienia skutecznej ochrony danych osobowych? Innymi słowy, czy w sferze korzystania z sieci informatycznych jednostka może doświadczyć zagrożeń dla swojej prywatności innych niż związane z naruszeniem ochrony danych osobowych? Ochrona prywatności jest pojęciem zdecydowanie pojemniejszym niż ochrona danych osobowych. W obszarze cyberprzestrzeni można wymienić cały zestaw zagrożeń i ryzyk, które mogą oddziaływać na prywatność

52 K. Motyka, Prawo do prywatności, op. cit., s. 25.
53 M. Safjan, Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym, Państwo i Prawo 2002, nr 6, s. 7.
użytkownika, a jednocześnie nie prowadzą do naruszenia przepisów dotyczących przetwarzania danych osobowych. Należy jednak dostrzec zauważalny w ostatnich latach trend do rozszerzania zakresu stosowania przepisów o ochronie danych. Jest on widoczny zarówno na płaszczyźnie przepisów krajowych (np. konsytucjonalizacja ochrony danych osobowych w Polsce, ale także wprowadzenie ponad 25 noweli do ustawy o ochronie danych osobowych od czasu jej uchwalenia w 1997 roku), jak i międzynarodowych (w szczególności zauważalne w prawie UE).

Porównując obecną definicję terminu *dane osobowe*, uwzględnioną w ogólnym rozporządzeniu o ochronie danych osobowych, z definicją, na której bazowały przepisy ustanawiane w latach siedemdziesiątych i osiemdziesiątych dwudziestego wieku, widać dużą ekspansywność zakresu ochrony zarówno pod kątem przedmiotowym, jak i podmiotowym. Biorąc pod uwagę wzmacnianie znaczenia ochrony praw podstawowych w krajach wysoko rozwiniętych, a także globalny trend do poszukiwania skutecznych – również prawnych – rozwiązań w zakresie ochrony przed cyberzagrożeniami, należy oczekiwać, że w kolejnych latach granica między prywatnością a ochroną danych osobowych będzie coraz trudniejsza do wyznaczenia.

1.4. **Cyberprzestrzeń jako nowa płaszczyzna budowania relacji społecznych**

Obszar badań niniejszej pracy jest wyznaczony dwoma kluczowymi terminami, którymi są *prywatność* oraz *cyberprzestrzeń*. O ile treść prawa do prywatności jest przedmiotem dyskursu naukowego od wielu dziesięcioleci, to kwestia zdefiniowania cyberprzestrzeni oraz odniesienia do niej obszaru praw podstawowych stanowi zagadnienie stosunkowo nowe. Odpowiednie umiejscowienie pojęcia cyberprzestrzeni ma natomiast kluczowe znaczenie nie tylko dla rozumienia nowych zagrożeń dla prywatności i wyzwań dla środków jej ochrony, ale również skuteczności istniejących i zasadności wprowadzania nowych regulacji prawnych.

---

55 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. UE L 119 z 4.5.2016).
1.4.1.1. Definicja techniczna

Cyberprzestrzeń jest terminem wprowadzonym do dyskursu naukowego przez W. Gibsona\textsuperscript{56} na początku lat osiemdziesiątych dwudziestego wieku w jego opowiadaniach \textit{science fiction}\textsuperscript{57}. Odwołując się do literatury W. Gibsona, J. Wasilewski wskazuje na najważniejsze cechy cyberprzestrzeni: „rozległość (zasięg światowy), spajanie wszelkich zasobów w jedną, olbrzymią bazę danych, złożoność oraz bezprzestrzenność rozumianą jako brak możliwości odniesienia cyberprzestrzeni do fizycznych (w tym geograficznych) wymiarów realnego świata”\textsuperscript{58}.

Z kolei zdaniem P. Sienkiewicza, pojęcie cyberprzestrzeni powinno być łączone z cybernetyką oraz jej twórcą – N. Wienerem\textsuperscript{59}. Cybernetyka jest nauką o działaniu i zasadach sterowania, u której podstaw znajduje się przekonanie, że organizmy i maszyny mogą być analizowane jak skomplikowane układy zamknięte. W propozycji N. Wienera badania w dziedzinie cybernetyki miały pomóc w zrozumieniu zasad rządzących komunikacją i zależnościami w układach, w których podejmowane decyzje wpływały na przedmiot badań (stąd dla cybernetyki kluczowe terminy to \textit{związek przyczynowo-skutkowy} oraz \textit{sprzędzenie zwrotne}). Dlatego podstawą metodą prowadzonych badań jest próba identyfikacji elementarnych operacji, których zrozumienie i opisanie pozwala lepiej zrozumieć zasady działania dużych, złożonych systemów. W efekcie, cybernetyka jest postrzegana jako nauka, która może pomóc w zrozumieniu zjawisk zachodzących w cyberprzestrzeni.

Jedna z bardziej znanych definicji cyberprzestrzeni została wprowadzona przez Departament Obrony USA: „Domena związana z użyciem elektronicznych i elektromagnetycznych urządzeń w celu gromadzenia, modyfikowania i wymiany danych za pomocą systemów sieciowych oraz związanej z nimi infrastruktury fizycznej”\textsuperscript{60}. W przedstawionej definicji zwraca uwagę podejście wyłącznie techniczne, nie uwzględniające elementów innych niż infrastruktura IT.


\textsuperscript{57} „To jest cyberprzestrzeń. Konsensualna halucynacja, doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych... Graficzne odczuwanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność...”. Cyt. za: W. Gibson, \textit{Neuromancer}, przekł. P. Cholewa, Poznań 1999, s. 43.

\textsuperscript{58} J. Wasilewski, \textit{Zarys definicji cyberprzestrzeni}, Przegląd Bezpieczeństwa Wewnętrznego 2013, nr 9, s. 226.


\textsuperscript{60} \textit{Joint Terminology for Cyberspace Operations}, The Vice Chairman of the Joint Chiefs of Staff, Department of Defense 2010, http://cli.re/GJvNXy, s. 7.
Rozważając formalne definicje cyberprzestrzeni, konieczne jest odniesienie się do koncepcji Internetu. Sieć Internet w kształcie znanym obecnie może być uznana za realizację wizji W. Gibsona i N. Weina. Jednocześnie jednak, termin ten służy do określania konkretniej, istniejącej i działającej sieci, o zasięgu globalnym oraz dającej się zwymiarować fizycznymi atrybutami. Cyberprzestrzeń jest natomiast koncepcją, przestrzenią zastosowań i możliwości technicznych, w przypadku której wymiar fizyczny jest trudno definiowalny. Jak celnie podsumował L. Strate, „cyberprzestrzeń jest wszędzie i jest używana w coraz szerszym kontekście, co sprawia, że sam termin staje się mniej precyzyjny i pozbawiony znaczenia”61.

Przykładem zbyt ekspansywnej definicji może być definicja wprowadzona przez NIST62: „globalne środowisko informacyjne, składające się z niezależnych sieci informatycznych, w tym z Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz powiązanych procesorów i kontrolerów”. W takim podejściu cyberprzestrzeń to sieć-sieci, koncepcja obejmująca wszystkie systemy przetwarzania danych oraz sieci informatyczne istniejące dzisiaj oraz takie, które dopiero powstaną. Propozycji takiej można przeciwstawić definicję przedstawioną w strategii cyberbezpieczeństwa Niemiec, w której wskazano, że systemy informatyczne nie podłączone do Internetu nie stanowią części cyberprzestrzeni63.

1.4.1.2. Konsekwencje braku terytorialnego charakteru

Według E. Haliżaka, obok płaszczyzny technologicznej cyberprzestrzeń można pojmować w kategoriach społeczno-politycznych64. W takim rozumieniu jest ona odmiennym, innym od tradycyjnego (fizycznego) obszarem aktywności jednostek. Aktywność ta, podobnie jak w przestrzeni fizycznej, może przybierać różne postaci – zarówno związane z odmiennymi formami ekspresji, jak i organizacji czy metodami działania. Cyberprzestrzeń jest zatem czymś znacznie bardziej złożonym niż tylko nowym medium komunikacji. Cyberprzestrzeń nie tylko łączy ludzi, ale również jest miejscem wyrażania poglądów, realizacji planów zawodowych, a także budowania więzi społecznych.

Charakteryzuje się przy tym zasadniczą cechą, odróżniającą ją od przestrzeni tradycyjnych – brak powiązania z terytorialnością. Przestrzeń fizyczna jest zazwyczaj

63 J. Wasilewski, Zarys definicyjny..., op. cit., s. 230.
64 E. Haliżak, Cyberprzestrzeń: Zagrożenia i nowe możliwości dla stosunków międzynarodowych, I Międzynarodowa Konferencja „Bezpieczeństwa państwa i biznesu w cyberprzestrzeni”, Wydział Zarządzania UW 2017, s. 19.
określana miarami geograficznymi i związana z funkcjonowaniem na jej obszarze określonej społeczności: lokalnej, regionalnej, narodowej czy ponadnarodowej. Cechą wspólną są jednak wyraźnie i zauważalne granice fizyczne, które stają się wyznacznikiem obszaru stosowania zasad (reguł) przyjętych przez daną społeczność. Zasady te w wyniku ich sformalizowania przyjmują postać norm prawnych, a w konsekwencji stają się podstawą do regulowania stosunków społecznych.

Terytorialność była od wieków podstawą budowy systemów prawnych na całym świecie. Chociaż w ostatnich dziesięcioleciach na znaczeniu zyskały normy prawa międzynarodowego, w tym także tworzone na ich podstawie organizacje międzynarodowe, to cały czas stroną takich aktów są głównie państwa, a nie inne grupy społeczne.65 Stosowane definicje państwa wskazują na monopol w stanowieniu prawa na określonym terytorium, co z kolei jest jednym z atrybutów suwerenności. Bez terytorium nie można mówić o powstaniu państwa, a w konsekwencji wprowadzeniu systemu prawa przez nie ustanowionego. Pojawienie się i dynamiczny rozwój cyberprzestrzeni wymaga odniesienia do powyższych pojęć. Skoro jednostki, grupy czy całe społeczeństwa mogą wyrażać się w przestrzeni innej niż fizyczna, to czy i w jakim zakresie tradycyjne systemy prawne będą miały do takich aktywności zastosowanie? Czy skoro cyberprzestrzeń nie ma granic, to próba zastosowania do niej regulacji wynikających z ustalonych, terytorialnych porządków prawnych ma szansę powodzenia?


66 Współcześnie także ugruntowany pogląd na definicję państwa musi być zmodyfikowany i dostosowany do nowych, szerszych uprawnień organizacji międzynarodowych. Dobrym przykładem jest Unia Europejska i jej relacje z państwami członkowskimi, które według niektórych badaczy mogą prowadzić do ograniczenia ich suwerenności. Teza ta znajduje potwierdzenie w sprawie Costa (C-6/64), w którym Trybunał potwierdził, że państwa-strony traktatów rzymskich dobrowolnie przekazały część swoich kompetencji, powołując EWG i w ten sposób ograniczając swoje suwerenne prawa. Także wprowadzenie wspólnej waluty (euro) oraz utworzenie wspólne nadzoru nad rynkiem bankowym są działaniami, które prowadzą do ograniczenia suwerenności państw w tradycyjnym ujęciu. Zob. także: J. Woś, A. Hnatyszyn-Dzikowska, Koncepcje suwerenności państwa w sferze polityki gospodarczej w warunkach europejskiej integracji gospodarczej, RPEiS 2007, nr 1 s. 173-184.
Nie są to pytania trywialne, a dodatkowo zyskują na znaczeniu po uwzględnieniu zakresu oddziaływania zdarzeń z cyberprzestrzeni na życie i funkcjonowanie jednostek. Dlatego państwa coraz częściej angażują się w zwalczanie negatywnych zjawisk mających miejsce w przestrzeni cybernetycznej. Jednym ze środków służących temu celowi jest dostosowanie istniejących oraz wprowadzanie nowych przepisów prawnych, a także udział w pracach organizacji międzynarodowych mających na celu ochronę praw jednostek w cyberprzestrzeni oraz zwalczanie pojawiających się w niej nadużyć.

1.4.1.3. Znaczenie dla polityki międzynarodowej oraz obronności

Oddzielna płaszczyzna postrzegania cyberprzestrzeni związana jest z postrzeganiem jej jako miejsce realizacji polityki: państw, grup społecznych, ale i prywatnych przedsiębiorców (w szczególności ponadnarodowych korporacji) oraz organizacji terrorystycznych. Poprzez dynamiczny rozwój technologii bardzo wiele obszarów funkcjonowania społeczeństw zależy od prawidłowego działania sieci informatycznych. Wpływ na prawidłowe działanie tych sieci może doprowadzić do negatywnych konsekwencji w działaniu powszechnych e-usług. Problem ten ma pierwszorzędne znaczenie w odniesieniu do tzw. infrastruktury krytycznej, związanej z dostarczaniem kluczowych usług z punktu widzenia interesów państwa (np. elektryczność, woda, telekomunikacja). Wydarzenia na Ukrainie w 2015 r., kiedy to nieznani sprawcy przeprowadzili udany atak cybernetyczny na systemy dystrybucji energii elektrycznej67, zobrazowały, w jaki sposób cyberprzestrzeń może stać się miejscem realizacji działań wymierzonych nie przeciwko jednostkom, ale państwom.

Cyberprzestrzeń stała się przedmiotem szerokich badań i prób regulacji jako miejsce potencjalnego konfliktu zbrojnego. W opracowywanych doktrynach omawia się takie zagadnienia, jak suwerenność, jurysdykcja i kontrola – w odniesieniu do działań państw mających miejsce w cyberprzestrzeni68. Następuje próba opracowania zasad prowadzenia działań obronnych, a także możliwości i zakresu realizacji działań ofensywnych. W konsekwencji pojęcie cyberbezpieczeństwa jest coraz częściej utożsamiane z obszarem bezpieczeństwa państwa. To z kolei wiąże się z naturalnym przypisaniem odpowiedzialności za przeciwdziałanie pojawiającym się zagrożeniom do struktur wojskowych. Jest to podejście błędne i świadczące o niezrozumieniu cyberprzestrzeni i zjawisk z nią związanych. Cyberprzestrzeni nie można bronić metodami konwencjonalnymi, a akty agresji w niej

realizowane mogą być inspirowane zarówno działaniem obcego rządu czy grupy terrorystycznej, jak i być niezwiązane z działalnością innych państw, a nawet motywowane względami innymi niż polityczne (chęć zdobycia pieniędzy, rozgłosu czy uznania w środowisku). Utożsamienie bezpieczeństwa w cyberprzestrzeni jedynie z wymiarem obronnym prowadzi do zmniejszenia rangi innych zagrożeń, o równie dużym znaczeniu z punktu widzenia praw jednostek – takich jak kradzież danych osobowych czy nadużycia dotyczące prywatności. W takim wypadku zagrożenia te nie mogą być prawidłowo rozpoznane i eliminowane, bowiem dobrane środki – związane z działalnością wojska – są w odniesieniu do nich nieadekwatne i nieskuteczne.

Niestety, taką sytuację obecnie możemy częściowo obserwować w Polsce, gdzie od lat toczy się dyskusja związana z opracowaniem i wdrożeniem efektywnej strategii cyberbezpieczeństwa państwa. Analizując kolejne dokumenty doktrynalne, prześledzić można ewolucję myśli planistów i decydentów dotyczących rozumienia zagrożeń związanych z cyberprzestrzenią. Jak wskazał prezydent B. Komorowski, „jedną z najważniejszych zmian we współczesnym środowisku bezpieczeństwa jest pojawienie się nowego obszaru aktywności państwa, podmiotów prywatnych i obywateli, jakim jest cyberprzestrzeń” 69. Takie rozumowanie doprowadziło autorów opublikowanej przez BBN w 2015 doktryny cyberbezpieczeństwa RP do wniosku, że cyberprzestrzeń jest nowym wymiarem bezpieczeństwa państwa, obok znanych wcześniej lądu, wody, powietrza i przestrzeni kosmicznej 70. Przywołując wcześniejsze rozważania, jest to ocena, w której błędnie próbuje się nadać cyberprzestrzeni cechy wymiaru fizycznego, co w oczywisty sposób prowadzi do dalszych nietrafionych wniosków. Konsekwencją takiego rozumowania jest próba wyodrębnienia cyberprzestrzeni RP jako fragmentu cyberprzestrzeni w obrębie „terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP ( placówki dyplomatyczne, kontynenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP, podlegające polskiej jurysdykcji)”. Chociaż autorzy doktryny wskazują na konieczność podejmowania działań związanych z cyberbezpieczeństwem z uwzględnieniem ochrony praw człowieka, w szczególności zaś z poszanowaniem wolności słowa oraz prawa do prywatności 71, to jednocześnie koncentrują się na opisaniu zadań związanych z cyberobroną, w szczególności z przygotowaniem i wdrażaniem scenariuszy postępowania w przypadku cyberataków. Dzięki w dokumentach strategicznych opracowanych przez

---

69 Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, BBN 2015, s. 4.
70 Ibidem, p. 1, s. 7.
71 Ibidem, p. 2, s. 7.
Ministerstwo Cyfryzacji\textsuperscript{72} wskazano, że „cyberbezpieczeństwo nie może być zapewniane przez państwo kosztem praw człowieka”\textsuperscript{73}.

Odmienne podejście do określenia kierunków działań państwa w zakresie zabezpieczenia cyberprzestrzeni zaprezentowano w Międzynarodowej Strategii dla Cyberprzestrzeni\textsuperscript{74} (International Strategy for Cyberspace), opracowanej i opublikowanej przez rząd Stanów Zjednoczonych w 2011 roku. Doktryna USA opisuje cyberbezpieczeństwo nie z perspektywy obronnej, ale z perspektywy celów i zadań koniecznych do budowy społeczeństwa informacyjnego. Stąd jako najważniejsze obszary wskazano wzmacnianie podstawowych wolności, w tym prywatności, oraz swobodny przepływ informacji. Podkreślono znaczenie uwzględnienia specyfiki cyberprzestrzeni w istniejących i planowanych aktach prawnomiydżynarodowych. Wśród zagadnień, które powinny być przedmiotem tego typu regulacji, wskazano: wzmacnianie praw podstawowych, poszanowanie własności oraz prywatności, zapobieganie i wykrywanie przestępceości, prawo do samoobrony, ale także globalną interoperacyjność systemów informatycznych czy zapewnianie stabilności działania sieci\textsuperscript{75}. Stany Zjednoczone w ten sposób podkreślili, że zagadnienie prawnej regulacji cyberprzestrzeni nie jest zadaniem, jakie może być podjęte i skutecznie zrealizowane wyłącznie na poziomie krajowym.

Z uwagi na oczywistą dysproporcję możliwości i środków, jakie są w dyspozycji państw oraz jednostek, zarysowuje się możliwość nadużycia władzy skutkująca ingerencją w prawa i wolności osobiste. Przykładem takich działań może być próba kontroli przekazywanych treści, sabotaż infrastruktury informatycznej jako narzędzie polityki międzynarodowej, ale i inwigilacja własnych obywateli lub działania wywiadowcze ukierunkowane na obywateli państw trzecich. Z uwagi na realizację tych działań w przestrzeni cybernetycznej środki ochrony prawnej ustanowione w celu ochrony przed tymi działaniami mogą okazać się nieodpowiednie lub nieskuteczne. Problem ten jest od lat rozpoznany jako jedno z głównych wyzwań związanych z rozwojem społeczeństwa opartego na informacji. W opinii Komisji Europejskiej, „aby cyberprzestrzeń pozostała otwarta i wolna, w środowisku internetowym powinny mieć zastosowanie te same normy, zasady i

\textsuperscript{72} Aktualna wersja: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, Ministerstwo Cyfryzacji 2017, http://cli.re/Lr5weG.
\textsuperscript{73} Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020, Ministerstwo Cyfryzacji 2016, http://cli.re/gVpA3Q , s. 7.
\textsuperscript{75} Ibidem, s. 14.
wartości, które UE wspiera w świecie rzeczywistym. W cyberprzestrzeni należy zapewnić ochronę praw podstawowych, demokracji i praworządności*76.

1.4.1.4. Perspektywa prawná

Definicja formalna cyberprzestrzeni została wprowadzona w polskim porządku prawnym w ustawie o stanie klęski żywiołowej77. Zgodnie z art. 3 ust. 1 pkt 4, pod pojęciem cyberprzestrzeni rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne78 wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Analogiczną definicję wprowadzono w ustawie o stanie wyjątkowym79. Zwraca uwagę brak odniesienia lub zdefiniowania kwestii cyberprzestrzeni w innych przepisach krajowych, w szczególności regulujących kwestie usług telekomunikacyjnych, ochrony konsumenta czy ochrony infrastruktury krytycznej.

Zakres pojęcia wynikający z ustawy o stanie klęski żywiołowej uwypukla aspekty techniczne cyberprzestrzeni. W pierwszym planie wskazuje na zbiór urządzeń (sieci i systemy informatyczne) jako elementy, tworzące przestrzeń do wymiany informacji. Definicja ta, choć poprawna pod względem formalnym, pomija złożoność badanego pojęcia, w efekcie jest niepełna, a przez to w pewnym zakresie tworzy mylne przekonanie, że cyberprzestrzeń jest zaledwie nowym, ale podobnym do istniejących, środkiem komunikacji.

1.4.1.5. Wnioski

Podsumowując powyższe rozważania, cyberprzestrzeń należy rozumieć jako sferę aktywności jednostek, odmienną od przestrzeni tradycyjnej. Termin ten w dalszej części pracy będzie utożsamiany z definicją wprowadzoną w normie ISO/IEC 27023:2012: „złożone środowisko, nie istniejące w żadnej formie fizycznej, będące efektem interakcji ludzi, oprogramowania oraz usług internetowych, realizowanej za pomocą podłączonych urządzeń i sieci informatycznych”80.

---

*76 Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, JOIN (2013) 1 final, s. 2.

*77 Ustawa z dn. 18.04.2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 Nr 62, poz. 558).

*78 Art. 3 pkt 3 ustawy z dn. 17.02.2005 r.o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565 ze zm.).

*79 Art. 2 ust. 1a ustawy z dn. 21.06.2002 r. o stanie wyjątkowym (Dz.U. Nr 113, poz. 985 ze zm.).

Powyższe rozważania prowadzą do zasadniczego pytania: czy i w jakim zakresie prawa stanowione przez państwa, a więc z definicji związane z geograficznymi granicami ich jurysdykcji, mogą skutecznie zapewnić ochronę jednostek przed zagrożeniami występującymi w cyberprzestrzeni? W szerszym ujęciu problem ten można przedstawić jako próbę poszukiwania transpozycji tradycyjnego systemu ochrony prawnej do środowiska, w którym nie istnieją granice państwowe, a narodowość czy suwerenność są terminami o ograniczonym znaczeniu praktycznym. Odpowiedź na te pytania jest zasadniczym celem niniejszej pracy i ma – w ocenie jej autora – fundamentalne znaczenie nie tylko dla dalszego nieskrępowanego rozwoju sieci Internet w jej globalnym wymiarze, ale również dla sukcesu budowy opartego na technologii i wiedzy społeczeństwa informacyjnego.

1.5. Prawne problemy regulacji cyberprzestrzeni

Zagadnienie niedostosowania regulacji prawnych do zjawisk mających miejsce w cyberprzestrzeni zostało zauważone w piśmiennictwie stosunkowo szybko, bo już w połowie lat dziewięćdziesiątych dwudziestego wieku – a więc w czasie, gdy sieć Internet w znanym obecnie kształcie jeszcze nie istniała. Problem jest dyskutowany na kilku płaszczyznach, z czego dwie najważniejsze to kwestia technicznej organizacji funkcjonowania cyberprzestrzeni oraz sposób określania prawa właściwego do zdarzeń, mających w niej miejsce.

Pierwsze z zagadnień nie dotyczy stricte cyberprzestrzeni, ale Internetu – jako globalnej sieci informatycznej. Internet wyewoluował z zastosowań wojskowych armii amerykańskiej, później przez wiele lat był rozwijany przez środowiska akademickie. W rezultacie większość mechanizmów regulacyjnych Internetu przybierała postać samoregulacji i powstawała jako standardy branżowe czy, w późniejszym okresie, normy międzynarodowe. Od strony nadzorczej, przez wiele lat jedynym podmiotem posiadającym kompetencje do regulowania działania kluczowych elementów Internetu był ICANN (Internet Corporation for Assigned Names and Numbers), formalnie organizacja pozarządowa, podlegająca prawu stanu Kalifornia w Stanach Zjednoczonych. Do 2016 roku ICANN był dodatkowo nadzorowany przez Departamentu Handlu Stanów Zjednoczonych82. Fakt ten był powszechnie krytykowany jako dowód braku pluralizmu oraz dominującą pozycję rządu jednego państwa

---

82 Quietly, symbolically, US control of the internet was just ended, The Guardian 14.03.2016, http://cli.re/6EWeBE.
w rozwoju Internetu\textsuperscript{83}. Od początku lat dwutysięcznych, potrzeba ponadnarodowej regulacji sieci Internet została dostrzegona na forum ONZ – i skutkowała powołaniem Światowego Forum Społeczeństwa Informacyjnego (\textit{World Summit of Information Society, WSIS}), a następnie Forum Zarządzania Internetem (\textit{Internet Governance Forum, IGF})\textsuperscript{84}. Z ich działalnością związana jest propozycja przyjęcia nowego międzynarodowego porozumienia zakładającego wprowadzenie wielostronnego nadzoru nad kluczowymi technicznymi elementami funkcjonowania sieci Internet\textsuperscript{85}. Działania te są wspierane przez KE, która wielokrotnie wskazywała jako swój cel „niezależny, otwarty i odpowiedzialny charakter zarządzania Internetem”\textsuperscript{86}. W chwili obecnej nie są prowadzone prace nad sformalizowaniem takiego porozumienia w postaci umowy międzynarodowej. Bez wystarczającej woli politycznej związanej z przeniesieniem części kompetencji realizowanej obecnie przez państwa, realizacja omówionej propozycji wydaje się mało prawdopodobna. Kluczowe znaczenie ma negatywne nastawienie Stanów Zjednoczonych, które są zainteresowane utrzymaniem obecnego status quo. Chociaż ICANN formalnie nie podlega już nadzorowi ze strony Departamentu Handlu, to nadal jest podmiotem regulowanym przez przepisy prawa amerykańskiego, a spory prawne dotyczące jego działalności rozstrzygane są przez właściwe sądy stanu Kalifornia.

Z perspektywy obszaru badawczego niniejszej pracy, istotniejszym zagadnieniem niż kwestia nadzoru nad technicznym funkcjonowaniem Internetu, jest problem określania prawa właściwego do regulacji zdarzeń, mających miejsce w cyberprzestrzeni.

W pierwszej kolejności należy wskazać, czy cyberprzestrzeń w ogóle wymaga wprowadzenia odmiennych od funkcjonujących obecnie mechanizmów prawnych, wynikających z norm prawa prywatnego międzynarodowego. J. Goldsmith argumentuje, że co do zasady cyberprzestrzeń jest tylko nową formą komunikacji, a działania realizowane za jej pośrednictwem mogą być oceniane i rozstrzygane przez istniejące przepisy prawa i

\begin{itemize}
  \item Tematyka szerszej omówiona przez J. Kulesza, \textit{Projekt Ramowej Konwencji Internetu}, Państwo i Prawo 2009, nr 10, s. 5-17.
\end{itemize}
wynikające z nich normy kolizyjne. Wskazuje, że zdarzenia mające miejsce w cyberprzestrzeni można przedstawić jako zbiór „aktywności podejmowanych przez znajdujące się w świecie rzeczywistym osoby, które (i) podejmują czynności prawne z innymi osobami, podlegającymi odmiennej jurysdykcji, lub (ii) wykonują działania w jednej jurysdykcji, którego skutki w świecie rzeczywistym występują w innej jurysdykcji”.

W efekcie doszedł do wniosku, że cyberprzestrzeń może być postrzegana jako „funkcjonalnie identyczna do tradycyjnych środków komunikacji, takich jak poczta, telefon czy znaki dymne”. Poglądy J. Goldsmitha spotkały się z krytyką. W przedstawionej polemice, D. Post wymienił szereg różnic przeczujących tezie o funkcjonalnej identyczności pomiędzy cyberprzestrzenią a innymi formami komunikacji. Wskazał przy tym, że każda z nich prowadzi do nowych, trudnych do przewidzenia konsekwencji, także prawnych.

W większości przypadków problem kwalifikacji prawnej zdarzeń mających miejsce w cyberprzestrzeni wymaga wskazania właściwej jurysdykcji, a więc zastosowania norm kolizyjnych wynikających z odpowiednich przepisów krajowych i międzynarodowych. K. Dobrzeniecki omawia cztery możliwe płaszczyzny prawnej regulacji cyberprzestrzeni:

1) jednostronna regulacja przez poszczególne państwa,
2) unifikacja norm kolizyjnych,
3) unifikacja praw materialnych odnoszących się do cyberprzestrzeni,
4) uznanie cyberprzestrzeni za autonomiczny obszar jurysdykcyjny.

Największe znaczenie praktyczne mają dwie pierwsze płaszczyzny – w dużej mierze opierające się na prawodawstwie krajowym. Każde państwo, dysponując swobodą w kształtowaniu norm prawnych, może we własnym zakresie określić normy jurysdykcyjne mające zastosowanie do cyberprzestrzeni.

W prawie międzynarodowym można wyróżnić jurysdykcję prawodawczą (legislacyjną), sądową oraz wykonawczą (egzekucyjną). Dla przedstawionych rozważań, największe znaczenie będzie miała jurysdykcja prawodawcza, jako pozwalająca na wskazanie przepisów materialnych mających zastosowanie w cyberprzestrzeni. Dalszy podział dotyczy przedmiotu rozstrzygania i pozwala na wyróżnienie jurysdykcji cywilnej oraz karnej. W przypadku jurysdykcji cywilnej dominuje zasada wyznaczania prawa właściwego względem miejsca zamieszkania powoda, uzupełniona o jurysdykcję wyłączną, przewidzaną dla

---

88 Ibidem, s. 1239-1240.
określonych typów spraw. Z uwagi na szczególną ochronę konsumentów przewidzaną w prawodawstwie UE, przykładem odstępstwa od powyższych zasad jest wskazanie dla rozstrzygania sporów umownych prawa właściwego dla miejsca zwykłego pobytu konsumenta. Odmienne łączniki stosowane są w przypadku jurysdykcji karnej – do najważniejszych należy zasada terytorialności, narodowości (jurysdykcja personalna), jurysdykcji ochronnej oraz uniwersalnej. Z każdą z nich wiążą się inne kryteria wyznaczania prawa właściwego. I tak, zgodnie z:

- jurysdykcją terytorialną subiektywną - właściwe jest prawo popełnienia czynu,
- jurysdykcją terytorialną obiektywną – właściwe jest prawo państwa, w którym wystąpił główny skutek popełnionego czynu,
- jurysdykcją personalną czynną – właściwe jest prawo według narodowości sprawcy,
- jurysdykcją personalną bierną – właściwe jest prawo według narodowości ofiary,
- jurysdykcją ochronną – państwo ma prawo ścigania czynów popełnionych poza jego terytorium, jeżeli mają one istotne znaczenie z punktu widzenia jego żywotnych interesów,
- jurysdykcją uniwersalną – dotyczącą w praktyce naruszenia norm ius cogens, a więc między innymi czynów naruszających podstawowe prawa człowieka (jak ludobójstwo, zbrodnie przeciwko ludzkości).

Z uwagi na mnogość zastosowań cyberprzestrzeni i zdarzeń, jakie mogą mieć w niej miejsce, w praktyce dochodzi do konieczności stosowania wszystkich wskazanych powyżej rodzajów jurysdykcji. Dodatkową trudnością jest globalny charakter sieci powodujący, że nawet gdy nadawca i odbiorca informacji znajdują się w tym samym państwie, sposób przekazania wiadomości może angażować łącza i serwery zlokalizowane w państwach trzecich. W przypadku cyberprzestrzeni trudnością jest nie tylko ustalenie tożsamości użytkowników, miejsca dokonania czynności prawnej, ale również wskazanie miejsca wystąpienia skutków (np. w przypadku publikacji informacji dostępnych globalnie).

Próby stosowania przez państwa terytorialnych zasad jurysdykcyjnych prowadzą do uzasadnionej krytyki społeczności międzynarodowej. Dla przykładu w szeroko komentowanej sprawie Yahoo v. LICRA, operator serwisu internetowego został zobowiązany do

92 Zob. art. 6 ust. 1 rozporządzenia 593/2008 z dn. 17.06.2008 w sprawie prawa właściwego dla zobowiązań umownych (Dz. Urz. UE z 2008 Nr L 177 s. 6).
uniemożliwienia dostępu z terenu Francji do treści aukcji zawierających symbolikę
nazistowską. Yahoo próbowało uniemożliwić wykonanie francuskiego wyroku za pomocą
powództwa wytoczonego przed sądami amerykańskimi, w których zabiegało o uznanie
jurysdykcji amerykańskiej. Z kolei firma Google została zobowiązana przez francuski organ
nadzoru nad ochroną danych osobowych (Commission nationale de l’informatique et des
libertés, CNIL), do realizacji żądań podmiotów danych dotyczących usunięcia informacji z
indeksu wyszukiwarki Google poprzez uniemożliwienie dostępu do nich nie tylko za pośrednictwem francuskojęzycznej wersji wyszukiwarki, ale ze wszystkich wersji
językowych – a więc ze skutkiem globalnym. Przyjęcie podejścia wyraźnego w decyzji
CNIL doprowadziłoby zatem do możliwości kształtowania nie tylko wolności wypowiedzi
(jak w sprawie Yahoo), ale i prawa do prywatności przez poszczególne państwa w
odniesieniu do wszystkich użytkowników cyberprzestrzeni. Niektórzy prawodawcy wprost
definiują, że prawo lokalne ma być stosowane we wszystkich przypadkach, w których
wiadomość jest kierowana i może być także odebrana z obszaru podległego ich jurysdykcji.
W przypadku nieterytorialnej cyberprzestrzeni, zastosowanie tej zasady prowadzi do
możliwości oceny tego samego zdarzenia niezależnie przez wiele państw. Słusznie J. Czekalska zauważa, że próba zastosowania jurysdykcji terytorialnej biernej do oceny zdarzeń
zachodzących w cyberprzestrzeni nieuchronnie prowadzi do zagrożenia naruszenia pewności
prawnej w obrocie, bowiem nadawca publicznej wiadomości pozbawiony jest możliwości
oceny skutków prawnych we wszystkich jurysdykcjach, w których treść ta może zostać
odczytaną.

94 Francuski sąd okręgowy zobowiązał Yahoo do: (1) modyfikacji zlokalizowanych w Stanach Zjednoczonych
ustawień serwerów udostępniających treści w sposób pozwalający na rozpoznanie adresów IP
użytkowników z Francji i blokowanie dla tych adresów dostępu do treści odnoszących się do symboliki
nazistowskiej; (2) wymagania od użytkowników, korzystających z nierozpoznanych adresów IP
zadeklarowania narodowości w momencie odwiedzenia głównej strony serwisu lub zainicjowania
wyszukiwania dla słowa “nazistowski”; (3) wykonania nakazu sądu w terminie trzech miesięcy pod groźbą
nałożenia grzywny w wysokości 100 tys. franków dziennie (ok. 13 tys. dolarów USD). C. Duh, Yahoo Inc. v.
LICRA, Berkeley Technology Law Journal 2002, nr 1, s. 361.

95 Decyzja CNIL z 10.3.2016 r., 2016-054, https://goo.gl/sycKpf; decyzja szerzej omówiona w: M. Rojszczak,
Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE. Prawo
Mediów Elektronicznych 2017, nr 3, s. 33.

96 Jednym z pierwszych przypadków jest amerykański stan Minnesota, w którym sądy uznały, że fakt
możliwości dostępu do informacji umieszczonych w Internecie z terenu stanu za wystarczający łącznik
prowadzący do uznania własnej jurysdykcji. W oświadczeniu z 18.07.1995 r. H Humphrey III, prokurator
generalny Minnesoty, wskazał, że „osoby znajdujące się poza stanem, które przekazują informacje za
pośrednictwem Internetu, wiedząc, że może być ona odczytana w Minnesocie mogą być pociągnięci do
odpowiedzialności za naruszenie karnych lub cywilnych przepisów stanowych”. Stanowisko to jest jednak
krytykowane także przez inne stany. Szerzej: D. Menthe, Jurisdiction in Cyberspace: A Theory of
International Spaces, Michigan Telecommunications and Technology Law Review 1998, nr 1, s. 75-78.

97 J. Czekalska, Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych, Państwo i Prawo 2004,
nr 11, s. 77.
K. Dobrzeniecki wskazuje, że skutkiem upowszechnienia takiej praktyki byłby tzw. efekt rozlania (ang. spillover effect), polegający na dostosowaniu dostawców treści internetowych do przepisów wynikających z najbardziej restrykcyjnej jurysdykcji\textsuperscript{98}. W takim przypadku doszło by do sytuacji, w której interpretacja praw i wolności jednostek byłaby kształtowana nie przez przepisy właściwe względem ich miejsca pobytu, ale przez regulacje państwa trzeciego, do przestrzegania których byłby pośrednio zobowiązany dostawca usług internetowych. Oddzielne trudności związane są z próbą zastosowania jurysdykcji terytorialnych do nowoczesnych form przetwarzania danych, których immanentną cechą jest przewarzenie rozproszone geograficznie, takie jak przetwarzanie w chmurze\textsuperscript{99}.

Z podobnymi kontrowersjami wiąże się próba odniesienia do cyberprzestrzeni zasad jurysdykcji personalnej. Podstawowy problem wynika z falszywego założenia, że transmisja i odbiór danych w Internecie wymagają obecności i udziału konkretnych osób. Tak nie jest: duża część ruchu internetowego to komunikacja maszyna-człowiek, a obecnie znacznie rośnie rola przekazów wymienianych wyłącznie przez urządzenia (\textit{Internet of Things})\textsuperscript{100}. W takim wypadku wiązanie norm jurysdykcyjnych z geograficzną lokalizacją stron komunikacji traci praktyczny sens. Co więcej, łączenie odpowiedzialności za funkcjonowanie e-usług nie z miejscem ich udostępnienia, ale z miejscem podstawowej siedziby podmiotu odpowiedzialnego za przekazywane treści prowadzi do kolejnych niejasności. Duża część globalnych usług internetowych udostępniana jest z wielu lokalizacji geograficznych jednocześnie. Także podmioty prowadzące te usługi zorganizowane są w formie transnarodowych organizacji. A zatem wskazanie osób odpowiedzialnych za konkretne działania (np. opublikowane treści) jest zadaniem trudnym, a z perspektywy użytkownika - praktycznie niewykonальным.

Unifikacja norm kolizyjnych jest najprostszym rozwiązaniem powyższych trudności, jednak o ograniczonym skutku praktycznym. Bez powszechnego zaakceptowania tych samych zasad określania jurysdykcji, wprowadzane regulacje mają wyłącznie skutek bilateralny lub regionalny. Przykładem mogą być unijne przepisy regulujące prawo właściwe do rozstrzygania sporów umownych i pozaumownych\textsuperscript{101}. Nawet w przypadku wypracowania

\textsuperscript{98} K. Dobrzeniecki, Prawo..., op. cit., s. 84.
\textsuperscript{99} Zob. szczegółowe omówienie w rozdziale 6.4.3 (s. 262).
\textsuperscript{100} Dlatego też straciły na aktualności poglądy wyrażane przez J. Czekalską oraz C. Duh na tle tzw. zasady nadawca-odbiorca (ang. uploader-downloader), prowadzące do zastosowania w cyberprzestrzeni reguły jurysdykcji personalnej. Zob. J. Czekalska, Jurysdykcja w cyberprzestrzeni..., op. cit., s. 78-79; D. Menthe, Jurisdiction in Cyberspace..., op. cit., s. 73-74.
\textsuperscript{101} Zob. treść rozporządzenia 593/2008 z dn. 17.06.2008 (zobowiązania umowne, Rzym I, zob. przypis 92) oraz rozporządzenia 864/2007 z 11.07.2007(zobowiązania pozaumowne, Rzym II, Dz. Urz. UE z 2007 Nr L 199 s.
globalnie akceptowalnych norm jurysdykcyjnych w odniesieniu do cyberprzestrzeni pamiętać należy, że efektem ich stosowania nie byłaby standaryzacja norm prawa materialnego. Niezgodność systemów prawnych mogłaby z kolei doprowadzić do faktycznej niewykonalności orzeczeń wydawanych przez obce sądy. Przykładem mogą być wyroki dotyczące wolności wypowiedzi, które nie są wykonywane przez sądy amerykańskie (zastosowanie klauzuli porządku publicznego), z uwagi na potencjalny skutek w postaci ograniczenia praw wynikających z Pierwszej Poprawki do Konstytucji.

Stąd też z perspektywy ochrony prywatności w cyberprzestrzeni, zwiększenia skuteczności regulacji prawnych należy upatrywać w unifikacji praw materialnych. Wprowadzenie za pomocą prawnie wiążących aktów międzynarodowych wspólnych norm ochronnych czy regulacyjnych może prowadzić do standaryzacji sposobu przetwarzania informacji na płaszczyźnie ponadnarodowej. Przykładem takiej regulacji jest Konwencja RE nr 185 o cyberprzestępczości, wprowadzająca typizację najważniejszych przestępstw realizowanych w przestrzeni wirtualnej oraz skutkującą uwzględnieniem ich w krajowych przepisach narodowych. Ostatnim ze sposobów rozwiązania problemu prawnej regulacji cyberprzestrzeni jest uznanie jej za autonomiczny obszar jurysdykcyjny. Propozycja ta nawiązuje do teorii przestrzeni międzynarodowych i wydzielenia cyberprzestrzeni na wzór przestrzeni kosmicznej, morza otwartego i Antarktydy spod suwerenności każdego z państw, a w efekcie spod regulacji przepisów krajowych. Podobnie jak w przypadku unifikacji przepisów materialnych, także i ta koncepcja zakłada potrzebę przyjęcia traktatu międzynarodowego.

Ostatnim ze sposobów rozwiązania problemu prawnej regulacji cyberprzestrzeni jest uznanie jej za autonomiczny obszar jurysdykcyjny. Propozycja ta nawiązuje do teorii przestrzeni międzynarodowych i wydzielenia cyberprzestrzeni na wzór przestrzeni kosmicznej, morza otwartego i Antarktydy spod suwerenności każdego z państw, a w efekcie spod regulacji przepisów krajowych. Podobnie jak w przypadku unifikacji przepisów materialnych, także i ta koncepcja zakłada potrzebę przyjęcia traktatu międzynarodowego.


102 C. Duh, Yahoo Inc., op. cit., s. 368.

103 Konwencja Rady Europy o cyberprzestępczości z dn. 23.11.2001 r. (Dz. U. z 2015 r. poz. 728).


105 Z zagadnieniem przestrzeni międzynarodowych związane jest także pojęcie wspólnego dziedzictwa ludzkości, wprowadzone po raz pierwszy w art. 136 konwencji z dn. 10.12.1982 r. o prawie morza (Dz.U. 2002 Nr 59, poz. 543). Użycie morsza otwartego (w tym dna morza), przestrzeni kosmicznej czy Antarktydy za wspólne dziedzictwo ludzkości, chociaż następowało na podstawie oddzielnych traktatów, prowadziło do zdefiniowania następujących cech wspólnych dla przestrzeni międzynarodowych: (i) nie może być przedmiotem zawłaszczenia ze strony jakiegokolwiek państwa, (ii) wykorzystywanie powinno następować wyłącznie w celach pokojowych, w zgodzie z Kartą NZ oraz w interesie wszystkich, zwłaszcza z korzyścią dla państw rozwijających się, (iii) militarne wykorzystanie powinno być zabronione. Należy zauważyć, że odniesienie każdego z tych postulatów do cyberprzestrzeni napotyka istotne trudności, co z kolei prowadzi do wniosku, że definicja wspólnego dziedzictwa ludzkości wynikająca z istniejących traktatów jest niewystarczająco pojemna, aby można ją zastosować do cyberprzestrzeni. Więcej nt. koncepcji wspólnego dziedzictwa ludzkości: E. Riedel, Trzecia generacja praw człowieka jako strategia urzeczywistniania praw politycznych i społecznych, RPEIS 1990, nr 3-4, s. 121-124.

107 Dla przykładu, w 2011 roku segment usług IT stanowił niemal 20% eksportu Irlandii; średnia dla UE (2,43%) została przekroczona jeszcze przez Finlandię, Szwecję, Luksemburg i Wielką Brytanię. Uwagę zwraca także duży stopień cyfryzacji usług publicznych w UE, wyrażany wskaźnikiem części populacji która w ciągu ostatnich 12 miesięcy skorzystała z e-usług udostępnianych przez administrację publiczną – według danych za 2017 rok w przypadku 8 państw członkowskich przekroczył on poziom 75% (Dania, Islandia, Szwecja, Norwegia, Finlandia, Holandia, Estonia i Luksemburg). Dane za portalem informacyjnym Digital Single Market EU, http://cli.re/GJBZP5.
108 K. Dobrzeniecki, Prawo..., op. cit., s. 91-100.
funkcjonowania Internetu¹⁰⁹. Nie jest jasne, czy w zakresie ochrony praw podstawowych z samoregulacją można wiązać podobne nadzieje. W nauce amerykańskiej, wyrażany jest pogląd, że samoregulacja może prowadzić do zwiększenia poziomu ochrony użytkowników Internetu i zrównoważyć brak właściwych norm prawa stanowionego¹¹⁰. Problem ten zostanie przeanalizowany w niniejszej pracy na przykładzie transatlantyckiej współpracy UE – USA w zakresie przekazywania danych oraz regulacji rynku Big Data.

1.6. Zagrożenia dla prywatności w cyberprzestrzeni

Z uwagi na globalny charakter, z cyberprzestrzenią wiążą się nowe zagrożenia i ryzyka dla ochrony praw podstawowych. Ważnym przykładem może być ochrona prywatności, która rozumiana jako prawo do decydowania jednostek o zakresie przekazywanych innym informacji na swój temat jest szczególnie podatna na zagrożenia płynące z poznanej anonimowej cyberprzestrzeni.

J. Rzucidło oraz J. Węgrzyn wskazują, że zagrożenia związane z aktywnością w cyberprzestrzeni można sklasyfikować w trzech kategoriach: cyberwojny, cyberprzestępstwa oraz cyberterroryzmu¹¹¹. Cyberprzestępstwa definiują natomiast jako „zwyczajne czyny kryminalne” lub ogólniej – jako przestępstwa komputerowe.

Z kolei J. Sienkiewicz proponuje przeprowadzenie analizy zjawiska, uwzględniając różne płaszczyzny bezpieczeństwa informacyjnego¹¹². Wskazuje na możliwość wyróżnienia sfer cyberprzestrzeni, które operują na innych poziomach funkcjonalnych i wobec tego oddziałują na nie inne typy zagrożeń. I tak wyróżnia płaszczyznę bezpieczeństwa informacyjnego obywateli, organizacji, państwa oraz UE. Z każdą z nich wiąże inne środki ochronne, zagrożenia oraz ich skutki. Zagrożenia klasyfikuje w następujący sposób:

1) zagrożenia systemowe, takie jak cyberataki, cyberterroryzm, cyberkontrolę oraz operacje informacyjne,
2) zagrożenia pospolite - związane z cyberprzestępstwami.

¹⁰⁹ Przykładem mogą być dokumenty RFC (Request for Comments), które pierwotnie stanowiły sposób wprowadzania nieformalnych standardów przez społeczność związaną z rozwojem Internetu. Dokumenty RFC służą do opisywania i standaryzowania wszystkich kluczowych elementów służących funkcjonowaniu Internetu, w tym najważniejszych protokołów komunikacyjnych.
¹¹¹ J. Rzucidło, J. Węgrzyn, Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni, Przegląd Prawa Konstytucyjnego 2015, nr 5, s. 146.
¹¹² P. Sienkiewicz, Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni, Automatyka 2009, nr 2, s. 587-589.
W modelu zaproponowanym przez J. Sienkiewicza zagrożeń oddziałujących na prywatność należy poszukiwać na płaszczyźnie bezpieczeństwa informacyjnego obywateli (np. kradzież danych) oraz bezpieczeństwa informacyjnego organizacji (np. ujawnienie dużych zbiorów informacji). Z kolei zagrożenia dotyczące cyberbezpieczeństwa krajowego i ponadnarodowego należy wiązać z atakami na stabilność pracy infrastruktury krytycznej.

W literaturze przedmiotu odnaleźć można różne propozycje szczegółowego podziału cyberprzestępstw. I tak S. Kotecka wprowadza podział na przestępstwa przeciwko: (1) Rzeczypospolitej Polskiej, (2) bezpieczeństwu powszechnemu, (3) wiarygodności dokumentów, (4) ochronie informacji oraz (5) mieniu. Z kolei M. Siwicki rozdziela przestępstwa dotyczące bezpieczeństwa przetwarzanych informacji od przestępstw związanych z ich treścią.

Natomiast M. Grzelak i K. Liedel, wskazując listę najpopularniejszych zagrożeń w cyberprzestrzeni, wyprowadzają poza obszar prawnokarny:
- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki itp.);
- kradzieże tożsamości,
- kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług (mail bomb, DoS oraz DDoS),
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Chociaż większość dostępnych systematyk koncentruje się na typizacji różnych typów działań przestępczych (cyberprzestępstwa) lub wymierzonych w bezpieczeństwo państwa (cyberataki, cyberterrororyzm), to pamiętać należy o zagrożeniach niezwiązanych z działaniami zabronionymi, które mogą mieć również duży wpływ na ochronę prywatności użytkowników cyberprzestrzeni. W szczególności w literaturze wskazuje się na ryzyka związane z nowoczesnymi technikami przetwarzania takimi, jak cloud computing, Big Data czy

---

113 S. Kotecka, Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem, [w:] Wybrane dobre praktyki w zakresie usług elektronicznych pod red. J. Gołaczyńskiego, CH Beck 2016.
114 M. Siwicki, Pojęcie cyberprzestępczości, [w:] Cyberprzestępczość, CH Beck 2013
116 Denial of Service (DoS) oraz Distributed Denial of Service (DDoS) są typami ataków wymierzonych w dostępność systemów informatycznych; ich celem jest uniemożliwienie uprawnionym użytkownikom korzystania z zasobów informatycznych (np. e-usług) poprzez ich przeciążenie.
117 X. Konarski, Przetwarzanie danych osobowych w chmurze obliczeniowej, Monitor Prawniczy 2013, nr 8 dodatek, s. 39-44.
Internet Rzeczy (Internet of Things). Dlatego, bazując na wcześniejszych propozycjach, zasadne jest wprowadzenie podziału w sposób wyraźniej uwypuklający zagrożenia dla prywatności związane z nowymi technikami przetwarzania informacji:

- cyberprzestępstwa – w tym także kradzież danych, ale również ich bezprawne niszczenie, opublikowanie,
- profilowanie – realizowane bez poszanowania praw podmiotu danych i niezgodnie z jego interesem, często wbrew wiedzy danej osoby,
- cyberinwigilacja – rozumiana jako nieuprawniona obserwacja, prowadzona zarówno w formie zinstytucjonalizowanej (działania władz państwowych) ale również jako skutek stosowania innych technik (np. korzystanie z geolokalizacji w usługach marketingu),
- ujawnienie informacji – będące skutkiem działań innych niż przestępce, np. błędu człowieka, awarii systemu, ale również wynikiem normalnego działania innych niż przestępce,
- utrata kontroli nad informacją – w efekcie np. przetwarzania niezgodnego z pierwotnie ustalonym celem lub zakresem, ale również wyniku niezrozumienia przez użytkownika charakteru usługi przetwarzania, z której korzysta.

Powyższy podział z pewnością nie jest kompletny, jest jednak wystarczający do zobrazowania, że istotna część zagrożeń dla prywatności użytkowników cyberprzestrzeni nie wynika z działań o charakterze przestępczym. Rozpatrując w niniejszej pracy problem ochrony prywatności, uwaga zostanie zwrócona nie na aspekty identyfikacji i penalizacji cyberprzestępstw, ale na prawne mechanizmy prowadzące do ochrony sfery prywatności przed zagrożeniami związanymi z rozwijaniem nowych sposobów przetwarzania danych.

---


119 P. Leja, Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych, Prawo Mediarów Elektronicznych 2017, nr 3, s. 10-17.
Rozdział 2. Prawomiedzinarodowe i konstytucyjne źródła norm w obszarze ochrony prywatności

2.1. Wprowadzenie

Wraz z zakończeniem II wojny światowej społeczność międzynarodowa podjęła znaczne wysiłki w celu budowy ponadnarodowego systemu ochrony praw człowieka. W budowie uniwersalnego modelu widziano sposób na wyrównanie różnic w rozumieniu zakresu praw podstawowych przynależnych jednostkom, a w efekcie mechanizm przyczyniający się do międzynarodowego pokoju i bezpieczeństwa. Już w preambule do przyjętej 26 czerwca 1945 roku Karty Narodów Zjednoczonych\(^{120}\) jako jeden z jej celów wskazano „przywrócenie wiary w podstawowe prawa człowieka”. Cel ten został następnie rozwinięty w art. 1 Karty poprzez wskazanie, że Narody Zjednoczone dążą do osiągnięcia współpracy „przy popieraniu i zachęcaniu do poszanowania praw człowieka i podstawowych swobód dla wszystkich, bez różnicy rasy, płci, języka lub religii”.

K. Vasak jako pierwszy zaproponował wprowadzenie podziału na generacje praw człowieka, przy czym prawa należące do pierwszej generacji wiązał głównie z negatywnymi obowiązkami państw\(^{121}\). Należy przez to rozumieć nakaz powstrzymania się władzy publicznej od ingerencji w prawa jednostek. W rezultacie do kategorii tej zalicza się prawa i wolności osobiste (między innymi prawo do życia, prawo do bezpieczeństwa, zakaz stosowania tortur), ale także prawa polityczne i obywatelskie (prawo do zgromadzeń, prawo do wyrażania opinii). Z kolei prawa drugiej generacji łączy się z pozytywnymi obowiązkami państw, skutkujących koniecznością podjęcia działań prowadzących do ich zagwarantowania w wewnętrznym systemie prawnym. Do praw tego typu zalicza się między innymi prawa społeczne, kulturalne i gospodarcze. Podział ten – jakkolwiek często przywoływany w literaturze przedmiotu – stracił częściowo na aktualności. Z. Kulińska-Kępa\(^{122}\) wskazuje na wpływ bogatego orzecznictwa sądów międzynarodowych, podkreślającego pozytywne obowiązki państw związane z zapewnieniem przestrzegania praw pierwszej generacji także w

---

\(^{120}\) Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych z dn. 26.06.1945 (Dz.U. 1947 Nr 23, poz. 90).


relacjach horyzontalnych. Egzemplifikacją tej tendencji może być prawo do poszanowania prywatności, które choć w literaturze przedmiotu zaliczane jest do pierwszej generacji praw człowieka, wiąże się zarówno z obowiązkami negatywnymi, jak i pozytywnymi ze strony władz publicznej.

W doktrynie wskazuje się, że prawa pierwszej generacji łączą się z obowiązkiem natychmiastowego rezultatu, podczas gdy prawa drugiej generacji – z obowiązkiem należytej staranności. Jak zauważa B. Gronowska, taki podział w przypadku praw pierwszej generacji pozwala na stosunkowo łatwe stwierdzenie niewywiązania się przez państwo z obowiązku i w konsekwencji szybkie podjęcie działań prawnych.123 Jednak i ten podział uwypukla głównie wertykalny skutek przypisywany prawom pierwszej generacji, nie oddaje zatem całej ich złożoności.

Istotnym elementem wpływającym na skuteczność każdego systemu ochrony praw podstawowych – zwłaszcza w relacji z władzą publiczną – jest dostępność drogi sądowej. W przypadku umów międzynarodowych funkcję tę pełnią organy kontrolne, powoływane na mocy postanowień traktatowych w celu nadzorowania przestrzegania uzgodnionych norm przez umawiające się strony. Z uwagi na znaczącą ewolucję międzynarodowych systemów ochrony praw człowieka na przestrzeni kilkudziesięciu ostatnich lat w wielu przypadkach organy kontrolne ewoluowały i obecnie mają pozycję oraz uprawnienia zbliżające je do sądów krajowych. Obserwacja ta jest szczególnie aktualna w przypadku Trybunału Sprawiedliwości UE (TSUE), a także – z pewnymi zastrzeżeniami124 – w odniesieniu do Europejskiego Trybunału Praw Człowieka (ETPC).


123 B. Gronowska, Europejska Konwencja Praw Człowieka a prawa drugiej generacji – kilka refleksji o zacieraniu granic, Europejski Przegląd Sądowy 2013, nr 9, s. 4.
124 Należy pamiętać, że jakkolwiek zarówno wyroki TSUE jak i EKPC wiążą państwa, do których są kierowane, to jednak w przypadku EKPC nie mają one skutku erga omnes, związane są także z odmiennym skutkiem z perspektywy spraw rozpatrywanych przed sądami krajowymi.
sądowych, przez co należy rozumieć fakultatywność rozstrzygania sporu oraz brak mocy wiążącej wydanego rozstrzygnięcia. Organy sądowe wydają wiążące wyroki, których adresatami mogą być państwa (strony traktatu). Instytucje należące do tej samej kategorii mogą mieć różne uprawnienia i kompetencje, zależne od szczegółowych uregulowań traktatowych. I tak np. orzeczenia wydawane przez różne międzynarodowe organy sądowe mogą wywierać odmienny skutek na płaszczyźnie prawa krajowego, w tym także mogą wpływać na przebieg konkretnych postępowań zawisłych przed sądami krajowymi.

W niniejszym rozdziale przedstawiono najważniejsze akty prawa międzynarodowego w obszarze ochrony praw człowieka, w których uwzględniono gwarancje związane z ochroną prywatności i których stroną jest Polska. Zostały one omówione nie w kolejności wynikającej z okresu ich powstania czy ratyfikacji, ale w kolejności odzwierciedlającej uniwersalność i powszechność danego aktu. Dlatego w pierwszej kolejności przedstawiony został dorobek prawnego Organizacji Narodów Zjednoczonych, następnie Rady Europy oraz Unii Europejskiej. W każdym przypadku przedstawione zostały nie tylko rozważania dotyczące zarówno treści prawa do prywatności, zakres przedmiotowy i podmiotowy, ale i dopuszczalne zasady limitacji i derogacji oraz funkcjonujące mechanizmy kontrolne wraz z analizą ich wpływu na system prawnym państw-stron poszczególnych umów. Rozważania uzupełniono przedstawieniem norm konstytucyjnych związanych z obszarem ochrony prywatności wynikających z polskiego porządku prawnego.

Celem analizy przedstawionej w niniejszym rozdziale jest próba zrekonstruowania treści prawa do prywatności na podstawie obowiązujących aktów prawnoświatowych oraz przepisów konstytucyjnych. Zdefiniowanie standardów ochrony wynikających z poszczególnych regulacji prawnych pozwoli na określenie ich adekwatności w odniesieniu do zdarzeń mających miejsce w cyberprzestrzeni, a w dalszych rozdziałach dysertacji – na odniesienie do tezy badawczej pracy, a więc weryfikację, czy istniejące akty prawne (krajowe oraz międzynarodowe) mogą prowadzić do skutecznej ochrony praw podstawowych, w szczególności prywatności, w cyberprzestrzeni.

2.2. *Dorobek prawny Organizacji Narodów Zjednoczonych*
2.2.1. *Powszechna Deklaracja Praw Człowieka*

Prawo do ochrony prywatności stało się po raz pierwszy przedmiotem międzynarodowej regulacji w Powszechnej Deklaracji Praw Człowieka (dalej: PDPC)\(^{126}\), uchwalonej przez Zgromadzenie Ogólne ONZ w dniu 10 grudnia 1948 roku.

Deklaracja nie ma charakteru wiążącego, jak jednak wskazano w jej preambule, celem jej uchwalenia jest propagowanie poszanowania praw i wolności jednostki oraz promowanie poprzez środki krajowe i międzynarodowe uznania oraz stosowania postulowanych gwarancji. Dzięki znacznemu wpływowi, jaki Deklaracja wywarła na przepisy konstytucyjne wielu krajów, jej praktyczne oddziaływanie jest znacznie większe, niż wynikałoby to z aktu prawa o charakterze niewiązącym. W nauce prawa wskazuje się, że obecnie PDPC można przypisać charakter prawa zwyczajowego. Jak zauważa J. Symonides, stwierdzenie, że Deklaracja „jest prawem zwyczajowym, ma doniosłe konsekwencje, gdyż oznacza, iż prawa sformułowane w dokumencie wiążą wszystkie państwa, niezależnie od stopnia ratyfikacji i przystąpienia do poszczególnych (tak powszechnych, jak i regionalnych) umów dotyczących praw człowieka”\(^{127}\).

Zgodnie z art. 12 PDPC zakazana jest samowolna ingerencja w czyjokolwiek życie prywatne, rodzinne, domowe ani w jego korespondencję, jak również uwłaczanie jego honorowi lub dobremu imieniu. Ponadto każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji.

Zakres gwarancji wyrażony w art. 12 odzwierciedla powszechne rozumienie celu stanowienia norm ochronnych w obszarze – jako gwarancji przed nieuprawnioną działalnością państwa\(^{128}\). Zakres przedmiotowy gwarancji łączył ponadto ochronę sfery prywatności z ochroną miru domowego, tajemnicą korespondencji oraz ochroną czci i dobrego imienia.

Poza ewolucją rozumienia zakresu prawa do prywatności i wpływu gwarancji z nią związanych na prawidłowe funkcjonowanie społeczeństwa demokratycznego przez lata zmianie ulegał zakres dopuszczalnych ingerencji i wyłączeń. Przyjęte w ar. 29 ust. 2 PDPC kryteria stosowania ograniczenia praw podstawowych – w rozumieniu dzisiejszych

\(^{127}\) J. Symonides, *Powszechna Deklaracja Praw Człowieka (po 60 latach od jej przyjęcia)*, Państwo i Prawo 2008, nr 12, s. 11.
\(^{128}\) W. Osiatyński wskazuje, że prawa i zakazy z minimalnej listy praw człowieka (na której wymienia autonomię w podstawowych kwestiach osobistych) mają chronić jednostkę przed przymusem państwa, jak również stanowić elementarną gwarancję samej zdolności posiadania praw. W. Osiatyński, *Prawa człowieka – uniwersalizm i różnorodność*, Państwo i Prawo 2013, nr 11, s. 111.
standardów prawa międzynarodowego – są szerokie i, obok porządku publicznego, obejmują kategorie takie jak względy moralności czy zapewnienie powszechnego dobrobytu.

2.2.2. Międzynarodowy Pakt Praw Obywatelskich i Politycznych


Gwarancje związane z ochroną prywatności zostały wyrażone w art. 17 ust. 1 MPPOP i wprowadzają zakaz samowolnej lub bezprawnej ingerencji w życie prywatne, rodzinne, dom oraz korespondencję, w tym prowadzące do naruszenia czci i dobrego imienia. Zgodnie z art. 17 ust. 2 Paktu każdy ma prawo do ochrony prawnnej przed tego typu ingerencjami i zamachami. Jak zauważa A. Siostrzonek-Siergiel, prawo to nie ma charakteru absolutnego – skoro bowiem przesłankami negatywnymi jest ingerencja samowolna lub bezprawna, to na zasadzie przeciwieństwa ograniczenie prawa do prywatności, które nie nosi tych cech, jest dopuszczalne132. Jak wskazuje A. Czubik, w trakcie pracy nad tekstem Paktu dyskutowano możliwość włączenia dodatkowego ustępu 3, precyzującego zakres dopuszczalnych ingerencji ze strony państwa133. Ostatecznie rozwiązanie takie nie zostało przyjęte.

133 Proponowana treść art. 3 nawiązywała do funkcji i brzmienia art. 8 ust. 2 EKPC. Postulat wprowadzenia nowego ustępu zgłosiły Dania, Holandia i Irlandia – a więc państwa uczestniczące w systemie europejskiej konwencji. Przeciwnicy tej propozycji – m.in. Stany Zjednoczone – argumentowali, że jej przyjęcie doprowadzi ograniczenia zakresu stosowania art. 17 wyłącznie do relacji wertykalnych oraz pociągałoby za sobą zbyt paraliżowa i zbyt kontrowersyjną w sferę prawadowstwa krajowego. Szerzej: A. Czubik, Prawo do prywatności..., op. cit., s. 264-265.

W komentarzu ogólnym nr 16 dotyczącym prawa do prywatności KPC wskazał, że gwarancje wprowadzone na podstawie art. 17 Paktu powinny przeciwdziałać wszelkim typom naruszeń, nie tylko wynikających z działalności władzy publicznej, ale także związanych z aktywnością innych osób lub podmiotów prywatnych. W efekcie obowiązkiem państwa jest wdrożenie takich przepisów wewnętrznych, które zapobiegną wystąpieniu takich naruszeń\footnote{Komitet Praw Człowieka, *General comment No. 16: Article 17 (Right to privacy)*, http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx, p. 1.}. Postulat ten został wzmocniony w komentarzu ogólnym nr 31, poświęconym ogólnym obowiązkom prawnym nałożonym na strony Paktu, w którym wskazano, że obowiązki dotyczące podstawowych praw człowieka wynikające z Paktu mają skutek *erga omnes*\footnote{Komitet Praw Człowieka, *General comment No. 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx, p. 2.}. Oznacza to w szczególności, że pozytywne obowiązki państw-stron związane z zapewnieniem gwarancji wynikających z Paku mogą być spełnione tylko wtedy, gdy jednostki będą chronione nie tylko przed naruszeniami ze strony władzy publicznej, ale również przed działaniami innych podmiotów lub osób prywatnych\footnote{Ibidem p. 8.}. Skutek *erga omnes* oznacza także zwiąзванie wszystkich organów państwa – a więc nie tylko władzy wykonawczej, ale też prawodawczej i sądowej – w zakresie odpowiedzialności za realizację obowiązków wynikających z Paktu\footnote{Ibidem, p. 4.}. W komentarzu KPC zauważył jednak, że celem przyjęcia Paktu nie było zastąpienie przepisów rangi krajowej oraz że przepisy Paktu jako aktu prawa międzynarodowego nie mają bezpośredniego skutku horyzontalnego.

W komentarzu ogólnym nr 16, Komitet odniósł się do kwestii ochrony prywatności w związku z przetwarzaniem informacji w formie elektronicznej, wskazując, że przetwarzanie takie musi być regulowane przez prawo krajowe. W tym zakresie podkreślono konieczność wprowadzenia adekwatnych zabezpieczeń, praw dla podmiotów danych związanych z możliwością uzyskania informacji o zakresie oraz celu przetwarzania danych osobowych, jak
również prawa do uzupełniania i korekty danych, a w przypadku przetwarzania z naruszeniem obowiązujących przepisów – do żądania sprostowania lub usunięcia danych\(^{139}\).

Komitet Praw Człowieka jest ponadto uprawniony do rozpatrywania zawiadomień składanych przez państwa w związku z nieprzestrzeganiem przez inne państwo postanowień Paktu (skargi międzypaństwowe). Aby sprawa mogła być podjęta, wymagane jest uznanie przez zaangażowane państwa właściwości Komitetu do rozstrzygnięcia sporu. W praktyce oznacza to, że działanie Komitetu bardziej zbliżone jest do organu arbitrażowego niż sądowego – w tym znaczeniu, że jest skoncentrowane na wypracowaniu rozwiązania akceptowalnego przez strony. Jest to cecha funkcjonowania KPC, która zmniejsza jego skuteczność, ponieważ nie pozwala na sprawne rozstrzyganie sporów przy niskim poziomie współpracy ze strony wielu państw. Ponadto rozstrzygnięcia Komitetu nie mają mocy wiążącej. Problem ten został dostrzeżony w nauce prawa i stał się przyczyną dyskusji na temat reformy mechanizmów ochrony praw człowieka funkcjonujących w ramach ONZ w kierunku utworzenia Międzynarodowego Trybunału Praw Człowieka\(^{140}\).

Pozycja prawna Komitetu została rozszerzona wraz z przyjęciem Pierwszego Protokołu Fakultatywnego\(^{141}\), który wprowadzał nową instytucję petycji (skargi) indywidualnej. W rezultacie możliwe stało się dochodzenie praw i gwarancji wynikających z Paktu w przypadku wyczerpania drogi przed sądami krajowymi. Środek ten stał się sposobem na wzmocnienie mechanizmów ochrony praw podstawowych oraz propagowanie dobrych standardów wśród państw-stron układu.

Dorobek orzeczniczy KPC w obszarze ochrony prywatności obejmuje wszystkie dobra wymienione w art. 17 Paktu\(^{142}\), w szczególności życie prywatne\(^{143}\), życie rodzinne\(^{144}\), nienaruszalność domu\(^{145}\), ochrona domu\(^{146}\) oraz korespondencji\(^{147}\). W sprawie *Toonen v*

\(^{139}\) Ibidem, p. 10.


\(^{141}\) Protokół fakultatywny do Międzynarodowego paktu praw obywatelskich i politycznych (Dz.U. 1994 Nr 23, poz. 80).


\(^{146}\) Decyzja KPC z 29.10.19981 w sprawie *Pinkney v. Kanada*, sygn. 27/1977; decyzja KPC z 29.03.1983 r. w sprawie *Estrella v. Urugwaj*, sygn. 74/1980.
Australia - Komitet, rozważając zakres dopuszczalnych wyłączeń przewidzianych w art. 17 MPPOP, nie podzielił poglądu, że kwestia ochrony moralności należy do obszarów wyłącznych prawa krajowego. Jak zauważono, przyjęcie takiego rozwiązania mogłoby doprowadzić do znacznego ograniczenia gwarancji związanych z prawem do prywatności. W tym zakresie Komitet wskazał na pogląd przedstawiony w komentarzu ogólnym nr 16, zgodnie z którym każda ingerencja w prawo do prywatności, nawet wynikająca z obowiązującego prawa, musi być zgodna z postanowieniami, przedmiotem i celem Paktu, a także w każdym przypadku pozostawać proporcjonalna do okoliczności. Zauważając, że przepisy prawa krajowego stanowiące przedmiot skargi nie były skutecznie egzekwowane przez władze państwowe, Komitet stwierdził, że nie można ich uznać za konieczne dla ochrony moralności, a zatem nie spełniają kryterium proporcjonalności, bowiem prowadzą do nieuzasadnionego ograniczenia prawa do ochrony prywatności.

Z kolei w sprawie van Hulst v. Holandia Komitet zajął się sprawą stosowania kontroli połączeń telefonicznych w toku postępowania karnego oraz trybu postępowania w przypadku zarejestrowania rozmów pomiędzy adwokatem a jego klientem. Na tym tle przedstawiono rozwiązania na temat możliwości zajęcia usunięcia danych, a w szczególności możliwości zajęcia usunięcia danych zgromadzonych w toku czynności operacyjnych, które z uwagi na swój charakter nie mogą zostać wykorzystane w postępowaniu karnym, a więc ich użycie zgodnie z celem, w jakim zostały zgromadzone jest niemożliwe. KPC zauważył, że w omawianej sytuacji wystarczające jest wyłącznie oddzielenie kwestionowanych nagrań od akt sprawy, ich fizyczne zniszczenie nie jest konieczne, bowiem może utrudnić późniejszą kontrolę poprawności prowadzenia dochodzenia.

Poza publikowaniem komentarzy ogólnych oraz rozpatrywaniem skarg międzypaństwowych i indywidualnych Komitet zajmuje się też analizą corocznych sprawozdań składanych przez państwa. Na podstawie art. 40 ust. 1 MPPOP strony Paktu zostały zobowiązane do przedkładania sprawozdań na temat środków przedsięwziętych w celu realizacji praw gwarantowanych Paktu oraz postępu dokonanego w dziedzinie korzystania z tych praw. Komitet poza badaniem sprawozdań ma prawo kierowania swoich uwag i rekomendacji związanych z rozpatrywanymi sprawami. Uprawnienie to jest często

151 Ibidem, p. 7.9.
wykorzystywane także w zakresie badania spraw dotyczących ochrony prywatności w związku z przetwarzaniem danych w systemach informatycznych. Przykładem mogą być kontrowersje dotyczące systemu EDVINE (fr. Exploitation Documentaire et Valorisation de l’Information Générale), który według informacji opublikowanych w 2008 roku służył do gromadzenia rozbudowanego zakresu danych osobowych (w tym danych sensytywnych – związanych z orientacją seksualną czy poglądami politycznymi) na temat osób przebywających we Francji będących obiektem zainteresowania służb specjalnych. Komitet w swoim sprawozdaniu z dnia 22 lipca 2008152 zauważył, że funkcjonalnie system EDVINE może prowadzić do naruszenia art. 17 Paktu. Komitet wskazał na wcześniejsze rekomendacje zawarte w komentarzach ogólnych a także przedstawił listę szczegółowych wytycznych, które powinny być rozważone przez władze francuskie153.

2.2.3. Pozycja MPPOP w krajowym systemie prawnym

Zgodnie z polskim porządkiem konstytucyjnym MPPOP jako ratyfikowana umowa międzynarodowa stanowi część krajowego porządku prawnego i jest bezpośrednio stosowalna154. Jak przy tym wskazuje się w doktrynie, dla bezpośredniej skuteczności unormowań umowy międzynarodowej nie ma znaczenia przyjęty tryb jej ratyfikacji. Ma on natomiast znaczenie dla określenia zasad pierwszeństwa w przypadku kolizji z ustawą155. Zgodnie z art. 91 ust. 1 Konstytucji umowa międzynarodowa ratyfikowana za uprzednią zgodą wyrażoną w ustawie ma pierwszeństwo przed ustawą, jeżeli ustawy tej nie da się pogodzić z umową. Jak ponadto potwierdził Naczelny Sąd Administracyjny, umowy ratyfikowane bez upoważnienia ustawy w przypadku kolizji norm ustępują swą skutecznością ustawie, ale mają pierwszeństwo przed innymi aktami prawnymi156.

Pakt został ratyfikowany w 1977 roku, a więc pod rządami Konstytucji z dnia 22 lipca 1952, zgodnie z którą ratyfikacja umów międzynarodowych była wyłączną prerogatywą Rady Państwa i czynność ta nie wymagała zgody parlamentu. W przypadku kolizji norm Paktu oraz prawa krajowego nie może mieć więc wprost zastosowania art. 91 ust. 2 Konstytucji.

Aby uniknąć niejasności interpretacyjnych, ustrojodawca wprowadził przepis przejściowy art. 241 ust. 1. Zgodnie z nim umowy międzynarodowe wcześniej ratyfikowane

153 Ibidem, p. 22.
154 Por. art. 91 ust. 1 Konstytucji Rzeczypospolitej Polskiej (Dz.U. 1997 Nr 78, poz. 483 ze zm.).
156 Wyrok NSA z 29.12.1999, sygn. I SA/Po 3057/98, ONSA 2001, nr 1, poz. 34..
na podstawie obowiązujących w czasie ich ratyfikacji przepisów konstytucyjnych i ogłoszone w dzienniku urzędowym uznaje się za umowy ratyfikowane za uprzednią zgodą wyrażoną w ustawie i stosuje się do nich przepisy art. 91 Konstytucji, jeżeli z treści umowy międzynarodowej wynika, że dotyczą one kategorii spraw wymienionych w art. 89 ust. 1 Konstytucji. Wśród kategorii wskazanych w art. 89 ust. 1 wskazany zostały między innymi obszar wolności, praw lub obowiązków obywatelskich określonych w Konstytucji.

Reasumując, w obecnym stanie prawnym MPPOP jest aktem funkcjonującym w porządku prawnym RP z pierwszeństwem przed krajowymi przepisami rangi ustawowej. Kwestią sporną w doktrynie jest, na ile pierwszeństwo to ma zastosowanie także w przypadku kolizji z przepisami rangi konstytucyjnej. Zgodnie z dominującym poglądem157, znajdującym potwierdzenie również w judykaturze158, ratyfikowane umowy międzynarodowe są usytuowane poniżej przepisów konstytucyjnych, z którymi muszą być zgodne.

Omówienia wymaga kwestia praktycznego wpływu przystąpienia Polski do Paktu w obszarze wzmocnienia ochrony podstawowych praw i wolności człowieka. Wiarygodnym sposobem dokonania tej oceny jest analiza dorobku orzecznego polskich sądów, w których jako wzorzec kontroli wskazano przepisy Paktu. W odpowiedzi na okresowe sprawozdanie rządu polskiego KPC wystosował 15 kwietnia 2010 roku dodatkowe pytania, z których jedno dotyczyło zaprezentowania informacji na temat przykładowych orzeczeń, w których sądy krajowe zastosowały jako wzorzec kontroli MPPOP159. W przesłanej odpowiedzi rząd wskazał pięć orzeczeń, w tym dwa Trybunału Konstytucyjnego oraz po jednym Sądu Najwyższego, Naczelnego Sądu Administracyjnego oraz Sądu Apelacyjnego w Warszawie160.

W krajowym orzeczniectwie MPPOP wskazywany jest jako wzorzec kontroli w różnych typach spraw dotyczących materii prawa karnego – między innymi prawa do obrony161, sprawiedliwego procesu, zakazu ponownego karania za to samo przestępstwo162 - ale i spraw z zakresu wolności sumienia163 czy możliwości objęcia funkcji członka zarządu w spółce kapitałowej164. W zakresie ochrony praw wynikających z art. 17 MPPOP na uwagę zasługują rozwiązania Trybunału Konstytucyjnego dotyczące kolizji norm związanych z

159 Komitet Praw Człowieka, List of issues to be taken up in connection with the consideration of the sixth periodic report of Poland, 15.04.2010, sygn. CCPR/C/POL/Q/6, p. 2.
160 Replies of the Government of Poland to the list of issues (CCPR/C/POL/Q/6) to be taken up in connection with the consideration of the third periodic report of Poland (CCPR/C/POL/6), 20.07.2010, sygn. CCPR/C/POL/Q/6/Add.1, s. 3.
161 Wyrok SN z 8.03.2007, sygn. V KK 200/06, Legalis 108255.
162 Por. wyroki TK w sprawach sygn. K 6/14, OTK-A 2016, poz. 98; P 29/09, OTK-A 2010, nr 9, poz. 104.
164 Wyrok WSA w Warszawie z 13.07.2010, sygn. VI SA/Wa 647/10, Legalis 565700.
wolnością wypowiedzi oraz ochroną dóbr osobistych, do których zgodnie z art. 23 kc zalicza się także sferę prywatności człowieka. Jak zauważył TK w wyroku z 30 października 2006, ochrona dobrego imienia powinna stanowić przesłankę do ograniczenia wolności wypowiedzi. Szczególnie interesującą jest jednak obserwacja poczyniona w dalszej części orzeczenia, w której sąd konstytucyjny wskazał na redakcję art. 17 Paktu, nie dopuszczającą możliwości wprowadzenia ograniczenia ochrony przed „zamachami na cześć lub dobre imię” z uwagi na wolność słowa czy wolność prasy. Co więcej, w ocenie TK zgodnie z art. 5 Paktu nie można domniemywać, że wolność słowa może w ogóle ograniczać ochronę dobrego imienia i czci. Na tej podstawie Trybunał uznał, że z MPPOP wynika, iż ochrona dóbr osobistych powinna mieć priorytet przed ochroną wolności słowa.

Należy odnotować także pogląd odmienny, obecny zwłaszcza w orzecznictwie sądów powszechnych – prowadzący do braku przyznania pierwszeństwa poszczególnym prawom zagwarantowanym w Pakcie. Jako przykład można wskazać wyrok SA z Gdańska z 25 kwietnia 2006, w którym na tle rozważań dot. art. 17 i art. 19 MPPOP wskazano, że oba prawa należą do praw podstawowych, dla funkcjonowania demokratycznego państwa jednak żadne z nich nie ma charakteru nadrzędnego wobec drugiego, jak również charakteru absolutnego. Sąd uznał, że za każdym razem, gdy dochodzi do kolizji obu norm, konieczne jest przeanalizowanie wszystkich okoliczności danej sprawy aby ustalić, czy w danym przypadku badane działanie mieściło się w granicach wolności wypowiedzi, czy też tę granicę przekraczało prowadząc do nieuprawnionej ingerencji w sferę prywatności powoda.

Zaznaczony powyżej problem, związany z kolizją gwarancji związanych z poszanowaniem życia prywatnego z innymi prawami podstawowymi, jest szczególnie aktualny w zakresie problematyki ochrony prywatności w mediach elektronicznych.

Globalny charakter sieci Internet wymaga, aby standaryzacja i normy prawne jej dotyczące były także wprowadzane w sposób ponadregionalny. Z uwagi na wiążący charakter postanowień Paktu, a także fakt, że stanowi on obecnie najpowszechniej stosowaną umowę międzynarodową gwarantującą podstawowe prawa człowieka, wydaje się słuszne, aby stał się on podstawą do dalszego rozbudowania mechanizmów prawnych dotyczących ochrony prywatności w cyberprzestrzeni. Aby tak się jednak stało, konieczne będzie przezwyciężenie na forum międzynarodowym najpoważniejszych niedoskonałości Paktu, związanych między

---


166 Wyrok TK z 30.06.2006, sygn. P 10/06, OTK-A 2006, nr 9, poz. 128.

167 Wyrok Sądu Apelacyjnego w Gdańsku z 25.04.2006, I ACa 1877/05.
innymi z brakiem nadania KPC kompetencji organu sądowego czy dobrowolnością uczestniczenia państw w procedurze rozstrzygania sporów\textsuperscript{168}.

### 2.3. Europejska Konwencja Praw Człowieka

#### 2.3.1. Geneza traktatu i zakres ochrony prywatności

Efektem kodyfikacji podstawowych praw wynikających z PDPC na płaszczyźnie europejskiej jest Konwencja o ochronie praw człowieka i podstawowych wartości\textsuperscript{169}, znana w literaturze przedmiotu także jako Europejska Konwencja Praw Człowieka (EKPC). Została ona otwarta do podpisu 4 listopada 1950 roku, a więc w rok po powołaniu Rady Europy\textsuperscript{170}, natomiast weszła w życie po uzyskaniu wymaganej liczby ratyfikacji 3 września 1953 roku.

Jednym z praw wprowadzonych w rozdziale II traktatu, poświęconym podstawowym prawom i wolnościami, jest prawo do poszanowania życia prywatnego i rodzinnego. Zgodnie z art. 8 ust. 1 EKPC każdy ma prawo do poszanowania życia prywatnego i rodzinnego, swojego mieszkania oraz korespondencji.

Jako wskazuje L. Garlicki, sfery chronione przez art. 8 nakładają się w pewnym zakresie na siebie łącznie, tworząc rozbudowany obszar szczegółowych praw i wolności jednostki, a także – odpowiadających im – negatywnych i pozytywnych obowiązków władzy publicznej\textsuperscript{171}. Z kolei L. Leszczyński zaznacza, że regulacja wyróżnia obok strefy prywatności rozumianej wprost także sferę odnoszącą się do stosunków rodzinnych, mieszkania oraz korespondencji\textsuperscript{172}. Podobnie zatem jak w przypadku MPPO twórcy EKPC – zamiast próbować wprowadzić jednolitą i zamkniętą prawną definicję prywatności – zdecydowali się na wskazanie katalogu dóbr, przez które należy interpretować zakres terminu.

\begin{footnotesize}
\textsuperscript{168} A. Gliszczyńska-Grabias, K. Sękowska-Kozłowska, R. Wieruszewski, \textit{Koncepcja ..., op. cit.}, s.5-6.
\textsuperscript{169} Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dn. 4.11.1950 (Dz.U. 1993 Nr 61, poz. 284).
\textsuperscript{170} Z uwagi na tragiczne doświadczenia II wojny światowej problematyka uwzględnienia podstawowych praw człowieka w fundamencie nowotworzonego porządku politycznego była szczególnie aktualna w Europie. W efekcie już w 1949 roku dziesięć krajów Europy Zachodniej utworzyło Radę Europy – organizację międzynarodową, której jednym z celów było „przestrzeganie i rozwój praw człowieka i podstawowych wolności” (zob. art. 1 pkt b Statutu Rady Europy z dn. 5.05.1949 r., Dz.U. 1994 Nr 118, poz. 565). Zgodnie z przekonaniem państw-założycieli RE, wyrażonym w preambule do statutu „utrwalenie pokoju oparte na sprawiedliwości i współpracy międzynarodowej ma podstawowe znaczenie dla przetrwania społeczności ludzkiej i cywilizacji”. Słuszne zatem jest stwierdzenie, że jednym z fundamentów, na bazie których budowany był bogaty dorobek prawnego RE, była ochrona praw człowieka i podstawowych wolności.
\textsuperscript{172} L. Leszczyński, B. Liżewski, \textit{Ochrona praw człowieka w Europie – szkie zagadnienia podstawowych}, Oficyna Wydawnicza Verba 2008, s. 88.
\end{footnotesize}
Biorąc pod uwagę cel aktu (standaryzacja i wprowadzenie jednakowych gwarancji w obszarze praw podstawowych), podejście takie trzeba uznać za słuszne i pozwalające uniknąć późniejszych problemów interpretacyjnych. Należy także zauważyć, że inaczej niż w przypadku MPPO zakres dóbr podlegających ochronie wskazanych w art. 8 EKPC nie obejmuje prawa do ochrony przed zamachami na cześć i dobre imię człowieka. W literaturze przedmiotu trwa dyskusja, czy fakt ten należy interpretować jako brak objęcia wskazanych obszarów ochroną wynikającą z Konwencji, czy – biorąc pod uwagę otwarty katalog wartości składających się na sferę prywatności – kwestia ochrony dobrego imienia jest też objęta zakresem gwarancji, pomimo braku jej wskazania \textit{expressis verbis} w treści normy\textsuperscript{173}.

M. Pryciak podkreśla, że prawo do ochrony prywatności w kształcie nadanym w art. 8 EKPC nierzerwalnie łączy się z innymi prawami Konwencji, w szczególności prawem do ochrony życia (art. 2), zakazem stosowania tortur oraz nieludzkiego i poniżającego traktowania i karania (art. 3), zakazem niewolnictwa i pracy przymusowej (art. 4) czy prawem do wolności i bezpieczeństwa osobistego (art. 5)\textsuperscript{174}.

W myśl art. 8 ust 2 EKPC niedopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa do prywatności, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. W treści przepisu na pierwszy plan należy wysunąć kwestię „konieczności w demokratycznym społeczeństwie”, która ma fundamentalne znaczenie dla zrozumienia możliwości zastosowania środków ograniczających prawo do prywatności przez władzę publiczną.

\subsection{2.3.2. Ewolucja i dorobek orzeczniczy ETPC}

Poza wprowadzeniem katalogu praw i wolności, przysługującym wszystkim podlegającym jurysdykcji państwa-strony Konwencji, EKPC rozszerzona została o ustanowienie Europejskiego Trybunału Praw Człowieka (ETPC) – mechanizmu kontrolnego, mającemu zapewnić przestrzeganie zobowiązań wynikających z Konwencji\textsuperscript{175}. Bogate

\textsuperscript{173} Por. A. Siostrzonek-Sergiel, \textit{Prawo do prywatności...}, op. cit., s. 409 i przytoczona tam literatura.

\textsuperscript{174} M. Pryciak, \textit{Prawo do prywatności}, Studia Erasmiana Wratislaviensia 2010, nr 4, s. 220.

\textsuperscript{175} Pierwotnie sposób funkcjonowania organu kontrolnego (sądowniczego) zorganizowany był odmiennie niż dzisiaj. Treść Konwencji przewidywała ustanowienie dwóch instytucji odpowiedzialnych za rozpatrywanie skarg – Europejskiej Komisji Praw Człowieka (EKPCz), której głowna rola dotyczyła rozpatrywania skarg indywidualnych oraz międzypaństwowych, oraz Europejskiego Trybunału Praw Człowieka (ETrPC) – rozpatrującego skargi międzypaństwowe, które zostały przekazane mu do rozpatrzenia po zakończeniu prac w Komisji. Kognicja Trybunału dotyczyła wyłącznie spraw międzypaństwowych i tylko takich, w których
orzecznictwo ETPC przyczyniło się do ukształtowania oraz ugruntowania prawnego rozumienia zakresu, granic oraz możliwości limitacji prawa do prywatności w kulturze prawnej państw-stron Konwencji.

Trybunał podzielił pogląd, że prywatność jest szerokim pojęciem, w którym nie można zastosować wyczerpującej definicji prawnej. W opinii Trybunału ważnymi elementami sfery życia osobistego, chronionej przez art. 8, jest tożsamość, przynależność etniczna czy orientacja seksualna. Ponadto w wyroku von Hannover v. Niemcy ETPC wskazał, że obszar życia prywatnego obejmuje aspekty związane z identyfikacją osoby, takie jak nazwisko, zdjęcie, integralność fizyczna i psychiczna. Celem gwarancji przewidzianych w art. 8 jest umożliwienie niezakłóconego rozwoju osobistego jednostki w ramach społeczeństwa. Dlatego, jak wskazał Trybunał, nawet niektóre działania podejmowane przez jednostkę w domenie publicznej mogą korzystać z ochrony przewidzianej dla czynności życia prywatnego.

Z kolei w sprawie Botta v. Włochy Trybunał zauważył, że chociaż zasadniczy cel art. 8 stanowi zapewnienie jednostce ochrony przed arbitralną ingerencją władz publicznych, nie oznacza to, że zakres normy powinien być sprowadzony wyłącznie do nakazu wyroku ETrPC.


177 Wyrok ETPC z 2.09.2010 w sprawie Uzun v. Niemcy, sygn. 35623/05, § 43.
178 Wyrok ETPC z 17.07.2003 w sprawie Perry v. Wielka Brytania, sygn. 63737/00, § 36.
179 Wyrok ETPC z 7.02.2012 w sprawie von Hannover v. Niemcy, sygn. 40660/08 i 60641/08.
180 Ibidem, § 95.
powstrzymywań się organów państwowych od tego rodzaju ingerencji. Równie ważnym obowiązkiem jest konieczność wdrożenia środków mających na celu zapewnienie poszanowania życia prywatnego w sferze relacji horyzontalnych. W sprawie Đorđević v. Chorwacja Trybunał uzupełnił powyższy pogląd konkluzją, że do pozytywnych obowiązków państwa należy zapewnienie ochrony integralności moralnej jednostki przed działaniami innych osób. Natomiast w sprawie K.U. v. Finlandia Trybunał zauważył, że chociaż dobór środków stosowanych w celu ochrony prywatności należy do marginesu uznania poszczególnych państw, to jednak w przypadku ochrony przed działaniami ingerującymi w fundamentalne wartości i kluczowe aspekty ochrony prywatności wdrożone powinny zostać skuteczne rozwiązania z zakresu prawa karnego.

ETPC odnosił się także do poszczególnych aspektów związanych z ochroną prywatności w związku z przetwarzaniem danych osobowych. W sprawie Segerstedt-Wiberg i in. v. Szwecja Trybunał wskazał na jakość danych oraz ich przydatność do realizacji celu przetwarzania jako przesłankę uznania, czy dane mogą być nadal przetwarzane zgodnie z prawem. Podkreślając wymaga fakt, że przedstawione rozważania dotyczyły danych gromadzonych przez uprawnione organy w celu zapobiegania przestępcstwom i ochrony porządku publicznego. Natomiast w wyroku Marper v. Wielka Brytania Trybunał wprost wskazał, że krajowy prawodawca powinien wprowadzić regulacje zapewniające, że przetwarzanie danych osobowych będzie realizowane w sposób zgodny z gwarancjami wynikającymi z art. 8. Jak podkreślono w wyroku, potrzeba zastosowania mechanizmów prawnych jest większa w przypadku wykorzystania automatycznych środków przetwarzania danych. Prawo krajowe powinno zapewniać, że zakres gromadzonych danych jest adekwatny do zamierzonego celu, a sposób ich przechowywania pozwalają na identyfikację podmiotu danych tylko przez czas, jaki jest konieczny z uwagi na cel przetwarzania. Z kolei w sprawie M.S. v. Szwecja Trybunał uznał, że ochrona danych osobowych – a w szczególności danych medycznych – ma podstawowe znaczenie dla zapewnienia gwarancji ochrony życia prywatnego i rodzinnego w zakresie przewidzianym art. 8 EKPC. W efekcie zapewnienie

182 Ibidem, § 33.
184 Ibidem, § 152.
186 Ibidem, § 43.
187 Wyrok ETPC z 6.06.2006 w sprawie Segerstedt-Wiberg i in. v. Szwecja, sygn. 62332/00.
189 Wyrok ETPC z 27.08.1997 w sprawie M. S. v. Szwecja, sygn. 20837/92.
poufności danych dotyczących stanu zdrowia jest kluczowym warunkiem, jaki powinien być zapewniony w krajowych regulacjach prawnych państw stron Konwencji.

Trybunał w swoim dorobku orzecznym zajmował się problematyką tajemnicy korespondencji, także w obszarze komunikacji elektronicznej. W interesującym wyroku *Copland v. Wielka Brytania* Trybunał uznał, że z ochrony wynikającej z art. 8 korzysta każda forma komunikacji, przy której jednostka może mieć uzasadnione poczucie prywatności. W szczególności, zakresem ochrony są objęte rozmowy telefoniczne czy e-maile wysłane z miejsca pracy, jeżeli użytkownik wcześniej nie został poinformowany o możliwości stosowania technik monitorowania przekazu i obowiązku wykorzystywania środków łączności wyłącznie do celów służbowych.

Z orzecznictwa Trybunału wynika też wniosek, że zarówno gromadzenie, udostępnianie informacji dotyczących życia prywatnego przez władzę publiczną, jak i odmowa usunięcia tych danych prowadzą do ingerencji w gwarancje wynikające z art. 8 ust. 1. Do ingerencji prowadzi każde systematyczne gromadzenie danych przez służby bezpieczeństwa, nawet jeżeli dane te nie są efektem zastosowania technik kontroli operacyjnej.

Nie każda ingerencja oznacza jednak naruszenie zobowiązań konwencyjnych. W szczególności nie jest nią ingerencja spełniająca kryteria określone w art. 8 ust. 2 EKPC – a więc zgodna z prawem i konieczna w społeczeństwie demokratycznym. W przypadku stwierdzenia ingerencji konieczne jest zatem zbadanie łącznego wystąpienia obu przesłanek pozytywnych – pamiętając przy tym, że z uwagi na charakter przepisu, wprowadzającego ograniczenie prawa gwarantowanego Konwencją, muszą być one interpretowane zawężająco.

W sprawie *Kruslin v. Francja* Trybunał uznał, że określenie „za wyjątkiem przypadków przewidzianych przez ustawę” wskazane w art. 8 ust. 2 wymaga nie tylko, aby środki ograniczające prawo do prywatności wynikały z powszechnie obowiązującego prawa, ale i były zgodne zasadą rządów prawa. Z tego powodu przepisy krajowe muszą być przystępne dla jednostki oraz zapewniać przewidywalność, rozumianą w tym kontekście jako odpowiednią ochronę przed arbitralnością. W przypadku stosowania przez państwo środków...

---

190 Ibidem, § 41.
191 Wyrok ETPC z 3.04.2007 w sprawie *Copland v. Wielka Brytania*, sygn. 62617/00.
192 Ibidem, § 41-42.
194 Wyrok ETPC w sprawie *Uzun v. Niemcy*, ..., § 46.
195 Tak: wyrok ETPC w sprawie *Rotaru v. Rumunia*, ..., § 47.
inwigilacyjnych oznacza to, że nadzór nad działaniem upoważnionych organów musi wynikać z przepisów prawa i nie może wiązać się z nieograniczoną swobodą podejmowania decyzji – także przez organy sądowe\textsuperscript{197}.

Dopiero w przypadkach, gdy spełniony jest warunek zgodności z prawem krajowym w powyższym rozumieniu, zasadne jest badanie drugiej przesłanki stosowania ograniczenia, a zastosowany środek musi być proporcjonalny do zamierzonego i uzasadnionego prawnie celu. Dodatkowo Trybunał podkreślił, że zakres swobody decyzyjnej państwa co do doboru środka nie może być podyktowany tylko osiągnięciem zamierzonego celu, ale również powinien uwzględniać naturę prawa, na które oddziałuje\textsuperscript{200}. Zasada ta była wielokrotnie potwierdzana przez Trybunał, przyczyniając się do utworzenia ugruntowanej linii orzeczniczej, zgodnie z którą tylko środek spełniający zasadę proporcjonalności (adekwatności stopnia inwaginości do zamierzonego celu) oraz konieczności (braku możliwości osiągnięcia celu w inny, mniej inwazyjny sposób) można uznać za uzasadniony w demokratycznym społeczeństwie.

Omawiając dorobek orzeczniczy ETPC, nie sposób pominać problemu stale rosnącej przewlekłości postępowania, wpływającej niekorzystnie na praktyczną przydatność drogi skargowej do ochrony praw i wolności osobistych. Każda propozycja zmierzająca do zapewnienia prawnomiedzynarodowej ochrony praw podstawowych w cyberprzestrzeni musi uwzględniać nie tylko problemy jurysdykcyjne czy dotyczące skutków wydawanych orzeczeń w krajowych systemach prawnym, ale także związane z faktyczną dostępnością prawnych środków ochrony wynikającą z okresu niezbędnego na wydanie prawomocnego orzeczenia. W tym zakresie, pomimo szeregu reform, nie udało się osiągnąć poziomu zadowalającego\textsuperscript{201}.

---

\textsuperscript{197} Postanowienie ETPC z 29.06.2006 w sprawie Weber i Saravia v. Niemcy, sygn. 54934/00, § 92-94.

\textsuperscript{198} Wyrok ETPC w sprawie Rotaru v. Rumunia..., § 62.

\textsuperscript{199} Wyrok ETPC z 14.09.1987 w sprawie Gillow v. Wielka Brytania, sygn. 9063/80.

\textsuperscript{200} Ibidem, § 55.

\textsuperscript{201} Przyczyn należy upatrywać w dużej liczbie napływających skarg oraz rozszerzeniu RE o nowe państwa, w których często system prawny odbiega od wypracowanych standardów europejskich – czego efektem jest brak możliwości skutecznego rozstrzygnięcia sprawy na etapie krajowym. Problem ten jest dobrze rozpoznanej w literaturze przedmiotu. Jak wskazuje L. Garlicki, w latach sześćdziesiątych dwudziestego wieku oba organy kontrolne (Komisja oraz Trybunał) wydały łącznie 64 rozstrzygnięcia, w latach siedemdziesiątych liczba ta wzrosła do niemal 200. Łącznie w latach 1959-1998 wydano 837 wyroki. Wraz z wejściem w życie postanowień Protokołu 11, reformującego mechanizmy kontrolne Konwencji, liczba ta zaczęła dynamicznie wzrastać, do poziomu 1625 wyroków wydanych w samym tylko 2005 roku ( Overview 1959-2016, ETPC 2017, http://cli.re/gzBWmw, s. 4). Liczba skarg zmalała po roku 2010, co należy łączyć z wejściem w życie Protokołu nr 14, jednak nadal oscyluje wokół liczby ok. 1000 wyroków rocznie. O popularności tej formy ochrony praw może świadczyć fakt, że do roku 2016 rozstrzygniętych merytorycznie przez Trybunał zostało ponad 700 000 skarg. Z jednej strony liczba ta może świadczyć, że Trybunał jest
2.3.3. Pozycja EKPC w krajowym systemie prawnym

Konwencja nie reguluje wprost relacji z krajowym porządkiem prawnym, a więc kwestia ta pozostaje do rozstrzygnięcia przez państwa-strony. W przypadku niektórych państw Konwencja ma status przepisów rangi konstytucyjnej (Austria), podczas gdy w innych ustawy zwyklej (Niemcy). Dominuje jednak model, w którym Konwencja jako umowa międzynarodowa znajduje się w hierarchii aktów prawnych pomiędzy konstytucją a przepisami rangi ustawowej. Rozwiązanie takie funkcjonuje także w polskim systemie prawnym. Podobnie jak w przypadku Międzynarodowego Paktu Praw Obywatelskich i Politycznych Konwencja stanowi część krajowego porządku prawnego (art. 91 ust. 1 Konstytucji) i jako ratyfikowana umowa międzynarodowa w przypadku kolizji norm korzysta z pierwszeństwa przed ustawami zwykłymi (art. 91 ust. 2 w zw. z art. 241 ust. 1 Konstytucji).

Zgodnie z zasadą wyrażoną w art. 46 Konwencji państwa członkowskie są zobowiązane do przestrzegania ostatecznych wyroków Trybunału, w których są stronami. Wyrok Trybunału tworzy zatem zobowiązanie prawnomiędzynarodowe państwa związane z usunięciem stwierdzonego naruszenia Konwencji, przy czym sposób realizacji tego celu – jeżeli nie został wskazany w sentencji orzeczenia – pozostaje w obszarze regulacji krajowych systemów prawnych. Co do zasady wyrok nie jest adresowany erga omnes, a więc jego wydanie nie rodzi skutków w innych sprawach jednostkowych zawisłych przed sądami krajowymi, jak i obowiązków po stronie innych państw-stron Konwencji. W orzecznictwie Trybunału podkreśla się, że jego wyroki mają charakter przede wszystkim deklaratyjny i w zakresie stwierdzenia naruszenia Konwencji korzystają z powagi rzeczy osądzonej. Jak wskazał Sąd Najwyższy w postanowieniu z dnia 17 kwietnia 2007 roku, moc wiążąca wyroków ETPC wyraża się tym, że w granicach, w jakich orzeczenie Trybunału ma moc wiążącą, państwo nie może kontestować tego, że do naruszenia Konwencji doszło, a ponadto państwo jest prawnie obowiązane przedsięwziąć określone kroki w celu zadośćuczynienia

---


203 Wyrok ETPC z 30.07.2009 w sprawie VgT v. Szwajcaria, sygn. 32772/02, § 61.

wyrokowi. W literaturze przedmiotu podkreśla się, że wyroki ETPC nie wywołują bezpośredniego skutku o kasacyjnym czy reformacyjnym charakterze, a więc nie prowadzą do uchylenia wyroku krajowego, a jedynie stanowią przesłankę do wznowienia postępowania oraz zmiany wcześniejszego rozstrzygnięcia. Dopóki to jednak nie nastąpi, wyrok krajowy zachowuje swoją moc wynikającą z przepisów wewnętrznych.

W polskiej procedurze karnej kwestia wznowienia postępowania w przypadku wydania wiążącego rozstrzygnięcia organu międzynarodowego wynika między innymi z przepisu art. 540 § 3 kpk. Przy czym, jak orzekł Sąd Najwyższy – Izba Karnia w uchwale z 26 czerwca 2014 wskazany przepis powinien być interpretowany w ten sposób, że stanowi przesłankę nie tylko dla wznowienia postępowania w określonej sprawie jednostkowej, której dotyczył wyrok organu międzynarodowego, ale w każdej sprawie, w której układ okoliczności faktyczno-prawnych jest tożsamy z tym, który stanowił podstawę do stwierdzenia naruszenia Konwencji w sprawie rozpoznawanej przez Trybunał.

Z kolei w zakresie procedury cywilnej Sąd Najwyższy – Izba Cywilna w uchwale z 30 listopada 2010 roku uznał, że ostateczny wyrok ETPC, w którym stwierdzono naruszenie prawa do sprawiedliwego rozpatrzenia sprawy przez sąd (art. 6 ust. 1 Konwencji), nie stanowi samoistnej podstawy wznowienia postępowania cywilnego. Rozważania sądu oparte były na obserwacji, że sama Konwencja nie wiąże wydania wyroku Trybunału z bezwzględną koniecznością wznowienia postępowania na poziomie krajowym, a ponadto ustawodawca nie przewidział takiej podstawy w obowiązujących przepisach procedury cywilnej. Ponadto, w ocenie Sądu, obowiązkowi wznowienia postępowania we wszystkich przypadkach może także przeciwstawiać się konieczność respektowania powagi rzeczy osądzonej i tkwiącej u jej podstawy zasad stabilności prawnej, a także ochrona nabytego w dobrej wierze prawa przez stronę przeciwną. Sąd Najwyższy w podjętej uchwale wyraził pogląd, że w wielu wypadkach podstawą wydania wyroków Trybunału są okoliczności niezwiązane z orzecznictwem sądowym (np. sprzeczne z Konwencją prawo krajowe), których skutków nie da się uchylić na drodze sądowej.

---

206 Por. także wyrok ETPC, sygn. 32772/02, p. 89.
207 Ustawa z 6 czerwca 1997 – Kodeks postępowania karnego (Dz.U. Nr 89, poz. 555 ze zm.).
2.4. Karta Praw Podstawowych Unii Europejskiej

2.4.1. Ewolucja ochrony praw podstawowych w prawie WE/UE

Chociaż obszar praw podstawowych nie był – z nielicznymi wyjątkami – przedmiotem postanowień Traktatu ustanawiającego EWG, stał się on tematem rozważań Trybunału Sprawiedliwości wskutek rozpoznania spraw, w których podnoszony był zarzut naruszenia praw człowieka. We wczesnym orzecznictwie TSUE dominował pogląd, że prawa człowieka jako niewynikające wprost z norm traktatowych nie podlegają ochronie przez Trybunał.

W sprawie Stork\(^{210}\) Trybunał uznał, że jego obowiązkiem jest wyrokowanie na podstawie traktatów i stanowionego w oparciu o nie prawa wtórne, bez sięgania do przepisów krajowych. Ponadto w ocenie Trybunału także Wysoka Władza (poprzedniczka Komisji Europejskiej), przeciwno działaniom której skierowano skargę, nie była uprawniona do wydawania decyzji z uwzględnieniem prawa krajowego, w tym także praw podstawowych wynikających z przepisów rangi konstytucyjnej\(^{211}\). Argumentacja ta została rozszerzona w sprawie Geitling\(^{212}\), w której Trybunał podkreślił, że nie jest jego rolą stać na straży stosowania prawa krajowego państw członkowskich, nawet jeżeli jest to prawo konstytucyjne. W tym zakresie Trybunał uznał się za niewłaściwy zarówno do interpretacji, jak i stosowania prawa krajowego\(^{213}\). Wskazał też, że prawo wspólnotowe nie zawierało żadnych zasad ogólnych, które służą ochronie praw nabytych\(^{214}\).

Z kolei w sprawie Sgarlata\(^{215}\) wnioskodawca podniósł argument, że oparcie rozstrzygnięcia wyłącznie na kwestionowanym prawie wspólnotowym doprowadzi do „naruszenia fundamentalnych praw wspólnych dla wszystkich państw członkowskich”. Skarga została przez Trybunał oddalona.

Jednak w późniejszych orzeczeniach ETS zaczął wywodzić istnienie gwarancji związanych z prawami podstawowymi z zasad ogólnych prawa wspólnotowego, a w efekcie uznawać kwestię ochrony tych praw jako jedno z zadań stojących przed Trybunałem\(^{216}\). W wyroku w sprawie Internationale Handelsgesellschaft Trybunał uznał, że ochrona praw podstawowych, choć inspirowana tradycjami konstytucyjnymi państw członkowskich, musi

\(^{210}\) Wyrok TS (TSUE) z 4.02.1959 w sprawie Stork, sygn. 1-58.
\(^{211}\) Ibidem, p. 3A uzasadnienia.
\(^{212}\) Wyrok TS (TSUE) z 15.07.1960 w sprawie Geitling, sygn. 36-58, 37-58, 38-59 i 40-59.
\(^{213}\) Ibidem, p. 1 podsumowania wyroku.
\(^{214}\) Ibidem, p. 2 podsumowania wyroku.
\(^{215}\) Wyrok TS (TSUE) z 1.04.1965 w sprawie Sgarlata, sygn. 40/64.
\(^{216}\) Wyrok TS (TSUE) z 12.11.1969 w sprawie Stauder, sygn. 29/69.
być gwarantowana w ramach struktury i celów Wspólnoty\textsuperscript{217}. Ewolucja orzecnictwa Trybunału była związana wprost z zagadnieniem przemaru prawa wspólnotowego. Trybunał, chcąc wykazać, że prawo wspólnotowe nie może być oceniane kryteriami wynikającymi z prawa krajowego – a więc także krajowych norm konstytucyjnych – stanął przed problemem braku uwzględnienia katalogu praw podstawowych w prawie wspólnotowym\textsuperscript{218}. Rysowało się zatem zagrożenie, że sądy krajowe odrzucą koncepcję bezwzględnego przymaru prawa wspólnotowego, jako grożącej pominięciem ochrony praw podstawowych wynikających z przepisów rangi konstytucyjnej. Problem ten został wyraźnie zarysowany w wyroku niemieckiego Federalnego Trybunału Konstytucyjnego w orzeczeniu \textit{Solange I}\textsuperscript{219} z 1974 roku, w którym stwierdzono, że „dopóki Wspólnoty nie wypracują katalogu praw zasadniczych, dopóty prawo wtórne WE będzie podlegało kontroli z punktu widzenia jego zgodności z prawami określonymi w Ustawie Zasadniczej RFN”\textsuperscript{220}. Ponadto Trybunał w swoim orzecznictwie zaczął wskazywać na EKPC jako wyznacznik w zakresie standardu ochrony praw podstawowych obowiązujących w prawie wspólnotowym\textsuperscript{221}. Obecnie w orzecznictwie Trybunału Sprawiedliwości dominuje pogląd o prymacie prawa UE także nad przeprzemarami konstytucyjnymi państw członkowskich\textsuperscript{222}. Pogląd ten nie jest powszechnie akceptowany przez sądy konstytucyjne państw członkowskich, czego najlepszym przykładem jest Polska\textsuperscript{223}. Jednak w niektórych państwach członkowskich zasada przymaru prawa UE została wprost uwzględniona w przeprzemarach rangi konstytucyjnej.

Efektem dyskusji na temat roli i znaczenia praw podstawowych w ponadnarodowym porządku prawnym ustanowionym traktatami rzymskimi było przyjęcie 5 kwietnia 1977 roku przez Parlament Europejski, Komisję i Radę wspólnej deklaracji\textsuperscript{224} wskazującej na znaczenie praw podstawowych wynikających w szczególności z dorobku konstytucyjnego państw członkowskich oraz EKPC. Chociaż deklaracja ta była pozbawiona mocy wiązącej, stanowiła kolejny krok w ewolucji Wspólnot Europejskich z organizacji o celach \textit{stricte} gospodarczych.

\textsuperscript{217} Wyrok TS (TSUE) z 17.12.1970 w sprawie \textit{Internationale Handelsgesellschaft}, sygn. 11/70.

\textsuperscript{218} T. Koncewicz, Zasada pierwszeństwa prawa wspólnotowego przed prawnem krajowym w orzecznictwie Trybunału Sprawiedliwości Wspólnot Europejskich, [w:] Węzłowe problemy w orzecznictwie Trybunału Sprawiedliwości Wspólnot Europejskich pod red. B. Banaszkiewicza, Biuro Trybunału Konstytucyjnego 2003, s. 8.

\textsuperscript{219} Wyrok FTK z 9.05.1974, sygn. BVerfGE 37, 271.

\textsuperscript{220} J. Sozański, \textit{Prawa człowieka w systemach prawnych Wspólnot i Unii Europejskiej}, Iuris 2008, s. 133.

\textsuperscript{221} Wyrok TS (TSUE) z 14.05.1974 w sprawie \textit{Nold}, sygn. 4/73.

\textsuperscript{222} Obok przywołanego wcześniej orzeczenia w sprawie \textit{Internationale Handelsgesellschaft}, TSUE pogląd taki wyraził między innymi w sprawie C-409/06 (p. 61).

\textsuperscript{223} Wyrok TK z 11.05.2004, sygn. K 18/04, p. 4.2.

do struktury ponadnarodowej, której jednym z celów działania jest ochrona praw podstawowych.


2.4.2. Charakter prawny oraz zakres przedmiotowy i podmiotowy

Przed wstępnym omówieniem praw i gwarancji przewidzianych w Karcie, konieczne jest przedstawienie rozważań na temat jej prawnego charakteru. W wyniku wejścia w życie postanowień Traktatu z Lizbony227, Karta stała się – obok Traktatu o Unii Europejskiej228 (dalej: TUE) i Traktatu o Funkcjonowaniu Unii Europejskiej229 (dalej: TFUE) – częścią prawa pierwotnego UE. Wniosek taki wynika wprost z przywołanego wcześniej art. 6 ust. 1 TUE, zgodnie z którym Unia uznała prawa, wolności i zasady określone w KPP, która ma moc prawną jak traktaty. Karta nie została włączona do żadnego z traktatów, nie stanowi zatem podstawy funkcjonowania Unii zgodnie z art. 3 TUE. Jest to istotna różnica w porównaniu do treści proponowanego Traktatu Konstytucyjnego, w którym KPP miała zostać zamieszczona jako część II traktatu. Należy zatem zadać pytanie o praktyczną różnicę wynikającą z nieuwzględnienia KPP w treści traktatów, a zatem i podstawy funkcjonowania UE (art. 1 TUE) przy jednoczesnym uznaniu, że ma moc prawną jak traktaty (art. 6 ust. 1 TUE). W pierwszej kolejności konieczne jest rozstrzygnięcie, czy KPP jest umową międzynarodową. Zgodnie z Konwencją wiedeńską o prawie traktatów230 każda umowa (porozumienie) międzynarodowa zawarta pomiędzy państwami, niezależne od tego, w ilu dokumentach została ujęta, i niezależnie od jej szczególnej nazwy, jest nazywana traktatem (art. 2 ust. 1). Natomiast zgodnie z art. 31 ust. 2 dla celów interpretacji traktatu uwzględnia się także jego wstęp oraz załączniki. Karta praw podstawowych nie została dołączona do Traktatu

225 Karta Praw Podstawowych Unii Europejskiej z dn. 30.03.2010 (Dz. Urz. UE z 2010 nr C 83, s. 389).
226 Traktat ustanawiający Konstytucję dla Europy z dn. 29.10.2004 (Dz. Urz. UE z 2004 nr C 310).
227 Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie 13 grudnia 2007 (Dz. Urz. UE C Nr 306, str. 1).
228 Traktat o Unii Europejskiej (Dz. Urz. UE z 2016 C Nr 202, s. 13).
229 Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE z 2016 C Nr 202, s. 47).
230 Konwencja wiedeńska o prawie traktatów z dn. 23.05.1969 (Dz.U. 1990 Nr 74, poz. 439).
lizbońskiego\textsuperscript{231}, nie była więc przedmiotem ratyfikacji ze strony państw członkowskich. W efekcie status prawny Karty jako umowy międzynarodowej jest nadal dyskutowany w literaturze przedmiotu\textsuperscript{232}. A. Bisztyga zauważa, że wraz z wejściem w życie traktatu lizbońskiego KPP uzyskała status umowy międzynarodowej\textsuperscript{233}. Odmienny pogląd zaprezentowała jeszcze przed zakończeniem procesu ratyfikacji A. Wyrozumska, twierdząc, że Karta nie stanie się umową międzynarodową, ponieważ nie jest integralną częścią Traktatu lizbońskiego i nie musi być ratyfikowana przez państwa członkowskie\textsuperscript{234}. Sytuację konkluduje B. Banaszak, stwierdzając, że przyjęcie KPP jako umowy międzynarodowej z punktu widzenia większości konstytucji państw członkowskich nie zwiększyłoby jej rangi w krajowych porządkach prawnym\textsuperscript{235}.

Sposób przyjęcia nie osłabił jednak znaczenia Karty z punktu widzenia prawa unijnego. Także wpływ Karty na krajowe systemy prawne nie uległ zmianie – prawa i gwarancje przewidziane w KPP korzystają z takich samych reguł pierwszeństwa, jakie zostały przewidziane dla Traktatu lizbońskiego. Prawką jest zatem, że przyjęcie KPP jako odrębnej umowy międzynarodowej nie wpłynęłoby na nadanie jej odmiennego statusu w krajowych porządkach prawnych. Jak zauważyła A. Wyrozumska, różnica w formie przyjęcia Karty ma zatem głównie wymiar polityczny i symboliczny, co jak należy przypuszczać było głównym zamiarem autorów Traktatu lizbońskiego\textsuperscript{236}. Usunięcie treści KPP z traktatów spowodowało, że przestały one sprawiać wrażenie konstytucji, co spotkało się wcześniej ze sprzeciwem w niektórych państwach członkowskich, czego efektem był nieudany proces ratyfikacyjny Traktatu Konstytucyjnego.

Karta praw podstawowych została zorganizowana w sześć części (tytułów), z których pięć pierwszych dotyczy praw i zasad w obszarach: godności, wolności, równości, solidarności oraz praw obywatelskich. Podział na prawa i zasady ma istotną konsekwencję praktyczną. Zgodnie z art. 52 ust 5 zasady określone w Karcie nie mają cechy bezpośredniej stosowalności, właściwej dla ogółu przepisów prawa UE. Nie mogą być więc samoistną podstawą, na której jednostka może dochodzić ochrony prawnej. Wyjątkiem od tej sytuacji jest włączenie zasad w krajowy porządek prawnego lub przepisy prawa wtórnego UE. W takim

\textsuperscript{231} W przypadku Polski, treść Karty została opublikowana w dzienniku ustaw razem z Traktatem lizbońskim
\textsuperscript{232} Por rozważania przedstawione w: Wprowadzenie, Nb 7, [w:] Karta Praw Podstawowych Unii Europejskiej. Komentarz pod red. A. Wróbla, CH Beck 2013.
\textsuperscript{233} A. Bisztyga, „Europejska Konwencja Praw Człowieka a Karta Praw Podstawowych Unii Europejskiej – stan kompatybilności czy konkurencyjności, Przegląd Prawa Konstytucyjnego 2011, nr 3, s. 182
\textsuperscript{234} A. Wyrozumska, Znaczenie prawne zmiany statusu Karty praw podstawowych Unii Europejskiej w Traktacie lizbońskim oraz protokołu polsko-brytyjskiego, Przegląd Sejmowy 2008, nr 2 (85), s. 26.
\textsuperscript{235} B. Banaszak, Zalety i wady Karta Praw Podstawowych Unii Europejskiej, Przegląd Sejmowy 2008, nr 2.
\textsuperscript{236} A. Wyrozumska, Znaczenie prawne..., op. cit., s. 26.
przypadkach zasady określone w Karcie mogą być powoływane w sądzie w celu wykładni tych aktów i kontroli ich legalności.

Kwestia ochrony prywatności została uregulowana w art. 7, zgodnie z którym każdy ma prawo do poszanowania swego życia prywatnego i rodzinnego, domu i komunikowania się. Natomiast w art. 8 wprowadzono gwarancje związane z ochroną danych osobowych. W szczególności, zgodnie z art. 8 ust. 2 dane osobowe muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą, a każdy ma prawo dostępu do zebranych danych, które go dotyczą, a także prawo do ich sprostowania. Ponadto – zgodnie z art. 8 ust. 3 – przestrzeganie norm określonych w ustępach wcześniejszych podlega kontroli niezależnego organu. W efekcie, zarówno ochrona prywatności, jak i ochrona danych osobowych zyskała w UE rangę praw podstawowych. Treścią art. 7 (ochrona prywatności) oraz art. 8 (ochrona danych osobowych) wprowadzono prawa, a nie zasady, co oznacza, że wskazane gwarancje mają cechę bezpośredniej skuteczności przynależną ogółowi prawa UE.

Rozpoczynając analizę obszaru ochrony prywatności na gruncie KPP, w pierwszej kolejności należy zwrócić uwagę na zakres podmiotowy i przedmiotowy prawa. Zarówno art. 7, jak i art. 8 ust. 1 wskazują, że prawa w nich przewidziane mają charakter powszechny, nie są więc kierowane wyłącznie do obywateli państw członkowskich. Podobnie jak w przypadku innych aktów międzynarodowych (w szczególności MPPOP czy EKPC), twórcy Karty zamiast wprowadzać definicję prywatności zdecydowali się wyrazić wartość chronioną przez zbiór pojęć – w tym wypadku są nimi poszanowanie życia prywatnego i rodzinnego, domu i komunikowania się. J. Sobczak zauważa, że problem prawa do prywatności na gruncie Karty należy łączyć z kwestią godności człowieka, która w koncepcji tego aktu nie tylko, że sama jest podstawowym prawem, ale także stanowi faktyczne źródło innych praw podstawowych.

Zgodnie z art. 52 ust. 3 KPP w zakresie, w jakim Karta zawiera prawa odpowiadające prawom zagwarantowanym w EKPC, ich znaczenie i zakres jest takie samo. Redakcja przepisów art. 7 KPP oraz art. 8 ust. 1 EKPC jest niemal identyczna, a jedyna różnica dotyczy zastąpienia terminu „mieszkanie” (EKPC) słowem „dom” (KPP) oraz ochrony „korespondencji” (EKPC), ochroną „komunikowania się” (KPP). Zasadne jest zatem pytanie, czy te różnice wpływają na możliwość zastosowania art. 52 ust. 3 − innymi słowy: czy przeprowadzając analizę zakresu ochrony wynikającej z art. 7 KPP należy wziąć pod uwagę

237 J. Sobczak, Komentarz do art. 7, Nb 2, [w:] Karta Praw Podstawowych..., op. cit.
bogaty dorobek orzeczniczy ETPC wypracowany na tle art. 8 EKPC. Słowa „dom” i „mieszkanie” można uznać za równoważne, a zakres ochrony wyrażający się przez ich użycie odnieść do ochrony miru domowego. Z kolei ochrona wszelkich form komunikowania się (KPP) wydaje się przewidywać szerszą ochronę niż wynikająca z ochrony korespondencji (EKPC). Warto w tym miejscu jednak przywołać orzecznictwo ETPC, który wielokrotnie wskazał, że gwarancje wynikające z Konwencji europejskiej powinny być interpretowane w przypadku wątpliwości rozszerzającco. W sprawie Copland v. Wielka Brytania Trybunał wprost orzekł, że gwarancje związane z ochroną korespondencji powinny być stosowane w odniesieniu także do komunikacji elektronicznej, takiej jak e-mail czy realizowanej za pośrednictwem Internetu\(^{238}\). W przypadku interpretacji zakresu ochrony prywatności wynikającej z KPP zastosowanie znajduje art. 52 ust. 3 Karty. Wnioskowanie takie można potwierdzić również w oficjalnym wyjaśnieniu dotyczącym KPP, w którym stwierdzono, że „prawa zagwarantowane w artykule 7 odpowiadają prawom zagwarantowanym na mocy artykułu 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności”\(^{239}\).

Rozgraniczenie gwarancji związanych z ochroną prywatności (art. 7) i ochroną danych osobowych (art. 8) wskazuje, że terminy te – w ocenie prawodawcy – są w pewnych obszarach rozłączne\(^{240}\), co oznacza w szczególności, że nie każde naruszenie ochrony danych osobowych prowadzi do ingerencji w prawo do prywatności.

Wprowadzając zakres praw i gwarancji związanych z ochroną danych osobowych, prawodawca zdecydował się jednocześnie określić najważniejsze zasady przetwarzania danych – w szczególności wskazany w art. 8 ust. 2 obowiązek przetwarzania rzetelnego, wyłącznie w określonym celu oraz w oparciu o podstawę prawną lub zgodę osoby, której dane dotyczą. Każda z tych zasad znajduje swoje rozwinięcie w przepisach prawa wtórnego UE (por. zasady ochrony danych wskazane w dyrektywie 95/46\(^{241}\)) oraz w innych dokumentach prawa międzynarodowowego, których państwa członkowskie UE są stronami (w szczególności należy tu wskazać na art. 8 Konwencji nr 108 RE\(^{242}\). Ponadto w art. 8 ust. 2 wymieniono najważniejsze prawa przysługujące podmiotowi danych, w szczególności związane z dostępem do zebranych danych oraz prawem ich sprostowania. Rozwinięcie tych praw można odszukać w przepisach prawa wtórnego UE oraz innych wiążących aktach prawnomiedzynarodowych. Prawdą jest, że o ile prawo do prywatności w kształcie

\(^{238}\) Wyrok ETPC w sprawie Copland v. Wielka Brytania, § 44.
\(^{240}\) Por. rozważania na tym tle przedstawione w odniesieniu do art. 48 i 51 Konstytucji RP w rozdziale 2.5.2.
\(^{241}\) Rozdział 4.5.1, s 143.
\(^{242}\) Szczegółowe informacje – zob. rozdział 3.4.
zaproponowanym w art. 7 zostało wzorowane na innych umowach międzynarodowych dotyczących obszaru ochrony praw człowieka (w szczególności EKPC), to definiując zakres art. 8 KPP, prawodawca wzorował się na dokumentach mniej uniwersalnych, dotyczących wprost zagadnienia ochrony prywatności w związku z przetwarzaniem danych w systemach informatycznych. Co zatem oczywiście, w przypadku art. 8 nie będzie miał zastosowania art. 52 ust. 3 KPP, ponieważ w treści EKPC nie przewidziano praw i gwarancji w obszarze ochrony danych osobowych w zakresie zgodnym z art. 8 Karty.

Prawa wynikające z Karty mogą zostać ograniczone, jeżeli ograniczenie takie jest przewidziane ustawą oraz spełnia kryteria konieczności i proporcjonalności (art. 52 ust. 1). Ponadto wymaga się, aby zastosowane środki „rzeczywiście odpowiadały celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób”. Wskazany przepis stanowi więc odpowiednik art. 8 ust 2 EKPC, dlatego przy analizowaniu zakresu dopuszczalnych ingerencji w prawa wynikające z KPP należy uwzględnić orzecznictwo ETPC wypracowane na tle konieczności i proporcjonalności zastosowanych środków. Odmienną w podejściu twórców Karty wyraża się w zdefiniowaniu jednej klauzuli limitacyjnej dla wszystkich wprowadzanych praw, a nie tak jak ma to miejsce w innych systemach ochrony praw człowieka (w tym EKPC) definiowaniu zakresu możliwych ograniczeń indywidualnie dla każdej z wprowadzanych gwarancji. Jak jednak wskazuje A. Wróbel, przepis art. 52 ust. 1 będzie miał zastosowanie tylko wtedy, gdy nie są spełnione warunki szczególne przewidziane w art. 52 ust. 2-4. Przyjęcie tego poglądu prowadzi do wniosku, że jeżeli prawo gwarantowane przez Kartę zostało przewidziane w Konwencji europejskiej, to na podstawie omówionego wcześniej art. 52 ust. 3 zakres ograniczeń związanych z tym prawem powinien wynikać z orzecznictwa EKCP a nie ze stosowania art. 52 ust. 1. Klauzula limitacyjna wynikająca z art. 52 ust. 1 może być stosowana tylko w zakresie, w jakim prowadzi do przyznania szerszych praw jednostkom, niż wynika to z Konwencji oraz orzecznictwa ETPC. W takim ujęciu art. 52 ust. 3 stanowi lex specialis wobec ogólnej zasady stosowania ograniczeń wynikającej z art. 52 ust. 1.

Treść przepisu art. 52 ust. 1 jest inspirowana wcześniejszym dorobkiem orzeczniczym TSUE dotyczącym uprawnionego zakresu stosowania ingerencji w prawa podstawowe. Jak wskazał Trybunał w sprawie Dokter i in., „prawa podstawowe (...) nie mają charakteru bezwzględnego. Mogą one podlegać ograniczeniom, pod warunkiem, że ograniczenia te

---

243 Zob. informacje przedstawione w rozdziale 2.3.1.

rzeczywiście odpowiadają celom interesu ogólnego, jakim służy omawiane działanie, i że nie stanowią z punktu widzenia realizowanych celów nieproporcjonalnej oraz niedopuszczalnej ingerencji w samą istotę praw w ten sposób gwarantowanych.”

2.4.3. Dorobek orzeczniczy TSUE na tle KPP

W ostatnich latach art. 7 i 8 KPP stały się podstawą wydania szeregu precedensowych wyroków przez TrybunałSprawiedliwości UE, które na stałe wpłynęły na umocnienie gwarancji w zakresie ochrony prywatności w systemach i sieciach informatycznych. Z uwagi na poświęcenie temu tematowi odrębnych rozdziałów w części II niniejszej pracy poniżej zostaną przedstawione tylko najważniejsze wyroki i główne tezy z nich wynikające.

W sprawie Digital Rights Ireland Ltd Trybunał rozpatrzył pytania prejudycjalne dotyczące zgodności z prawem krajowych przepisów implementujących dyrektywę 2006/24 (tzw. dyrektywa retencyjna) w zakresie wprowadzenia ogólnego obowiązku zatrzymania danych związanych z łącznością elektroniczną. W ostatnich latach kwestia ochrony przed nieuprawnionymi działaniami władzy publicznej skutkującymi nieuprawnioną ingerencją w prawo do prywatności zyskała na znaczeniu wraz z ujawnianiem w domenie publicznej kolejnych informacji na temat działań państw związanych z prowadzeniem rozbudowanych programów inwigilacji elektronicznej. Sprawa zawisła przed Trybunałem dotyczyła zakresu dopuszczalnej ingerencji w prawo do prywatności uzasadnianej względami bezpieczeństwa publicznego. Trybunał zauważył, że gromadzenie danych telekomunikacyjnych, także danych niestanowiących treści przekazu (tzw. metadane) i ich udostępnianie uprawnionym organom pozostaje w bezpośrednim i szczególnym związku z prawem do poszanowania życia prywatnego zagwarantowanego w art. 7 KPP oraz musi spełniać wymagania dotyczące ochrony danych osobowych wynikające z art. 8 KPP. Dla uznania, że doszło do ingerencji w prawo do poszanowania życia prywatnego nie ma znaczenia zakres przetwarzanych informacji, a w szczególności to, czy mają one charakter wrażliwy, ani też to, czy ze względu na tę ingerencję zainteresowane osoby doświadczyły ewentualnych niedogodności.

Natomiast, zgodnie z przedstawionymi wcześniej rozważaniami w zakresie art. 52 ust. 1, istotne jest zbadanie, czy spełnione zostały kryteria uznania ingerencji za uzasadnioną. W badanej sprawie Trybunał uznał, że wprowadzony środek nie spełniał kryterium proporcjonalności, co biorąc pod uwagę faktyczną użyteczność środka do realizacji

245 Wyrok TSUE z 15.06.2005 w sprawie Dokter i in, sygn. C-28/05, p. 75.
246 Wyrok TSUE z 8.04.2014 w sprawie Digital Rights Ireland Ltd, sygn. C-293/12 i C-594/12.
247 Ibidem, p. 33.
zamierzonego celu, prowadzi do wniosku, że zakres ingerencji w prawa podstawowe był nieuzasadniony. W konsekwencji TSUE stwierdził nieważność dyrektywy retencyjnej. Z kolei w sprawie Tele2 Sverige Trybunał uznał, że środki krajowe przewidujące wprowadzenie ogólnego obowiązku zatrzymania danych i w tym zakresie służące transpozycji unieważnionej we wcześniejszym orzeczeniu dyrektywy retencyjnej także nie mogą być uznane za spełniające kryteria proporcjonalności określone w art. 52 ust. 1, a w konsekwencji prowadzą do naruszenia gwarancji przewidzianych w art. 7 i 8 KPP. Trybunał zaznaczył, że funkcjonowanie przepisów krajowych przewidujących ogólny obwózke zatrzymania danych telekomunikacyjnych może pociągnąć za sobą powstanie po stronie użytkowników wrażenia, iż ich prywatne życie podlega ciągłej obserwacji, co w sposób oczywisty stanowi daleko posuniętą ingerencję w prawa podstawowe, o których mowa w art. 7 i 8 Karty.

Należy podkreślić, że zarówno w wyroku Digital Rights Ireland, jak i Tele2 Trybunał podjął temat ochrony praw podstawowych przed nieuprawnioną ingerencją ze strony władzy publicznej. W obu przypadkach precedensowe rozstrzygnięcia Trybunału miały duże konsekwencje praktyczne w krajowych porządkach prawnych państw członkowskich UE i doprowadziły do wzmocnienia gwarancji wynikających z art. 7 i art. 8 KPP. Innym rozstrzygnięciem TSUE o doniosłym znaczeniu był wyrok w sprawie Google Spain SL, w którym Trybunał zawarł rozszerzającą interpretację zakresu prawa wynikającego z art. 8 KPP. Zawisła przed Trybunałem sprawą związana była z pytaniem prejudycjalnym zadanym przez irlandzki sąd najwyższy i dotyczyła zakresu stosowania obowiązków wynikających z prawa UE związanego z ochroną danych osobowych wobec przedsiębiorców świadczących usługi dla użytkowników na terytorium Unii, ale nieposiadających siedziby ani oddziału w żadnym z państw członkowskich UE. Trybunał uznał, że dla określenia, czy podmiot powinien być zobowiązany do stosowania prawa UE (w tym KPP), konieczne jest ustalenie, czy aktywnie kieruje swoje usługi do użytkowników na terenie Unii – np. poprzez sprzedaż usług reklamowych za pośrednictwem podmiotów zależnych zarejestrowanych w dowolnym państwie członkowskim. Pozytywna odpowiedź pozwala na stwierdzenie, że przedsiębiorca taki powinien stosować prawo UE. Druga część wyroku w sprawie Google Spain SL miała jeszcze bardziej doniesie skutki. Trybunał uznał bowiem, że każdy podmiot danych ma prawo, pod pewnymi warunkami, wnioskować o usunięcie swoich danych, a

248 Ibidem, p. 63.
250 Ibidem, p. 100.
251 Ibidem, p. 60.
żądanie takie może być kierowane do operatora wyszukiwarki internetowej. W ten sposób Trybunał zdefiniował nowe prawo, znane w literaturze przedmiotu jako *prawo do bycia zapomnianym*, i określił, że jest ono przejawem stosowania szerszego prawa do ochrony prywatności wynikającego z art. 7 i 8 KPP\textsuperscript{252}. Trybunał ocenił też, że w omawianym przypadku prawo do poszanowania prywatności jednostki jest nadrzędne wobec prawa dostępu do informacji ogółu społeczeństwa oraz interesu gospodarczego operatora wyszukiwarki\textsuperscript{253}.

Z kolei w sprawie *Schrems* Trybunał zajął się kwestią skuteczności gwarancji związanych z ochroną danych osobowych w operacjach międzynarodowego transferu danych\textsuperscript{254}. Osnową sprawy była skarga wniesiona przez obywatela Austrii z powodu przekazywania przez Facebook Ireland Ltd do Stanów Zjednoczonych danych osobowych swoich użytkowników i przechowywania tych danych na serwerach zlokalizowanych poza obszarem UE. Max Schrems uznał, że dane go dotyczące nie są przetwarzane w sposób przewidziany w prawie UE, w szczególności poprzez możliwość niekontrolowanego dostępu do nich amerykańskich służb wywiadowczych. Trybunał przeanalizował warunki realizacji transatlantyckiego programu „*Bezpieczna przystań*”, ustalonego decyzją KE 2000/520\textsuperscript{255} o adekwatności zabezpieczeń, na podstawie którego możliwe było przekazywanie danych osobowych do przedsiębiorców zlokalizowanych w Stanach Zjednoczonych. Jak podkreślił TSUE, uregulowania prowadzące do ingerencji w prawa podstawowe gwarantowane w art. 7 i 8 Karty muszą zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania tych środków, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane osobowe zostają dotknięte ingerencją, miały wystarczające gwarancje rzeczywistej ochrony przed ryzykiem nadużyć\textsuperscript{256}. W każdym przypadku wprowadzenie uregulowania nieprzewidującego dla podmiotów danych skutecznego trybu uzyskania dostępu, żądania sprostowania lub usunięcia danych prowadzi do naruszenia prawa do skutecznej ochrony prawnej\textsuperscript{257}.

Rozwój możliwości technicznych powoduje powstawanie nowych zagrożeń i problemów związanych z zapewnieniem odpowiedniego poziomu ochrony prywatności,

\textsuperscript{252} Szczegółowe rozważania w: M. Rojszczak, *Analiza i praktyczne uwagi*..., op. cit., s. 30-41.
\textsuperscript{253} Ibidem, p. 97.
\textsuperscript{254} Wyrok TSUE z 6.10.2015 w sprawie *Schrems*, sygn. C-362/14.
\textsuperscript{255} Decyzja Komisji z 26.07.2000 przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz.Urz. WE z 2000 nr L 215).
\textsuperscript{256} Wyrok TSUE w sprawie *Schrems*, p. 91.
\textsuperscript{257} Wyrok TSUE w sprawie *Schrems*, p. 95.
zwłaszcza w zakresie korzystania z mediów elektronicznych. Rozpatrując sprawę Breyer\textsuperscript{258}, Trybunał potwierdził, że definicja danych osobowych wynikająca z prawa UE musi być interpretowana w odniesieniu do istniejących możliwości technicznych. W szczególności oznacza to, że podmiot posiadający środki i możliwości korelowania informacji skutkujące możliwością ustalenia tożsamości osoby korzystającej z mediów elektronicznych musi traktować gromadzone przez siebie zbiory jako dane osobowe, nawet jeżeli innym podmiotom informacje te nie pozwalają na identyfikację użytkowników\textsuperscript{259}. Wydany wyrok dotyczył konkretnego pytania prejudycjalnego związanego z potwierdzeniem, czy dynamiczne adresy IP w szczególnych przypadkach mogą być traktowane jako dane osobowe. Orzeczenie to stanowi wskazówkę, w jaki sposób należy odnosić prawa i gwarancje wynikające z prawa UE, także KPP, do dynamicznie rozwijającego się rynku e-usług świadczonych w sieciach informatycznych\textsuperscript{260}.

W sprawach ze skargi Komisji Europejskiej przeciwko Węgrom\textsuperscript{261} oraz Austrii\textsuperscript{262} Trybunał podjął również problem niezależności krajowych organów ochrony danych osobowych (art. 8 ust. 3 KPP). Trybunał przypomniał, że ustanowienie w państwach członkowskich organów nadzorczych stanowi istotny element ochrony osób w związku z przetwarzaniem danych osobowych\textsuperscript{263}, a samo tylko zagrożenie możliwością wpływu politycznego organów władzy wykonawczej na decyzje organów nadzorczych jest wystarczającą przeszkodą w niezależnym wykonywaniu przez nie zadań\textsuperscript{264}.

### 2.4.4. Relacja pomiędzy KPP a EKPC

Oddzielnego omówienia wymaga konsekwencja funkcjonowania w obrębie państw członkowskich UE dwóch norm prawa międzynarodowego, definiujących zbliżone lub – jak w przypadku art. 7 KPP - identyczne swobody i gwarancje w obszarze prawa do prywatności. Skoro art. 7 KPP jest powtórzeniem art. 8 ust. 1 EKCP, a sama Karta wskazuje na konieczność interpretacji art. 7 w zakresie wynikającym z Konwencji europejskiej, to powstaje ryzyko, że poddanie dwóch identycznych praw wynikających z obu aktów

\textsuperscript{258} Wyrok TSUE z 19.10.2016 w sprawie Breyer, sygn. C-582/14.

\textsuperscript{259} Ibidem, p. 49.

\textsuperscript{260} Analogicznie uznał NSA w wyroku z 19.05.2011 (I OSK 1079/10) uznając, że „adres IP nie zawsze może być traktowany jako dane osobowe w rozumieniu art. 6 ust. 1 i 2 ustawy. Jednak tam, gdzie adres IP jest na dłuższy okres czasu lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową, jest to bowiem informacja umożliwiająca identyfikację konkretniej osoby fizycznej”.

\textsuperscript{261} Wyrok TSUE z 8.04.2014 w sprawie KE v. Węgry, sygn. C-288/12.

\textsuperscript{262} Wyrok TSUE z 16.10.2012 w sprawie KE v. Austria, sygn. C-614/10.

\textsuperscript{263} Wyrok TSUE w sprawie KE v. Węgry, p. 48.

\textsuperscript{264} Ibidem, p. 53.
normatywnych pod ochronę dwóm różnym trybunałom doprowadzi do utworzenia odrębnych linii orzeczniczych, a w efekcie do naruszenia zasady pewności prawa.

Należy pamiętać, że zobowiązania traktatowe wynikające z EKPC oraz traktatów ustanawiających UE (w tym związanych z KPP) nie zawsze mogą być w oczywisty sposób pogodzone. W sprawie Bosphorus265 ETPC uznał, że co do zasady państwa-strony Konwencji mają prawo przekazywać część swoich kompetencji organizacji międzynarodowej, nie zmienia to jednak odpowiedzialności państwa za wykonywanie zobowiązań konwencyjnych także w przypadku transpozycji aktów prawa wydanych przez tę organizację do krajowego systemu prawnego266. Trybunał podkreślił jednocześnie, że jeżeli organizacja międzynarodowa zapewnia ochronę praw podstawowych na równoważnym Konwencji poziomie, działanie państwa związane z implementacją przepisów ponadnarodowych nie może być interpretowane jako prowadzące do naruszenia Konwencji267. Zarówno w sprawie Bosphorus268, jak i innych orzeczeniach dotyczących kwestii transpozycji prawa UE269, Trybunał uznawał Unię Europejską (Europejską Wspólnotę Gospodarczą) za organizację spełniającą ten warunek. W efekcie odstępował od oceny merytorycznej prawa krajowego, stanowiącego implementację przepisów UE. Podejście takie zakładało, że ponadnarodowa kontrola tego typu przepisów krajowych będzie realizowana przez TSUE.

Sytuacja częściowo zmieniła się wraz z wydaniem wyroku w sprawie Michaud270, w którym ETPC uznał się za właściwy do dokonania oceny merytorycznej przepisów krajowych stanowiących implementację dyrektywy UE. Należy podkreślić, że tłem badanej sprawy była skarga na naruszenie prawa do prywatności, a z uwagi na odmowę zadania pytania prejudycjalnego przez sąd francuski sprawa nie była przedmiotem badania przez TSUE. Trybunał strasburski wskazał brak skierowania pytania prejudycjalnego do TSUE jako jedną z przyczyn niezastosowania wcześniejszej linii orzeczniczej wynikającej ze sprawy Bosphorus271. Orzeczenie w sprawie Michaud otwiera drogę do pośredniej oceny prawa UE przez ETPC oraz wydania w przyszłości wyroku stwierdzającego niezgodność z Konwencją przepisów krajowych, stanowiących implementację przepisów UE. L. Garlicki zauważa, że głównym adresatem wyroku Michaud powinny być sądy krajowe, które powinny wykazywać

265 Wyrok ETPC z 30.06.2005 w sprawie Bosphorus, sygn. 45036/98.
266 Ibidem, § 153.
267 Ibidem, § 155.
268 Ibidem, § 165.
269 Ibidem, § 165.
271 Ibidem, § 115.
większą gotowość do współpracy z TSUE w zakresie interpretacji zobowiązań traktatowych związanych z prawami podstawowymi\textsuperscript{272}.

Potencjalny problem wynikający z różnych linii orzeczniczych trybunałów europejskich sygnalizuje także A. Bisztyga, określając stan relacji między konwencyjnym systemem ochrony praw człowieka a systemem wynikającym z Karty jako niejednoznaczny. Jak wskazuje, „należy mieć nadzieję, że między obydwoma europejskimi sądami kreującymi europejskie standardy praw człowieka, ETPC i TSUE, nie zaistnieje stan rozbieżności linii orzeczniczych albo wręcz stan konkurencyjności obu sądów. W tej nowej i dynamicznej sytuacji wzajemne respektowanie argumentacji, a w konsekwencji zbieżność czy wręcz jednolitość linii orzeczniczych obu sądów, należy traktować jako prawnie doniosłą wartość. Tylko takie ich działanie pozwoli na uniknięcie potencjalnych konfliktów między ETPC a TSUE”\textsuperscript{273}.

Odrębne zaznaczenia wymaga kwestia planowanego przystąpienia Unii Europejskiej jako organizacji międzynarodowej do Konwencji europejskiej. Uwzględnienie takiej możliwości było jedną ze zmian uwzględnionych w Traktacie lizbońskim i zostało przewidziane w art. 6 ust. 1 poprzez sformułowanie „Unia przystępuje do europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności”. Jak zauważa L. Garlicki, tryb oznajmujący zastosowany w przepisie oznacza zobowiązanie o charakterze bezwzględnym i wyłącza polityczną swobodę przy podejmowaniu decyzji przez organy UE oraz jej państwa członkowskie\textsuperscript{274}. Zgodnie z art. 6 ust 2 TUE przystąpienie UE do EKPC nie ma wpływu na kompetencje Unii określone w traktatach. W protokole (nr 8)\textsuperscript{275} do Traktatu lizbońskiego wskazano dodatkowe warunki, które powinny być uwzględnione w umowie dotyczącej przystąpienia Unii do Konwencji europejskiej. W szczególności zagwarantowano, że postanowienia projektowanej umowy nie będą ograniczały ani zmieniały warunków, na jakich państwa członkowskie UE przystąpiły do Konwencji, w szczególności środków podjętych w drodze odstępstw lub dokonanych zastrzeżeń.

\textsuperscript{272} L. Garlicki, Europejski Trybunał Praw Człowieka a prawo UE (refleksje nad wyrokiem ETPCz z 6.12.2012 r. w sprawie Michaud przeciwko Francji), EPS 2014, nr 1 s. 23.
\textsuperscript{273} A. Bisztyga, Europejska Konwencja..., op. cit., s. 185.
\textsuperscript{274} L. Garlicki, Przystąpienie UE do Europejskiej Konwencji Praw Człowieka – przygotowania i problemy, EPS 2011, nr 1, s. 15
\textsuperscript{275} Protokół (nr 8) dotyczący artykułu 6 ustęp 2 Traktatu o Unii Europejskiej w sprawie przystąpienia Unii do europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (Dz.U. 2009 Nr 203, poz. 1569).
Zmiana prawa traktatowego UE była potrzebna, bowiem TSUE stwierdził w opinii wydanej 28 marca 1996 roku\textsuperscript{276} brak kompetencji Wspólnoty do przystąpienia do EKPC w istniejącym wówczas stanie prawnym. Wkrótce po wejściu w życie reformy Lizbońskiej Komisja Europejska wraz z Radą zainicjowały prace nad przygotowaniem projektu umowy akcesyjnej, które zostały zakończone przedstawieniem końcowego projektu 5 czerwca 2013 roku\textsuperscript{277}. Na podstawie art. 218 ust. 11 TFUE, przewidującego możliwość wydania opinii przez TSUE w sprawie zgodności przewidywanej umowy z traktatami, projekt został skierowany 4 lipca 2013 roku przez Komisję do Trybunału Sprawiedliwości. Trybunał w opinii wydanej 18 grudnia 2014 roku\textsuperscript{278} zakwestionował przedstawiony projekt, wskazując na jego niezgodność z prawem UE. W szczególności Trybunał uznał za nieprawidłowe przyjęcie założenie polegające na utożsamieniu Unii z państwem i przypisaniu Unii roli identycznej pod każdym względem z rolą państwa-strony Konwencji, czego efektem jest ignorowanie specyficznego charakteru UE prowadzące do podważenia prymatu prawa Unii\textsuperscript{279}. Trybunał zauważył, że chociaż zawarcie umowy międzynarodowej przewidującej ustanowienie organu sądowego, który miałby dokonywać wykładni postanowień prawa UE i którego orzeczenia wiązałyby instytucje, w tym Trybunał, nie jest co do zasady niezgodne z prawem Unii, to jednak interwencja organów zewnętrznych względem Unii nie może prowadzić do związania Unii i jej instytucji w wykonywaniu ich wewnętrznych kompetencji poprzez narzucenie określonej wykładni przepisów. Taka sytuacja miałaby miejsce w przypadku dokonania wykładni postanowień konwencyjnych przez ETPC związanych z interpretacją prawa UE, czego efektem byłoby związywanie na mocy prawa międzynarodowego Unii oraz jej instytucji, w tym Trybunału\textsuperscript{280}. TSUE zauważył też, że relacja taka nie zachodziłaby w drugą stronę – tj. ustalenia poczynione przez organ sądowy UE – także na tle stosowania KPP - nie miałyby charakteru wiążącego dla ustaleń dokonywanych przez trybunał konwencyjny. W efekcie sytuacja potencjalnie mogłaby skutkować możliwością kwestionowania przez ETPC zakresu stosowania prawa Unii przez państwa członkowskie, co bezpośrednio zagroziłoby zapewnieniu spójności, pełnej skuteczności i autonomii prawa UE.


\textsuperscript{279} Ibidem, p. 194.

\textsuperscript{280} Ibidem, p. 184.
Trybunał zauważył również, że konstrukcja współpozwania przewidziana w umowie akcesyjnej, pozwalająca na kierowanie skarg przeciwko państwu członkowskemu lub UE, w zależności od podmiotu odpowiedzialnego za naruszenie, może doprowadzić do sytuacji, w której prawo UE regulujące podział kompetencji pomiędzy Unię oraz państwa członkowskie byłoby oceniane przez podmiot zewnętrzny, jakim jest ETPC. W efekcie – jak wskazał Trybunał – istniałoby ryzyko, że o wzajemnych relacjach oraz podziale kompetencji pomiędzy UE oraz państwami członkowskimi decydowałby ETPC, co biorąc pod uwagę wiąjący charakter wyroków, mogłoby naruszyć utrwalony podział kompetencji.

Ponadto możliwość wnoszenia spraw do ETPC przez państwa członkowskie przeciwko innemu państwu członkowskemu lub UE mających za przedmiot domniemane naruszenie zobowiązań konwencyjnych w związku ze stosowaniem prawa Unii, stałaby w sprzeczności z art. 344 TFUE, zgodnie z którym państwa członkowskie zobowiązują się do niepoddawania sporów dotyczących wykładni lub stosowania traktatów procedurze rozstrzygania innej niż w nich przewidziana. W tym zakresie w wydanym przez Trybunał komunikacie prasowym zaznaczono, że projekt porozumienia nie naruszałby art. 344 TFUE tylko wówczas, gdyby właściwość ETPC została wyraźnie wyłączona w odniesieniu do sporów między państwami członkowskimi lub między nimi a Unią w przedmiocie stosowania EKPC w ramach prawa Unii.

Powyższe zastrzeżenia doprowadziły do uznania przez Trybunał projektu umowy akcesyjnej za niezgodny z prawem UE, co zgodnie z art. 218 ust. 11 TFUE oznacza brak możliwości zawarcia umowy w proponowanym kształcie. W konsekwencji wznawienie prac nad przystąpieniem UE do EKPC wymaga przeradagowania projektu umowy, z uwzględnieniem uwag TSUE wynikających z opinii 2/13 lub zmiany prawa pierwotnego, co biorąc pod uwagę kwestie polityczne, ale i praktyczne, jest niemożliwe. W planie działań na 2016 i 2017 roku Komisja Europejska zasygnalizowała chęć wznowienia prac nad umową akcesyjną, należy więc oczekiwać, że temat ten będzie przedmiotem dalszych prac na forum europejskim. Biorąc pod uwagę treść opinii 2/13, sprowadzający się do zaprzeczenia możliwości poddania UE kontroli sądowej instytucji zewnętrznej, uzgodnienie modelu

281 Ibidem, p. 234.
282 Ibidem, p. 207.
284 Zastrzeżenia TSUE odnoszą się do niezgodności projektu aktu z szeregiem przepisów szczegółowych UE, z których część dotyczy zasad podstawowych funkcjonowania Unii, takich jak zasada przyznania czy zasada pomocniczości.
285 Por. argumentacja przedstawiona w p. 256 opinii 2/13.
akcesji UE do EKPC spełniającego kryteria TSUE, ale zachowującego jednocześnie obecne ramy Konwencji oraz uprawnienia EKPC, wydaje się trudne w realizacji.

Przystąpienie Unii jako organizacji międzynarodowej do Konwencji europejskiej pozwoliłoby na zlikwidowanie obecnego dualizmu związanego z istnieniem dwóch niezależnych systemów ochrony praw człowieka. W literaturze przedmiotu podkreśla się, że nastawienie TSUE wyrażone w wydanych opiniach, uzasadnione jest głównie obawą o pozycję prawną orzeczeń Trybunału po dokonaniu akcesji. Trzeba jednak podkreślić, że w obecnym stanie prawnym – wynikającym z reformy lizbońskiej – stopień i skuteczność ochrony praw człowieka realizowane przez TSUE w oparciu o KPP nie ustępują mechanizmom wynikającym z EKPC.

2.4.5. **Zakres stosowania KPP w prawie krajowym**

Zgodnie z art. 51 ust. 1 KPP postanowienia Karty mają zastosowanie w pierwszej kolejności do instytucji, organów i jednostek organizacyjnych Unii, natomiast do państw członkowskich wyłącznie w zakresie, w jakim stosują one prawo Unii. Przepis ten jest rozwinięciem ograniczenia wskazanego w art. 6 ust. 1 zdanie drugie TUE, zgodnie z którym postanowienia Karty w żaden sposób nie rozszerzają kompetencji Unii określonych w traktatach. Dlatego prawdą jest, że Karta nie stanowi samodzielnego aktu prawa międzynarodowego, a jej zastosowanie w krajowym porządku prawnym ograniczone jest do sytuacji, w której stosowane jest prawo UE – a więc w granicach wynikających z zasady przyznania. Jest to istotna różnica w zakresie stosowania KPP w porównaniu do innych norm prawa międzynarodowego, takich jak np. EKPC.

Powyższe rozważania znalazły potwierdzenie w orzecznictwie TSUE. W wyroku z dnia 26 lutego 2013 w sprawie *Fransson*286 Trybunał zauważył, że poszanowanie praw podstawowych chronionych na mocy Karty jest konieczne w sytuacji, gdy przepisy krajowe mieszczą się w zakresie zastosowania prawa Unii. Oznacza to, że stosowanie prawa Unii prowadzi do obowiązku stosowania praw podstawowych wynikających z KPP. W konsekwencji postanowienia Karty nie mogą stanowić samodzielnego podstawy skierowania skargi do TSUE, jeżeli sprawa jednostkowa nie dotyczy stosowania prawa UE287.

W literaturze przedmiotu288 zauważa się, że brak poszukiwania łącznika europejskiego, a w efekcie brak analizy możliwości zastosowania KPP, jest jednym z błędów

---

287 Ibidem, p. 22.
popelnianych przez polskie sądy. Bardziej dobitnie problem wyraził M. Wróblewski, stwierdzając, że „odniesienia do KPP niespełniają tego wymagania [brak łącznika europejskiego], które można odnaleźć w dotychczasowym orzecznictwie polskich sądów, można ocenić wyłącznie w perspektywie ornamentacyjnego wzbogacania zawartości uzasadnienia orzeczeń”\(^{289}\).

Rozpatrując wpływ KPP na obszar praw podstawowych obowiązujących w polskim systemie prawnym, należy przypomnieć o dołączeniu do Traktatu lizbońskiego protokołu (nr 30) w sprawie stosowania Karty Praw Podstawowych UE do Polski i Zjednoczonego Królestwa\(^{290}\). Zgodnie z art. 1 protokołu Karta nie rozszerza zdolności TSUE ani żadnego sądu krajowego do uznania, że przepisy ustawowe, wykonawcze lub administracyjne, praktyki lub działania administracyjne są niezgodne z podstawowymi prawnami, wolnościami i zasadami, które są w niej potwierdzone. W art. 1 ust. 2 doprecyzowano, że nic, co zawarte jest w tytule IV Karty, nie tworzy praw, które mogą być dochodzone na drodze sądowej, z wyjątkiem przypadków, gdy prawo takie wynika z porządku krajowego. Ponadto protokół został uzupełniony o art. 2, w którym wskazano, że w przypadku gdy postanowienie Karty odnosi się do przepisów lub praktyk krajowych, ma ono zastosowanie wyłącznie w zakresie, w jakim prawa i zasady zawarte w tym postanowieniu są uznanne przez krajowe ustawodawstwo lub obowiązujące praktyki. W doktrynie przyjmuje się, że do katalogu praw objętych art. 2 protokołu należą: art. 9 (prawo do zawarcia małżeństwa i prawo do założenia rodziny), art. 10 ust. 2 (wolność myśli, sumienia i religii), art. 14 ust. 3 (prawo do nauki), art. 28 (prawo do rokowań i prawo do działań zbiorowych); art. 34 (zabezpieczenie społeczne i pomoc społeczna), art. 35 (ochrona zdrowia)\(^{291}\).

Protokół nr 30, często wskazywany jako mający charakter opt-out, w rzeczywistości nie prowadzi do wyłączenia stosowania Karty na terytorium Polski.

W pierwszej kolejności należy przypomnieć, że uzasadnieniem dołączenia protokołu przez Polskę było ryzyko, które ówczesny rząd widział w możliwości narzucenia Polsce uznawania małżeństw jednopłciowych oraz ułatwienia dostępu do aborcji poprzez mechanizm wiązających orzeczeń TSUE wydanych na tle art. 8 (prawo do prywatności) oraz art. 9 (prawo

\(^{289}\) M. Wróblewski, *Karta Praw Podstawowych Unii Europejskiej w polskim sądownictwie – problemy i wyzwania*, Kwartalnik Krajowej Rady Sądownictwa, 2015, nr 2, s. 18.

\(^{290}\) Protokół w sprawie stosowania Karty Praw Podstawowych Unii Europejskiej do Polski i Zjednoczonego Królestwa (Dz.U. 2009 Nr 203, poz. 1569).

do zawarcia małżeństwa i prawo do założenia rodziny) KPP\textsuperscript{292}. Stąd, w zamierzeniu, protokół miał uniemożliwić wycofanie z obrotu prawnego przepisów krajowych regulujących te kwestie poprzez stwierdzenie ich niezgodności z KPP. Z drugiej strony, protokół miał zapewnić, że prawa wynikające z KPP zbieżne z prawami funkcjonującymi w krajowym porządku prawnym będą respektowane, a dorobek orzeczniczy ich dotyczący będzie stosowany także w Polsce.

Trybunał Sprawiedliwości UE w wyroku z dnia 21 grudnia 2011\textsuperscript{293} dokonał wykładni przepisów, z której wynika, że protokół nr 30 nie podważa zastosowania Karty wobec Zjednoczonego Królestwa oraz Polski. W ocenie TSUE art. 1 ust. 1 protokołu należy interpretować w taki sposób, że nie ma on na celu zwolnienia z obowiązku przestrzegania postanowień Karty ani uniemożliwienia sądom i trybunałom w tych państwach członkowskich czuwania nad przestrzeganiem jej postanowień\textsuperscript{294}. Celem wskazanej normy jest zapewnienie, że przyjęcie Karty nie prowadzi do przyznania praw wcześniej nieobecnych w krajowych porządkach prawnych\textsuperscript{295}. Jak zatem zauważa K. Kowalik-Bańczyk\textsuperscript{296}, faktyczny skutek prawny protokołu nr 30 sprowadza się do pozbawienia przepisów Karty dwóch cech przynależnych prawu UE: zasady pierwszeństwa nad prawem krajowym, oraz – w zakresie praw zawartych w tytule IV KPP oraz zawierających odwołania do prawa krajowego – zasady bezpośredniego skutku.

Zarówno prawo do poszanowania prywatności, jak i ochrony danych osobowych zostało zagwarantowane w krajowych przepisach konstytucyjnych. Dlatego, ograniczając się do zakresu związanego z problematyką ochrony prywatności cyberprzestrzeni, słuszny jest pogląd, że przyjęcie protokołu 30 nie wpływa na ograniczenie zakresu praw i wolności wynikających z KPP w krajowym porządku prawnym.

W efekcie, uwzględniając przedstawione rozważania, powołanie się przed polskimi sądami na prawa wynikające z Karty wymaga wykazania łącznika z prawem europejskim (art. 51 ust. 1 KPP) oraz uwzględnienia zapisów protokołu 30. Wnioskowanie takie potwierdził Sąd Najwyższy w wyroku z dnia 4 maja 2016\textsuperscript{297}, przypominając jednocześnie, że chociaż Karta jest związana ze stosowaniem prawa UE przez sądy krajowe, to zarzut jej naruszenia

\textsuperscript{294} Ibidem, p. 120.
\textsuperscript{295} Ibidem, p. 119.
\textsuperscript{296} K. Kowalik-Brańczyk, Protokół w sprawie..., op. cit., Nb 5.
\textsuperscript{297} Wyrok SN z 4.05.2016, sygn. IV CSK 270/15, OSNC 2017, nr 1, poz. 12.
może być podnoszony tylko w sytuacji, gdy w sprawie mają lub powinny mieć zastosowanie inne niż Karta przepisy prawa Unii Europejskiej.

2.5. Przepisy konstytucyjne

2.5.1. Ochrona prywatności w polskim porządku prawnym przed rokiem 1997

Rozważania na temat źródeł prawa do poszanowania życia prywatnego nie byłyby kompletnie bez omówienia praw i gwarancji wynikających z przepisów krajowych.

Analizując przepisy konstytucyjne okresu II RP (Konstytucja marcowa z 1921 r.\textsuperscript{298} oraz Konstytucja kwietniowa z 1935 r.\textsuperscript{299}) i PRL (Konstytucja PRL z 1952 r.\textsuperscript{300}), należy zauważyć, że prawo do prywatności nie zostało w nich ujęte \textit{expressis verbis}. Zamiast tego wskazać można cząstkowe gwarancje, które w nauce prawa wskazuje się jako przynależne do sfery prywatności. I tak w Konstytucji marcowej przewidziano gwarancje związane z ochroną nietykalności osobistej (art. 97), ochroną miru domowego (art. 100), zachowaniem tajemnicy korespondencji (art. 106). Z kolei zgodnie z art. 68 ust. 2 Konstytucji kwietniowej poręczono „\textit{wolność osobistą, mieszkania i tajemnicę korespondencji}”. Pamiętać jednak należy, że Konstytucja kwietniowa w rzeczywistości znacząco ograniczała prawa i wolności osobiste w relacji z władzą publiczną. Wyrazem tego była norma art. 10 ust. 1, zgodnie z którą żadne działanie nie mogło stanąć w sprzeczności z celami państwa, wyrażonymi w jego prawach, oraz przepis art. 5, zgodnie z którym państwo zapewniało obywatelom możliwość rozwoju wartości osobistych oraz wolności słowa, sumienia i zrzeszeń, ale granicą tych wolności było dobro powszechne.

W Konstytucji PRL przewidziano utrzymanie gwarancji związanych z nietykalnością osobistą (art. 74 ust. 1), jednak kwestię zakresu nienaruszalności mieszkania i tajemnicy korespondencji delegowano do regulacji zwykłej ustawy (art. 74 ust. 2). Z uwagi na brak poszanowania zasady rządów prawa w okresie PRL faktyczne znaczenie tych regulacji było niewielkie.

Błędem byłoby stwierdzenie, że przed konstytucjonalizacją zasad ochrony prywatności kwestia ochrony życia prywatnego nie była obecna w polskim porządku prawnym. W pierwszej kolejności wskazać należy, że źródłem norm prawnych w tym

\textsuperscript{298} Ustawa z dn. 17 marca 1921 r. - Konstytucja Rzeczypospolitej Polskiej (Dz.U. 1921 nr 44 poz. 267).
\textsuperscript{299} Ustawa Konstytucyjna z dn. 23 kwietnia 1935 (Dz.U. 1935 nr 30 poz. 227).
\textsuperscript{300} Konstytucja Polskiej Rzeczypospolitej Ludowej uchwalona przez Sejm Ustawodawczy w dn. 22 lipca 1952 (Dz.U. 1952 nr 33 poz. 232 ze zm.).
zakresie były akty prawa międzynarodowego, których Polska była stroną – w szczególności EKPC oraz MPPOP. Ponieważ oba traktaty zostały ratyfikowane przez Polskę, ustalone w nich normy stanowiły źródło prawa w krajowym porządku prawnym.

Ponadto istotne znaczenie miały także przepisy cywilistyczne związane z obszarem ochrony dóbr osobistych. Wskazać należy art. 23 oraz art. 24 ustawy – Kodeks cywilny (dalej: kc)301, który już w brzmieniu pierwotnym z 1964 roku wprowadzał prawną ochronę nietykalności mieszkania, tajemnicy korespondencji oraz ochronę czci i dobrego imienia. Obszar sfer życia objętych ochroną obejmował zatem znaczną część aktywności uwalnionych w definicji życia prywatnego w międzynarodowych systemach ochrony praw człowieka (por. wcześniejsze rozważania dot. art. 12 PDPC, art. 17 MPPOP i art. 8 EKPC).

Na tle norm cywilistycznych oraz wskazanych traktatów międzynarodowych wyróżnić trzeba jednak dwie zasadnicze różnice. Po pierwsze, w redakcji art. 23 kc nie posłużono się expresis verbis terminem ochrony życia prywatnego. W efekcie przepisu tego nie można traktować jako samodzielnego i wystarczającego źródła ochrony jednostki przed ingerencją w sferę prywatności rozumianą w ujęciu szerokim, znany w nauce jako „prawo do bycia pozostawionym w spokoju”. Drugim istotnym ograniczeniem wskazanej normy jest jej cywilistyczny charakter – a więc z definicji mający ograniczone zastosowanie w relacjach z władzą publiczną.

Wraz z przemianami politycznymi po 1989 roku oraz wzmocnieniem znaczenia ochrony praw człowieka problem potwierdzenia istnienia oraz zakresu prawnej ochrony prywatności, w szczególności przed ingerencją ze strony władzy publicznej, zyskał na aktualności i stał się przedmiotem analizy judykatury. Jak zauważył Sąd Najwyższy w wyroku 8 kwietnia 1994 „w demokratycznym państwie prawa zasadą jest, iż jednostka winna być chroniona, a sądy mają w tym zakresie szczególną rolę, przed wszelkimi niezasadnymi i arbitralnymi ograniczeniami wolności ustanawianymi przez władze publiczne. Wolności obywatelskie są zatem elementem wspólnego, demokratycznego i legalistycznego porządku, przeto mogą być również z uwagi na wspólne dobro i interesy w rozsądny i odpowiadający prawu sposób ograniczone, przy uwzględnieniu służącego każdemu obywatelowi prawa do prywatności chroniącego indywidualną sferę jego osobistego życia” 302.

Z kolei Trybunał Konstytucyjny przeprowadził rozważania związane z zakresem ochrony prywatności na gruncie nadal obowiązujących przepisów Konstytucji PRL. Podstawą

301 Ustawa z dn. 23 kwietnia 1964 – Kodeks cywilny (Dz.U. z 2017 r. poz. 459 ze zm.).
analizy był znowelizowany art. 1 Konstytucji303, w którym wskazano, że Rzeczpospolita Polska jest demokratycznym państwem prawa. Na tym tle Trybunał uznał, że z zasady tej można wywieźć istnienie samodzielnego prawa do prywatności, rozumianego między innymi jako prawo do zachowania w tajemnicy informacji o swoim życiu prywatnym304.

2.5.2. Konstytucja RP z 1997 roku

Wraz z wejściem w życie Konstytucji RP z 1997 roku ochrona prywatności zyskała rangę gwarancji konstytucyjnej. Jej podstawę stanowi art. 47 Konstytucji, zgodnie z którym każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Podobnie jak w omówionych w poprzednich podrozdziałach traktatach międzynarodowych również polski ustrojodawca nie zdecydował się na wprowadzenie zamkniętej definicji terminu prywatność. Zamiast tego norma wskazana w art. 47 Konstytucji określa sfery życia tradycyjnie kojarzone z życiem prywatnym. W doktrynie wskazuje się, że katalog określony w art. 47 nie wprowadza zamkniętej listy dóbr chronionych, a jedynie służy wyliczeniu przykładowych wartości podlegających ochronie305. Wniosek taki wynika również z analizy orzecznictwa306. Jest to przy tym katalog zbliżony do wskazanego w art. 12 PDPC. Uwzględniając fakt, że kwestia ochrony tajemnicy korespondencji została uregulowana w polskiej ustawie zasadniczej w art. 49, należy uznać obie wyżej wskazane normy za znaczeniowo tożsame.

W orzecznictwie TK wskazuje się na silne zwią zestanie ochrony prywatności z godnością człowieka: „zachowanie godności wymaga bowiem poszanowania jego sfery czysto osobistej, gdzie nie jest narażony na konieczność bycia z innymi czy dzielenia się z innymi swoimi przeżyciami czy doznaniami o intymnym charakterze”307.

Z poglądu tego, a także z zasady powszechności korzystania z konstytucyjnych praw i wolności (art. 37) oraz z redakcji samego art. 47 („każdy”) wnioskować należy, że konstytucyjna ochrona prywatności przysługuje wszystkim osobom fizycznym, niezależnie od

305 K. Łakomiec wskazuje, że przepisy konstytucyjne wprowadzające zasadę ochrony prywatności „należy uznać za agregat norm (instytucję), na który ze względu na więź funkcjonalną składają się normy kształtujące prawa podmiotowe jednostki i nakładające na państwo określone obowiązki skorelowane z tymi prawami”. K. Łakomiec, Konstytucyjne gwarancje ochrony prywatności informacyjnej wobec rozwoju nowych technologii, Przegląd Legislacyjny 2015, nr 1, s. 64.
306 Przykładem może być postanowienie Sądu Najwyższego z 27.10.2005 (sygn. III CK 155/05), w którym z normy art. 47 Konstytucji wywiedziono prawo do decydowania o wyborze metody leczenia, w tym także wyrażenia sprzeciwu na wykonanie zabiegu leczniczego pro futuro.
jej obywatelstwa. Kwestię dyskusyjną w doktrynie pozostaje zakres gwarancji związanych z ochroną prywatności przynależny innym osobom308.

Odpowiedzialność władzy publicznej wynikająca z art. 47 nie ogranicza się do obowiązków negatywnych, związanych z powstrzymaniem się przed nieuprawnioną ingerencją w dobro chronione, ale również wyraża się koniecznością realizacji przesłanek pozytywnych – polegających na zapewnieniu poszanowania prywatności jednostki w relacjach horyzontalnych. Środkiem realizacji tego obowiązku jest wdrożenie skutecznych i dostępnych mechanizmów ochrony praw. Jak wskazuje się w orzecznictwie TK, w przypadku naruszenia prawa do prywatności każdy powinien dysponować możliwością ochrony prawnej na drodze sądowej – a pominięcie w ustawie dostępu do sądu jest wystarczającą przesłanką do uznania badanego przepisu za niezgodnego z ustawą zasadniczą309.

Przepis art. 47 został uzupełniony normą art. 51 odnoszącą się do kwestii ochrony danych osobowych W szczególności, zgodnie z art. 51 ust. 1 nikt nie może być obowiązywany, inaczej niż na podstawie ustawy, do ujawniania informacji dotyczących jego osoby. Jak zauważał TK, przepis ten dotyczy wszelkich przypadków, w których jednostka zobowiązana zostaje do ujawniania informacji o sobie innym podmiotom, a więc także podmiotom prywatnym310. Z kolei biorąc pod uwagę kształt przepisów określonych w art. 51 ust. 2-5, w treści których odwołano się do władzy publicznej, w doktrynie przyjmuje się, że mają one skutek wyłącznie wertykalny311.

Uwagę zwraca ponadto redakcja art. 51 ust. 2 określająca ograniczenia władzy publicznej w gromadzeniu danych dotyczących obywateli. Przepis art. 47 oraz art. 51 ust. 1 i 3-4 odnoszą się do kwestii ochrony prywatności wszystkich osób, niezależnie od faktu posiadania przez nich polskiego obywatelstwa. Błędem byłoby jednak wyprowadzenie z ograniczenia stosowania normy art. 52 ust. 2 wyłącznie do obywateli wniosku, że uprawnienia władzy publicznej w gromadzeniu danych dotyczących pozostałych osób są niczym nieskrępowane. W takim przypadku zakres ochrony jednostki oraz związaną z nią granicę dopuszczalnej ingerencji władzy publicznej należy wywieźć z bardziej ogólnej normy art. 47.

W judykатурze podkreśla się, że art. 47 i art. 51 Konstytucji są ze sobą ścisłe powiązane i chronią tę samą wartość konstytucyjną, jaką jest sfera prywatności. Prywatność jest w takim rozumieniu utożsamiana ze stanem niezależności jednostki, w ramach której może ona decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu, a także prawem do kształtowania własnego wizerunku w stosunkach społecznych. Na tym tle wypracowana została koncepcja tzw. autonomii informacyjnej, rozumianej jako prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby oraz sprawowania kontroli nad informacjami znającymi się w posiadaniu innych podmiotów.

W konsekwencji, jak wskazał SA w Warszawie, sama jednostka swoim zachowaniem wyznacza sferę zdarzeń, które mogą być ujawniane bezpośrednio lub pośrednio innym osobom, oraz sferę zdarzeń chronionych, które zgodnie z wolą jednostki nie są dostępne dla osób trzecich. W efekcie jednostka swoim zachowaniem, w ramach przysługującej jej autonomii, wyznacza zakres chronionej prywatności. Przy czym należy zaznaczyć, że pod pojęciem zachowania należy rozumieć nie tylko działania jednostki, ale i zaniechania (np. tolerowanie publikowania określonych informacji w sferze publicznej).

Gwarancje związane z ochroną prywatności w kształcie wynikającym z art. 47 i 51 zostały uzupełnione przepisami szczegółowymi, regulującymi obszary takie jak gwarancja nietykalności i wolności osobistej (art. 41), tajemnica korespondencji (art. 49), nienaruszalność mieszkania (art. 50) czy wolność sumienia i wyznania (art. 53). Ponadto z art. 76 Konstytucji wynika ochrona konsumentów, użytkowników i najemców przed działaniami zagrażającymi między innymi ich prywatności.

K. Łakomiec zwraca uwagę, że na podstawie art. 47 i 51 Konstytucji można zrekonstruować publiczne prawo podmiotowe po stronie jednostki. Jednocześnie jednak prawo to ma skutki horyzontalny, „ponieważ w ramach jego realizacji powstają normy kształtujące relacje między jednostkami w dziedzinie przetwarzania danych osobowych. W ten sposób z publicznym prawem podmiotowym sprzężone jest prywatne prawo podmiotowe, związane z oczekiwaniami dotyczącymi ochrony prywatności informacyjnej w stosunkach prywatnoprawnych.”

---

314 Por. wyrok SN 11.02.2015, sygn. I CSK 868/14 (Legalis 1231461) i przywołane tam orzecznictwo.
315 Por. na tym tle rozważania przedstawione w rozdziale 1.2 dotyczące koncepcji sfer A. Kopffa.
316 Wyrok SA w Warszawie z 29.07.2014, sygn. VI ACa 1657/13, Legalis 1093024.
317 K. Łakomiec, Konstytucyjne gwarancje..., op.cit., s. 64.
2.5.3. Limitacja i derogacja

Ochrona prywatności i autonomia informacyjna nie mają charakteru absolutnego. Ustrojiodawca przewidział zarówno możliwość limitacji, jak i derogacji praw i gwarancji osobistych. Rozważania o zakresie możliwych do wprowadzenia środków ograniczających prawa i wolności konstytucyjne ma tym większe znaczenie, że zgodnie z powszechnym w doktrynie i krajowej judykaturze poglądem konstytucja jest aktem najwyższego rzędu, zatem prawnomiędzynarodowe ograniczenia w stosowaniu ingerencji w prawa podstawowe nie mają zastosowania do krajowych przepisów konstytucyjnych. Jak wynika z orzecznictwa TK, konstytucja jest „prawem najwyższym Rzeczypospolitej Polskiej” w stosunku do wszystkich wiążących umów międzynarodowowych, nie wyłączając prawa unijnego. W konsekwencji korzysta ona na terytorium Polski z pierwszeństwa obowiązywania i stosowania.

Zgodnie z przepisem art. 31 ust. 3, nazywanym w doktrynie tzw. ogólną klauzulą ograniczającą, ograniczenia w korzystaniu z 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 także naruszać istoty wolności i praw. W odniesieniu do ochrony prywatności kryteria ustanowione w art. 31 ust. 3 są zatem zbieżne z warunkami wynikającymi z art. 8 ust. 2 EKPC i opierają się na łącznym spełnieniu dwóch warunków: pierwszy to nakaz istnienia ustawowej podstawy prawnej (w przypadku EKPC interpretowanej przez ETPC jako wymaganej zgodności zasadą rządów prawa), drugi to niezbędność wprowadzenia rozpatrywanego środka w celu ochrony najważniejszych funkcji państwa demokratycznego lub wolności i praw innych osób.

---


319 Ibidem, p. 10: interpretacja zasady pierwszeństwa konstytucji w kontekście prawa europejskiego jest rezultatem bogatego już orzecznictwa polskiego TK, zob. wyroki: TK z 27 maja 2003 r., K 11/03 (referendum ogólnokrajowe o akcesji Polski do UE); z 21 kwietnia 2004 r., K 33/03 (biopaliwa); z 31 maja 2004 r., K 15/04 (wybory do PE – prawo wybieralności obywateli innych państw członkowskich); z 12 stycznia 2005 r., K 24/05 („ustawa kooperacyjna”); z 11 maja 2005 r., K 18/04 (konstytucyjność Traktatu akcesyjnego); z 20 lutego 2006 r., K 9/05 (wybory samorządowe – wymóg stałego zamieszkania); z 16 lipca 2009 r., Kp 8/08 (rola opinii Europejskiego Banku Centralnego w procesie ustawodawczym w Polsce); z 5 października 2010 r., SK 26/08 (Europejski nakaz aresztowania); z 24 listopada 2010 r., K 32/09 (konstytucyjność Traktatu z Lizbony); z 16 listopada 2011 r., SK 45/09 (konstytucyjność prawa pochodnego); z 26 czerwca 2013 r., K 33/12 (tryb ratyfikacji decyzji Rady Europejskiej 2011/199/UE w sprawie zmiany art. 136 TUE) oraz postanowienia: z 19 grudnia 2006 r., P 37/05 (akcyza – podział kompetencji między TK a TFUE); z 17 grudnia 2009 r., U 6/08 (rybolowstwo – krajowe akty prawne wykonujące prawo UE).


322 Należy pamiętać o odmiennym stanowisku TSUE – zob. 2.4.1.
Trybunał Konstytucyjny w wyroku z dnia 25 lipca 2006 uznał, że sformułowanie „tylko w ustawie” wskazane w art. 31 ust. 3 wskazuje na konieczność kompletnego uregulowania ograniczenia w formie ustawowej. Nie może więc prawodawca usankcjonować na drodze delegacji ustawowej środka służącego ograniczeniu praw podstawowych, wprowadzonego aktem niższego rzędu (np. rozporządzeniem). Potwierdzenia poprawności takiego wnioskowania odszukać można we wcześniejszym orzeczeniu Trybunału, w którym wskazano, że dosłowne rozumienie zastrzeżenia wyłącznie ustawowej rangi na szczególne znaczenie dla ograniczeń odnoszących się do sfery wolności i praw człowieka: „w żadnym wypadku, 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”. W opinii Trybunału rozwiązanie takie byłoby możliwe, gdyby w redakcji art. 31 ust. 3 przyjąć sformułowanie „w drodze ustawy”, zastosowane np. przy regulacji dotyczącej swobody działalności gospodarczej (art. 22).


Obok ogólnej klauzuli ograniczającej w Konstytucji wyróżnić można też klauzule szczegółowe, odnoszące się swoim zakresem do poszczególnych praw lub grupy praw.

---

326 Szersze rozważania nt. zasady proporcjonalności na tle krajowych norm konstytucyjnych w: M. Korycka, Zasada proporcjonalności – refleksje na gruncie aksjologicznych podstaw Konstytucji z 1997 roku oraz orzecznictwa Trybunału Konstytucyjnego, [w:] Wykładnia prawa i inne problemy filozofii prawa pod. red. L. Morawskiego, Toruń 2005, s.43-58.
Przykładem takich klauzul może być np. wymóg zgodności ograniczenia z umowami międzynarodowymi (art. 59 ust. 4) lub nakaz istnienia podstawy ustawowej wraz z wydaniem prawomocnego orzeczenia sądu (art. 48 ust. 2). Ustrojodawca nie zastosował w redakcji art. 47 (prawo do prywatności) dodatkowych warunków ograniczających. Klauzule takie zostały natomiast wprowadzone w art. 51 (ochrona danych osobowych). W szczególności zgodnie z art. 52 ust. 2 uprawnienie władzy publicznej do gromadzenia danych o obywatelach zostało ograniczone do sytuacji „niezbędnych” w demokratycznym państwie prawnym. Sformułowanie to może budzić wątpliwości interpretacyjne – różnica pomiędzy art. 31 ust. 3 (ogólna klauzula ograniczająca) a art. 51 ust. 2 (klauzula szczegółowa w odniesieniu do danych osobowych) sprowadza się do zastąpienia słowa „konieczne” terminem „niezbędne”.

Należy zauważyć, że art. 31 ust. 3 dotyczy zastosowania środków ograniczających prawa i wolności, natomiast art. 51 ust. 2 do ogólnej zasady gromadzenia tylko takich danych, które są konieczne z punktu widzenia celów demokratycznego państwa prawa. Prawdą jest jednak, że w art. 52 ust. 2 nie wskazano katalogu celów uzasadniających zastosowanie ograniczenia. Powstaje zatem pytanie o wzajemną relację art. 31 ust. 3 oraz art. 52 ust. 2 – a w szczególności, czy cele wymienione w art. 31 ust. 3 (np. bezpieczeństwo i porządek publiczny, ochrona praw i wolności innych osób) wyznaczają granice dopuszczalnej ingerencji także dla środków wprowadzanych na podstawie art. 52 ust. 2. Kwestię tę można również przedstawić inaczej – czy istnieje cel szczególny, który jest „niezbędny” w państwie demokratycznym, ale nie został wskazany w art. 31 ust. 3.

W kontrowersyjnym wyroku z 13 grudnia 2011 TK uznał, że sytuacja taka może mieć miejsce – „oprócz wartości wymienionych w art. 31 ust. 3 Konstytucji, mogą także wystąpić dalsze stosowne do art. 51 ust. 2 Konstytucji, jeśli uzna się je za niezbędne w demokratycznym państwie prawnym”329. Podgląd ten jest krytykowany w doktrynie jako prowadzący do przypisania autonomii informacyjnej mniejszego zakresu ochrony, niż wynikałoby ze stosowania klauzuli ogólnej z art. 31 ust. 3330. Co więcej, uznanie zasadności ingerencji w prawo do ochrony prywatności w oparciu o inne, niewymienione w normie konstytucyjnej, ale „niezbędne” cele mogłoby doprowadzić do nieograniczonej swobody wprowadzania ograniczeń przez prawodawcę. Konsekwencją byłaby kolizja z innymi

normami konstytucyjnymi i przepisami prawa międzynarodowego (w szczególności art. 8 ust. 2 EKPC\(^{331}\)).

Oddzielnego omówienia wymaga zakres stosowania klauzuli derogacyjnej przewidzianej w art. 233 Konstytucji do obszaru prawa do poszanowania prywatności (art. 47) oraz ochrony autonomii informacyjnej (art. 51). Ustrojodawca zdecydował się wymienić w ust. 1 przepisu zamknięty katalog wolności i praw, które nie mogą być ograniczone w przepisach ustawowych dotyczących czasu stanu wojennego i wyjątkowego. Do katalogu tego należy prawo do ochrony prywatności (art. 47), nie wymieniono natomiast w nim prawa do ochrony danych osobowych (art. 51). Z kolei w ust. 3 wskazano enumeratywnie prawa i wolności, które mogą zostać ograniczone w związku z wprowadzeniem stanu klęski żywiołowej. Na liście nie uwzględniono art. 47 i 51, co oznacza, że ogłoszenie stanu klęski żywiołowej nie może wiązać się z wprowadzeniem środków ograniczających zakres tych praw.

Jak zauważa M. Safjan\(^{332}\), konsekwencją zaliczenia prywatności do praw, które nie mogą podlegać ograniczeniom nawet z uwagi na stan wojenny lub wyjątkowy, jest uznanie, że ochrona prywatności należy do grona praw i gwarancji o najsilniejszej ochronie konstytucyjnej\(^{333}\).

### 2.6. Podsumowanie

Prawo do prywatności, jako nierozwalnie związane z godnością człowieka, zostało zaliczone do katalogu praw podstawowych we wszystkich omówionych systemach ochrony praw człowieka. Zwraca uwagę podobną, mającą genezę w PDPC, treść prawa ochronnego – w której skoncentrowano się na podkreślaniu aspektu negatywnego obowiązku władzy publicznej, a samą prywatność zdefiniowano poprzez wyliczenie przykładowych wartości chronionych. Zastosowanie takiego podejścia prowadzi do możliwości stosowania interpretacji rozszerzających, skutkujących objęciem ochroną dóbr niewymienionych wprost w przyjętej treści normy. W efekcie możliwe jest uwzględnienie w tak zdefiniowanym prawie do prywatności sferę aktywności jednostki w cyberprzestrzeni, a także wprowadzenie pozytywnego obowiązku państwa w regulacji i zapobieganiu negatywnym zjawiskom, które na tę sférę mogą oddziaływać.

\(^{331}\) Postanowienie ETPC w sprawie Weber i Saravia v. Niemcy, § 92-94.


\(^{333}\) Tak też: TK w wyroku K 41/02, p. 25.
Chociaż we wszystkich omawionych traktatach treść prawa materialnego wyrażono w podobny sposób, to jednak w przedstawionej analizie wykazano istotne różnice pomiędzy faktycznymi gwarancjami z perspektywy jednostek. Różnice te mają dwie najważniejsze przyczyny: odmienną rolę i umocowanie ustanowionego organu kontrolnego (sądowego) oraz różny zakres wpływu norm traktatowych na możliwość dochodzenia praw przed sądami krajowymi.

We wszystkich przedstawionych systemach ochrony praw funkcjonuje organ kompetentny do rozstrzygania sporów – o uprawnieniach kontrolnych (KPC) lub sądowych (ETPC, TSUE). Ograniczone kompetencje KPC, zwłaszcza w zakresie konieczności wcześniejszego uznania jurysdykcji do rozstrzygnięcia konkretnej sprawy, a także brak wiążącego charakteru wydanych orzeczeń stanowią istotne ograniczenie Paktu. Chociaż KPC wydał liczne komentarze ogólne mające wpływ na interpretację postanowień art. 17 MPPOP, również te dokumenty nie mają charakteru prawnie wiązającego. W rezultacie w zakresie ochrony prywatności w cyberprzestrzeni przepisy Paktu nie prowadzą do standaryzacji prawodawstwa krajowego państw-stron układu. Istotną funkcją budowania ponadnarodowej przestrzeni przetwarzania danych jest wspólne regulowanie zasad i minimalnych wymagań, jakie wszystkie państwa zobowiązują się stosować. Zasady te nie mogą być a priori zawarte w traktacie, ponieważ w sposób oczywisty uległy szybkiej dezaktualizacji. Stąd też potrzeba wprowadzenia mechanizmu dostosowawczego, który mając odpowiednie umocowanie traktatowe, stanowilby podstawę do wydawania interpretacji wiążących prawnie wszystkie strony. Pakt nie posiada takiego potencjału, zwłaszcza biorąc pod uwagę ograniczoną skuteczność orzeczeń KPC (niebędących de facto wyrokami, a „uzasadnionymi poglądami”), jak i niewiążący charakter wydawanych komentarzy ogólnych. Chociaż KPC wypowiedział się w komentarzu ogólnym nr 31, że przepisy Paktu mają charakter erga omnes, to jednak zauważył, że nie wywierają one bezpośredniego skutku horyzontalnego, a zatem nie tworzą obowiązków w relacjach pomiędzy jednostkami. Należy też pamiętać, że niektóre państwa-strony zastosowały ograniczenia w tym zakresie w ramach procedury ratyfikacji. Najważniejszym przykładem, zwłaszcza biorąc pod uwagę badaną problematykę, są Stany Zjednoczone. Kongres Stanów Zjednoczonych zgłosił największą liczbę zastrzeżeń i oświadczeń w procedurze ratyfikacji spośród wszystkich państw-stron Paktu. Efektem jednej z nich jest brak bezpośredniego skutku postanowień traktatu w prawodawstwie amerykańskim. Porównanie systemu prawnego Stanów Zjednoczonych oraz państw

334 Komitet Praw Człowieka, General comment No. 31..., op. cit., p. 8.
335 Zob. przypis 734 (s. 281).
europejskich obrazuje, jak różny model ochrony prywatności może funkcjonować w prawodawstwie różnych państw, z których wszystkie są stronami MPPOP – a więc tej samej umowy międzynarodowej, tworzącej ramy prawnej ochrony prywatności. Dlatego, chociaż Pakt jest obecnie traktatem o największym globalnym zasięgu, to w obecnej formie nie może stanowić skutecznego środka prawnego służącego zbudowaniu wspólnych, ponadnarodowych i spójnych ram ochrony prywatności w cyberprzestrzeni.

System europejskiej konwencji, chociaż funkcjonuje w oparciu o traktat przyjęty ponad 10 lat wcześniej niż Pakt, jest pozbawiony większości z omówionych powyżej wad. Po pierwsze, ETPC jest organem sądowym, a nie kontrolnym czy quasi-sądowym\(^{336}\). W efekcie jego orzeczenia mają moc wiążącą państwa, do których są adresowane. Konsekwencją jest także możliwość stosowania rozszerzającej interpretacji przepisów konwencji, jak i wypracowanie ugruntowanej linii orzeczniczej w konkretnych typach spraw – w tym dotyczących kwestii inwigilacji i naruszeń związanych z prawem do prywatności. W przypadku EKPC problemem jest jednak brak odniesienia wydanych wyroków do sytuacji prawnej jednostki przed sądami krajowymi. Ta cecha oraz dodatkowo długi okres związany z wydaniem rozstrzygnięcia powoduje, że Trybunał w wielu przypadkach nie może stanowić skutecznej drogi ochrony sądowej w jednostkowych przypadkach związanych z naruszeniami prywatności. Co więcej, konstrukcja Konwencji utrudnia ochronę praw w przypadku, gdy naruszenie nie ma charakteru wertykalnego, ale horyzontalne – z perspektywy jednostki skarżenie do Trybunału państwa, a nie podmiotu odpowiedzialnego za naruszenie, jest kłopotliwe w sytuacji, gdy podmiot jest organizacją wielooddziałową i prowadzącą działalność w różnych państwach. Ostatni z problemów w stosowaniu Konwencji stanowi brak skutecznych mechanizmów obligowania państwa do dostosowania się do wydanego przez Trybunał wyroku\(^{337}\).

Zarówno w treści przepisów MPPOP, jak i EKPC nie uwzględniono *explicit* prawa do ochrony danych osobowych. W obu systemach przyjmuje się, że dane osobowe należą do sfery prywatności człowieka i jako takie podlegają ochronie na podstawie norm traktatowych związanych z ochroną prywatności. Wskazane traktaty nie definiują jednak szczegółowych obowiązków związanych z ochroną danych osobowych, a ponadto nie wprowadzają

---

\(^{336}\) Definicje organów kontrolnych, quasi-sądowych i sądowych przedstawiono w rozdziale 2.1.

konieczności powołania niezależnego organu nadzoru. Rozszerzająca interpretacja traktatów nie może prowadzić do zdefiniowania nowych obowiązków instytucjonalnych dla państw-stron układu, wobec czego w obecnym kształcie traktatów brak jest możliwości zapewnienia, aby obszar ochrony danych podlegal niezależnemu nadzorowi. Z drugiej strony, nadzór taki stanowi jeden z fundamentów unijnego modelu ochrony danych osobowych i wprost wynika z art. 8 ust. 3 KPP.


Postulat ten w dużej mierze realizuje prawo UE, w szczególności KPP (a także regulacje prawa wtórnego, szeroko omówione w rozdziale 4). Prawodawstwo unijne prowadzi do stworzenia spójnego i jednolitego rynku wewnętrznego, także w obszarze przetwarzania informacji. Otwarte pozostaje pytanie, czy przyjęte rozwiązania są wystarczające do zapewnienia odpowiedniej ochrony przewarzanych danych także w przypadku ich przekazywania po obszar UE338.

Krajowe przepisy konstytucyjne uzupełniają regulacje wynikające z omówionych aktów prawnomiędzynarodowych, których Polska jest stroną. Jak wskazano, również przed przyjęciem obecnej ustawy zasadniczej Trybunał Konstytucyjny potwierdził istnienie prawa do prywatności jako gwarancji chronionej konstytucyjne. Jakkolwiek nowoczesne regulacje konstytucyjne, obowiązujące w Polsce, w dużej mierze pokrywają się z normami MPPOP, EKCP i KPP i uzupełniają je, to należy pamiętać o ich istotnym ograniczeniu – zasięgu stosowania tylko do terytorium Polski. Nie zmienia to faktu, że normy konstytucyjne powinny

338 Szersze omówienie w rozdziale 4 (prawo UE) oraz rozdziale 6 (przetwarzanie w chmurze obliczeniowej).
być podstawowym gwarantem w zakresie realizacji przez władzę publiczną zarówno obowiązków pozytywnych, jak i negatywnych w obszarze ochrony prywatności\textsuperscript{339}.

Przedstawiona analiza systemów ochrony praw człowieka wskazuje na ich ograniczoną przydatność w zakresie ochrony prywatności w cyberprzestrzeni. Funkcja ochronna przepisów pozwala na wyznaczenie granic nieuprawnionej ingerencji, nie prowadzi jednak do wypracowania wspólnych, ponadnarodowych standardów przetwarzania informacji w cyberprzestrzeni. Brak takich mechanizmów, prowadzących do powstania bezpiecznej przestrzeni przetwarzania danych, powoduje, że cyberprzestrzeń nadal traktowana jest jako obszar podlegający znacznej swobodzie regulacyjnej ze strony poszczególnych państw. Systemy ochrony praw człowieka pozwalają zatem na określenie ram, w jakich należy się poruszać szukając odpowiedzi na pytanie o skuteczne środki ochrony praw podstawowych w cyberprzestrzeni, jednak \emph{per se} nie stanowią rozwiązania tak zdefiniowanego problemu.

\textsuperscript{339} Szersze omówienie w rozdziale 5. (obowiązki pozytywne) oraz rozdziale 8. (obowiązki negatywne).
Rozdział 3. Ewolucja zasad ochrony danych osobowych

3.1. Wprowadzenie

Jak wskazano we wcześniejszych rozważaniach, prawo do poszanowania życia prywatnego oraz ochrona danych osobowych są ze sobą ścisłe powiązane, a ich cel stanowi ochrona tego samego dobra – sfery prywatności człowieka340.

Celem niniejszego rozdziału jest przedstawienie najważniejszych międzynarodowych aktów prawa dotyczących obszaru ochrony danych osobowych, z których większość miała charakter wytycznych, a więc niewiążący prawnie. Tym niemniej wywarły poważny wpływ na przepisy krajowe i prawo UE. W szczególności omówiona zostanie ewolucja podstawowych zasad przetwarzania oraz sposób definiowania zakresu przedmiotowego i podmiotowego prawa do ochrony danych osobowych.

Dziwić może zestawienie i łączne omówienie razem z dokumentami o charakterze rekomendacji i wytycznych, Konwencji 108 Rady Europy, będącej prawnie wiążącą umową międzynarodową. Trzeba jednak przypomnieć, że w czasach, gdy Konwencja 108 była opracowywana i przyjmowana, jej głównym celem było propagowanie podstawowych zasad ochrony danych osobowych w krajowych systemach prawnych – w tym zakresie jej cel był zbieżny z pozostałymi dokumentami, publikowanymi przez organizacje międzynarodowe w latach siedemdziesiątych i osiemdziesiątych dwudziestego wieku.

Rozdział zakończy omówienie tzw. Rezolucji Madryckiej, a więc propozycji międzynarodowych standardów ochrony danych osobowych opracowanych w 2009 roku. Dokument stanowi ważny głos w dyskusji, ponieważ został przygotowany przez krajowe organy nadzoru i prezentuje wyniki ponad dwudziestoletnich doświadczeń w stosowaniu krajowych przepisów o ochronie danych osobowych. Można zatem widzieć w Rezolucji Madryckiej przykład drugiej generacji wytycznych w zakresie zasad przetwarzania danych osobowych.

3.2. Wczesne rozwiązania prawne

Wraz z dynamicznym rozwojem technik przetwarzania informacji w II połowie dwudziestego wieku coraz częściej podnoszony był problem wprowadzenia odpowiednich

gwarancji prawnych związanych z prawami osób, których dane są przetwarzane. Problem ten był rozpatrywany zarówno na poziomie krajowym, jak i organizacji międzynarodowych. W literaturze przedmiotu wskazuje się szwedzką ustawę o ochronie danych z 1973 roku jako pierwszy akt prawny wprowadzony w celu zwiększenia gwarancji dotyczących ochrony prywatności w związku z przetwarzaniem danych osobowych w systemach komputerowych. W ustawie tej przyjęto model ochrony niestosowany później – zamiast wprowadzać określone zasady przetwarzania danych oraz określać prawa i gwarancje dla jednostek prawodawca zdecydował się zastosować model obowiązkowej rejestracji systemów informatycznych, koniecznej w celu dopuszczenia systemu do przetwarzania danych osobowych. W trakcie procesu rejestracji upoważniony do tego organ wskazywał konkretne zasady przetwarzania, które administrator systemu był zobowiązany wdrożyć. Podejście takie bardzo szybko okazało się trudne w praktycznym zastosowaniu – z uwagi na dynamiczny rozwój branży przetwarzania informacji oraz lawinowy wzrost liczby systemów przetwarzających dane osobowe. Warto jednak zauważyć, że do dzisiaj podejście polegające na certyfikacji systemów przetwarzających informacje jest nadal stosowane w Polsce w obszarze dopuszczania do eksploatacji systemów przetwarzających informacje niejawne.

Odmienne podejście zastosowano w amerykańskiej ustawie Fair Credit Reporting Act z 1970 roku (dalej FCRA), dotyczącej ochrony informacji gromadzonych i przetwarzanych w celu analizy informacji kredytowych. Prawodawca określił minimalne zabezpieczenia proceduralne, które muszą być spełnione przez administratorów danych – takie jak dbanie o jakość danych (rozumiana jako zapewnienie ich dokładności i aktualności), udostępnienie danych na żądanie osób, których dane dotyczą. Podejście zastosowane w FCRA zostało zauważone także na płaszczyźnie międzynarodowej.

W 1973 roku Komitet Ministrów Rady Europy przyjął rezolucję 73/22 dotyczącą ochrony prywatności jednostek w stosowaniu elektronicznych banków danych w sektorze prywatnym. Dokument miał formę rekomendacji i podsumowywał dotychczasowe

---

343 Szersze omówienie ustawy w: J. Kosik, Ochrona jednostki w prawie szwedzkim przed zastosowaniami komputera, Państwo i Prawo 1975, nr 6, s. 111-121.
344 Por. art. 50 ustawy z dn. 5.08.2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228 ze zm.).
345 Ustawa federalna USA z dn. 26.10.1970 r. o uczciwych informacjach kredytowych (Fair Credit Reporting Act), 84 Stat. 1114-2.
347 Por. odwołanie p. 9 w rezolucji 73/22 (zob. przypis 218).
348 Komitet Ministrów Rady Europy, Rezolucja (73) 22 z 26.09.1973 dotyczącą ochrony prywatności jednostek w odniesieniu do elektronicznych banków danych w sektorze prywatnym.
rozważania związane z potrzebą i sposobami ochrony danych przetwarzanych w systemach informatycznych. W załączniku do rezolucji wskazano dziesięć najważniejszych zasad, które powinny zostać uwzględnione w krajowych przepisach dotyczących ochrony danych osobowych. W pierwszej kolejności podkreślono znaczenie jakości danych oraz ogólnej reguły, zgodnie z którą sensytywne dane osobowe – czyli takie, których przetwarzanie może prowadzić do bezprawnej dyskryminacji – nie powinny być gromadzone oraz rozpowszechniane. Ponadto zdefiniowano postulaty przetwarzania danych tylko w zakresie zdefiniowanego celu, wprowadzenia prawa dostępu i poprawienia informacji przez podmioty danych, jak i zakazu gromadzenia danych z wykorzystaniem oszukańczych lub bezprawnych środków. W dokumencie wskazano także na potrzebę wprowadzenia międzynarodowej konwencji, będącej środkiem ponadnarodowej standaryzacji oraz podniesienia minimalnych wymagań prawnych związanych z przetwarzaniem danych osobowych na grunt krajowych systemów prawnych członków RE.

W ogłoszonej rok później rezolucji 74/29 określono zasady ochrony prywatności w stosowaniu elektronicznych banków danych w sektorze publicznym. Podobnie jak w przypadku wcześniej omawianej rezolucji również przedmiotowy dokument miał charakter niewiążących rekomendacji dla państw członkowskich. Jako jedną z najważniejszych reguł wskazano jawność w tworzeniu, eksploatacji i rozwoju elektronicznych systemów informacyjnych funkcjonujących w sektorze publicznym. Ponadto rozbudowano i doprecyzowano zasady związane z przetwarzaniem informacji sensytywnych oraz zapewnianiem jakości danych. Zgodnie z wytycznymi wynikającymi z rezolucji 73/22 dane sensytywne (zawierające informacje wrażliwe) lub dane, które mogą posłużyć do bezprawnej dyskryminacji, co do zasady nie powinny być rejestrowane oraz rozpowszechniane. W rezolucji 74/29 rozszerzono tę rekomendację, wskazując, że wszystkie tego typu zbiory muszą być gromadzone i przetwarzane wyłącznie w granicach wynikających z prawa krajowego. Podkreślono, że w każdym przypadku konieczne jest zapewnienie, że dane tego typu są przetwarzane wyłącznie w ustalonym celu, a sposób ich przekazywania innym podmiotom publicznym czy prywatnym powinien jasno wynikać z przepisów prawa. Jakiekolwiek odstępstwo od tych zasad powinno być możliwe wyłącznie w oparciu o zgodę wyrażoną przez ustanowiony organ nadzoru.

Warto podkreślić, że obydwie analizowane rezolucje dotyczyły wyłącznie przetwarzania danych jednostek, wyłączając w tym zakresie przetwarzanie danych osób osobowych w obrębie sektora publicznego.

349 Komitet Ministrów Rady Europy, Rezolucja (74) 29 z 20.09.1974 dotycząca ochrony prywatności jednostek w odniesieniu do elektronicznych banków danych w sektorze publicznym.
prawnych. Natomiast na płaszczyźnie terminologicznej w dokumentach tych nie wprowadzono podstawowych definicji, ograniczając się do wskazania, że „dane osobowe” obejmują informacje odnoszące się do osób fizycznych – bez wskazania, czy dane te muszą pozwalać na identyfikację jednostki.

3.3. **Wytyczne OECD**

Pierwszą próbę systematycznego opisania zasad przetwarzania danych osobowych, wraz z wprowadzeniem prawnej definicji terminu „dane osobowe”, podjęto na forum Organizacji Współpracy Gospodarczej i Rozwoju (Organisation for Economic Co-operation and Development, OECD) wraz z przyjęciem 23 września 1980 przez Radę, organ polityczny organizacji, formalnej rekomendacji wraz z załączonym do niej dokumentem „Wytyczne w zakresie ochrony prywatności i przepływu danych osobowych przez granice” (dalej: Wytyczne lub Wytyczne OECD)\(^\text{350}\). Wytyczne miały fundamentalne znaczenie dla ewolucji i ukształtowania zasad przetwarzania danych osobowych w systemach prawnych na całym świecie, w tym także dla norm przyjętych przez inne organizacje międzynarodowe – takie jak Rada Europy czy Unia Europejska.

Wytyczne składały się z pięciu głównych części. W pierwszej przedstawiono najważniejsze definicje, w drugiej zasady przetwarzania danych, natomiast część trzecia była poświęcona zasadom transgranicznego przepływu danych. Dwie ostatnie części były związane z implementacją Wytycznych przez państwa-członków OECD oraz współpracą międzynarodową.

W dokumencie wprowadzono definicje trzech pojęć: dane osobowe, administrator danych\(^\text{351}\) oraz transgraniczny przepływ danych osobowych. Każda z tych definicji w prawie niezmienionej formie jest stosowana do dzisiaj. Zgodnie z przyjętą definicją, jako „dane osobowe” należy rozumieć wszelkie informacje związane z zidentyfikowaną lub identyfikowalną osobą. Z kolei „administrator danych” oznacza podmiot, który zgodnie z prawem krajowym jest upoważniony do decydowania o zawartości i zakresie użycia danych osobowych, bez względu na to, czy takie dane są zbierane, przechowywane, przetwarzane albo rozpowszechniane przez stronę, czy też przez przedstawiciela występującego w jej imieniu.


\(^\text{351}\) Bezpośrednie tłumaczenie to „kontroler danych”, jednak w pracy wykorzystywany jest termin „administrator danych”, stosowany w polskim porządku prawnym.
Wprowadzenie obu terminów pozwoliło na wskazanie zakresu stosowania regulacji – zgodnie z art. 2 Wytycznych zakresem podmiotowym objęci byli administratorzy danych, natomiast zakres przedmiotowy dotyczył przetwarzania danych osobowych, w ramach którego, ze względu na sposób przetwarzania, wrażliwość lub kontekst przetwarzanych informacji, powstawało zagrożenie dla prywatności i wolności osobistych. Należy podkreślić, że z literalnego brzmienia art. 2 wynika, że Wytyczne powinny być stosowane zarówno w sektorze prywatnym, jak i publicznym.

Przedstawiona definicja danych osobowych była na tyle uniwersalna, że nie ograniczała zakresu regulacji do konkretnych kategorii informacji czy sektorów gospodarki, w jakim informacje te są przetwarzane. W jej redakcji zdecydowano się na podkreślenie zawartości informacyjnej danych z punktu widzenia odbiorcy – a więc wskazanie, że dany zbiór informacji należy traktować jako zawierający dane osobowe, jeżeli możliwe jest na ich podstawie przeprowadzenie identyfikacji osoby, której informacje te dotyczą. Warto podkreślić, że podejście takie prowadzi do rozszerzania zakresu przedmiotowego regulacji w czasie – bowiem z uwagi na rozwój techniki i środków przetwarzania informacji zbiór danych, który wcześniej nie spełniał opisanego powyżej kryterium identyfikowalności, poddany bardziej nowoczesnym technikom przetwarzania mógł już być zakwalifikowany do zbioru danych osobowych. Innymi słowy: bez potrzeby aktualizacji Wytycznych faktyczny zakres przedmiotowy regulacji w dniu jej wprowadzania (rok 1980) oraz obecnie istotnie się roszzerzył.

W rozdziale drugim dokumentu wprowadzono podstawowe zasady, które powinny zostać zaimplementowane w prawie krajowym oraz stanowić podstawę przetwarzania danych osobowych. Należą do nich:

- zasada ograniczonego gromadzenia,
- zasada jakości danych,
- zasada określonego celu,
- zasada ograniczenia użycia,
- zasada zabezpieczeń,
- zasada jawności,
- zasada udziału jednostki,
- zasada odpowiedzialności.
Zasada ograniczonego gromadzenia wskazuje, że proces rejestrowania danych osobowych musi odbywać się zgodnie z prawem oraz za wiedzą zainteresowanego. Z zasady tej wynika zakaz gromadzenia danych osobowych bez podstawy prawnej.

Zgodnie z zasadą jakości danych dane osobowe powinny być dokładne, kompletne i aktualne oraz związane z celem przetwarzania. W szczególności postuluje się niezbędną cechę wątpliwości zakres przetwarzanych danych z celem ich przetwarzania.

Z kolei z zasady określonego celu wynika konieczność wskazania celu przetwarzania nie później niż w momencie pozyskania danych, a także ograniczenia ich użycia do realizacji uzgodnionych celów lub innych z nimi zgodnych.

Natomiast zgodnie z zasadą ograniczenia użycia dane osobowe nie powinny być ujawniane, udostępniane lub wykorzystywane do celów innych niż wcześniej ustalone za wyjątkiem sytuacji, gdy działanie takie jest zatwierdzone przez podmiot danych lub wynika z obowiązującego prawa.

Zasada zabezpieczeń zobowiązuje do wprowadzenia adekwatnych zabezpieczeń przeciwdziałania ryzykom takim jak nieautoryzowany dostęp, zniszczenie, użycie, modyfikacja lub ujawnienie przetwarzanych danych.

Stosowanie zasady jawności związane jest z udostępnieniem informacji na temat praktyk, polityk i reguł związanych z danymi osobowymi. Postuluje się ustanowienie sposobów potwierdzenia faktu istnienia oraz rodzaju gromadzonych danych wraz z celem ich przetwarzania. Ponadto wprowadzone powinny zostać środki pozwalające na identyfikację tożsamości oraz siedziby administratora danych.

Zgodnie z zasadą udziału jednostki podmiot danych powinien mieć prawo do otrzymywania od administratora danych lub innego źródła potwierdzenia, czy przetwarza on dane z nim związane. Ponadto podmiot powinien mieć prawo dostępu do swoich danych, które powinny być udostępnione w rozsądnym terminie, bezpłatnie lub za umiarkowaną opłatą, w odpowiedni sposób oraz w formie dla niego zrozumiałej. W przypadku braku wykonania obowiązków wskazanych powyżej podmiot powinien otrzymać informację na temat przyczyny odmowy, a także powinien mieć możliwość zastosowania drogi odwoławczej. Ponadto zgodnie z zasadą udziału jednostki podmiot powinien mieć prawo zakwestionowania gromadzenia danych jego dotyczących, a w przypadku uznania wniosku – do żądania usunięcia, korekty, uzupełnienia lub poprawienia tych danych.

Ostatnia z reguł wprowadzonych w Wytycznych to zasada odpowiedzialności (znana w literaturze również jako zasada rozliczalności), zgodnie z którą administrator danych
powinien być odpowiedzialny za przestrzeganie reguł wprowadzających w życie zdefiniowane wcześniej zasady.

Jakkolwiek treść większości zasad ma charakter ogólny, a przyjęta redakcja tekstu Wytycznych pozostawia dużą swobodę do interpretacji dla państw-stron OECD, to jednak należy uznać, że przyjęty w Wytycznych zestaw reguł stał się podstawą dla wszystkich późniejszych rozwiązań prawnych regulujących obszar przetwarzania danych osobowych.

Chociaż Wytyczne nie miały charakteru prawnie wiążącego, wskazano, że powinny być traktowane jako wyznaczający minimalny poziom ochrony, który może być uzupełniany dodatkowymi środkami zwiększającymi gwarancje w obszarze prywatności i wolności osobistych (art. 6).

Biorąc pod uwagę datę opracowania dokumentu, podkreślenia wymaga także fakt rozpoznania przez autorów znaczenia ryzykazanego z potencjalną kolizją norm związanych z bezpieczeństwem publicznym oraz ochroną prywatności. W tym obszarze, zgodnie z art. 4 Wytycznych, wyłączenia w stosowaniu zasad określonych w części drugiej oraz trzeciej z uwagi na względy bezpieczeństwa narodowego i porządku publicznego powinny być możliwie nieliczne oraz zakomunikowane opinii publicznej.

Kolejnym wartym zaznaczenia elementem Wytycznych są rekomendacje związane z transgranicznym przepływem danych. W szczególności zgodnie z art. 17 państwo członkowskie może wprowadzić ograniczenia w transgranicznej wymianie danych, jeżeli doprowadziłoby ona do omijania stosowania przepisów krajowych lub dotyczyłaby eksportu określonych kategorii danych, które ze względu na swoją wrażliwość są regulowane w sposób szczególny w krajowym prawodawstwie. Należy podkreślić, że ta ogólna zasada nie straciła na aktualności do dziś, a jej niestosowanie jest jedną z przyczyn trwających obecnie sporów prawnych w obszarze gwarancji dotyczących ochrony prywatności (por. dalsze rozważania dotyczące programu Tarcza prywatności lub wymiany danych przez krajowe służby specjalne z pominięciem przepisów krajowych).

3.4. Konwencja nr 108 Rady Europy

Konsekwencją przyjęcia przez Komitet Ministrów Rady Europy rezolucji 73/22 i 74/29, a także rozwoju krajowego prawodawstwa w obszarze ochrony danych wśród państw członkowskich RE było wypracowanie i przyjęcie Konwencji nr 108 o ochronie osób w

Przyjęcie Konwencji stanowiło znaczący krok milowy w historii rozwoju wymagań prawnych związanych z ochroną prywatności w sieciach informatycznych. Z jednej strony, Konwencja nr 108 jako umowa międzynarodowa jest aktem prawnie wiążącym – co oznacza, że określone w niej obowiązki muszą, a nie mogą, zostać zaimplementowane w krajowych porządkach prawnych państw-sygnatariuszy. Z drugiej strony, postanowienia Konwencji określają nowe oraz rozszerzały istniejące prawa i gwarancje związane z ochroną prywatności i wzmacniały obszar ochrony praw podstawowych.

Według definicji wprowadzonej w art. 2 Konwencji 108 przez dane osobowe należy rozumieć wszelkie informacje dotyczące osoby fizycznej o ustalonej albo dającej się zidentyfikować tożsamości. Jest to zatem definicja zbieżna z przedstawioną w Wytycznych OECD, co do zasady nieuwzględniająca kosztów potrzebnych do zidentyfikowania danej osoby jako kryterium uznania zbioru za zawierający dane osobowe. Wprowadzono też definicję „kontrolera zbioru” (w polskim systemie prawnym administrator danych), będącego jednostką odpowiadającą za przetwarzanie danych – przy czym wskazano jednocześnie, że może być nim zarówno podmiot publiczny, jak i prywatny. W Konwencji 108 określono także zakres terminu „automatyczne przetwarzanie”, wskazując enumeratywnie operacje składające się na proces przetwarzania danych, tj. rejestrowanie, modyfikowanie, usuwanie, odzyskiwanie oraz rozpowszechnianie. Warto zauważyć, że zgodnie z definicją zawartą w umowie przekowywanie danych nie jest ich przetwarzaniem, w tym zakresie zastosowana definicja odbiega od standardów stosowanych współcześnie (np. w polskiej ustawie o ochronie danych osobowych).

---


Podstawowe zasady ochrony danych zostały przedstawione w rozdziale II Konwencji 108. Zgodnie z nimi państwa-strony powinny wprowadzić do swoich systemów prawnych rozwiązania zapewniające:

- dbanie o odpowiednią jakość danych (art. 5), przez co należy rozumieć między innymi zobowiązanie do zbierania i przetwarzania rzetelnie oraz zgodnie z prawem, a także rejestrowania danych wyłącznie dla określonych celów oraz zakaz wykorzystywania ich w sposób niezgodny z tymi celami, a także dbanie o dokładność i aktualność danych;
- zakaz automatycznego przetwarzania danych osobowych ujawniających pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne oraz danych dotyczących stanu zdrowia i życia seksualnego (art. 6); przy czym w prawie krajowym można odstąpić od tego zakazu przy jednoczesnym zobowiązaniu do zastosowania odpowiednich zabezpieczeń;
- odpowiednie środki bezpieczeństwa (art. 7) zmierzające do ochrony przetwarzanych danych przed zniszczeniem przypadkowym lub umyślnym oraz przed przypadkową utratą danych, udostępnieniem, zmianą lub rozpowszechnieniem bez zezwolenia;
- gwarancje dla podmiotu danych, w szczególności: prawo do informacji – rozumiane jako prawo do ustalenia faktu istnienia zbioru danych osobowych, jego celach, a także tożsamości i siedzibie administratora danych; prawo do sprostowania lub usunięcia informacji, jeżeli zostały przetworzone z naruszeniem przepisów prawa wewnętrznego; prawo wglądu w przetwarzane informacje w rozsądnym czasie i bez nadmiernych kosztów; prawo do zadośćuczynienia w przypadku naruszenia zobowiązań związanych z potwierdzeniem, udostępnieniem, sprostowaniem lub usunięciem danych.

Zgodnie z art. 4 Konwencji 108 każda ze stron zobowiązała się do zastosowania niezbędnych środków dla wprowadzenia w swoim prawie wewnętrznym podstawowych zasad ochrony danych ustawionych w rozdziale II najpóźniej do chwili wejścia w życie zapisów umowy w odniesieniu do danej strony.

Zgodnie z art. 9 wyjątki w stosowaniu zobowiązań wynikających z Konwencji 108 są dopuszczalne tylko w ograniczonym zakresie (art. 5, 6 i 8) oraz możliwe wyłącznie w granicach określonych przez prawo krajowe, przy jednoczesnym spełnieniu warunku, że odstępstwo takie jest środkiem koniecznym w społeczeństwie demokratycznym w interesie
ochrony państwa, bezpieczeństwa publicznego, interesów walutowych państwa lub zwalczania przestępczości, a także ochrony podmiotu danych oraz praw i wolności innych osób.

Dla pełnego zrozumienia zakresu możliwego wyłączenia opisanego w art. 9 Konwencji 108 przydatne może okazać się skorzystanie z bogatego orzecznictwa ETPC – zwłaszcza w zakresie interpretacji przesłanki „konieczny w społeczeństwie demokratycznym” w odniesieniu do obszaru bezpieczeństwa publicznego. Chociaż kognicja Trybunału związana jest ze skargami na naruszenia praw i wolności wynikających z EKPC, to w wydawanych orzeczeniach Trybunał wskazuje na znaczenie Konwencji 108 w obszarze zwiększania standardów ochrony danych osobowych. Przykładem może być wyrok wydany w sprawie S. i Marper v. Wielka Brytania355, w którym Trybunał podkreślił fundamentalne znaczenie ochrony danych osobowych dla zapewnienia ochrony życia prywatnego i rodzinnego w zakresie wynikającym z art. 8 EKPC. W orzeczeniu wskazano na wynikającą z art. 5 Konwencji 108 konieczność zapewnienia w prawie krajowym, że dane nie są gromadzone w zakresie szerszym niż konieczny do realizacji ustalonego celu przetwarzania oraz animizowane ich tak szybko, jak jest to możliwe. Trybunał przywołał też regulację wynikającą z art. 6 (przetwarzanie danych sensytywnych) oraz art. 7 (stosowanie odpowiednich środków zapobiegających bezprawnemu wykorzystaniu danych) Konwencji 108, zauważając, że ich wdrożenie powinno odbyć się także na płaszczyźnie prawa wewnętrznego. Trybunał podkreślił zatem bliski związek stosowania Konwencji 108 z gwarancjami wynikającymi z art. 8 EKPC. Dlatego, chociaż w Konwencji 108 nie powołano odrębnego organu kontrolnego, to w przypadku państw będących stronami obu traktatów naruszenia obowiązków wynikających z Konwencji 108 mogą być dochodzone w drodze skargi przed ETPC ze wskazaniem jako jej podstawy jednoczesnego naruszenia art. 8 Konwencji europejskiej.

Umawiające się strony uregulowały w Konwencji 108 również dwa obszary istotne, biorąc pod uwagę praktyczne stosowanie zasad przetwarzania danych osobowych: obszar transgranicznego przekazywania i przetwarzania danych, a także obszar międzynarodowej współpracy w zakresie standaryzacji i ochrony prywatności.

Zgodnie z art. 12 ust. 2 strona traktatu nie może zabronić ani uzależnić od uzyskania dodatkowego zezwolenia z powodów wyłącznie dotyczących ochrony prywatności, przepływu danych osobowych przez granicę na terytorium innego państwa-strony Konwencji.

Istnieje możliwość zastosowania odstępstwa od tej reguły, w przypadku, gdy prawo krajowe określa odrębnie reżim związany z przetwarzaniem danych ze względu na ich rodzaj lub transmisja danych realizowana jest za pośrednictwem terytorium państwa, które nie jest stroną umowy. Przepis ten ma na celu realizację motywów wskazanych w preambule traktatu, związanych z ułatwieniem swobodnego obiegu informacji między narodami oraz stowarzzeniem w obrębie państw-stron Konwencji 108 jednolitego obszaru przepływu informacji. Aby dodatkowo przybliżyć możliwość realizacji tego celu, zdecydowano się na wprowadzenie mechanizmów współpracy międzynarodowej pomiędzy stronami Konwencji oraz określenie zasad udzielania pomocy podmiotom danych zamieszkałym za granicą przez wyznaczony organ strony, na terenie którego mieszka. W rezultacie każdy z obywateli państw-stron Konwencji ma możliwość dochodzenia swoich praw wynikających z niej także w przypadku, gdy mieszka na terytorium innego państwa-strony Konwencji. Prawo to może być dochodzone bezpośrednio na podstawie przepisów Konwencji, co jest rozwiązaniem nietypowym, biorąc pod uwagę, że omawiany dokument jest aktem prawa międzynarodowego.

Zgodnie z pierwotnym tekstem konwencji jej strony nie były zobowiązane do wyznaczenia organów nadzoru odpowiedzialnych za zapewnienie zgodniej z prawem krajowym realizacji zasad przetwarzania danych wprowadzonych w rozdziale II traktatu. Zagadnienie to zostało doprecyzowane wraz z zawarciem Protokołu Dodatkowego, sporządzonego 8 listopada 2001 roku[^356]. Na podstawie art. 1 Protokołu wprowadzono obowiązek wyznaczenia organu nadzorczego oraz nadania mu uprawnień i kompetencji (w tym dochodzeniowych i interwencyjnych) koniecznych do realizacji postanowień Konwencji. Ponadto w protokole uregulowano zasady transgranicznego przepływu danych osobowych w przypadku, gdy odbiorca nie podlega jurysdykcji państwa-strony Konwencji.

Sporządzona ponad 30 lat temu Konwencja nr 108 nadal pozostaje aktualna. Co oczywiste, postęp techniki spowodował, że niektóre zagrożenia związane z ochroną prywatności pojawiające się współcześnie nie zostały w niej odpowiednio omówione, jednak nie zmienia to faktu, że przyczyniła się w sposób trwały do wzmocnienia gwarancji związanych z prawem do poszanowania prywatności w gronie jej państw sygnatariuszy.

W efekcie w piśmiennictwie wskazuje się, że omawianą konwencję można uznać za pierwsze europejskie ramy prawne wprowadzające gwarancje w obszarze ochrony danych osobowych.

osobowych\textsuperscript{357}. Ponadto Konwencja nr 108 była i pozostaje jedynym prawnie wiążącym międzynarodowym aktem dotyczącym ochrony danych\textsuperscript{358} (wniosek ten będzie aktualny aż do wejścia w życie rozporządzenia 2016/679\textsuperscript{359}). Dowodem na rosnące znaczenie konwencji może być także przystąpienie do niej państw spoza europejskiego kręgu kulturowego (np. Mauritius, Senegal, Urugwaj), w efekcie czego staje się ona ramą do budowy ponadregionalnych standardów ochrony danych osobowych.

Konwencja nie jest jednak pozbawiona istotnych wad i ograniczeń. W pierwszej kolejności należy wskazać, że jej postanowienia są kierowane do państw i rolą państw jest przeniesienie szczegółowych rozwiązań do krajowego porządku prawnego. Dlatego przepisy umowy mogą być różnie interpretowane i wdrażane w poszczególnych państwach. Obserwacja ta była jedną z przyczyn leżących u podstaw decyzji KE w zakresie przygotowania własnego projektu regulacji w obszarze ochrony danych osobowych (przyszła dyrektywa 95/46)\textsuperscript{360}. Nawet uwzględniając treść Protokołu Dodatkowego, Konwencja 108 jest pozbawiona wielu elementów na trwałe wpisanych zarówno w europejski model ochrony danych, jak również prawodawstwo krajowe. Przykładem może być brak uwzględnienia w Konwencji 108 zgody podmiotu danych jako podstawy do gromadzenia i przetwarzania danych.


\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{358} Podręcznik europejskiego prawa o ochronie danych, Urząd Publikacji Unii Europejskiej 2014, s. 16
\item \textsuperscript{359} Szczegółowe omówienie unijnego modelu ochrony danych osobowych, w tym ogólnego rozporządzenia o ochronie danych, przedstawiono w rozdziale 4.
\item \textsuperscript{360} Komunikat Komisji Europejskiej z 13 września 1990 na temat ochrony jednostek w związku z przetwarzaniem danych osobowych we Wspólnotie oraz bezpieczeństwa informacji, COM (90) 314 final, CELEX: 51990DC0314, s 3-4.
\end{itemize}
\end{footnotesize}
Zgodnie z art. 18 konwencji powołano Komitet Doradczy – stały organ uprawniony w szczególności do wydawania wytycznych rekomendacji w obszarze interpretacji poszczególnych postanowień traktatowych. Opinie wydawane przez Komitet nie mają charakteru prawnie wiązającego, jednak co do zasady mają zapewnić „uprzystępnienie oraz usprawnienie stosowania konwencji” (art. 19 pkt a). Jest to zatem ciało o funkcji i zadańach zbliżonych do Grupy Roboczej Art. 29. Opinie wydawane przez Komitet dotyczą wielu aktualnych i ważnych problemów dla rynku przetwarzania danych, np. roli analityki Big Data, przetwarzania danych PNR czy masowej inwigilacji. Nie można zatem uznać, aby były to tematy nieistotne z punktu widzenia materii badanej problematyki. Jednocześnie jednak Komitet ma bardzo ograniczone kompetencje w zakresie oceny spełnienia wymagań przez państwa-strony, także w zakresie wydawania zaleceń czy rekomendacji (por. wcześniejsze rozważania na temat uprawnień KPC wynikających z MPPOP). Łącząc tę cechę z brakiem ustanowienia innego organu kontrolnego czy sądowego, unaocznia się istotne ograniczenie Konwencji – brak możliwości monitorowania i odpowiedniego reagowania w przypadku niewystarczającej lub nieskutecznej implementacji rozwiązań konwencyjnych do krajowego porządku prawnego.

W efekcie powyższych ograniczeń rola Konwencji 108 w faktycznym budowaniu jednolitej przestrzeni przetwarzania informacji, działającej w oparciu o te same podstawowe prawa i zasady, jest ograniczona. Do chwili obecnej do traktatu nie przystąpiła Unia Europejska, chociaż zamiar taki był wcześniej wielokrotnie wyrażany. W 1999 uzgodniono zakres nowelizacji traktatu w sposób pozwalający na przystąpienie Unii Europejskiej do konwencji. Według danych na 22 marca 2018 roku, zaproponowane zmiany nadal nie zostały zatwierdzone przez niektóre umawiające strony, do których należą też państwa członkowskie UE. O ile jeszcze na początku lat dziewięćdziesiątych dwudziestego wieku instytucje UE sygnalizowały zamiar i potrzebę przystąpienia organizacji do Konwencji, to w późniejszym czasie cel ten przestał być wyraźnie sygnalizowany. Przyczyną zmiany priorytetów była decyzja o budowie własnego systemu ochrony danych w oparciu o unijne akty prawne oraz instytucje sądowe.

---


364 Rada Europy, *Amendments approved by the Committee of Ministers*, Strasbourg, 15.06.1999, https://rm.coe.int/168008c2b8

Do Konwencji nie przystąpiły także najważniejsi partnerzy handlowi UE – w tym Stany Zjednoczone, Kanada, Australia, Japonia czy Izrael. W efekcie nie jest uzasadnione twierdzenie o realnym sukcesie Konwencji w zakresie wprowadzenia powszechnie rozpoznawalnych standardów w zakresie ochrony danych. Z drugiej strony G. Greenleaf wskazuje, że do Konwencji przystąpiło już niemal 50% państw, w których przyjęto krajowe przepisy o ochronie danych.


Zakres postulowanych zmian w dużej mierze dostosowuje definicje, prawa podmiotów danych, obowiązki administratorów oraz zasady przetwarzania do znanych z unijnego modelu ochrony danych, w szczególności wprowadzonych w ogólnym rozporządzeniu. Stąd też w przedstawionej treści art. 2 projektu zaproponowano wprowadzenie znanego z prawa UE podziału podmiotów przetwarzających na kontrolerów oraz procesorów. Kolejne podobieństwa można odnaleźć w zbliżonych formalnych warunkach przetwarzania danych, a także oparciu zasad transferu danych do państw trzecich na spełnieniu przesłanki „adekwatnego poziomu ochrony” (art. 12 ust. projektu). Jak wskazuje M. Ciechomska, „projekt zmiany Konwencji uwzględnia większość postulowanych zmian w zakresie ochrony danych osobowych, tj. zasadę odpowiedzialności, proporcjonalności, transparentności, minimalizacji danych, zgody podmiotu danych czy ochrony w fazie projektowania (privacy by design)”.

Doprecyzowanie, rozszerzenie i wzmocnienie zasad

---


367 Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, https://rm.coe.int/16806a616c.


369 M. Ciechomska, Zmiana Konwencji nr 108 Rady Europy o chronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych, Monitor Prawniczy 2017, nr 16, s. 877.


Bardziej rozbudowaną listę korzyści wynikających z przystąpienia do Konwencji – w szczególności dla państw nie należących do UE – przedstawia G. Greenleaf. Wymienia on aż trzynaście najważniejszych zalet, wśród nich między innymi oparcie traktatu na „roszanych standardach”, które są osiągalne dla większości państw i nie są prostym przeniesieniem

[370] Ibidem, s. 876.
[371] Por. preambuła do Projektu Zmiany Konwencji.
wysokich norm wprowadzonych w UE\textsuperscript{372}. Ponadto wskazuje na takie zagadnienia, jak brak obowiązku stosowania (dobrowolność przystąpienia), możliwość wypracowania najlepszych praktyk, ułatwienie współpracy międzynarodowej, korzyści biznesowe z perspektywy administratorów i indywidualne z perspektywy podmiotów danych, jak również uproszenie zasad międzynarodowego transferu danych\textsuperscript{373}.

Jakkolwiek G. Greenleaf czyni interesujące obserwacje – zwłaszcza że odzwierciedlają spojrzenie na badany problem z perspektywy australijskiego systemu prawnego, a więc państwa nienależącego do UE – to jednak trudno nie zauważyć, że pomija jednocześnie problem skuteczności norm stanowionych przez Konwencję. Historia prawa międzynarodowego jest bogata w przykłady porozumień wprowadzających ważne i potrzebne regulacje, które jednak z uwagi na różne – często geopolityczne – okoliczności nie były stosowane. Można zatem uznać, że przywołane zalety w istocie mogą służyć do opisania każdego aktu prawnomiędzynarodowego, mającego aspirację do promowania ponadnarodowej standaryzacji w określonej dziedzinie prawa.

Według J. Cannataciego, Specjalnego Sprawozdawcy ds. Prywatności ONZ, skuteczna ochrona prywatności w cyberprzestrzeni implikuje stosowanie „zabezpieczeń bez granic oraz środków ochrony ponad granicami”\textsuperscript{374}. Aby Konwencja 108 mogła stanowić odpowiedź na tak zdefiniowaną potrzebę, jej przepisy nie powinny podlegać subiektywnej interpretacji dokonywanej z perspektywy prawa krajowego przy jednoczesnym braku powołania ponadnarodowego organu sądowego.

W chwili obecnej nie jest znany termin wejścia w życie zmodernizowanej Konwencji, nie jest także pewne, czy uzgodniona treść nie będzie podlegała dalszym modyfikacjom i zmianom. Nie można zatem wykluczyć, że przedstawione powyżej uwagi krytyczne stracą na aktualności w całości lub w części w wyniku dalszych modyfikacji wprowadzonych do projektu, jednak bazując na obecnym kształcie Projektu Zmiany Konwencji, należy uznać, że traktat ten będzie nadal odgrywał ważną rolę w promowaniu globalnych standardów ochrony danych, nie stanie się jednak faktycznym mechanismem, który standard ten zapewni.

---

\textsuperscript{372} G. Greenleaf, \textit{Balancing Globalisation's...}, op. cit., s. 3.
\textsuperscript{373} Ibidem, s. 3-6.
3.5. Wytyczne ONZ

W 1985 roku w ramach Komisji Praw Człowieka ONZ wypracowano projekt wytycznych dotyczących przetwarzania danych osobowych w systemach komputerowych. Projekt ten został przyjęty i ogłoszony przez Zgromadzenie Ogólne ONZ w formie rezolucji 45/95 z dnia 14 grudnia 1990 roku. Podobnie jak w przypadku wytycznych opracowanych przez OECD rezolucja ONZ nie ma charakteru prawnie wiążącego, jednak z uwagi na globalny charakter organizacji stanowiła kolejny impuls na drodze do standaryzacji prawnych wymagań związanych z przetwarzaniem danych osobowych w systemach informatycznych.

Rekomendacje ONZ zostały opracowane z myślą o ich stosowaniu zarówno przez podmioty sektora publicznego, jak i prywatnego. Autorzy wskazali ponadto, że wytyczne mogą być stosowane w ograniczonym zakresie do przetwarzania danych osób prawnych, zwłaszcza w sytuacji, gdy zbiory danych zawierają także informacje na temat osób fizycznych.

Wytyczne załączone do rezolucji 45/95 zorganizowane zostały w dwie części – w pierwszej przedstawiono zasady przetwarzania danych osobowych, które powinny zostać zaimplementowane w prawie krajowym, w drugiej zaś omówiono najważniejsze reguły związane z przetwarzaniem danych osobowych przez organizacje międzynarodowe. Na wstępie warto zauważyć, że dokument nie został uzupełniony definicją podstawowych terminów, takich jak „dane osobowe”, „administrator danych” czy „przetwarzanie danych”.

W pierwszej części wytycznych wprowadzono sześć reguł określających minimalne zasady przetwarzania danych osobowych, jakie powinny być zapewnione w krajowym prawodawstwie:

- legalności i słuszności (działania w granicach prawa),
- dokładności (jakości danych),
- określonego celu,
- dostępu podmiotu danych,
- niedyskryminacji,
- bezpieczeństwa.

Większość z nich – jak np. zasada legalności i słuszności czy zasada określonego celu – odzwierciedla wskazówki wprowadzone wcześniej w wytycznych OECD. Należy zauważyć, że chociaż nazwy zasad często są zbliżone w obu dokumentach, ich znaczenie jest

szersze lub bardziej szczegółowe w wytycznych ONZ. Przykładem jest zasada dokładności, która w znaczeniu OECD związana była z zagwarantowaniem odpowiedniej jakości przetwarzanych danych – rozumianej jako zapewnienie dokładności, kompletności i aktualności, a także związana z celem przetwarzania. Natomiast w wytycznych ONZ w ramach tej samej zasady postuluje się przeprowadzanie okresowych sprawżeń mających na celu potwierdzenie, że kryteria zapewnienia odpowiedniej jakości danych są spełnione. Z kolei w ramach zasady dostępu podmiotu do danych wskazano, że uprawnienie powinno być nadane wszystkim zainteresowanym, niezależnie od ich narodowości oraz miejsca zamieszkania. W ramach zasady bezpieczeństwa uznano, że dane powinny być zabezpieczone zarówno przed zagrożeniami naturalnymi, skutkującymi uratą lub zniszczeniem danych, jak i działaniami umyślnymi, związanymi w szczególności z nieuprawnionym dostępem, wykorzystaniem danych niezgodnie z przeznaczeniem czy negatywnym wpływem działalności wirusów komputerowych.

Nową zasadą, niemającą bezpośredniego odpowiednika w wytycznych OECD, jest reguła niedyskryminacji – rozumiana jako zakaz gromadzenia danych sensytywnych, a więc danych związanych z rasą lub pochodzeniem etnicznym, kolorem skóry, orientacją seksualną, poglądami religijnymi filozoficznymi czy politycznymi, jak również informacji związanych z przynależnością do związków zawodowych lub innych zgromadzeń. Zasada niedyskryminacji stała się podstawą dla funkcjonującego w systemach prawnych wielu państw (także Polski376) szczególnego reżimu przetwarzania danych wrażliwych.

Ponadto w wytycznych ONZ postuluje się wyznaczenie w systemie prawnym każdego państwa upoważnionego organu właściwego do nadzorowania przestrzegania zasad związanych z przetwarzaniem danych osobowych. Organ ten powinien zapewnić bezstronność i niezależność od administratorów danych, jak i powinien dysponować koniecznymi kompetencjami technicznymi. Naruszenie wynikających z prawa krajowego obowiązków związanych z przetwarzaniem danych powinno być powiązane z zastosowaniem sankcji wobec osób odpowiedzialnych, powinno też łączyć się z możliwością dochodzenia odpowiedniego zadośćuczynienia. Warto podkreślić, że rekomendacja związana z powołaniem organu nadzorczego nie występowała w wytycznych OECD.

**3.6. Międzynarodowe Standardy Ochrony Prywatności**

376 Por. art. 27 ustawy z 29.08.1997 o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922).
W 2009 roku, a więc ponad dwadzieścia lat po wejściu w życie Konwencji Rady Europy nr 108 oraz ponad dziesięć lat po przyjęciu dyrektywy 95/46, stanowiącej podstawę dla funkcjonowania jednolitego rynku UE w obszarze współpracy i wymiany danych osobowych, podczas 31. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności przyjęto wspólną propozycję projektu Międzynarodowych Standardów Ochrony Prywatności (dalej: MSOP)\(^{377}\).

Nowy dokument miał pozwolić na określenie powszechnego systemu zasad i praw gwarantujących skuteczną i jednolitą dla wszystkich krajów ochronę prywatności w odniesieniu do przetwarzania danych osobowych, a także usprawnienie transgranicznych przepływów danych niezbędnych w zglobalizowanym świecie\(^{378}\). Projekt powstał przy współpracy organów ochrony danych z 50 krajów reprezentujących pięć kontynentów, jest więc przyczynkiem do prawdziwie globalnej standaryzacji obszaru ochrony danych osobowych.

Na płaszczyźnie merytorycznej MSOP stanowią podsumowanie wcześniejszych doświadczeń związanych z ochroną prywatności w świecie elektronicznym, zarówno wynikających z prawa krajowego, jak i związanych z uczestnictwem w organizacjach międzynarodowych. Chociaż Standardy nie mają mocy prawnie wiążącej, ich uzgodnienie i przyjęcie to kolejny krok w ewolucji myślenia o ochronie danych – tym razem w kategoriach rozwiązań globalnych. W tym zakresie interesująca może być analiza propozycji przedstawionych w dokumencie, w szczególności zasad przetwarzania, wynikających z dokumentów o charakterze niewiączącym (wytyczne OECD i ONZ) oraz umów międzynarodowych (Konwencja nr 108). Rozważania te mogą być wartościowe, biorąc pod uwagę, że autorem MSOP nie są bezpośrednio rządy, realizujące poprzez akty prawa międzynarodowego swoje cele polityczne i gospodarcze, ale organy nadzoru, powołane do ochrony prywatności i danych osobowych, dla których kwestie wprowadzenia spójnego modelu ochrony danych mają pierwszorzędne znaczenie przed celami związanymi z ułatwieniem współpracy gospodarczej czy likwidacją barier w międzynarodowej wymianie handlowej.

Rozpoczynając analizę dokumentu, należy omówić rozwiązania zastosowane w warstwie definicyjnej. W Standardach wprowadzono definicję pięciu najważniejszych

---


\(^{378}\) Ibidem, p. I.1, s. 4.
terminów: „dane osobowe”, „przetwarzanie”, „osoba, której dane dotyczą” (podmiot danych), „osoba odpowiadzalna” (administrator danych), „dostawca usługi przetwarzania”. Zestawiając Standardy z wcześniejszymi regulacjami (w szczególności wytycznymi OECD), zauważyć można, że już na etapie definicji przyjęto rozwiązanie rozdzielające uprawnienia i kompetencje administratora danych oraz podmiotu przetwarzającego dane na zlecenie, co pozwala lepiej dopasować ramy regulacji do złożoności i wielowarstwowości rynku e-usług funkcjonującego współcześnie. Ponadto wprowadzając definicję terminu „dane osobowe”, uwzględniono, że identyfikowalność określonej osoby musi być interpretowana przez pryzmat dostępnych środków technicznych, a ponadto ich racjonalności – której elementem jest nakład czasowy i finansowy związany z analizą przetwarzanych danych. Podobne rozwiązanie wprowadzono także do polskiej ustawy o ochronie danych osobowych nowelizacją z dnia 25 sierpnia 2001 (por. treść przepisu art. 6 ust. 3). W krajowym systemie prawnym brak wystarczającej precyzji w zdefiniowaniu pojęcia dane osobowe stał się wcześniej przyczyną wydania kontrowersyjnego wyroku NSA z 17 listopada 2001, w którym sąd wskazał, że za dane osobowe można przyjąć tylko takie informacje, które pozwalają na identyfikację podmiotu danych, „a więc imię, nazwisko, adres, PESEL, NIP itp.”. Podgląd ten został słusznie skrytykowany w doktrynie – jak wskazywano, za dane osobowe powinny zostać uznane wszelkie informacje, jeżeli tylko możliwe jest ich odniesienie do konkretnej osoby. Dyskusja ta obrazuje ryzyko związane z przyjęciem zamkniętych czy enumeratywnych definicji w aktach prawnych regulujących obszary, w których następuje dynamiczny postęp techniczny.

Z kolei w definicji terminu „przetwarzanie” wskazano, że jest nim każda operacja – zautomatyzowana lub nie – dokonywana na danych osobowych. Lista możliwych czynności przetwarzania została wskazana w redakcji przepisu jako przykładowa, niewyczerpująca możliwych form. Rozwiązanie takie także pozwala na uniknięcie w przyszłości sytuacji, w której pojawienie się nowej formy przetwarzania, związanej np. z rozwojem możliwości technicznych, uwypukli niedoskonałość przyjętych rozwiązań prawnych.

Przenosząc dorobek i doświadczenie organów nadzoru uczestniczących w pracach nad przygotowaniem Standardów, zdecydowano się podzielić regulacje związane z ochroną danych na trzy główne obszary: podstawowe zasady, zasady związane z legalnością

---

379 W nawiasach podano terminy stosowane w polskim porządku prawnym a wynikające z ustawy o ochronie danych osobowych.

380 Wyrok NSA z 17.11.2001, sygn. II SA 1860/00, niepubl.

przetwarzania oraz prawa podmiotu danych. Ponadto odrębnie określono regulacje związane ze środkami bezpieczeństwa oraz zapewnieniem zgodności i nadzoru nad przestrzeganiem regulacji.

Wśród podstawowych zasad ochrony danych wyszczególniono: zasadę zgodności z prawem i rzetelności, określonego celu, proporcjonalności oraz jawności. Każda z nich była zdefiniowana we wcześniejszych regulacjach (por. wcześniejsze rozważania dot. wytycznych ONZ), ich zakres został jednak zmodyfikowany, aby lepiej odzwierciedlać rozwój techniki w zakresie przetwarzania danych. I tak np. w obrębie zasady jawności wskazano, że podmiot danych ma prawo otrzymać informację o źródle pochodzenia dotyczących go danych. Ponadto uwzględniono, że w przypadku gromadzenia danych z wykorzystaniem elektronicznych środków komunikacji, obowiązki informacyjne względem podmiotów danych mogą być wypełnione przez odpowiednie zredagowanie i opublikowanie polityki prywatności (art. 10.6). Z kolei zasadę jakości danych uzupełniono o zastrzeżenie, że zakres gromadzonych danych osobowych powinien być ograniczony do niezbędnego minimum, koniecznego do realizacji zamierzonego celu przetwarzania. Oznacza to, że dane, które stają się niepotrzebne do wypełnienia celu, powinny być usunięte lub anonimizowane (art. 8.2).

W obszarze zasad dotyczących legalności przetwarzania wyróżniono zasadę odpowiedzialności oraz legalności, a także wymagania dotyczące przetwarzania danych szczególnie chronionych oraz świadczenia usług przetwarzania. Zasady odpowiedzialności i legalności wzmacniają znaną w nauce prawa regułę domyślnego zakazu przetwarzania danych osobowych bez spełniania jednej z enumeratywnie wskazanych przesłanek pozytywnych. Z kolei warunki przekazania (zlecenia) przetwarzania danych osobowych podmiotom trzecim przez administratora danych oraz regulacje związane z transgranicznym przekazywaniem danych zmierzają do uregulowania stanu, w którym administrator danych prowadzi przetwarzania z wykorzystaniem pomiotów zewnętrznych, często podlegającym różnym jurysdykcjom. Rekomendacje te dobrze obrazują różnicę pomiędzy wcześniej omówionymi wytycznymi OECD i ONZ a Standardami. Wytyczne OECD i ONZ powstawały w latach osiemdziesiątych dwudziestego wieku, w czasach gdy dane w postaci elektronicznej były przetwarzane głównie z wykorzystaniem dedykowanych środowisk informatycznych (serwery, komputery typu mainframe). MSOP z kolei powstały w czasach, gdy usługi świadczone w sieci Internet oraz przetwarzanie z wykorzystaniem chmury obliczeniowej stały się powszechne, wobec czego model zaproponowany w Standardach musiał odzwierciedlać nowe potrzeby regulacyjne związane ze zmienionym rynkiem przetwarzania danych.
Chociaż Międzynarodowe Standardy Ochrony Prywatności pozostają nadal dokumentem niewiązającym oraz obecnie nie trwają żadne prace nad przyjęciem umowy międzynarodowej odzwierciedlającej rekomendacje w nich przedstawione, to należy przyjąć, że na płaszczyźnie standaryzacji ochrony danych osobowych wypracowanie globalnych i powszechnie wiążących norm prawa jest nieuniknione. Jak wskazano w analizie „Przyszłość prywatności”, „globalne standardy w zakresie ochrony danych stają się niezbędne”, a ich przyjęcie „ułatwiłoby transgraniczny przepływ danych, który w wyniku globalizacji staje się regułą, nie wyjątkiem” 382.

3.7. Podsumowanie

Po niemal czterdziestu latach od wprowadzenia pierwszych aktów prawnych w obszarze ochrony danych osobowych zagadnienie to stało się przedmiotem wielu regulacji o zasięgu zarówno krajowym, jak i ponadnarodowym. Według danych z czerwca 2016 roku, 111 państw na całym świecie przyjęło przepisy prowadzące do standaryzacji obszaru ochrony danych 383. Co warte podkreślenia, począwszy od roku 2015 większość z tych państw to kraje pozaeuropejskie 384. Zatem prymat państw europejskich we wprowadzaniu przedmiotowych regulacji się zakończył, co jest najlepszym dowodem na globalne zrozumienie potrzeby prawnej regulacji obszaru ochrony danych osobowych.

Naturalnie zarówno charakter prawny, jak i szczegółowość wprowadzanych przepisów krajowych jest różna. Przyczyną jest odmienne otoczenie prawne (związane np. z innymi normami ustrojowymi), ale również oddziaływanie na prawo krajowe różnych systemów prawnomieędzynarodowych. Państwa niefunkcjonujące w systemach ochrony praw człowieka mają większą swobodę w kształtowaniu granic oraz szczegółowości przepisów o ochronie danych. Z drugiej strony, przepisy krajowe funkcjonujące w państwach europejskich, w szczególności należących do UE, stanowią odzwierciedlenie wysokich standardów związanych z prawem unijnym (KPP), konwencji europejskiej (EKPC) i prawa ponadregionalnego (MPPOP).

Szczególne znaczenie dla upowszechniania norm krajowych mają przepisy międzynarodowe – zarówno o charakterze rekomendacji (np. wytyczne OECD czy MSOP),

382 Grupa Robocza Artykułu 29 ds. Ochrony Danych, Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości, Przyszłość prywatności, op. cit., p. 29, s. 11.
383 Zob. przypis 366.
jak i prawnie wiążące (Konwencja 108). Już we wczesnych regulacjach akcentowana była potrzeba wypracowania ponadnarodowych standardów jako warunkująca możliwość swobodnej transgranicznej wymiany danych. Potrzeba ta miała zasadnicze znaczenie dla rozwoju regionalnej współpracy ekonomicznej (szczególnie w zakresie budowania jednolitego rynku WE/UE), ale również budowania partnerstwa transatlantyckiego.

Zestawiając wczesne dokumenty, takie jak rekomendacje RE czy wytyczne OECD, ze współczesnymi opracowaniami, których przykładem są MSOP, wyróżnić można kilka najważniejszych różnic. Najbardziej wyraźna jest dużo większa szczegółowość w określeniu praw podmiotów danych, a także ograniczeń i wyłączeń związanych z prowadzeniem czynności przetwarzania przez administratorów. O ile w pierwszych regulacjach koncentrowano się na wprowadzeniu podstawowych praw (prawo do informacji czy do niepodlegania decyzjom automatycznym), to we współczesnych regulacjach skoncentrowano się na wyrażeniu w pełni prawa do autonomii informacyjnej jednostki (w szczególności np. przez prawo do usunięcia danych czy wzmacnienie zasady proporcjonalności).


Coraz częściej prawodawcy oraz organizacje międzynarodowe zauważają ograniczenie związane z terytorialnym zasięgiem stosowanych przepisów. W sposób oczywisty problem ten jest skorelowany z dynamicznym rozwójem usług cyfrowych,  

385 Więcej o Grupie Roboczej Art. 29 w rozdziale 4.5.4.2.
zwłaszcza świadczonych w sieci Internet. W efekcie sformułowanych zostało kilka odmiennych poglądów na przyszłość przepisów o ochronie danych, różniących się sposobem zapewnienia ich uniwersalnej skuteczności w cyberprzestrzeni\textsuperscript{386}.

Warto wymienić dwie dominujące propozycje, wraz z ich najważniejszymi zaletami, ale także najpoważniejszymi ograniczeniami i wadami. Obie co do zasady mają podobną konstrukcję i związane są z połączeniem szczegółowych standardów w zakresie ochrony danych z ponadregionalnym systemem ochrony praw człowieka, a dokładnie z MPPOP. Pierwsza z propozycji – przedstawiona i promowana przez Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności – związana jest z nadaniem MSOP aktu powszechnie wiążącego poprzez jego przyjęcie, w odpowiednio dostosowanej formie, jako nowy, trzeci protokół fakultatywny do Paktu. Propozycję taką zapisano wprost w Rezolucji na rzecz zapewnienia ochronie danych i prywatności stałego miejsca w prawie międzynarodowym, w której podkreślono, że „istnieje pilna potrzeba istnienia wiążącego międzynarodowego porozumienia w sprawie ochrony danych, które zabezpiecza prawa człowieka, chroniąc prywatność, dane osobowe i integralność sieci oraz zwiększa przejrzystość przetwarzania danych, osiągając przy tym równowagę w zakresie bezpieczeństwa, interesów gospodarczych i wolności wypowiedzi”\textsuperscript{387}.

Jak z kolei wskazano w Rezolucji przyjętej podczas 37. Międzynarodowej Konferencji, zadanie promowania na rzecz rozpoczęcia negocjacji dodatkowego protokołu do MPPOP zostało podjęte w ramach mandatu sprawowanego przez Specjalnego Sprawozdawcę ds. Prywatności ONZ\textsuperscript{388}.

Zgodnie z drugą propozycją, promowaną zarówno przez Radę Europy oraz niektórych przedstawicieli nauki prawa\textsuperscript{389}, postuluje się budowę globalnego systemu ochrony danych na bazie Konwencji 108. Jak wskazano w rezolucji Zgromadzenia Parlamentarnego Rady Europy, „kaźda globalna inicjatywa [w zakresie ochrony danych – przyp. autora] powinna

\footnotetext[386]{Obok propozycji \textit{stricto} prawnych, prowadzących do wypracowania nowych przepisów o mocy wiążącej, w piśmiennictwie omawiane są także podejścia bazujące na samoregulacji oraz normach \textit{soft-law}. Z uwagi na zakres przedmiotowej pracy, propozycje te nie są szerzej omawiane. Relacje pomiędzy prawem stanowionym a samoregulacją, a także sposób w jaki oba podejścia mogą się uzupełniać omówiono w: D. Johnson, D. Post, \textit{Law And Borders…}, op. cit., s. 1367-1402.}

\footnotetext[387]{Rezolucja na rzecz zapewnienia ochronie danych i prywatności stałego miejsca w międzynarodowym prawie, https://goo.gl/YnVNgR, s. 1.}

\footnotetext[388]{Rezolucja na temat współpracy ze Specjalnym Sprawozdawcą ONZ ds. Prywatności, https://goo.gl/kyu4PD, p. 4.}

\footnotetext[389]{G. Greenleaf, \textit{Balancing…}, s. 3-4.}
bazować na Konwencji 108 i jej protokole dodatkowym, które są otwarte do podpisu także dla państw nie należących do Rady Europy\textsuperscript{390}.

W efekcie Zgromadzenie zawnioskowało do Sekretarza Generalnego Rady Europy o zapewnienie odpowiedniego poparcia ze strony Organizacji Narodów Zjednoczonych w promowaniu przystąpienia do Konwencji 108 przez państwa na całym świecie, w szczególności poprzez działania w ramach podległych instytucji\textsuperscript{391}.

Przedstawiciele nauki prawa proponują alternatywne podejścia – np. G. Greenleaf postuluje, aby nowy, uniwersalny model ochrony danych oprzeć na wzajemnym powiązaniu MPPOP oraz Konwencji 108 według następujących założeń:

- uznanie przez KPC znaczenia Konwencji 108 poprzez aktualizację treści komentarza ogólnego nr 16 i wskazanie powiązania pomiędzy treścią art. 17 Paktu a Konwencją 108,

- wprowadzenie przez Radę Europy wymagania dla nowych państw przystępujących do Konwencji, które nie są jednocześnie stroną EKPC, związanego z koniecznością przyjęcia Pierwszego Protokołu Fakultatywnego do MPPOP,

- rozpatrywanie przez KPC skarg indywidualnych na naruszenia przepisów Konwencji 108 przez państwa-strony Paktu; w rezultacie KPC miałby realizować podobną funkcję do ETPC w systemie europejskiej konwencji\textsuperscript{392}.

Každa z propozycji opiera się zatem na wiodącej roli MPPOP jako systemu ochrony praw człowieka na ponadregionalnym zasięgu, uzupełnionego o szczegółowe wymagania związane z ochroną danych, wynikające z nowego protokołu fakultatywnego (propozycja Międzynarodowej Konferencji) lub z oddzielnego traktatu (w szczególności Konwencji 108). Wartość, jaką autorzy tych koncepcji postrzegają w oparciu postulowanych rozwiązań na Pakcie, wydaje się jednocześnie największym ograniczeniem. W obecnej formie Pakt i ustanowiony na jego podstawie system ochrony praw jest dalece niedoskonały – zwłaszcza biorąc pod uwagę funkcjonujące mechanizmy kontroli, brak skutecznego organu sądowego oraz niewiążący charakter wyroków. Nie jest jasne, w jaki sposób ustanowiony w ten sposób model ochrony miałby być kompatybilny ze standardami obowiązującymi w UE – pamiętając o silnych kompetencjach TSUE i ETPC jako ponadnarodowych organach sądowych

\textsuperscript{390} Rezolucja 1843 (2011) Zgromadzenia Parlamentarnego Rady Europy nt. ochrony prywatności i danych osobowych w Internecie i mediach online, https://goo.gl/AWMGu6, p. 11.

\textsuperscript{391} Ibidem, p. 21.1.

oddziałujących na prawodawstwo państw członkowskich, rozbudowanie uprawnień KPC w kierunku organu sądowego mogłoby w rzeczywistości utrudnić ujednolicenie interpretacji i orzecznictwa. Pamiętając o potencjalnym konflikcie w zakresie kognicji i orzecznictwa TSUE i ETPC\textsuperscript{393}, ustanowienie trzeciego międzynarodowego trybunału o podobnych uprawnieniach mogłoby nie przyczynić się do wzmocnienia praw, ale – w skrajnym przypadku – do ich osłabienia poprzez wprowadzenie do obrotu prawnego orzeczeń zawierających odmienne interpretacje tych samych praw czy obowiązków.

Dlatego wydaje się, że systemy ochrony praw co do zasady powinny koncentrować się na realizacji funkcji ochronnej dla jednostek, natomiast prawodawstwo (także ponadnarodowe) dotyczące ochrony danych osobowych – na wzmacnianiu obowiązków regulacyjnych i nadzorczych. Odmienny cel stanowienia przepisów pozwala na skorzystanie z różnych środków, w celu zapewnienia ich skuteczności. W przypadku systemów ochrony praw kluczowe jest zdefiniowanie oczekiwanego rezultatu, z kolei w przypadku ochrony danych – wykazanie należytej staranności. Stąd też regulacje wprowadzane w tym drugim obszarze powinny koncentrować się na określeniu standardów przetwarzania, minimalnych zabezpieczeń oraz sposobu nadzoru i kontrolowania przekazywania zbiorów danych. W tym zakresie pomocne może być skorzystanie z kilkudziesięcioletnich doświadczeń w definiowaniu standardów dla systemów informatycznych przetwarzających informacje niejawne. O ile w przypadku pierwszych norm wprowadzanych w tym obszarze, próbowało opisać wymagania funkcjonalne „bezpiecznego systemu”\textsuperscript{394}, to na skutek niepowodzenia i braku elastyczności w takim podejściu – w późniejszych normach definiowano i opisywano proces zarządzania bezpieczeństwem\textsuperscript{395}. W takim podejściu kluczowe nie jest osiągnięcie stanu bezpieczeństwa (który w praktyce jest trudno definiowalny), ale podejmowanie systematycznych działań zwiększających pewność, że informacje będą przetwarzane w

---

\textsuperscript{393} Por. rozważania przedstawione w rozdziale 2.4.4.


\textsuperscript{395} Przykładem może być norma międzynarodowa ISO/IEC 15408, nazywana w literaturze jako „wspólne kryteria” (Common Criteria, CC), określająca proces oceny bezpieczeństwa systemu IT za pomocą analizy zabezpieczeń istniejących w szeregu procesów – począwszy od projektowania, rozwoju, na implementacji i utrzymaniu skończyszy. CC prezentuje zatem bardziej holistyczne podejście do tematu bezpieczeństwa informacji w systemach IT niż w przypadku TCSEC. Zob. L. Grocholski, A. Niemieć, Jakość i bezpieczeństwo – wymagania i kryteria oceny, [w:] Bezpieczeństwo systemów informatycznych pod red. A. Niemieć, J. Nowak, J. Grabała, Katowice 2006, s. 67-73; K. Lange-Sadzińska, Common Criteria i polskie unormowania dotyczące bezpieczeństwa systemów informatycznych, Acta Universitatis Lodziensis Folia Oeconomica 2003, s. 201-204.
sposób bezpieczny. Przenosząc powyższe wnioski na analizowany obszar badawczy, przepisy dotyczące ochrony danych osobowych powinny wprowadzać wymagania związane z ustanowieniem systemu zarządzania bezpiecznym przetwarzaniem informacji (np. na wzór normy ISO/IEC 27001396), którego stosowanie przez podmiot przetwarzający zwiększy prawdopodobieństwo, że wymagania prawne związane z ochroną prywatności (wynikające m.in. z systemów ochrony praw człowieka) nie zostaną naruszone.

Rozdział 4. Prawo UE jako narzędzie podnoszenia standardów w obszarze prywatności w cyberprzestrzeni

4.1. Wprowadzenie i uwagi ogólne

Model ochrony prywatności i danych osobowych funkcjonujący w Unii Europejskiej jest powszechnie uznawany za najbardziej kompleksowy i odzwierciedlający złożoność rynku przetwarzania informacji w erze społeczeństwa informacyjnego. Nadanie ochronie prywatności oraz danych osobowych rangi praw podstawowych stanowiło kolejny impuls do rozwoju i dalszego wzmocnienia gwarancji jednostek wynikających z przepisów prawa UE. W rezultacie nie tylko żadna inna organizacja międzynarodowa, ale również żadne inne państwo nie wypracowało tak rozbudowanych i nowoczesnych prawnych mechanizmów ochrony prywatności w cyberprzestrzeni. Konsekwencją bycia liderem w tym obszarze jest jednak trudność w rozwijaniu relacji zewnętrznych, związana z jednej strony z chęcią ułatwienia wymiany handlowej i gospodarczej, z drugiej zaś z potrzebą poszanowania wprowadzonych wysokich standardów ochrony przekazywanych informacji. Problem ten coraz częściej jest zauważany w relacjach UE –USA, jednak de facto dotyczy współpracy UE ze wszystkimi innymi partnerami handlowymi – w przypadku Stanów Zjednoczonych, z uwagi na wzajemne znaczenie gospodarcze, jest po prostu lepiej rozpoznany i omówiony w literaturze przedmiotu.

W niniejszym rozdziale zostanie zaprezentowana ewolucja, obecny kształt oraz oczekiwane zmiany prawodawstwa UE dotyczącego ochrony prywatności w cyberprzestrzeni. Z uwagi na charakter wyroków TSUE i ich wpływ na interpretację i stosowanie prawa odpowiednia uwaga zostanie zwrócona na precedensowe orzeczenia Trybunału. Analizowany obszar należy do dziedzin prawa dynamicznie rozwijających się acquis. Dlatego przedstawione rozważania zostaną przeprowadzone z podziałem nie na poszczególne akty normatywne, ale zagadnienia (obszary) podlegające regulacji. W ten sposób w kolejnych punktach przedstawione i omówione zostaną:

- przepisy wprowadzające ogólny model ochrony danych – w szczególności dyrektywa 95/46 oraz rozporządzenie 2016/679 (ogólne rozporządzenie o ochronie danych),

397 G. Buttarelli, The EU GDPR as a clarion call for a new global digital gold standard, International Data Privacy Law 2016, t. 6, z. 2, s. 77.
398 Por. informacje na temat charakteru prawnego praw i wolności przewidzianych w Karcie Praw Podstawowych, rozdział 2.4.2, s. 70 i n.
przepisy szczegółowe związane z ochroną prywatności w łączności elektronicznej – dyrektywa 2002/58 wraz z projektem zastępującego ją rozporządzenia, a także dyrektywa 2006/24,
przepisy odnoszące się do obszaru współpracy w sprawach karnych, w ujęciu zarówno przed reformą Lizbońską, jak i po niej, ze szczególnym uwzględnieniem dyrektywy 2016/680 oraz 2016/681.

Chociaż w niedługim czasie (od maja 2018) podstawę do przetwarzania danych na terenie UE stanowić będzie ogólne rozporządzenie, to nie sposób zrozumieć przyczyn, obecnego kształtu i ograniczeń istniejącego modelu ochrony danych bez odwołania do ponaddwudziestoletnich doświadczeń w stosowaniu dyrektywy 95/46. Dlatego wiele z przedstawionych rozważań bazować będzie na dyrektywie i orzecznictwie z nią związanym, z tym wszakże zamiarem, aby za pomocą komparatystyki wykazać zasadność wprowadzonych zmian lub zaznaczyć obszary, w których zauważone niedoskonałości legislacji mogą skutkować ograniczeniem ich skuteczności.

Oddzielną, równie interesującą płaszczyzną analizy będzie omówienie współpracy transatlantyckiej UE – USA w zakresie przekazywania i przetwarzania danych obywateli UE – która niczym pryzmat ogniskuje obawy wyrażane w literaturze przedmiotu w zakresie praktycznej skuteczności i przydatności budowania regionalnych systemów ochrony danych w zglobalizowanym rynku przetwarzania informacji, w którym nie istnieją granice i bariery w przepływie danych.

4.2. Geneza i ewolucja przepisów wspólnotowych

Dyskusja nad zasadnością i zakresem prawnej ochrony danych osobowych, jaka została zapoczątkowana w latach siedemdziesiątych dwudziestego wieku, objęła swoim zasięgiem także instytucje Wspólnot Europejskich. Należy pamiętać, że we wskazanym okresie w Europie obszar ochrony praw człowieka wiązał się z działalnością Rady Europy oraz EKPC.

Z kolei ochrona danych osobowych była postrzegana z jednej strony jako związana z ochroną prywatności, a więc obszarem wolności jednostki, z drugiej jednak miała bezpośredni związek z obszarem współpracy gospodarczej. Zdefiniowanie zbyt restrykcyjnych lub

---

399 Por. np. polemikę przedstawioną przez C. Kuner w Reality and Illusion in EU Data Transfer Regulation Post Schrems, University of Cambridge Faculty of Law Research Paper 2016, nr 14, ssrn.com/abstract=2732346.
400 Szersze informacje na temat genezy EKPC w rozdziale 2.3.1 (s. 60 i nast.), natomiast na temat ewolucji rozwiązań prawnych w obszarze danych osobowych w rozdziale 3.2 (s. 98 i nast.).
niedopasowanych zasad ochrony danych osobowych na poziomie krajowym mogło skutecznie utrudnić transfer informacji, a co za tym idzie stanąć na przeszkodzie w harmonizacji rynku wewnętrznego. Dlatego już w 1975 roku Parlament Europejski, rozpoznając potrzebę regulacji w tym obszarze oraz ryzyka związane z brakiem wdrożenia lub funkcjonowaniem niezgodnych przepisów krajowych, powołał specjalny komitet w celu zbadania między innymi metod automatycznego gromadzenia danych, praw jednostek w zakresie przetwarzania informacji, a także zasadności wprowadzenia wspólnych standardów dla sektora prywatnego i publicznego. W kolejnych latach Parlament ponawiał rezolucje w tym obszarze, przy czym wraz z ewolucją międzynarodowych rekomendacji oraz wnioskami z debaty trwającej w ramach WE rozbudowywane były także wytyczne dla wspólnotowego projektodawcy wskazujące charakter i ramy przyszłej regulacji. Załącznikiem do rezolucji z 8 maja 1979 roku w sprawie ochrony praw jednostek w związku z rozwojem technologii przetwarzania danych była lista siedemnastu rekomendacji Parlamentu Europejskiego, podsumowującej wnioski z dotychczasowych prac nad przyszłą legislacją.402

Nie wszystkie rekomendacje PE zostały zaadaptowane do późniejszych projektów aktów prawnych. Niektóre z nich, jak np. postulat powołania wspólnotowego organu nadzoru, właściwego do kontroli transferu danych poza obszar Wspólnoty, czekał na realizację kilkudziesiąt lat i został częściowo zrealizowany dopiero wraz z ustanowieniem Europejskiego Inspektora Ochrony Danych w 2004 roku.

Przedstawione wytyczne, zgodnie z zasadami stanowienia prawa wynikającymi z procedury współdecydowania określonej w art. 189b TWE (obecnie zwykła procedura ustawodawcza, opisana w art. 294 TFUE), nie wiązały projektodawcy, którym była KE, jednak stanowiły ważny głos w dyskusji oraz zakreślały oczekiwany kierunek, w jakim przepisy powinny zmierzać.

Komisja Europejska w rekomendacji wydanej 29 lipca 1981 roku potwierdziła, że „ochrona danych jest niezbędną częścią ochrony praw jednostki”, a przez swoje fundamentalne znaczenie jest „pożądane, aby państwa członkowskie osiągnęły podobny poziom ochrony danych”. Komisja podkreśliła znaczenie działań podejmowanych w tym

**401** Rezolucja PE z dn. 21 lutego 1975 w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych (Dz.U. WE z 1975 Nr C 60, s. 48).
**402** Rezolucja PE z dn. 8 maja 1979 w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych (Dz.U. WE z 1979 Nr C 140, s. 34).
**404** Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, 81/679/EEC, CELEX: 31981H0679.
zakresie na forum Rady Europy, a w szczególności rolę Konwencji nr 108. Wskazano, że przystąpienie do konwencji jest najlepszym sposobem zapewnienia standaryzacji nie tylko wśród państw członkowskich WE, ale również w całej Europie. Ponieważ KE (ani żadna instytucja WE) nie miała kompetencji do skutecznego zobowiązania państw członkowskich do zawarcia określonej umowy międzynarodowej, Komisja w swojej rekomendacji zaznaczyła, że w przypadku braku przystąpienia wszystkich członków WE do Konwencji 108 konieczne może być wprowadzenie wspólnotowych rozwiązań prawnych.


Zaproponowany model ochrony danych wprost odniósł się do dorobku RE oraz OECD. Wskazywano jednocześnie, że celem przepisów jest zapewnienie wysokiego poziomu ochrony, tak aby wprowadzone prawo wspólnotowe nie skutkowało obniżeniem standardów wynikających z przepisów krajowych. Projektodawcy wskazali, że cele przepisów jest zapewnienie wysokiego poziomu ochrony prywatności. Dlatego propozycje wypracowane na poziomie wspólnotowym, chociaż zmierzające do realizacji celów traktatowych – w szczególności harmonizacji rynku wewnętrznego – nie mogły doprowadzić do powstania konfliktu w obszarze gwarancji i wolności wynikających z dorobku konstytucyjnego państw członkowskich407.

Prawodawca wspólnotowy zapewnił, aby dyrektywa 95/46 była zgodna z wymaganiami wynikającymi z Konwencji 108, a jednocześnie uszczegóławiała i doprecyzowała wymagania wszędzie tam, gdzie zobowiązania konwencyjne były zbyt ogólne lub pozostawiały duży margines uznania dla prawodawcy krajowego. Podejście to było

405 Ibidem, s. 110.
406 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.101995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE z 1995 Nr L 281, str. 31).
407 Por motyw 1 dyrektywy 95/46.
słuszne, zwłaszcza pamiętając, że Komisja przedkładając w 1990 roku wytyczne do projektu dyrektywy jednocześnie zakładała przystąpienie Wspólnoty do Konwencji 108.

Dyrektyna 95/46 w założeniu miała stanowić normę obejmującą wszystkie formy przetwarzania danych (w tym przetwarzanie ręczne), we wszystkich obszarach – a więc zarówno w sektorze prywatnym, jak i publicznym. Prawodawca przewidywał możliwość utworzenia przepisów szczegółowych zarówno na poziomie prawa wspólnotowego oraz krajowego 408. Określił przy tym rygorystyczne zasady limitacji i derogacji praw określonych w dyrektywie.

Komisja, przedkładając projekt dyrektywy o ochronie danych, opublikowała też drugi projekt – dyrektywy o ochronie danych osobowych oraz prywatności w zakresie publicznych cyfrowych sieci telekomunikacyjnych 409. Projekt stał się podstawą dla opracowania i przyjęcia dyrektywy 97/66 z dnia 15 grudnia 1997 roku 410.

Regulacja stanowiła rozwinięcie i uzupełnienie dyrektywy 95/46 w obszarze publicznej łączności telekomunikacyjnej. W szczególności przepisy dyrektywy nakładały na dostawców i operatorów usług publicznych obowiązki związane z wprowadzeniem odpowiednich technicznych oraz organizacyjnych środków w celu zapewnienia bezpieczeństwa usług oraz sieci (art. 4 ust. 1). W tym zakresie podejmowane działania miały uwzględniać nie tylko koszty podejmowanych działań, ale także odniesienie poziomu bezpieczeństwa do istniejącego stopnia ryzyka. Dyrektywa wprowadzała również na poziomie przepisów wspólnotowych zobowiązanie do zachowania tajemnicy telekomunikacyjnej – przy czym w tym zakresie podmiotem zobowiązanym były państwa, które miały zaimplementować do krajowych systemów prawnych środki konieczne do wprowadzenia zakazu słuchania, nagrywania, przechowywania oraz innych rodzajów kontroli łączności przez osobę inną niż uprawniony użytkownik (art. 5 ust. 1).

Chociaż co do zasady dyrektywa 97/66 stanowiła szczegółowienie zasad wynikających z dyrektywy 95/46, to z uwagi na objęcie jej regulacjami także abonentów będących osobami prawnymi nie można uznać, że jej zakres podmiotowy jest tożsamy z przepisami dyrektywy 95/46.

Dwa lata po terminie dostosowania przepisów krajowych do regulacji dyrektywy 97/66 Komisja Europejska wystąpiła z propozycją przyjęcia zaktualizowanej regulacji.

408 Por. motyw 68 dyrektywy 95/46.
410 Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym (Dz.U. WE z 1998 L 24, s. 1).
Podstawową przyczyną był dynamiczny rozwój środków łączności – zwłaszcza w zakresie usług mobilnych oraz Internetu. W efekcie niektóre z postanowień dyrektywy 97/66, odwołujące się wprost do łączności telefonicznej oraz usług głosowych, okazały się zbyt szczegółowe i nieadekwatne do rozwoju rynku. Krajowi prawodawcy odmiennie interpretowali poszczególne zapisy dyrektywy, w wyniku czego transpozycja przepisów wspólnotowych nie doprowadziła do ustanowienia jednolitych wymagań prawnych w obszarze państw członkowskich. Przykładem była odmienna interpretacja terminu „połączenie” w odniesieniu do innych niż głosowe usługi łączności elektronicznej.

Biorąc pod uwagę powyższe problemy, Komisja przygotowała projekt zaktualizowanej dyrektywy, która po zakończeniu procedury legislacyjnej została zatwierdzona jako dyrektywa 2002/58. Poza wprowadzeniem zmian o charakterze porządkującym i dostosowującym wcześniejsze wymagania do nowoczesnych sieci telekomunikacyjnych (np. określenie zasad przetwarzania i zapewnienia poufności informacji o lokalizacji czy danych o ruchu) w dyrektywie 2002/58 wskazano także bezpośrednie odwołanie do KPP, podkreślając, że jednym z celów aktu jest zapewnienie praw podstawowych związanych z poszanowaniem prywatności oraz ochroną danych osobowych.

Podsumowując doświadczenia ze stosowania przepisów opartych na dyrektywach – a więc aktach prawnych wymagających implementacji do porządku krajowego państw członkowskich – Komisja Europejska zauważyła, że „nie zapobiegły one rozdrobnieniu sposobów realizacji ochrony danych osobowych w całej Unii, ugruntowaniu niepewności prawnej oraz upowszechnieniu istniejącego w społeczeństwie poglądu, zgodnie z którym z działalnością prowadzoną w Internecie wiąże się istotne ryzyka”. Dlatego KE zaproponowała wprowadzenie nowej ramy ochrony danych osobowych, opartej nie na dyrektywie, ale na rozporządzeniu – a więc akcie prawnym, który wiąże bezpośrednio i nie wymaga transpozycji na poziomie krajowym. Taki kierunek zmian został zasygnalizowany przez KE już w listopadzie 2011 oraz poparty przez Parlament Europejski oraz Radę Europejską.

---

412 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. Urz. UE Nr L 201, s. 37).
413 Por. motyw 2. dyrektywy 2002/58.
415 Rezolucja Parlamentu Europejskiego z dnia 6 lipca 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej, P7_TA(2011)0323 (CELEX: 52011IP0323, Dz. Urz. UE z 2013 Nr CE 33, s. 101).
Postanowienia reformy lizbońskiej doprowadziły do zasadniczego wzmocnienia pozycji prawodawczej instytucji Unii w obszarze całościowej ochrony danych osobowych w państwach członkowskich. Dyrektywa 95/46 została przyjęta w oparciu o art. 100a TWE (obecnie art. 114 TFUE), a więc przepis kompetencyjny dotyczący harmonizacji rynku. Jakkolwiek celem dyrektywy była „ochrona podstawowych praw i wolności osób fizycznych, w szczególności prawa do prywatności w odniesieniu do przetwarzania danych osobowych”, to wybrana podstawa formalna związana była z realizacją działań gospodarczych (ułatwienie wymiany handlowej, funkcjonowanie rynku wewnętrznego). W Traktacie lizbońskim wprowadzone zostały dwie zmiany, prowadzące do wzmocnienia znaczenia ochrony prywatności w systemie prawa unijnego. Po pierwsze, na mocy art. 6 ust. 1 TUE nadano Karcie Praw Podstawowych moc wiążącą równą traktatom. W efekcie prawa wynikające z Karty, w tym prawo do poszanowania życia prywatnego (art. 7 KPP) oraz ochrony danych osobowych (art. 8 KPP) stały się częścią prawa pierwotnego UE. Po drugie, wprowadzono nowy przepis art. 16 ust. 1 TFUE, w którym wskazano, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Artykuł uzupełniono także przepisem kompetencyjnym (art. 16 ust. 2), który stał się podstawą do przyjęcia norm prawa wtórnego UE. W rezultacie w zaproponowanym przez Komisję projekcie ogólnego rozporządzenia o ochronie danych jako podstawę kompetencyjną wskazano art. 16, a cele gospodarcze ustąpiły pierwszeństwa celomwiązanym z ochroną praw podstawowych416.

Projekt został ostatecznie zatwierdzony przez Komisję 25 stycznia 2012 roku i stał się przedmiotem intensywnych prac organów Unii, włączając w to opinie wydawane przez instytucje utworzone po wejściu w życie dyrektywy 95/46 – Europejskiego Inspektora Ochrony Danych417 oraz Agencji Praw Podstawowych UE. Uwagę zwracała duża liczba uwag zgłoszonych przez PE: w przypadku pierwszego projektu dyrektywy 95/46 Parlament zgłosił 7418 uwag, natomiast pod projektem ogólnego rozporządzenia – 207419. Zakres wnioskowanych zmian nie pozwala uznać, aby były to uwagi o charakterze edycyjnym czy nieistotnym z punktu widzenia planowanej regulacji. Zmiany proponowane przez Parlament dotyczyły praktycznie każdego artykułu projektu, łącznie z zakresem materialnym, terytorialnym oraz stosowanymi definicjami.

416 Por. motyw 2. rozporządzenia 2016/679.
417 Opinia EIOD z 7 marca 2012 (CELEX: 52012XX0630(01)) oraz 20 lutego 2016 (CELEX: 52016XX0220(01)).
418 Lista uwag PE zgłoszonych do pierwszego projektu dyrektywy: Dz. Urz. WE z 1995 Nr C 166, s. 105.

Rada w opinii opublikowanej 19 maja 2017 roku zgłosiła szereg zastrzeżeń, w tym dotyczących wyboru formy aktu (rozporządzenie w miejsce dyrektywy), poszczególnych rozwiązań prawnych, w tym dotyczących zastosowanych definicji, mających bezpośrednie

420 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. UE L 119 z 4.5.2016).

421 Wniosek: Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), CELEX: 52017PC0010.

4.3. Terminologia

Doświadczenia związane z ponad dwudziestoma latami stosowania dyrektywy 95/46 przyczyniły się do znacznego rozbudowania warstwy definicyjnej w zastępującym ją rozporządzeniu 2016/679. O ile w Konwencji 108 wyróżniono 3 podstawowe terminy, w dyrektywie 95/46 – 8, to w rozporządzeniu 2016/679 jest to już 26 pojęć. Wprowadzono szereg nowych terminów, odnoszących się do szczegółowych kategorii danych („dane genetyczne”, „dane biometryczne”, „dane dotyczące zdrowia”), form organizacyjnych działania administratora danych („główna jednostka organizacyjna”, „przedsiębiorstwo”, „przedsiębiorstwo”, „grupa przedsiębiorstw”), sposobów przetwarzania danych („profilowanie”, „pseudonimizacja”).

W zakresie definicji pojęcia „dane osobowe” w RODO rozszerzono wcześniejszą definicję o informacje związane z aktywnością podmiotu danych w cyberprzestrzeni (numer identyfikacyjny, identyfikator internetowy) lub lokalizacją (dane o lokalizacji).

Jedną z niedoskonałości związanych z modelem ochrony danych opartym na dyrektywie 95/46 był brak wystarczającego uwzględnienia stosowania coraz powszechniejszych technik zabezpieczenia informacji, które prowadzą do ograniczenia lub pozbawienia osób trzecich możliwości identyfikacji osób za pomocą informacji przechowywanych w zbiorze danych. Przykładem takich środków jest pseudonimizacja lub szyfrowanie danych.

---


423 Ibidem, s. 6, p. 10.
Termin „pseudonimizacja” nie powinno być mylony z anonimizacją. Celem anonimizacji jest nieodwracalne pozbawienie zbioru danych cech pozwalających na identyfikację poszczególnych podmiotów danych. Anonimizacja jest techniką stosowaną w badaniach naukowych czy statystycznych. Dane poddane anonimizacji przestają posiadać atrybuty pozwalające uznać je za dane osobowe, nie podlegają zatem ochronie przewidzianej dla zbiorów danych osobowych. Z kolei pseudonimizacja polega na przetworzeniu zbioru danych do postaci, w której nie ma możliwości bezpośredniej identyfikacji podmiotów danych. Jest to proces odwracalny i w przypadku użycia odpowiedniego algorytmu oraz danych dodatkowych (np. zestawiających identyfikatory z bazy danych z nazwiskami podmiotów danych) pozwala na odtworzenie pierwotnego zbioru. Dlatego nie ma racji M. Siwicki, twierdząc, że „jedynie w przypadku anonimizacji powstają dane pseudonimiczne”\(^{424}\). Podobnie sytuacja ma się z danymi pseudolosowymi, których nie można uznać za losowe. Zgodnie z definicją zastosowaną w RODO pseudonimizacja musi wiązać się z oddzielnym przechowywaniem informacji dodatkowej (stanowiącej składnik potrzebny do odtworzenia oryginalnego zbioru) i objęciem tej informacji odpowiednimi środkami technicznymi i organizacyjnymi.

Wprowadzenie terminu danych pseudonomicznych nastąpiło w wyniku uwzględnienia poprawki 98 zgłoszonej do projektu rozporządzenia przez Parlament Europejski\(^{425}\). W tej samej poprawce Parlament postulował także dodanie definicji danych zaszyfrowanych, przez co należałoby rozumieć dane osobowe, które za pomocą technicznych środków ochrony stały się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich. Ten element poprawki nie został jednak uwzględniony, w wyniku czego RODO nie zawiera definicji szyfrowania danych. Co ciekawe, pojęcie to jest nadal stosowane w rozporządzeniu dla określenia jednego z podstawowych zabezpieczeń, jakie może wdrożyć administrator w celu ochrony przetwarzanego przez siebie zbioru. Co do zasady zbiór zaszyfrowany jest szczególnym przypadkiem zbioru pseudonomicznego, w którym klucz kryptograficzny pełni funkcję dodatkowej informacji, potrzebnej do odtworzenia pierwotnej postaci zbioru danych osobowych. Pojęcie danych pseudonomicznych jest w takim rozumieniu szersze i obejmuje także dane zaszyfrowane.

Oddzielnego omówienia wymagają terminy wprowadzone w rozporządzeniu 2002/58. Pamiętając, że akt ten stanowi lex specialis w zakresie przetwarzania danych osobowych,

---

\(^{424}\) M. Siwicki, *Ochrona osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych*, Państwo i Prawo 2016, nr 3, s. 76.

\(^{425}\) Lista uwag PE zgłoszonych do projektu ogólnego rozporządzenia: A7-0402/2013, http://cli.re/GDM73M.
wprowadzone w nim definicje mają na celu uszczegółowienie i doprecyzowanie pojęć wskazanych w dyrektywie 95/46. Stąd w omawianym akcie zdefiniowano kluczowe terminy „komunikat” oraz „dane o ruchu”. Komunikat stanowi merytoryczną część przekazu (np. treść rozmowy głosowej, wiadomości e-mail, korespondencja przekazana za pośrednictwem komunikatorów internetowych), podczas gdy dane o ruchu związane są z informacjami towarzyszącymi przesłaniu komunikatu, ale nie stanowią jego części. W zależności od zastosowanego środka łączności należą do nich informacje techniczne służące przekazaniu komunikatu lub rozliczania usługi, ale i dane statystyczne lub pozwalające na odpowiednie przedstawienie treści odbiorcy lub nadawcy (np. identyfikator konwersacji). Dane o ruchu są często nazywane w literaturze przedmiotu „metadany”\footnote{Zob. definicję metadanych w internetowym słowniku Harvard Law School: http://hls.harvard.edu/dept/its/what-is-metadata/}. Analiza zbioru metadanych może pozwolić nie tylko na identyfikację komunikujących się stron, ale także posłużyć do analizowania osobistych preferencji lub przewidywania zachowania osób, zatem w oczywisty sposób może prowadzić do inwazji na sferę prywatności. Typowym przykładem danych o ruchu są informacje o lokalizacji użytkownika lub dane związane z użyciem usług – w szczególności pozwalające na identyfikację sieci, w której komunikat powstaje lub zostaje przerwany, a także informacje o początku, końcu lub długości połączenia\footnote{Zob. motyw 15. dyrektywy 2002/58.}.

### 4.4. Zakres regulacji

#### 4.4.1. Dyrektywa 95/46

Zakres stosowania regulacji UE w obszarze ochrony prywatności i danych osobowych należy omówić z uwzględnieniem zakresu przedmiotowego, podmiotowego, terytorialnego oraz granic stosowania prawa UE.

Zakres obowiązywania dyrektywy 95/46 został wskazany w art. 3 i obejmuje czynności przetwarzana danych osobowych realizowane w całości lub w części w sposób zautomatyzowany oraz czynności innego przetwarzania danych osobowych. Katalog sposobów przetwarzania danych wskazany w dyrektywie jest przykładowy, dlatego należy przyjąć, że jej zakresem objęte są wszelkie możliwe formy przetwarzania danych – nie tylko wymienione wprost w art. 2 pkt b. Zakres podmiotów zobowiązanych obejmuje natomiast administratorów danych, a więc podmioty, które zgodnie z przepisami odpowiadają za dobór
celu i sposobów przetwarzania danych, przy czym nie ma znaczenia, czy są to podmioty sektora prywatnego, czy publicznego.

Prawodawca unijny wyłączył z zakresu stosowania dyrektywy czynności związane z przetwarzaniem danych realizowane przez osoby fizyczne o czysto osobistym lub domowym charakterze (art. 3 ust. 2 tiret 2). Jak wskazano w preambule dyrektywy, przykładem takich czynności jest korespondencja czy przechowywanie spisów adresów. Natomiast każda forma upubliczniania danych osobowych, także realizowana przez osoby fizyczne w sposób niezwiązany z prowadzeniem działalności gospodarczej czy zarobkowej, nie korzysta ze wskazanego zwolnienia przedmiotowego. Jak podkreślił TSUE, wyłączenie to powinno być interpretowane jako obejmujące wyłącznie działania wchodzące w zakres życia prywatnego lub rodzinnego jednostki, co w sposób oczywisty nie ma miejsca w przypadku przetwarzania danych osobowych polegającego na ich opublikowaniu w Internecie w taki sposób, że staną się one dostępne dla nieograniczonej liczby osób428. Jak jednak zauważył rzecznik generalny w sprawie Ryneš, z faktu, że publikowanie danych jest przesłanką często wymienianą wśród przesłanek wskazujących na brak możliwości zastosowania wyjątku przewidzianego w art. 3 ust. 2 tiret drugi, to – a contrario – nie można uznać, że brak publikacji jest wystarczający, aby stwierdzić, że wyjątek ten może być zastosowany429. Dlatego nie stanowi czynności o wyłącznie osobistym lub domowym charakterze wykorzystywanie przez osobę fizyczną systemu kamer rejestrującego obraz osób na sprzęcie nagrywającym w sposób ciągły, nawet jeżeli urządzenia te są wykorzystywane w celu ochrony własności, zdrowia i życia właścicieli domu, jeżeli system ten monitoruje także przestrzeń publiczną – nawet jeżeli informacje te nie są nigdzie publikowane430.

Zgodnie z art. 3 ust. 2 tiret 1 poza obszarem regulacji znalazły się czynności przetwarzania danych, wykraczające poza zakres prawa UE – w szczególności związane z obszarem bezpieczeństwa publicznego, obronnością, bezpieczeństwem państwa oraz działalnością państwa w obszarach prawa karnego. W tym miejscu należy przywołać zasadę przyznającą znikomoczącą z art. 4 ust. 1 TUE, zgodnie z którą kompetencje nieprzyznane Unii w traktatach należą do państw członkowskich. W szczególności, zgodnie z art. 4 ust. 2 TUE, bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego. Jak jednak podkreślił TSUE, uprawnienie państwa członkowskiego

428 Wyrok TSUE z 6.11.2003 w sprawie Lindqvist, sygn. C-101/01, p. 47.
do skorzystania z odstępstwa przewidzianego w traktatach nie stoi na przeszkodzie sądowej kontroli działań podjętych w ramach tego odstępstwa\textsuperscript{431}.

Obszary wymienione w art. 3 ust. 2 tiret 1 stanowią w każdym razie działania właściwe państwowom i władzom państwowym, obce dziedzinom działalności jednostek\textsuperscript{432}. W rezultacie wyłączenie to należy interpretować zawężając i zastosować wyłącznie do takich działalności, które zostały w nim wyraźnie wymienione i które nie mogą być zaliczone do tego samego rodzaju\textsuperscript{433}.

Przepisem kompetencyjnym dla wprowadzenia dyrektywy był art. 114 TFUE (wcześniej 94 TWE), dotyczący zbliżania ustawodawstw państw członkowskich i harmonizacji rynku wewnętrznego. Przy czym, jak wskazał TSUE, zastosowanie art. 114 nie wymaga w każdym przypadku rzeczywistego związku regulowanej działalności ze swobodnym przepływem w ramach rynku wewnętrznego między państwami członkowskimi\textsuperscript{434}. Dlatego zakres stosowania dyrektywy nie powinien być ograniczony wyłącznie do czynności, w których pojawia się międzynarodowy kontext przetwarzania danych (np. przetwarzanie następuje w kilku państwach członkowskich lub administrator danych i podmiot danych podlegają przepisom innego prawa krajowego). Dlatego, zgodnie z art. 4 ust. 1 dyrektywy, obowiązek stosowania przepisów prawa krajowego będącego implementacją dyrektywy następuje w każdym przypadku, gdy przetwarzania danych odbywa się „w kontekście” prowadzenia przez administratora danych działalności gospodarczej na terytorium dowolnego państwa członkowskiego. Ponadto zgodnie z art. 4 ust. 3 zakres stosowania dyrektywy rozszerzono na sytuacje, gdy administrator danych nie prowadzi działalności gospodarczej na terenie UE, ale wykorzystuje w jej ramach środki znajdujące się na terytorium państwa członkowskiego.

Kwestia terytorialnego zakresu stosowania dyrektywy szybko stała się jednym z praktycznych problemów, które rozstrzygnąć musiał Trybunał Sprawiedliwości. W szczególności dynamiczny rozwój Internetu spowodował, że coraz częściej popularne e-usługi, z których korzystało miliony użytkowników na terenie UE, świadczone były przez przedsiębiorców formalnie prowadzących działalność poza terenem Unii. W takim przypadku sporny był zakres stosowania dyrektywy, powstawały także niejasności, w jaki sposób zagraniczny operator ma pogodzić stosowanie przepisów UE ze swoim – często sprzecznym – prawem krajowym. Wątpliwości budziła także redakcja przepisu art. 4 ust. 1 pkt c w zakresie,

\begin{itemize}
\item \textsuperscript{431} Wyrok TSUE z 4.12.1974 w sprawie \textit{van Duyn}, sygn. C-41/74.
\item \textsuperscript{432} Wyrok TSUE w sprawie \textit{Lindqvist}, sygn. C-101/01, p. 43.
\item \textsuperscript{433} Ibidem, p. 44.
\item \textsuperscript{434} Wyrok TSUE z 12.12.2006 w sprawie \textit{Niemcy v. Komisja Europejska}, sygn. C-380/03.
\end{itemize}
w jakim odwołano się do wykorzystywania przez administratorów danych środków przetwarzania zlokalizowanych na terytorium dowolnego państwa UE. W praktyce niejasne było, czy w takim przypadku stosowanie prawa UE ma być ograniczone do czynności faktycznie wykonywanych na terytorium Unii (np. związanych z eksploatacją centrum przetwarzania danych zlokalizowanego na terenie państwa członkowskiego), czy do całego procesu przetwarzania danych, nawet jeżeli tylko jego część i to w ograniczonym zakresie była wykonywana na terenie UE.

Kwestie te zostały rozstrzygnięte przez TSUE w precedensowym orzeczeniu w sprawie Google Spain SL, w którym stwierdził, że do uznania konieczności stosowania przepisów dyrektywy 95/46 wystarczy, aby przedsiębiorca ustanowił w państwie członkowskim oddział lub spółkę zależną, którego celem jest promocja i sprzedaż powierzchni reklamowych oferowanych za pośrednictwem świadczonej e-usługi\(^435\).

W tym kontekście Trybunał przypomniał, że w szczególności z motywów 18–20 i z art. 4 dyrektywy 95/46 wynika, iż celem prawodawcy unijnego było niedopuszczenie do pozbawienia jednostek ochrony, do której mają one prawo na mocy tej dyrektywy i dlatego przewidział dla tej ochrony szczególnie szeroki terytorialny zakres zastosowania. Adresowanie przez dostawcę e-usługi reklam do użytkowników zlokalizowanych na terenie UE poprzez aktywną sprzedaż powierzchni reklamowej za pośrednictwem spółki zależnej lub zarejestrowanej na terenie dowolnego państwa członkowskiego prowadzi do uznania, że świadczona działalność spełnia kryterium ustanowione w art. 4 ust. 1 lit. a dyrektywy.

Wyrok w sprawie Google Spain SL zapoczątkował ożywioną dyskusję w doktrynie na temat celu i skuteczności ustanawiania przez unijnego prawodawcę norm prawnych, które mają być stosowane przez firmy świadczące swoje usługi spoza granic UE\(^436\). W szczególności sygnalizowano brak efektywnych mechanizmów egzekwowania norm oraz brak możliwości skutecznej ochrony prawnej na drodze prawnoadministracyjnej i sądowej.

Z kolei w wyroku w sprawie Weltimmo TSUE przychylił się do elastycznej koncepcji pojęcia prowadzenia działalności gospodarczej. W rezultacie, w celu ustalenia, czy dany przedsiębiorca będący administratorem danych prowadzi działalność gospodarczą w rozumieniu dyrektywy 95/46 w innym państwie członkowskim niż państwo formalnej rejestracji, Trybunał wskazał na konieczność oceny stopnia stabilności rozwiązania organizacyjnego, jak również faktyczny charakter prowadzenia działalności w danym

\(^{435}\) Wyrok TSUE z 13.05.2014 w sprawie Google Spain SL, sygn. C-131/12, p. 60.

państwie członkowskim. Przedstawione rozważania miały w szczególności zastosowanie do przedsiębiorców, którzy zajmują się oferowaniem usług wyłącznie za pośrednictwem Internetu – a więc na odległość, z obszaru innego państwa437. Na tym tle Trybunał zauważył, że w szczególnych sytuacjach nawet obecność pojedynczego, odpowiednio umocowanego przedstawiciela, który prowadzi faktyczną i rzeczywistą działalność, choćby nawet drobną, wystarczy do uznania istnienia stabilnego rozwiązania organizacyjnego438. Równorzędną przesłanką do uznania, że czynności przetwarzania danych odbywają się w kontekście działalności gospodarczej prowadzonej w UE, jest zredagowanie stron internetowych e-usługi w języku powszechnie wykorzystywanym w tym państwie członkowskim. Fakt ten może dowodzić, że prowadzona działalność jest w głównej mierze, a nawet w całości, nakierowana na to państwo439.

Wyrok w sprawie Weltimmo ma istotne znaczenie, zwłaszcza w sektorze operatorów usług internetowych, w przypadku których może wiązać się z koniecznością uwzględnienia europejskich przepisów o ochronie danych osobowych niezależnie od miejsca faktycznego prowadzenia działalności gospodarczej.

Należy przypomnieć, że w systemie prawnym UE prawo do ochrony danych osobowych znalazło rozwinięcie nie tylko w przepisach prawa wtórnego (takich jak omawiana dyrektywa 95/46), ale przede wszystkim w przepisach prawa pierwotnego (art. 8 KPP)440. Obserwacja ta ma doniosłe znaczenie, jeżeli uwzględnimy, że zakres wyłączeń zastosowany w przepisach prawa wtórnego (dyrektywy) jest szerszy niż wynikający z przepisów prawa pierwotnego. Dlatego sam fakt zastosowania wyłączenia danego obszaru spod regulacji dyrektywy 95/46 nie oznaczał, że w zakresie tym nie mogły znaleźć zastosowanie przepisy Karty Praw Podstawowych. Rozróżnienie to zauważała rzecznik generalna J. Kokott w opinii wydanej w sprawie Puškár, podkreślając różny zakres stosowania przepisów o ochronie danych osobowych wynikających z dyrektywy 95/46 oraz Karty Praw Podstawowych w dziedzinie karnoprawnej441.

---

437 Wyrok TSUE z 1.10.2015 w sprawie Weltimmo, sygn. C-230/14, p. 29.
439 Ibidem, p. 41.
440 Szczegółowe omówienie przepisów KPP w obszarze ochrony prywatności przedstawiono w rozdziale 2.4, s. 68 i nast.
4.4.2. Dyrektywa 2002/58

Przepisy dyrektywy 2002/58 co do zasady uzupełniają i doprecyzowują regulacje wynikające z dyrektywy 95/46 w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej. Dlatego analizując zakres przedmiotowy i podmiotowy dyrektywy 2002/58, nie tracą nic na aktualności wcześniejsze rozważania związane z dyrektywą 95/46.

Zauważyć trzeba, że o ile krąg podmiotów zobowiązanych z dyrektywy 2002/58 stanowi podzbiór i nie wykracza poza zakres zobowiązań na podstawie przepisów dyrektywy 95/46, o tyle już zakres osób uprawnionych, a także zakres przedmiotowy obu regulacji w niektórych obszarach jest rozbieżny.

Do grona podmiotów uprawnionych należą przede wszystkim użytkownicy usług łączności elektronicznej, a więc wszystkie osoby fizyczne korzystające z takich usług, zarówno do celów prywatnych, jak i handlowych oraz niezależnie od podstawy formalnej korzystania z usług (w szczególności zawarcia imiennej umowy z operatorem). Dodatkowo dyrektywa 2002/58 zgodnie z art. 1 ust. 2 zapewnia ochronę uzasadnionych interesów abonentów będących osobami prawnymi. Dyrektywa 95/46 swoim zakresem nie obejmowała ochrony osób prawnych, zakresem jej stosowania była ochrona praw i wolności osób fizycznych.

Zakres przedmiotowy aktu nie obejmuje wyłącznie obszaru przetwarzania danych osobowych. Nadrzędnym celem dyrektywy 2002/58 jest ochrona prywatności, co w tym wypadku może wiązać się z szerszym zakresem ochrony niż dotyczącym wyłącznie danych osobowych. Z punktu widzenia zasad związanych z poufnością komunikacji (art. 5), przetwarzaniem danych o ruchu (art. 6) czy danych dotyczących lokalizacji (art. 9) nie jest istotne, czy stanowiące przedmiot ochrony informacje zawierają dane osobowe. Jednocześnie jednak prawodawca we wszystkich obszarach, w których w trakcie realizacji obowiązków wynikających z dyrektywy 2002/58 nastąpi konieczność przetwarzania danych osobowych, odwołał się do wymagań dyrektywy 95/46.

Zgodnie z art. 1 ust. 3, dyrektywa 2002/58 nie ma zastosowania do działalności wykraczającej poza zakres prawa UE, w szczególności do działalności dotyczącej bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa i działalności państwa w dziedzinie prawa karnego. Norma ta jest przeniesieniem regulacji art. 3 ust. 1 tiret 1 dyrektywy 95/46, dlatego w tym zakresie aktualne pozostają uwagi przedstawione w punkcie poprzednim.
Zgodnie z art. 3 dyrektywa 2002/58 ma zastosowanie do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii, włącznie z publicznymi sieciami łączności służącymi do zbierania danych i obsługi urządzeń identyfikacyjnych. Z treści przepisu TSUE wywiodł wniosek, że zakresem regulacji dyrektywy objęta jest działalność dostawców tych usług, a więc podmiotów innych niż organy władzy publicznej\[442\]. W efekcie uznać należy, że dyrektywa 2002/58 nie jest adresowana do organów władzy publicznej.

4.4.3. Rozporządzenie 2016/679

Doświadczenia w ponaddwudziestoletnim stosowaniu przepisów dyrektywy 95/46, w tym w szczególności bogaty dorobek orzeczniczy TSUE dotyczący zakresu i możliwych ograniczeń w stosowaniu unijnych przepisów dotyczących ochrony prywatności i danych osobowych, znalazły odszczepienie w rozporządzeniu 2016/679. Uwagę zwraca rozdzielono przepisy związanych z zakresem materialnym (art. 2) oraz terytorialnym (art. 3) w nowej regulacji.

Podobnie jak w przypadku dyrektywy 95/46, rozporządzenie ma zastosowanie do przetwarzania danych osobowych niezależnie od jego formy (automatyczne oraz manualne) i zastosowanych środków. Z uwagi na zmianę formy regulacji (rozporządzenie w miejsce dyrektywy) prawodawca nie wskazał warunków transpozycji wymagań wynikających z regulacji do prawa krajowego, ponieważ inaczej niż w przypadku dyrektywy rozporządzenie nie wymaga implementacji i jest stosowane wprost. Zamiast tego w art. 2 ust. 2 określono kryteria pozwalające na uznanie, że szczególne kategorie przetwarzania nie są objęte zakresem rozporządzenia. Należy do nich działalność:

- nieobjęta zakresem prawa Unii,
- prowadzona przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze,
- prowadzona przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE,
- prowadzona przez właściwe оргany do celów zapobiegania przestępczości, postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Dwa pierwsze wyłączenia są znaczeniowo tożsame ze wskazanymi w art. 3 ust. 2 dyrektywy 95/46, dlatego przy ich analizie należy posłkować się interpretacją i uwagami przedstawionymi w rozdziale poprzednim. Parlament Europejski w uwagach do projektu rozporządzenia proponował, aby rozszerzyć zakres wyłączenia dotyczący czynności życia osobistego o uwzględnienie, aby „odstępstwo to miało również zastosowanie do publikacji danych osobowych, gdy istnieją racjonalne podstawy, by oczekiwać, że dostęp do nich będzie miała jedynie ograniczona liczba osób”\[^{443}\]. Uwzględnienie tej poprawki uczyniłoby nieaktualną tezę wynikającą z wyroku TSUE w sprawie Lindqvist, zgodnie z którą publikacja informacji przez osobę fizyczną uniemożliwia uznanie, że czynność przetwarzania ma charakter „czysto” osobisty i domowy. Poprawka ta nie została uwzględniona.

Zaproponowany przez KE tekst rozporządzenia uwzględniał, że wyłączenie w odniesieniu do działalności nieobjętej zakresem prawa Unii dotyczyć będzie „w szczególności bezpieczeństwa narodowego”. Rozwinięcie to zostało usunięte w wyniku wprowadzenia poprawki zaproponowanej przez PE. W zamian dodano do ostatniego tiretu, dotyczącego zapobiegania, wykrywania i ścigania przestępczości, rozwinięcie: „w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom”. Innymi słowy wyłącznie dotyczące „bezpieczeństwa narodowego” zastąpiono wyłączeniem w obszarze „zagrożeń dla bezpieczeństwa publicznego”. Nie jest to zmiana wyłącznie semantyczna i ma doniosłe skutki praktyczne. Kwestia możliwości stosowania ograniczeń prawa do prywatności oraz ochrony danych osobowych przez władzę publiczną motywowanych wymaganiami bezpieczeństwa narodowego była wielokrotnie przedmiotem rozważań TSUE. Przyjęta regulacja wydaje się w sposób właściwy odzwierciedlać argumentację TSUE, wskazującą na konieczność traktowania wszelkich ograniczeń praw podstawowych w sposób zawężający oraz badania istnienia faktycznych (realnych) przesłanek do ich zastosowania. Stąd też wymaganie, aby wyłączenie stosowania rozporządzenia miało za podstawę nie cały obszar bezpieczeństwa publicznego, ale zadania związane z ochroną i zapobieganiem zagrożeniom dla tego bezpieczeństwa, pozwala na skonkretyzowanie okoliczności, w jakich wprowadzona limitacja będzie mogła być uznana za usprawiedliwioną.

Przepisem kompetencyjnym przyjętym dla wprowadzenia rozporządzenia nie jest art. 114 TFUE – związany z harmonizacją rynku wewnętrznego – tylko nowo wprowadzony

\[^{443}\] Poprawka 96 zgłoszona przez PE do projektu ogólnego rozporządzenia (A7-0402/2013).
reformą lizbońską art. 16 ust. 2 TFUE. Rozwiązanie takie pozwoliło przesunąć na pierwszy plan kwestie ochrony praw podstawowych jako celu samoistnego regulacji, bez konieczności uzasadniania jej wprowadzania argumentacją związaną z funkcjonowaniem rynku wewnętrznego.

Prawodawca unijny uwzględnił w RODO tezy wyroków TSUE w sprawie Weltimmo i Google Spain SL, rozszerzając i doprecyzowując regulacje związane ze stosowaniem rozporządzenia w sytuacjach zlecania danych do przetwarzania poza obszarem UE oraz wykonywania operacji przetwarzania przez przedsiębiorców nie posiadających siedziby ani oddziału na terenie żadnego z państw członkowskich. Zgodnie z art. 3 ust. 1 przepisy RODO mają zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy samo przetwarzanie odbywa się w Unii. Przepis uzupełnia lukę prawą istniejącą w dyrektywie 95/46 w zakresie rozproszonego geograficznie przetwarzania informacji (np. przetwarzania w chmurze obliczeniowej) i nakazuje, aby w takich przypadkach właściwe było prawo UE, co w praktyce rozstrzyga także problem wskazania właściwej jurysdykcji. Natomiast w sytuacjach, w których administrator danych nie ma jednostek organizacyjnych w Unii, przepisy rozporządzenia powinny być stosowane, jeżeli przedsiębiorca ten oferuje towary lub usługi osobom przebywającym na terenie UE, niezależnie od tego, czy wymaga od nich zapłaty, lub stosuje środki monitorowania ich zachowania. Przyjęta w rozporządzeniu definicja zakresu terytorialnego jest więc szersza niż ustanowiona przez TSUE w orzeczeniu Google Spain SL. Prawodawca zdecydował się zobowiązać do stosowania europejskich przepisów o ochronie danych osobowych nie tylko dostawców e-usług, sprzedających reklamy za pośrednictwem zarejestrowanych w dowolnym państwie członkowskim spółek zależnych, ale przyjął szerszą redakcję przepisu – wskazującą na oferowanie towarów lub usług jako kryterium wystarczające do uznania jurysdykcji przepisów unijnych. Na tej podstawie P. Wirksa wnioskuje, że wystarczające do uznania konieczności stosowania RODO przez przedsiębiorców z krajów trzecich mogą być takie przesłanki, jak udostępnienie serwisu internetowego w języku lub operowanie walutą powszechnie stosowaną w co najmniej jednym państwie członkowskim lub wzmianka o klientach lub użytkownikach znajdujących się w UE.  

profilowaniem, a więc analizowaniem i przewidywaniem ich zachowania) prowadzi do znacznego rozszerzenia terytorialnego zakresu stosowania omawianych przepisów na podmioty, które wcześniej nie były objęte regulacjami dyrektywy 95/46.

Zgodnie z art. 27 ust. 1 podmioty spoza UE, które są obowiązane do stosowania rozporządzenia, powinny wyznaczyć na piśmie swojego przedstawiciela w Unii. Przedstawiciel ten musi mieć siedzibę w dowolnym państwie członkowskim oraz być umocowany do kierowania do niego przez organy nadzorcze i podmioty danych wszystkich spraw związanych z przetwarzaniem danych. Na gruncie dyrektywy 95/46 także istniał obowiązek wyznaczania przedstawiciela (zob. art. 4 ust. 2), ale z uwagi na odmienny zakres przedmiotowy aktu miał on zastosowanie tylko wobec przedsiębiorców posiadających siedzibę w państwie trzecim, którzy prowadzili czynności przetwarzania danych z wykorzystaniem środków technicznych znajdujących się na terenie UE
dlatego wprowadzony w ogólnym rozporządzeniu obowiązek wskazania przedstawiciela w związku z przetwarzaniem danych osobowych mieszkańców UE (także gdy czynności przetwarzania są realizowane poza obszarem Unii) prowadzi do znacznego rozszerzenia kręgu podmiotów zobowiązanych. Obowiązek ten dotyczy wszystkich przedsiębiorców, za wyjątkiem tych, którzy przetwarzają dane sporadycznie, oraz zagranicznych organów i podmiotów publicznych.

W ostatecznej treści przepisu nie uwzględniono możliwości zastosowania wyjątku od obowiązku ustanowienia przedstawiciela dla przedsiębiorców zatrudniających mniej niż 250 osób (projekt KE
dla przedsiębiorców zatrudniających mniej niż 250 osób (projekt KE
dla przedsiębiorców zatrudniających mniej niż 250 osób (projekt KE446), a także administratorów przetwarzających dane osobowe mniej niż 5.000 osób (projekt PE447).

4.5. Obszary regulacji

4.5.1. Podstawowe zasady przetwarzania

Prawodawca unijny, przyjmując dyrektywę 95/46, określił ogólne zasady legalności przetwarzania danych w trzech sekcjach, zawierających przepisy związane z zasadami

---

445 Także na gruncie krajowym obowiązek wyznaczania przedstawiciela wynikający z art. 31a uodo (implementacja art. 4 ust. 2 dyrektywy 95/46) interpretowano jako obejmujący wyłącznie przedsiębiorców zagranicznych, którzy prowadzą czynności przetwarzania za pomocą środków zlokalizowanych na obszarze RP. Zob. P. Barta, Komentarz do art. 31a, Nb 1, [w:] P. Barta, P. Litwiński, Ustawa o ochronie danych osobowych, CH Beck 2016.
446 Zob. brzmienie art. 25 ust. 2 pkt b w projekcie KE z 25.01.2012 ogólnego rozporządzenia, CELEX: 52012PC0011.
dotyczącymi jakości danych, kryteriami legalności przetwarzania oraz zasadami przetwarzania danych szczególnych kategorii. Odwołanie się do dorobku prawnego Rady Europy (Konwencja 108) oraz wytycznych OECD spowodowało, że dyrektywę należy rozpatrywać w kategoriach ewolucji wynikającego z tych aktów modelu ochrony danych osobowych.

Wśród podstawowych zasad przetwarzania danych wymieniono zasady:

- legalności i rzetelności (art. 6 ust 1 pkt a),
- określenia celu (art. 6 ust 1 pkt b),
- jakości danych (art. 6 ust 1 pkt d-e),
- proporcjonalności (art. 6 ust 1 pkt c).

Pierwsze trzy były zdefiniowane na gruncie wcześniej opublikowanych aktów prawnomiedzynarodowych (w szczególności art. 6 Konwencji 108), przy czym ich znaczenie może być szersze i mogą prowadzić do nałożenia dodatkowych obowiązków na administratorów danych. Dla przykładu: zgodnie z Konwencją 108 przetwarzane dane powinny być dokładne i w razie potrzeby aktualizowane. W dyrektywie rozbudowano tę regułę, wskazując dodatkowo, że należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane. Wyłącznie zasada proporcjonalności, zgodnie z którą postuluje się, aby zakres gromadzonych danych był prawidłowy, adekwatny i nienadmierny w stosunku do celu przetwarzania, nie została wcześniej zdefiniowana na gruncie przepisów Konwencji 108.

Wprowadzone w dyrektywie kryterium legalności przetwarzania danych opierało się na przyjęciu domyślnego zakazu przetwarzania danych uzupełnionego o zamknięty katalog możliwych do zastosowania wyjątków. Odmienne niż w przypadku zasad przetwarzania, kryterium nie bazowało na rozwiązaniach przyjętych w Konwencji 108 RE, ponieważ traktat ten nie regulował szczegółowo przesłanek uzasadniających przetwarzanie danych osobowych, ograniczając się w tym zakresie do wskazania, że zbieranie i gromadzenie danych ma się odbywać „zgodnie z prawem”448.

448 W pierwszym projekcie dyrektywy z 1990 r. (zob. Komunikat Komisji Europejskiej z 13 września 1990…, CELEX: 51990DC0314), Komisja Europejska zaproponowała, aby oddzielnie uregulować kwestię legalności przetwarzania w odniesieniu do podmiotów publicznych (art. 5 projektu) oraz prywatnych (art. 8 projektu). Podstawowym warunkiem uzasadniającym legalność przetwarzania przez podmioty publiczne miała być konieczność gromadzenia danych dla wykonania zadań administracji publicznej, natomiast w przypadku podmiotów prywatnych – zgoda podmiotu danych.
W ostatecznej, obowiązującej wersji dyrektywy zdecydowano się na wprowadzenie jednego zestawu warunków uzasadniających przetwarzanie danych osobowych (art. 7) – były nimi:

- wyrażenie zgody przez podmiot danych,
- przetwarzanie danych w celu zawarcia lub realizacji umowy z podmiotem danych,
- przetwarzanie danych dla wykonania zobowiązania prawnego,
- przetwarzanie danych w celu ochrony żywotnych interesów podmiotów danych,
- przetwarzanie danych w celu realizacji zadania wykonywanego w interesie publicznym,
- przetwarzanie danych dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej – za wyjątkiem sytuacji, w której interesy te będą kolidowały z podstawowymi prawami i wolnościami podmiotu danych.

Prawodawca zdecydował się na dopuszczenie tylko dwóch sytuacji, w których dane mogły być przetwarzane niezależnie od interesu podmiotu danych: w przypadku wykonania zobowiązania prawnego nałożonego na administratora lub w przypadku realizacji zadania wykonywanego w interesie publicznym. W pozostałych przypadkach administrator danych musiał uzyskać zgodę podmiotu danych lub musiał wykazać, że działał w interesie podmiotu danych. Natomiast w zakresie ostatniej przesłanki, dotyczącej istnienia uzasadnionego interesu administratora danych lub osoby trzeciej, należy zauważyć, że mogła być ona zastosowana wyłącznie do podmiotów sektora prywatnego, bowiem dla organów publicznych prawną podstawę przetwarzania danych osobowych powinien określić ustawodawca. Jak ponadto wyjaśniła Grupa Robocza Art. 29, aby interes administratora danych uznać za uzasadniony, powinny być łącznie spełniać następujące przesłanki:

- legalności (zgodny z prawem UE i krajowym);

---

449 Por. także uzasadnienie do identycznie brzmiącego przepisu ogólnego rozporządzenia przedstawione w: Stanowisko Rady w pierwszym czytaniu w sprawie przyjęcia Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), CELEX: ST_5419_2016_REV_1, s. 15.
dostatecznie jasno sformułowany, aby umożliwić przeprowadzenie testu równowagi w odniesieniu do interesów i praw podstawowych osoby, której dane dotyczą (szczegółowy);

nieoparty na przypuszczeniach (rzeczywisty)

Zgodnie z ugruntowanym orzecznictwem Trybunału, chociaż dyrektywy są co do zasadzaki aktami kierowanymi do państw i wymagają transpozycji do krajowego systemu prawnego, to w przypadku, gdy wprowadzane przepisy są bezwarunkowe i dostatecznie precyzyjne, mogą zostać powołane przeciw każdemu niezgodnemu przepisowi krajowemu. Kryterium bezwarunkowości oznacza w tym przypadku, że badany przepis dyrektywy nie może zawierać marginesu uznania dla prawodawcy krajowego, a więc jego wdrożenie nie może wiązać się z podjęciem dalszych działań na gruncie prawa krajowego. W przypadku dwóch zasad prawodawca nadał kompetencje państwom członkowskim pozwalające na doprecyzowanie ich treści – dotyczy to zasady określonego celu (art. 6 ust. 1 pkt b) oraz jakości danych (art. 5 ust. 1 pkt e). Natomiast wszystkie z przesłanek wskazanych w art. 7 stwierdzają obowiązki bezwarunkowe. Na tej podstawie Trybunał w sprawie Rechnungshof uznał, że przepisy art. 6 ust. 1 lit. c) oraz art. 7 lit. c) i e) dyrektywy 95/46 podlegają bezpośrednimu stosowaniu.

Kryteria legalności przetwarzania danych osobowych, wprowadzone w art. 7 nie mają zastosowania do przetwarzania danych osobowych szczególnie wraźliwych. Przyjęty w art. 8 ust. 1 dyrektywy katalog definiujących zakres danych wraźliwych jest zbieżny ze wskazanym w art. 6 Konwencji 108 i obejmuje dane ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak i dane dotyczące zdrowia i życia seksualnego. Prawodawca wprowadził przy tym rozbudowany katalog odstępstw od zakazu (art. 8 ust. 2), w szczególności związanych z realizacją uzasadnionego interesu prawnego administratora danych (np. przetwarzanie danych w ramach stosunku pracy), ochrony żywotnych interesów podmiotu danych czy świadczenia usług medycznych. Zgodnie z art. 8 ust. 3, z uwagi na istotny interes publiczny państwa członkowskie mogą ponadto ustanowić dodatkowe wyłączenia pod warunkiem wprowadzenia ich na mocy ustawy krajowej lub decyzji organu nadzorczego. W takim przypadku konieczne jest jednak notyfikowanie odpowiednich przepisów Komisji.

450 Grupa Robocza Art. 29, Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, WP 217, s. 28.
451 Wyrok TSUE z 19.01.1982 w sprawie Becker, sygn. 8/81, p. 25.
452 Wyrok TSUE z 20.05.2003 w sprawie Rechnungshof, sygn. C-465/00, p. 95-101.
Ograniczenie (limitacja) w stosowaniu praw i wolności wynikające z art. 6-8 dyrektywy może co do zasady zostać wprowadzone przez państwa członkowskie tylko w dwóch przypadkach. Po pierwsze, zgodnie z art. 9 dyrektywy w zakresie potrzebnym dla ochrony wolności wypowiedzi państwa członkowskie mogą wyłączyć lub odstąpić od przepisów art. 6-8, ale wyłącznie w celach dziennikarskich lub w celu uzyskania wyrauzu artystycznego lub literackiego i to jedynie wówczas, gdy jest to konieczne dla pogodzenia prawa do zachowania prywatności z przepisami dotyczącymi wolności wypowiedzi. Z kolei zgodnie z art. 13 ust. 1 państwa członkowie mogą przyjąć ograniczenia zakresu praw i obowiązków, wynikających między innymi z art. 6 ust. 1 (zasady dotyczące przetwarzania), gdy środek taki byłby konieczny dla zabezpieczenia najważniejszych funkcji państwa, w szczególności bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, ochrony podmiotów danych.

W żadnym przypadku przepisy dyrektywy 95/46 nie zezwalają na odstępnie od kryteriów legalności przetwarzania danych czy zastosowania dodatkowego wyłączenia od zakazu przetwarzania danych wrażliwych wyłącznie z uwagi na interes związany z ochroną bezpieczeństwa publicznego. W tym miejscu konieczne jest przywołanie wcześniejszych rozważań dotyczących zakresu stosowania prawa UE do obszaru bezpieczeństwa narodowego, związanych z zakresem stosowania dyrektywy oraz znaczeniem Karty Praw Podstawowych w krajowych porządkach prawnych.

Regulacje dotyczące podstawowych zasad przetwarzania danych osobowych wprowadzone w RODO stanowią ewolucję i rozwinięcie przepisów dyrektywy 95/46. Do znanych wcześniej zasad dodano zobowiązanie administratora do przetwarzania danych w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Chociaż zasada ta nie została wprost zdefiniowana w dyrektywie 95/46, zobowiązanie administratora danych do stosowania odpowiednich środków technicznych wynikało z przepisu art. 17 ust. 1 dyrektywy, określającego obowiązki w zakresie bezpieczeństwa przetwarzania danych. W porównaniu z dyrektywą, rozporządzenie rozszerza jednak obowiązki związane ze stosowaniem istniejących wcześniej zasad. Nowością jest także wprowadzona w art. 5 ust. 2 rozporządzenia zasada rozliczalności, zgodnie z którą administrator musi wykazać przestrzeganie podstawowych zasad przetwarzania danych, co w

453 Szersze informacje na temat zakresu wyłączenia związanego z obszarem bezpieczeństwa narodowego przedstawiono przy omówieniu zakresu stosowania dyrektywy 95/46 (s. 135) oraz rozporządzenia 2016/679 (s. 141).
454 Zob. rozdział 2.4.5, s. 82 i nast.
praktyce zwalnia podmiot danych lub organ nadzoru z ciężaru przeprowadzenia dowodu w tym zakresie.

W zakresie podstawowych kryteriów legalności utrzymano model, w którym przetwarzanie danych jest możliwe tylko po spełnieniu jednego z enumeratywnie wymienionych warunków. Ich lista – określona w art. 6 ust. 1 rozporządzenia – nie zmieniła się w porównaniu z dyrektywą, chociaż z uwagi na nową formę aktu prawnego skutkującą brakiem konieczności implementacji do porządku krajowego, poszczególne kryteria zostały doprecyzowane i szerzej omówione. I tak w przypadku gdy przetwarzanie jest konieczne dla wykonania zobowiązania prawnego lub realizacji zadania uzasadnionego interesem publicznym, dodano wymaganie (art. 6 ust. 3), aby podstawa przetwarzania była określona w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator. Ponadto musi ona uwzględniać zasadę proporcjonalności zakresu przetwarzania do wyznaczonego, prawnie uzasadnionego celu.

Biorąc pod uwagę, że w praktyce stosowania przepisów dyrektywy 95/46 najczęstszą podstawą przetwarzania danych była zgoda podmiotu danych, prawodawca unijny zdecydował się doprecyzować warunki uzyskiwania takiej zgody oraz kryteria uznania jej ważności. Problemy na tym tle były dyskutowane zwłaszcza w zakresie usług internetowych oraz marketingu bezpośredniego, gdzie użytkownikom często przedstawiano nieczytelne i niezrozumiałe klauzule, których elementem było wyrażenie zgody na przetwarzanie danych osobowych455. Dlatego zgodnie z art. 7 wymaga się, aby zgoda udzielona przez podmiot danych łącznie spełniała wszystkie poniższe warunki:

- została udzielona wprost, przez co należy rozumieć, że w przypadku jednoczesnego pytania o inne kwestie, zapytanie o zgodę musi być wyraźnie oddzielone oraz być przedstawione w zrozumiałyj i łatwo dostępiej formie, jasnym i prostym językiem,
- była dobrowolna, przez co należy rozumieć, aby od jej udzielenia nie warunkowało wykonania umowy, jeżeli przetwarzanie danych nie jest konieczne dla jej wykonania,
- umożliwiała wycofanie zgody w sposób jak najmniej uciążliwy, w sposób równie łatwy jak jej wyrażenie.

455 Szerzej na temat klauzul stosowanych w usługach marketingu bezpośredniego w: M. Kaczorowski, Przetwarzanie danych osobowych w działaniach marketingowych prowadzonych on-line, Monitor Prawniczy 2014, nr 9, dodatek s. 34-38; K. Reszczyn-Król, Prawne granice przetwarzania danych osobowych do celów marketingu bezpośredniego bez zgody podmiotu danych – perspektywa prawa polskiego i niemieckiego w świetle Ogólnego rozporządzenia o ochronie danych, Monitor Prawniczy 2017, nr 19, s. 1023-1031.
Podobnie, jak w przypadku spełniania podstawowych zasad przetwarzania także i w zakresie potwierdzenia faktu wyrażenia zgody ciężar dowodu spoczywa na administratorze danych. Biorąc pod uwagę coraz częstsze problemy związane z ochroną prywatności osób niepełnoletnich – związane między innymi z nieodpowiednim użyciem przez nich nowoczesnych środków komunikacji takich, jak media społecznościowe, prawodawca unijny doprecyzował w art. 8 ust. 1, że w przypadku dzieci poniżej 16. roku życia zgodę musi wyrazić lub potwierdzić prawny opiekun. W tym zakresie przepisy rozporządzenia pozostawiają swobodę prawodawcy krajowemu w obniżeniu granicy wieku – ale do poziomu nie niższego niż 13 lat.

W obszarze przetwarzania danych szczególnie wrażliwych przepisy rozporządzenia w większości powielają rozwiązania wprowadzone w dyrektywie 95/46. Zakres definicji danych wrażliwych, wprowadzony w art. 9 ust. 1 rozporządzenia, jest tożsamy ze wskazanym w art. 8 ust. 1 dyrektywy. Także katalog dopuszczalnych sytuacji, w których przetwarzania danych wrażliwych jest możliwe jest zbliżny z rozwiązaniami stosowanymi w dyrektywie. Prawodawca zdecydował się jednak na wprowadzenie kilku zmian, skutkujących dalszym ograniczeniem możliwości legalnego przetwarzania danych wrażliwych. Przykładem może być doprecyzowanie, że przetwarzanie danych wrażliwych podanych do wiadomości publicznej jest dopuszczalne tylko wtedy, gdy „w sposób oczywisty” zostały one upublicznione przez podmiot danych. Prawodawca unijny przewidział też w art. 9 ust. 4 możliwość wprowadzenia przez przepisy krajowe dalszych warunków, jakim musi podlegać przetwarzanie danych genetycznych, biometrycznych lub dotyczących stanu zdrowia.

Bliższego omówienia wymaga redakcja przepisu art. 9 ust. 2 pkt a, w którym wskazano, że podstawą przetwarzania może być tylko wyraźna zgoda podmiotu danych. Prawodawca rozróżnił zatem zwykłą zgodę (art. 6 ust. 1 pkt a), stanowiącą podstawę do przetwarzania danych, od zgody wyraźnej, koniecznej, aby administrator mógł przetwarzać dane wrażliwe. Podobne rozróżnienie było stosowane także na gruncie dyrektywy 95/46. W przypadku rozporządzenia, w art. 4 pkt 11 rozszerzono jednak definicję „zgody”, zgodnie z którą jest nim każde dobrowolne, konkretne, świadomie i jednoznaczne okazanie woli podmiotu danych, wyrażone w formie oświadczenia lub wyraźnego działania potwierdzającego. Powstaje zatem wątpliwość, czy termin „wyraźna zgoda” użyty w art. 9 ust. 2 pkt a (przetwarzanie danych wrażliwych) powinien być utożsamiany z „wyraźnym działaniem” wskazanym w art. 4, a w efekcie prowadzić do wyłączenia możliwości złożenia
przez podmiot danych oświadczenie jako formy wystarczającej do wyrażenia zgody na przetwarzanie danych wrażliwych. Wniosek taki należy uznać za będnyn°

Uwzględniając dynamiczny rozwój usług internetowych oraz fakt, że coraz częściej użytkownicy przekazują dostawcom e-usług swoje dane wrażliwe (np. dane dotyczące stanu zdrowia), wprowadzenie do rozporządzenia wymagania zachowania formy pisemnej dla zgody podmiotu danych mogłoby doprowadzić do zbyt dużego formalizmu i utrudnić zamiast ułatwić świadczenie usług i harmonizację rynku wewnętrznego. Na gruncie polskich przepisów cywilistycznych zachowanie formy pisemnej wymaga złożenia własnoręcznego podpisu na dokumencie obejmującym treść oświadczenia woli. Jest to oczywiście wymaganie trudne w realizacji w przypadku usług świadczonych elektronicznie. W takim przypadku bardziej adekwatną formą wydaje się forma elektroniczna, która z kolei jest rzadko stosowana z uwagi na konieczność użycia kwalifikowanego podpisu elektronicznego. Kompromisem pomiędzy pewnością, że podmiot danych wyraził świadomą zgodę (forma pisemna), oraz ułatwieniem świadczenia usług elektronicznych może być zastosowanie na gruncie krajowym formy dokumentowej – polegającej na wymianie oświadczeń woli trwale zapisanych na nośniku danych (a więc np. za pośrednictwem załączników do wiadomości e-mail).

Biorąc pod uwagę redakcję art. 9 ust. 2 pkt a – w której nie przewidziano możliwości doprecyzowania formy wyrażenia oświadczenia woli przez podmiot danych na gruncie prawa krajowego – sposób interpretacji „wyraźnej zgody” stanie się prawdopodobnie przedmiotem dalszych analiz i wyjaśnień instytucji unijnych (w szczególności Europejskiego Inspektora Ochrony Danych), a w dalszej kolejności być może także Trybunału Sprawiedliwości UE.

456 Przepisy rozporządzenia dotyczące legalnych podstaw przetwarzania danych wrażliwych bazują na rozwiązaniach wprowadzonych w dyrektywie 95/46. W pierwszym projekcie dyrektywy przygotowanym w 1990 roku Komisja Europejska wskazała zgodę podmiotu danych jako jedyną możliwość odstępstwa od zasady zakazu przetwarzania danych wrażliwych. Zgoda ta musiała być jednak „dobrowolna i wyrażona w formie pisemnej” (Komunikat Komisji Europejskiej z 13 września 1990..., s. 62). W zaktualizowanym w 1992 roku projekcie KE rozszerzyła katalog sytuacji uzasadniających przetwarzanie danych wrażliwych, pozostawiając jednak w art. 8 ust. 2 pkt a projektu wymaganie, aby uzyskana od podmiotu danych zgoda miała formę pisemną (Zmieniony projekt dyrektywy..., COM (1992) 42, s. 18). Dopiero we wspólnym stanowisku Rady dotyczącym przedstawionego projektu wymóg pisemnej zgody zastąpiono terminem wyraźnej zgody (por. treść art. 8 ust. 2 pkt a we wspólnym stanowisku w sprawie projektu dyrektywy przekazanym z dn. 20.02.1995, Dz. Urz. WE z 1995 Nr C 93 s. 1). Jak zauważa się w piśmiennictwie, przyczyny tej decyzji nie zostały wystarczająco wyjaśnione (zob. np. Opinia WP29 15/2011 w sprawie definicji zgody, WP 187, s. 5.). W polskich przepisach implementujących dyrektywę (art. 27 ust. 2 pkt 1 udo) prawodawca pozostawił przy wymaganiu formy pisemnej i wydaje się, że taka interpretacja wyraźnej zgody jest najbardziej zbliżona do zamierzeń prawodawcy. Z kolei Grupa Robocza Art. 29 w swojej opinii dotyczącej definicji zgody na gruncie przepisów europejskich wskazuje, że pojęcie „wyraźnej zgody” obejmuje obok formy pisemnej także aktywną reakcję ustnią podmiotu danych, za pośrednictwem której osoba fizyczna wyraża swoją wolę, aby jej dane były przetwarzane w określonych celach (Opinia 15/2011...., s. 30).
4.5.2. Prawa podmiotów danych

Kwestia określenia zakresu praw przysługujących podmiotom danych w związku z przetwarzaniem ich danych osobowych była historycznie jedną z pierwszych przesłanek uzasadniających potrzebę wprowadzenia regulacji prawnych w tym obszarze. Już we wczesnych rezolucjach Parlamentu Europejskiego, wskazujących na zasadność opracowania europejskich ram ochrony danych, wskazywano na podstawowe prawa, jakie powinny przysługiwać osobom, których dane są przetwarzane – w szczególności prawo do informacji, prawo dostępu, poprawiania i żądania usuwania danych, prawo do kontroli przez upoważniony organ nadzoru legalności operacji przetwarzania przez administratora⁴⁵⁷. Postulaty te zostały uwzględnione w projekcie dyrektywy, a w wersji zatwierdzonej przybrały formę czterech najważniejszych praw:

- prawa do informacji (art. 10) – przez które należy rozumieć możliwość żądania przez podmiot danych podstawowych informacji o administratorze danych oraz celu, a także sposobie przetwarzania danych,

- prawa dostępu do danych (art. 12) – rozumiane nie tylko jako pozwalające uzyskać w odpowiednim dostępie czasu oraz bez nadmiernego opóźnienia i kosztów potwierdzenia, czy dane są przetwarzane, ale również prawo żądania sprostowania, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z przepisami dyrektywy,

- prawo sprzeciwu (art. 14) – prowadzące do uniemówliewania realizacji czynności przetwarzania co najmniej w przypadku, gdy ich podstawą formalną jest realizacja zadania wykonywanego w interesie publicznym (art. 7 pkt e) lub uzasadniony interes administratora danych art. 7 pkt f); prawo sprzeciwu obejmuje także sytuacje przetwarzania danych dla potrzeb bezpośredniego obrotu, jak i prawo do bycia poinformowanym przed ujawnieniem danych po raz pierwszy osobom trzecim.

- prawo nieobjęcia decyzją zautomatyzowaną (art. 15) – związane z możliwością zastrzeżenia przez osobę fizyczną żądania nieobjęcia jej skutkami decyzji, która jest oparta wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych aspektów o charakterze osobistym, takich jak np. wyniki osiągane w pracy, zdolność kredytowa, wiarygodność, sposób zachowania itp.

⁴⁵⁷ Rezolucja PE z dn. 8 maja 1979…, Dz.U. WE z 1979 Nr C 140, s. 37.
Wszystkie opisane powyżej przepisy były kierowane do tego samego kręgu podmiotów zobowiązanych (administratorzy danych) oraz podmiotów uprawnionych (osoby, których dane są przetwarzane).

Prawodawca przewidział w art. 13 ust. 1 dyrektywy 95/46 możliwość ograniczenia zakresu praw i obowiązków związanych z prawem do informacji oraz prawem dostępu do danych, jeżeli środki takie okażą się konieczne dla zabezpieczenia celów interesu ogólnego, między innymi bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, ważnego interesu ekonomicznego lub finansowego państwa członkowskiego, jak i funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych z wykonywaniem władzy publicznej. Jak zauważył TSUE, każde odstępstwo wprowadzone na podstawie art. 13 ust. 1 wymaga poszanowania zasady proporcjonalności do zamierzonego celu, jakim jest interes ogólny.

Blędna jest zatem interpretacja omawianego wyłączenia w taki sposób, że może stanowić on podstawę do wprowadzenia krajowych środków ustawodawczych prowadzących do ingerencji w prawo do prywatności w sposób sprzeczny z art. 8 EKPC. Z uwagi na ogólność przepisów wprowadzających prawa podmiotów danych obszar ten stał się przyczyną niejasności interpretacyjnych, a co za tym idzie dyskusji w doktrynie oraz przedmiotem analizy judykatury. Także rozwój środków przetwarzania informacji, w szczególności usług świadczonych w sieci Internet, spowodował, że możliwość realizacji praw wskazanych w dyrektywie 95/46 była ograniczona, a ich praktyczna skuteczność w zakresie umożliwienia podmiotom danych kontroliowania informacji ich dotyczących nie zawsze wystarczająca. Wnioski płynące z tych doświadczeń stały się podstawą dla Komisji do znacznego rozbudowania przepisów projektowanego rozporządzenia właśnie w obszarze praw podmiotów danych. Zaproponowane, a następnie wprowadzone zmiany można podzielić na trzy kategorie:

- doprecyzowanie i rozbudowanie istniejących praw (zdefiniowanych w dyrektywie 95/46);
- wyróżnienie w formie oddzielnych przepisów praw, które zaleźnie od przyjętej interpretacji były wcześniej elementem innych praw przewidzianych w dyrektywie 95/46 lub stanowią nowe gwarancje (np. prawo do usunięcia danych, powszechnie nazywane w literaturze przedmiotu prawem do bycia zapomnianym);
- wprowadzenia nowych praw, nieujętych wcześniej w dyrektywie 95/46 (np. prawo do ograniczenia przetwarzania, prawo do przenoszenia danych).

Wyrok TSUE w sprawie Rechnungshof, sygn. C-465/00, p. 91.
Do pierwszej grupy należą prawa, które zdefiniowano w przepisach dyrektywy 95/46, natomiast w rozporządzeniu zostały rozbudowane i doprecyzowane. Przykładem może być prawo do informacji, w redakcji którego podkreślono, że celem wprowadzenia jest zachowanie zwięzłej, przejrzystej i łatwo dostępnej formy udzielanych informacji, przy jednoczesnym zachowaniu prostego i jasnego języka (art. 12 ust. 1). Prawodawca ponadto doprecyzował, że administrator danych jest zobowiązany do wykonania obowiązków informacyjnych względem podmiotu danych w terminie nie dłuższym niż 30 dni od daty otrzymania żądania.

Praktyczna trudność w realizacji praw podmiotów danych na gruncie przepisów dyrektywy 95/46 była związana z możliwością potwierdzenia przez administratora tożsamości osoby, składającej określone żądanie – zwłaszcza w przypadku stosowania elektronicznych środków komunikacji. Dlatego w rozporządzeniu doprecyzowano, że administrator danych ma prawo uwarunkować realizację żądania od otrzymania dodatkowych informacji niezbędnych do potwierdzenia tożsamości (art. 12 ust. 6). Natomiast w przypadku udzielenia informacji ustnie, administrator ma obowiązek potwierdzenia tożsamości osoby za pośrednictwem dodatkowych środków komunikacji.

Prawodawca znacznie rozszerzył także obowiązki informacyjne, które administratorzy muszą dochować w trakcie gromadzenia danych. Obok tożsamości administratora danych oraz wskazania celów przetwarzania konieczne jest między innymi ujawnienie zamiaru przekazania danych do państwa trzeciego wraz z informacją, czy Komisja wydawała decyzję o adekwatności zabezpieczeń stosowanych w prawodawstwie tego państwa. Ponadto administrator zobowiązany jest do przekazania informacji związanych z planowanym okresem przetwarzania lub – gdy jest to niemożliwe – kryteriami ustalenia tego okresu, oraz informacji o prawie wniesienia skargi do organu nadzorczego, wskazaniu, czy podanie danych jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy, jak i ewentualnych konsekwencji związanych z niepodaniem danych.

W rezultacie, zgodnie z reżimem przepisów rozporządzenia, powierzając swoje dane osobowe, osoby fizyczne dysponują bez porównania bardziej rozbudowaną i kompletną informacją na temat podstawy, celu, odbiorców i środków użytych do przetwarzania informacji. Są też poinformowane o podmiotach przetwarzających ich dane (również znajdujących się poza obszarem UE) oraz przysługujących im środków ochrony prawnej.

Jedną z częściej omawianych i dyskutowanych zmian związanych z reformą unijnych przepisów o ochronie danych osobowych jest wprowadzenie nowego prawa podmiotu danych – powszechnie znanego w literaturze jako „prawo do bycia zapomnianym”. Podstawę do
konstrukcji nowych przepisów stanowił wyrok TSUE w sprawie *Google Spain SL*, w którym Trybunał stwierdził, że obowiązujące przepisy dyrektywy 95/46 oraz Karty Praw Podstawowych są wystarczające do uznania zasadności żądania przez podmiot danych usunięcia konkretnej informacji z indeksu wyszukiwarki internetowej w sposób, który uniemożliwia prezentowanie tej informacji użytkownikom w odpowiedzi za zapytanie, którego podstawą jest imię i nazwisko tej osoby\(^{459}\). Trybunał dokonał w tym względzie wykładni przepisu art. 12 lit. b (prawo żądania usunięcia lub zablokowania usunięcia danych, których przetwarzanie jest niezgodne z przepisami) oraz art. 14 lit a (prawo sprzeciwu co do dalszego przetwarzania informacji z ważnych i uzasadnionych przyczyn) dyrektywy 95/46 i na ich podstawie wywnioskował, że prawo podmiotu danych do kontrolowania informacji udostępnianych na swój temat obejmuje także prawo do wycofania tych informacji z domeny publicznej. Możliwość skorzystania z tego uprawnienia nie może być przy tym warunkowana wystąpieniem szkody czy ochroną dobrego imienia (np. publikacją informacji nieprawdziwych)\(^{460}\). Trybunał zauważył też, że prawo to jest nadrzędne nie tylko wobec interesu gospodarczego operatora wyszukiwarki internetowej, lecz również wobec interesu, jaki odbiorcy mogą mieć w znalezieniu rzeczonej informacji w ramach wyszukiwania prowadzonego w przedmiocie imienia i nazwiska tej osoby\(^{461}\).

Tezy wyroku w sprawie *Google Spain* spotkały się w większości z akceptacją w doktrynie, przy czym nie brakowało także głosów krytycznych wskazujących na problemy techniczne związane z jego praktyczną realizacją\(^{462}\). Podkreślano także brak mechanizmów zapewniających ochronę prawa do usunięcia danych w przypadku operatorów wyszukiwarek i serwisów internetowych zlokalizowanych poza terenem UE oraz brak wskazań co do tego, w jaki sposób podmiot danych może wykonywać swoje prawa w przypadku, gdy administrator przestał istnieć, zniknął lub nie można go zidentyfikować albo nawiązać z nim kontaktu\(^{463}\). Wskazywano także na ryzyko związane z możliwością wprowadzenia mechanizmów zbyt daleko ingerujących w swobodę wypowiedzi, które w skrajnych przypadkach doprowadzić mogą do cenzury treści publikowanych w Internecie\(^{464}\).

W toku prac legislacyjnych nad reformą przepisów o ochronie danych tezy wyroku *Google Spain* wpłynęły na ostateczny zakres przepisu art. 17 rozporządzenia 2016/679,

\(^{459}\) Wyrok TSUE z 13.05.2014 w sprawie *Google Spain SL*, sygn. C-131/12, p. 99.  
\(^{460}\) Ibidem, p. 96.  
\(^{461}\) Ibidem, p. 100/4.  
\(^{462}\) M. Rojszczak, *Analiza i praktyczne uwagi...*, op. cit., s. 34-37.  
\(^{463}\) Grupa Robocza Art. 29, Opinia 01/2014 w sprawie stosowania pojęć konieczności i proporcjonalności oraz ochrony danych w sektorze egzekwowania prawa, WP 211, s. 14.  
\(^{464}\) O. Solon, *EU 'right to be forgotten' ruling paves way for censorship*, www.wired.co.uk/article/right-to-be-forgotten-blog
definiującego prawo do usunięcia danych. Orzeczenie TSUE dotyczyło bezpośrednio wyłącznie operatorów wyszukiwarek internetowych, zatem zakres stosowania prawa do bycia zapomnianym był ograniczony do wąskiego kręgu podmiotów zobowiązanych. Przyjęta redakcja przepisu art. 17 ust. 1 rozszerza zakres podmiotowy na wszystkich administratorów oraz wskazuje, że żądanie do usunięcia danych powinno być wykonane bez zbędnej zwłoki między innymi w przypadkach, gdy dane takie nie są już potrzebne do celów, dla jakich zostały zgromadzone lub podmiot danych cofnął zgodę lub zgłosił sprzeciw co do dalszego ich przetwarzania. Prawodawca doprecyzował także dwie praktyczne kwestie, wskazywane w piśmiennictwie jako trudności związane z realizacją prawa do bycia zapomnianym.465

Pierwszą jest uregulowana w art. 17 ust. 2 kwestia obowiązku informowania przez administratora danych innych wydawców treści, że osoba, której dane są przetwarzane, zgłosiła żądanie ich usunięcia, co powinno skutkować wtórnym usunięciem wszystkich łącz (odnośników internetowych) do tych danych. Obowiązek nałożony na administratorów jest przy tym ograniczony dostępną technologią i względami kosztów realizacji, co należy pozytywnie ocenić, zwłaszcza biorąc pod uwagę trudności w realizacji obowiązku informacyjnego w odniesieniu do dostawców treści zlokalizowanych w państwach trzecich. Drugim zagadnieniem problemowym była natomiast kwestia wskazania katalogu wyłączeń niepodlegających realizacji prawa do bycia zapomnianym. W szczególności prawodawca określił w art. 17 ust 3, że prawo do usunięcia danych nie może być zastosowane w zakresie, w jakim przetwarzanie jest niezbędne do korzystania ze swobód związanych z wolnością wypowiedzi i dostępu do informacji, do celów archiwalnych w interesie publicznym, badań naukowych lub historycznych, jak i do ustalenia, dochodzenia lub obrony roszczeń. Należy pamiętać, że katalog ten ma strukturę zamkniętą, a co za tym idzie – każde z wyłączeń powinno być traktowane w sposób wąski. Z uwagi na brak orzecznictwa TSUE na tle stosowania art. 3 w chwili obecnej nie można określić, czy przyjęta redakcja przepisu będzie wystarczająca, aby uniknąć ryzyka wykorzystania przepisów do faktycznego ograniczenia prawa dostępu do informacji czy wprowadzenia wybiorczej kontroli (cenzury) prezentowanych treści.

W wyniku uwag zgłoszonych przez PE w trakcie prac legislacyjnych z projektu rozporządzenia usunięto sformułowanie wskazujące na szczególną przesłankę stosowania prawa do usunięcia danych „w odniesieniu do danych osobowych, które zostały udostępnione

przez podmiot danych, kiedy był on dzieckiem”\textsuperscript{466}. Zamiast tego wprowadzono przepis art. 17 ust. 1 pkt f, stanowiący samodzielną przesłankę do żądania usunięcia danych w sytuacji, gdy żądająca osoba opublikowała kwestionowane treści w okresie, gdy była jeszcze dzieckiem.

Kwestia ochrony informacji obejmujących sferę prywatności osób wstępujących w dorosłość, a wprowadzonych do domeny publicznej wcześniej przez osoby im bliskie (np. rodziców, opiekunów prawnych) staje się coraz częściej przedmiotem wyroków sądowych. Pierwsze sprawy tego typu są rozpatrywane na poziomie sądów krajowych poszczególnych państw członkowskich. W roku 2016 media informowały\textsuperscript{467} o sprawie pozwu skierowanego w Austrii przeciwko rodzicom przez ich już pełnoletnią córkę o ochronę dóbr osobistych w związku z publikacją w domenie publicznej kilkuset zdjęć z jej dzieciństwa. Z kolei w prawomocnie rozstrzygniętej w marcu 2017 roku sprawie, Sąd Okręgowy Warszawa-Praga skazał ojca 2-letniego dziecka na 3 miesiące ograniczenia wolności, uznając go winnym popełnienia przestępstwa z art. 191a §1 kk, polegającego na publikacji w portalu Facebook nagich zdjęć chłopca\textsuperscript{468}. Dlatego należy pozytywnie ocenić możliwość zastosowania trybu wynikającego z art. 17 rozporządzenia (prawo do usunięcia danych) w odniesieniu do treści publikowanych przez dzieci.

Do ostatniej grupy praw jednostek, które zostały zdefiniowane w RODO, należą nowe prawa, po raz pierwszy wprowadzone do europejskich przepisów o ochronie danych osobowych. Do tej grupy zaliczyć należy prawa do ograniczenia przetwarzania danych (art. 18) oraz do przenoszenia danych (art. 20). Prawo do ograniczenia przetwarzania danych w istocie prowadzi do zawężenia możliwości użycia danych przez administratora do konkretnych, enumeratywnie wskazanych przypadków. Jego źródłem można szukać w art. 12 ust b dyrektywy 95/46, w którym wskazano na możliwość „zablokowania danych” jako jedno z uprawnień podmiotu danych. Jest środkiem przejściowym pomiędzy przetwarzaniem danych na zasadach ogólnych a ich usunięciem – i może być stosowane w szczególności w trakcie rozpatrywania zgłoszonego żądania sprstowania danych lub sprzeciwu co do ich dalszego przetwarzania. Ograniczenie przetwarzania powinno być także zastosowane, gdy dane nie są już potrzebne z uwagi na pierwotny cel przetwarzania, ale nadal muszą być wykorzystane np. z uwagi na dochodzenie lub egzekucję roszczeń. Pewną

\textsuperscript{466} Zob. treść poprawki 112 PE do projektu ogólnego rozporządzenia, A7-0402/2013.


niejasność interpretacyjną może budzić przyjęta redakcja art. 18 ust. 2, w którym wskazano
na możliwość dalszego (ograniczonego) przetwarzania danych, z wyjątkiem ich
przechowywania, wyłącznie za zgodną podmiotu danych. Wydaje się, że ustęp ten należy
interpretować w ten sposób, że przechowywanie danych (będące formą przetwarzania) nie
wymaga zgody podmiotu danych, natomiast ich przetwarzanie w inny sposób – zgody takiej
wymaga. Ograniczenie przetwarzania należy do nowych form przetwarzania, nieznanych
wcześniej w prawodawstwie polskim i unijnym, dlatego praktyczna ocena przydatności tego
mechanizmu dla zabezpieczenia praw jednostek nie jest w chwili obecnej możliwa. Brak
zakreślenia maksymalnego okresu, w jakim ograniczone przetwarzanie może być stosowane,
może okazać się istotną luką w regulacji. Jeżeli bowiem celem prawodawcy było
wprowadzenie oddzielnego reżimu przetwarzania dla danych, których dalsza potrzeba
przetwarzania została z przyczyn wskazanych w przepisie zakwestionowana, naturalne
powinno być zobowiązanie administratora do poczynienia niezbędnych ustaleń i
zakończenia przetwarzania we wskazanym, z góry zakreślonym, czasie.

Drugie z wprowadzonych w RODO uprawnień dotyczy możliwości przenoszenia
danych pomiędzy administratorami. Na mocy art. 20 ust. 1 osoba, której dane dotyczą,
ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie dane osobowe jej
dotyczące, które dostarczyła administratorowi. Z uwagi na brak wskazania konkretnych
standardów wymiany komunikatów uznać należy, że definicję „powszechnie używanego
formatu” będą spełniały w szczególności pliki XML lub inne powszechnie akceptowane
formaty wymiany informacji. Dane te będą mogły być następnie przekazane innemu
administratorowi lub przesłane bezpośrednio pomiędzy administratorami. W zamierzeniu
Komisji celem wprowadzenia nowego przepisu jest umożliwienie przenoszenia danych
pomiędzy systemami elektronicznego przetwarzania, bez możliwości uniemożliwienia tej
operacji ze strony administratora.\textsuperscript{469}

Jak podkreślono w wytycznych Grupy Roboczej Art. 29, skorzystanie z prawa do
przenoszenia danych przez użytkownika nie prowadzi do ograniczenia jego uprawnień
względem administratora danych – w szczególności nie oznacza usunięcia danych czy
zakończenia świadczenia usługi\textsuperscript{470}. Z drugiej strony, przekazanie danych nowemu
administratorowi nakłada na niego obowiązek przetwarzania ich tylko w zakresie związanym
z celem przetwarzania. Prawo do przenoszenia danych nie obejmuje wyłącznie informacji
osobowych, ale wszelkich zgromadzonych w związku z wykonaniem umowy z podmiotem

\textsuperscript{469} Zob. uzasadnienie KE do projektu ogólnego rozporządzenia o ochronie danych, CELEX: 52012PC0011, s. 8.
\textsuperscript{470} Grupa Robocza Art. 29, „Wytyczne w zakresie prawa do przenoszenia danych”, WP 242, s. 6.
danych. Jak wskazuje się w literaturze, przykładem zestawień objętych wskazaną regulacją jest np. lista zakupionych książek w księgarni internetowej czy ulubione utwory odsłuchiwane w usłudze mediów streamingowych.

Prawo do przenoszenia danych, chociaż w obecnej formie regulacji przybiera postać ogólną, powinno zostać uwzględnione przy projektowaniu nowych systemów informatycznych, zwłaszcza w obszarze administracji publicznej. W piśmiennictwie podkreśla się korzystny wpływ prawa do przenoszenia danych w promowaniu konkurencji pomiędzy dostawcami usług oraz zapobieganiu „zamknięcia” technologicznego, skutkującego trwałym związywaniem użytkownika do konkretnego usługodawcy z uwagi na brak możliwości migracji wytworzonych danych. Na gruncie krajowym zasadne wydaje się wskazanie na potrzebę nowelizacji rozporządzenia KRI w sposób uwzględniający potrzebę zaimplementowania funkcjonalności związanej z wymianą (w szczególności eksportem) informacji osobowych, ale także wskazaniem uniwersalnych i akceptowalnych formatów stosowanych w tym zakresie w administracji publicznej.

Ostatnim z praw podmiotu danych, które zostało wprowadzone w rozporządzeniu 2016/679, jest prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanych przetwarzaniu. Prawo to było zdefiniowane wcześniej w dyrektywie 95/46, jednak w rozporządzeniu jego zakresem objęto też czynności profilowania. Zgodnie z definicją przedstawioną w art. 4 lit 4 rozporządzenia profilowanie stanowi formę przetwarzania danych, które polega na ich wykorzystaniu do oceny niektórych czynników osobowych osoby fizycznej, takich jak analiza lub prognoza aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji czy przemieszczania się. Profilowanie jest zatem techniką służącą do wykorzystania zgromadzonych danych w celu tworzenia nowej zawartości informacyjnej, pozwalającej na prognozowanie cech lub przyszłych działań jednostki. W sposób oczywisty profilowanie może ingerować w prywatność osoby, stąd potrzeba objęcia tej formy przetwarzania przepisami o ochronie danych osobowych była zgłaszana w literaturze od lat. Z tego samego powodu niekontrolowane profilowanie jest wskazywane w

Ibidem, s. 7.

I. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, International Data Privacy Law 2013, nr 2, s. 80.

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 526 ze zm.).

piśmiennictwie jako jedno z największych współczesnych zagrożeń dla prywatności użytkowników Internetu⁴⁷⁵.

Zwraca uwagę fakt osłabienia wymagań regulacyjnych w zakresie czynności profilowania obowiązujących w wersji zatwierdzonej rozporządzenia względem rozwiązań proponowanych przez Komisję. W przyjętym przez Komisję projekcie postulowano zakaz możliwości stosowania środków profilowania użytkowników, za wyjątkiem trzech enumeratywnie wymienionych sytuacji – udzielenia zgody przez podmiot danych, potrzeby przetwarzania z uwagi na wykonanie zawieranej lub istniejącej umowy bądź istnienia wyraźnej podstawy prawnej. Parlament Europejski zaproponował osłabienie tego reżimu poprzez wskazanie, że co do zasady profilowanie jest dopuszczalne, ale osoba fizyczna ma prawo zgłosić sprzeciw wobec stosowania tej techniki. W ostatecznej wersji rozporządzenia przyjęto model, w którym realizacja czynności profilowania nie jest warunkowana udzieleniem zgody przez podmiot danych ani spełnienia innej koniecznej przesłanki, stanowiącej podstawę dla działania administratora. Prawodawca przyjął, że ochrona przed profilowaniem stanowi uprawnienie podmiotu danych, z którego może on skorzystać, ale nie wprowadził domyślnego zakazu w tym względzie, który wiąże administratora. W doktrynie zauważa się, że odpowiednikiem prawa do zgłoszenia sprzeciwu jest z perspektywy administratora obowiązek do powstrzymania się od działań, które to prawo by naruszały⁴⁷⁶.

Zgodnie z art. 13 ust. 2 lit f rozporządzenia administrator ma obowiązek w trakcie pozyskiwania danych osobowych przekazać informację między innymi o fakcie stosowania środków zautomatyzowanego podejmowania decyzji, w tym profilowania, istotne informacje o zasadach ich podejmowania, o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania względem osoby, której dane dotyczą. Wskazany przepis nie wymaga udzielenia przez podmiot danych wyraźnej zgody na same czynności profilowania, a dotyczy wyłącznie obowiązków informacyjnych administratora, które mogą być zrealizowane poprzez uwzględnienie w polityce prywatności czy innych, często rozbudowanych, dokumentach, które użytkownik akceptuje przed rozpoczęciem korzystania z usługi. Podmiot danych ma co do zasady możliwość wniesienia ex post sprzeciwu wobec przetwarzania w celu profilowania (art. 2 ust. 1).

Na gruncie przyjętej treści rozporządzenia uzasadnione wątpliwości może budzić ponadto możliwość i granice stosowania technik profilowania z wykorzystaniem danych

⁴⁷⁵ C. Castelluccia, A. Narayanan, Privacy considerations of online behavioural tracking, ENISA 2012, s. 3.
wrażliwych (art. 9 ust. 1), w szczególności w sposób prowadzący do nieuzasadnionej dyskryminacji ze względu na płeć, rasę, pochodzenie etniczne czy przynależność związkową. Potrzeba ściślejszej regulacji w tym zakresie była wskazywana w piśmiennictwie jeszcze na etapie prac legislacyjnych. W motywie 23 rozporządzenia wskazano, że dyskryminacja oparta na danych genetycznych powinna być co do zasady zakazana. Zgodnie z art. 22 ust. 4, wykorzystanie do profilowania danych wrażliwych jest możliwe tylko pod warunkiem uzyskania zgody podmiotu danych (art. 9 ust. 2 lit a) lub realizacji ważnego interesu publicznego (art. 9 ust. 2 lit g). Skoro przetwarzanie (profilowanie) danych wrażliwych jest w pewnych sytuacjach dopuszczalne, należy przeanalizować, jakie zabezpieczenia zostały zastosowane, aby te techniki nie mogły zostać wykorzystane do nieuprawnionej dyskryminacji. W nieuwzględnionej w dalszych pracach legislacyjnych poprawce 115 KE do projektu rozporządzenia postulowano uwzględnienie zakazu „profilowania, które skutkuje dyskryminacją osób ze względu na ich rasę lub pochodzenie etniczne, poglądy polityczne, religię bądź przekonania, przynależność do związków zawodowych, orientację seksualną bądź tożsamość płciową lub skutkuje środkami mającymi taki efekt”. Brak formalnego zakazu wprowadzenia tego typu technik przetwarzania można jednak wyprowadzić na podstawie innych przepisów, w szczególności art. 9 ust. 1 – dotyczącego ogólnego zakazu przetwarzania (w tym także profilowania) danych wrażliwych. Na gruncie rozporządzenia nierzozstrzygnięta pozostaje jednak kwestia dopuszczalności przetwarzania w przypadku wyrażenia zgody przez podmiot danych oraz braku odpowiednich przepisów krajowych. W takim przypadku zakaz taki można wywieźć z regulacji wyższej rangi, w szczególności art. 21 ust. KPP. Uwzględnienie w treści rozporządzenia zakazu profilowania danych na potrzeby zautomatyzowanego podejmowania decyzji w sposób prowadzących lub zakładający dyskryminację podmiotów danych i to bez względu na ew. udzielenie zgody przez osoby zainteresowane przyczyniłoby się do wzmocnienia europejskich standardów ochrony danych.

4.5.3. Międzynarodowy transfer danych

4.5.3.1. Wprowadzenie

Historycznie potrzeba wprowadzenia przepisów regulujących obszar ochrony danych osobowych uzasadniana była dwoma podstawowymi celami: skuteczniejszą ochroną praw jednostek oraz ułatwieniem w transgranicznym przekazywaniu danych. Cele te są silnie

K. Szymielewicz, A. Walkowiak, Autonomia informacyjna w kontekście usług internetowych: o znaczeniu zgody na przetwarzanie danych i ryzykach związanych z profilowaniem, Monitor Prawniczy 2014, nr 9.
powiązane, na co zwracano uwagę już w pierwszych analizach i rekomendacjach publikowanych w latach siedemdziesiątych dwudziestego wieku⁴⁷⁸. Ponieważ pierwsze rekomendacje w obszarze ochrony danych osobowych były opracowywane przez organizacje międzynarodowe, kwestia transgranicznego transferu danych była oczywistym zagadnieniem, które znalazło w nich omówienie⁴⁷⁹. Wprowadzenie jednakowych zasad ochrony w poszczególnych państwach miało doprowadzić do zniesienia barier w międzynarodowowej wymianie danych i skutkować stworzeniem wspólnego, ponadnarodowego obszaru, w którym przepływ danych nie wymaga uzyskiwania oddzielnych zgód czy zezwoleń, a poszczególne państwa nie mogą stosować niezgodnych przepisów krajowych. Ideę tę dobrze wyrażono w przepisach Konwencji 108, w szczególności w rozdziale III poświęconym przekazywaniu danych za granicę. Zgodnie z art. 12 ust. 2 Konwencji żadna z umawiających się stron nie może zabronić ani uzależnić od specjalnego zezwolenia, wyłącznie w celu ochrony prywatności, przepływu danych osobowych poprzez granicę na terytorium innej strony. Uznano zatem, że norma prawa międzynarodowego, jaką jest Konwencja 108, powinna być jedynym i wystarczającym źródłem praw i obowiązków w zakresie ochrony danych osobowych, wyłączającą konieczność wprowadzania dodatkowych obowiązków na poziomie krajowym, nieuregulowanych w postanowieniach traktatu.

Wbrew początkowym założeniom wprowadzenie Konwencji nie przyczyniło się jednak do zniesienia barier w międzynarodowym transferze danych, także na terenie Wspólnoty Europejskiej. Główne przyczyny związane były ze zbytnią ogólnośnością przepisów Konwencji, skutkującą możliwością stosowania odmiennych i niezgodnych norm na poziomie krajowym, jak i brakiem powszechności przyjęcia traktatu, także wśród państw należących do WE.

Kwestia zniesienia przeszkód w przepływie danych osobowych pomiędzy państwami członkowskimi była jedną z przyczyn zaproponowania przez KE i zatwierdzenia przez Radę i Parlament dyrektywy 95/46⁴⁸⁰. Zbliżenie przepisów krajowych – związane bezpośrednio z art. 104 TFUE, stanowiącym przepis kompetencyjny dla wprowadzenia dyrektywy – nie mogło być osiągnięte przez państwa członkowskie, a jednocześnie miało kluczowe znaczenie w zapewnieniu swobodnego przepływu danych w ramach Wspólnoty. Istotnym obszarem regulacji dyrektywy była także wymiana danych osobowych z państwami trzecimi – a więc, zgodnie z przyjętą w prawie UE terminologią, z państwami nienależącymi do Europejskiego

⁴⁷⁸ Zob. rozdział 3.2 (s. 98).
⁴⁷⁹ Por. np. wytyczne OECD przedstawione w rozdziale 3.3 (s. 101 i nast.).
⁴⁸⁰ Por. motyw 7 dyrektywy 95/46.
Obszaru Gospodarczego. W ramach przekazywania danych w obrębie państw należących do Wspólnoty (obecnie UE), zgodnie z przepisami dyrektywy 95/46, jak i obecnie obowiązującym rozporządzeniem 2016/679, nie jest konieczne stosowanie żadnych dodatkowych zgód czy zezwoleń. Co więcej, wprowadzenie na poziomie prawa krajowego przepisu nakładającego dodatkowe obowiązki na administratora warunkujące przekazywanie danych do innego państwa UE jest niezgodne z prawem Unii i jako takie nie rodzi ani żadnych obowiązków. Dlatego mówiąc o „międzynarodowym” transferze danych, należy rozróżnić przekazywanie danych w ramach wspólnego rynku UE (brak dodatkowych obowiązujących przekazywanie danych do innego państwa UE jest niezgodne z prawem Unii i jako takie nie rodzi ani żadnych obowiązków) z transferem do państw trzecich. W dalszej części rozdziału, dla uproszczenia, z międzynarodowym przekazywaniem danych należy utożsamiać transfer do państw trzecich.

Zgodnie z dyrektywą 95/46 podstawowym kryterium, warunkującym transfer danych do państwa trzeciego jest zapewnienie „odpowiedniego stopnia ochrony” – który należy oceniać z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazywania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przez przekazane danych, przepisy prawa obowiązujące w państwie trzecim oraz stosowane w tym kraju środki bezpieczeństwa i zachody zawodowe. Administrator może przekazywać dane tylko do państwa trzeciego zapewniającego równoważne prawa i gwarancje w obszarze poszanowania prywatności i ochrony danych osobowych. Istotne jest przy tym nie tylko miejsce formalnej siedziby firmy, otrzymującej dane w przetwarzanie, ale również prawo właściwe dla miejsca samego przetwarzania. Dlatego ocena adekwatności stopnia ochrony nie jest zadaniem prostym i wymaga przeanalizowania prawa krajowego państwa trzeciego oraz jego zobowiązań międzynarodowych, jak i procedur, przepisów wewnętrznych oraz zobowiązań przedsiębiorcy, będącego odbiorcą transferowanych danych.

Europejskie przepisy o ochronie danych nie przewidują, aby ocena stopnia ochrony mogła być przeprowadzana przez administratora (eksportera) danych. Po części jest to spowodowane złożonością omawianego zadania, z którym wiąże się potrzeba posiadania odpowiedniej wiedzy i doświadczenia. Pozostawienie kwestii uznania możliwości transferu danych do podmiotu trzeciego do wyłącznej decyzji administratora pozwalaoby jednak podmioty danych możliwości skutecznej ochrony i kontrolowania obiegu swoich informacji. Także przekazanie tego obowiązku na poziom krajowych organów nadzorczych byłoby nieskuteczne. Sytuacja taka mogłaby doprowadzić do odmiennego traktowania tych samych podmiotów zewnętrznych przez administratorów mających siedzibę w różnych państwach.
członkowskich, co w oczywisty sposób uniemożliwiłoby realizację jednego z celów ustanowienia europejskich przepisów o ochronie danych osobowych, jakim była harmonizacja rynku.

Dlatego w przyjętym na gruncie dyrektywy 95/46 modelu ochrony danych zaproponowano następujące mechanizmy przekazywania danych osobowych do podmiotów zlokalizowanych w państwach trzecich:

- bez decyzji indywidualnej, w oparciu o wydaną przez KE decyzję o adekwatności zabezpieczeń wydaną na podstawie art. 25 dyrektywy 95/46 lub art. 45 ust. 1 rozporządzenia 2016/679;
- bez decyzji indywidualnej poprzez zastosowanie w umowie łączącej administratora z podwykonawcą tzw. modelowych klauzul umownych, zatwierdzonych i opublikowanych przez KE w formie decyzji;
- na podstawie decyzji indywidualnej krajowego organu nadzoru, w tym w oparciu o tzw. wiązące reguły korporacyjne.

Przepisy rozporządzenia 2016/679 stanowią rozwinięcie i uszczegółowienie wcześniejszych rozwiązań wprowadzonych w dyrektywie. Stanowią także odpowiedź prawodawcy unijnego na potrzeby rozwijającego się rynku globalnej wymiany informacji, przy jednoczesnym uwzględnieniu praw i gwarancji osób fizycznych, których dane są przekazywane.

Niezależnie od możliwości zastosowania mechanizmów wskazanych w przepisach europejskiego prawa o ochronie danych osobowych, odrębną podstawę formalną stanowią umowy międzynarodowe – zarówno zawierane przez państwa członkowskie, jak i UE jako organizację międzynarodową. W wyniku zmiany wprowadzonej w procesie legislacyjnym przez Radę treść projektu rozporządzenia uzupełniono o przepis, zgodnie z którym traktaty, których stroną są państwa członkowskie, zawarte przed dniem 24 maja 2018 roku i zgodne z obowiązującym prawem UE, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia481. Jakkolwiek poprawka ta była motywowana względami zachowania zasady pewności prawa, brak wyznaczenia terminu granicznego na dostosowanie niezgodnych przepisów prawnomiedzinadrowodowych do wymagań rozporządzenia może powodować, że nawet umowy niespełniające europejskich regulacji o ochronie danych osobowych będą

481 Stanowisko Rady do projektu ogólnego rozporządzenia o ochronie danych, CELEX: ST_5419_2016_REV_1, s. 35
jeszcze przez bardzo długi czas elementem krajowych porządków prawnych państw członkowskich.

4.5.3.2. Decyzje o odpowiednim stopniu ochrony

Decyzja Komisji wydawana w pierwszym ze wskazanych trybów odnosi się do państwa trzeciego, a nie konkretnego podmiotu w nim działającego. W przypadku wydania decyzji transfer danych do wskazanego państwa jest możliwy bez uzyskania dodatkowych zezwoleń administracyjnych oraz bez obowiązku stosowania przez administratora danych dodatkowych zabezpieczeń kontraktowych482. W efekcie postępowania administracyjne dotyczące wydania decyzji indywidualnej na transfer danych do państwa objętego istniejącą decyzją o adekwatności zabezpieczeń powinny być umarzane jako bezprzedmiotowe. Dotychczas w okresie obowiązywania dyrektywy 95/46 Komisja wydała decyzje o adekwatności zabezpieczeń w odniesieniu do 12 państw483, w tym decyzję 2000/520484 dotyczącą Stanów Zjednoczonych, zawierającą warunki realizacji programu „Bezpieczna przystań”. Decyzja ta została uznana za nieważną przez TSUE w sprawie Schrems z uwagi na przekroczenie przez Komisję kompetencji oraz błędną ocenę prawodawstwa i zobowiązań międzynarodowych Stanów Zjednoczonych poprzez uznanie, że państwo to „rzeczywiście zapewnia odpowiedni stopień ochrony” w rozumieniu art. 25 ust. 5 dyrektywy 95/46485. Tłem rozważań Trybunału było wyważenie roli praw podstawowych – w tym prawa do ochrony prywatności – oraz interesu bezpieczeństwa narodowego, a w szczególności możliwość istnienia uzasadnianego kwestiami bezpieczeństwa publicznego odstępstwa pozwalającego na inwazję w prawa podstawowe osób, których dane osobowe zostały lub mogły zostać przekazane z Unii do Stanów Zjednoczonych.

W następstwie orzeczenia w sprawie Schrems Komisja wynegocjowała z Departamentem Handlu USA nowe porozumienie o nazwie Tarcza prywatności, zatwierdzone decyzją wykonawczą 2016/1250486 o adekwatności zabezpieczeń. Także ta decyzja jest

483 Lista decyzji Komisji o adekwatności zabezpieczeń danych osobowych w państwach trzecich, http://cli.re/LK2835.
484 Decyzja Komisji z 26.07.2000 przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz. Urz. WE z 2000 nr L 215).
485 Wyrok TSUE w sprawie Schrems, sygn. C‑362/14, p. 96-97.
486 Decyzja wykonawcza Komisji (UE) 2016/1250 z 12.07.2016 przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA (CELEX: 32016D1250, Dz. Urz. UE z 2016 Nr L 207 s. 1).
krytykowana w literaturze przedmiotu, wskazuje się przede wszystkim fakt, że została oparta na tych samych ramach formalnych, a więc programie samocertyfikacji podmiotów zamiast na przepisach prawa powszechnego lub – w przypadku ich braku – zobowiązań międzynarodowych państwa trzeciego.

Wydawanie decyzji o adekwatności jest trybem udostępniania danych osobowych poza obszar UE, z którym wiąże się najwięcej kontrowersji i dyskusji w doktrynie. Na gruncie przepisów dyrektywy 95/46 wskazywano na liczne niejasności i słabości przyjętego modelu, związane w szczególności z zakresem uprawnień krajowych organów nadzoru do kontrolowania realizacji transferów realizowanych w oparciu o decyzje o adekwatności, brakiem mechanizmu cyklicznej weryfikacji wydanych decyzji ale również niewielkiej praktycznej możliwości w dochodzeniu swoich praw przez podmioty danych. Uwagi te, jak również wnioski z wyroku w sprawie Schrems, zostały uwzględnione w przepisach rozporządzenia 2016/679.

Podobnie jak w przypadku dyrektywy 95/46 na gruncie rozporządzenia przekazanie danych może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie zapewnia odpowiedni stopień ochrony. Nowością jest jednak wskazanie w art. 45 ust. 1, że decyzja może odnosić się nie do całego obszaru państwa trzeciego, ale fragmentu jego terytorium, określonego sektora w tym państwie lub organizacji międzynarodowej. Ponadto prawodawca w art. 45 ust. 2 wskazał kryteria, które Komisja powinna uwzględnić, dokonując oceny stopnia ochrony. Zostały one znacznie rozbudowane i doprecyzowane względem dyrektywy 95/46 – dodano między innymi odwołanie do istnienia odpowiedniego prawodawstwa w obszarze poszanowania praw człowieka i podstawowych wolności także w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego. Uwzględniono również konieczność zbadania, czy w państwie trzecim istnieje i skutecznie działa co najmniej jeden niezależny organ nadzorczy, mający obowiązek zapewniania i egzekwowania przepisów o ochronie danych osobowych. Wprowadzono obowiązek cyklicznych przeglądów (art. 45 ust. 3), przynajmniej raz na cztery lata, w zakresie aktualności wydanych decyzji, w efekcie którego możliwe jest uchylenie, zmiana lub zawieszenie wydanej wcześniej decyzji (art. 45 ust. 5). Nowością jest także wskazanie, że w zastosowaniu trybu określonego w ust. 5 – w

487 Zob. także uwagi krytyczne oraz wskazane piśmiennictwo w: A. Michałowicz, Nowe zasady transferu danych osobowych z Unii Europejskiej do Stanów Zjednoczonych w ramach Tarczy Prywatności, Monitor Prawniczy 2016, nr 23, s. 1264.

488 Brak możliwości wydania decyzji o adekwatności w odniesieniu do określonego sektora państwa trzeciego był bezpośrednią przyczyną uznania przez TSUE decyzji KE 2004/535, dotyczącej przekazywania danych PNR do Stanów Zjednoczonych; zob. więcej informacji w kontekście sprawy C-317/04 w rozdziale 4.6.2 (s. 197).
szczegółności uchylenia lub zawieszenie decyzji o adekwatności zabezpieczeń – pozostaje bez wpływu dla przekazywania danych osobowych do państwa trzeciego realizowanego w innym trybie (np. w oparciu o standardowe klauzule umowne).

Wydane w oparciu o dyrektywę 95/46 decyzje o adekwatności zabezpieczeń nie utracą mocy wraz z wejściem w życie rozporządzenia 2016/679 (art. 45 ust. 9 rozporządzenia). Ponieważ stanowią one formalną podstawę dla międzynarodowego transferu danych z obszaru UE do głównych globalnych dostawców usług przetwarzania danych, należy oczekiwać, że także w kolejnych latach po wejściu w życie rozporządzenia 2016/679 ich faktyczne znaczenie dla poziomu ochrony danych obywateli UE przekazywanych do państw trzecich nie zmaleje. Prawodawca przewidział, że decyzje wydane na podstawie dyrektywy 95/46 będą podlegały cyklicznym ocenom przewidzianym w rozporządzeniu. Podstawą do tych ocen będą już znowelizowane przepisy zawarte w RODO, znacznie rozbudowujące przesłanki formalnej oceny adekwatności zapewnianego poziomu ochrony przez państwo trzecie. Dlatego w przypadku gdy TSUE wcześniej nie stwierdzi nieważności decyzji 2016/1250, warunki realizacji programu „Tarcza prywatności” i tak będą musiały zostać dostosowane do bardziej rygorystycznych przepisów rozporządzenia, jeżeli program ten nadal będzie miał stanowić podstawę wymiany danych z przedsiębiorcami działającymi na terytorium Stanów Zjednoczonych.

4.5.3.3. Klauzule umowne oraz wiążące reguły korporacyjne

W przypadku braku możliwości uznania państwa trzeciego jako zapewniającego odpowiedni stopień ochrony dyrektywa 95/46 wprowadzała możliwość przekazywania danych osobowych do tego państwa, jeżeli administrator zobowiązał importera danych do stosowania odpowiednich zabezpieczeń dotyczących ochrony prywatności oraz podstawowych praw i wolności, które w szczególności mogły wynikać z odpowiednich klauzul umownych.

Na podstawie art. 26 ust. 4 dyrektywy Komisja została upoważniona do wydawania decyzji stwierdzających, że wskazane w nich klauzule umowne stanowią wystarczający środek do zabezpieczenia transferu danych do państwa trzeciego. W literaturze przedmiotu nazywa się je „standardowymi” lub „modelowymi” klauzulami umownymi. Projektując propozycję rozwiązań kontraktowych, Komisja korzystała przy tym z doświadczeń wypracowanych na forum innych organizacji międzynarodowych, takich jak
Międzynarodowa Izba Handlowa, Organizacja Współpracy Gospodarczej i Rozwoju czy Rada Europy\(^{489}\).


Odmiennym trybem, stosowanym zwłaszcza przed podmioty należące do tej samej grupy kapitałowej, jest wystąpienie o zatwierdzenie „wiązących reguł korporacyjnych” (binding corporate rules, BCR), które określają tryb i zasady przekazywania oraz przetwarzania informacji w obrębie podmiotów stale ze sobą współpracujących, często powiązanych kapitałowo. Możliwości stosowania BCR jako podstawy międzynarodowego transferu danych nie wskazano w treści dyrektywy 95/46, a została zaproponowana i doprecyzowana w kolejnych rekomendacjach i opiniach publikowanych przez Grupę Roboczą Art. 29. Jest więc efektem współpracy organów nadzoru państw członkowskich. Dlatego BCR są wskazywane w literaturze przedmiotu jako przykład soft-law, którego podstawę stanowi samoregulacja wynikająca z zatwierdzonych i stosowanych przez grupę podmiotów zasad przetwarzania danych\(^{490}\). Po raz pierwszy kwestia możliwości stosowania wiążących reguł korporacyjnych stała się przedmiotem analizy ze strony Grupy Roboczej Art. 29 wraz z publikacją dokumentu roboczego WP 74, w którym przedstawiano rozważania na temat

\(^{489}\) B. Fisher, D. Karwala, *Umowy transferowe jako instrument przekazywania danych osobowych do państw trzecich*, Przegląd Prawa Handlowego 2007, nr 10, s. 16

\(^{490}\) D. Karwala, *Wiążące reguły korporacyjne dla przetwarzających dane osobowe (processor binding corporate rules)*, Monitor Prawniczy 2014, nr 13, s. 672
przydatności stosowania BCR, zaproponowano definicję oraz omówiono najważniejsze aspekty stosowania. Ponieważ z definicji przynajmniej jeden podmiot objęty wiążącymi regulami korporacyjnymi posiada siedzibę na terenie UE, przyjęto, że do podmiotu tego powinny zostać oddelegowane obowiązki i uprawnienia konieczne do pełnienia funkcji administratora bezpieczeństwa informacji dla całą grupy. Ponieważ wiążące reguły korporacyjne stanowią zestaw wewnętrznych dokumentów danej grupy kapitałowej (takich jak polityki, procedury czy instrukcje) oddzielnego zbadania wymaga kwestia ich wiążącego charakteru oraz możliwości dochodzenia na ich podstawie praw przez podmioty danych. Jak wskazano w rekomendacji Grupy Roboczej Art. 29, niezależnie od prawa właściwego dla podmiotów grupy kapitałowej, funktionujących poza obszarem UE, prawa i gwarancje podmiotów danych muszą pozostać niezmienione i gwarantowane na poziomie stosowanym w Unii. Oznacza to w szczególności konieczność stosowania przepisów o środkach sądowych oraz odpowiedzialności w taki sam sposób oraz w takim samym zakresie, jaki miałby zastosowanie, gdyby przetwarzanie danych odbywało się na obszarze Unii. Prowadzi to także do konkluzji, że wyznaczony podmiot funkcjonujący na terenie UE, do którego delegowano odpowiedzialność za przetwarzanie danych w ramach BCR, może zostać pozwany w przypadku naruszenia obowiązków wynikających z przepisów ochrony danych, niezależnie od tego, gdzie miało miejsce naruszenie i jaki podmiot z grupy kapitałowej za nie odpowiadał. Podmiot ten musi być także odpowiedzialny przed krajowym organem nadzoru za przestrzeganie wszelkich obowiązków administracyjnoprawnych wynikających z europejskich przepisów o ochronie danych osobowych.

Kwestia stosowania BCR była rozwijana i przybliżana w kolejnych opracowaniach Grupy Roboczej Art. 29. W dokumencie WP 107 z 14 kwietnia 2005 wskazano zasady współpracy krajowych organów nadzoru przy zatwierdzaniu BCR, obejmujące podmioty funkcjonujące w więcej niż jednym państwie członkowskim. Przyjęto, że podmiot zgłaszający wniosek o zatwierdzenie reguł korporacyjnych powinien wskazać wiodący organ nadzoru, który po przeprowadzeniu wstępnej oceny skieruje pytanie o opinię do pozostałych organów ustanowionych w państwach członkowskich, w których funkcjonuje dana grupa kapitałowa. W późniejszych opracowaniach propozycję tę zmodyfikowano, proponując, aby proces

---

491 Grupa Robocza Art. 29, Dokument roboczy: Transfer danych osobowych do państw trzecich: Stosowanie art. 26 ust. 2 dyrektywy o ochronie danych do wiążących regul korporacyjnych dla międzynarodowych transferów danych, WP 74, s. 18.
akceptacji był realizowany przez organ wiodący oraz dwa wybrane organy z państw członkowskich, a skutki decyzji były respektowane przez pozostałe organy nadzoru⁴⁹².

Grupa Robocza Art. 29 wypracowała też zestaw pomocniczych rekomendacji, takich jak przykładowa lista kontrolna oraz wytyczne do uwzględnienia we wniosku o zatwierdzenie BCR (WP 102 oraz WP 108), odpowiedzi na często zadawane pytania (WP 155), szablon dokumentu (WP 154) oraz listę elementów i zasad (WP 153), które mogą stanowić podstawę do opracowania wiążących regul korporacyjnych. W kolejnych latach opublikowano także szablon standardowego wniosku o zatwierdzenie wiążących regul korporacyjnych w formie edytowalnego formularza (WP 133). Grupa Robocza Art. 29 przygotowała również wytyczne w zakresie możliwości i warunków stosowania regul w odniesieniu do zagranicznych procesorów (podmiotów przetwarzających) dane osobowe. Zostały one opisane w dokumentach WP 195 i WP 204. Dokumenty te miały szczególne znaczenie dla grup kapitałowych, w ramach których wydzielono wyspecjalizowane centra przetwarzania danych zlokalizowane poza UE, a także usługodawców świadczących usługi przetwarzania w chmurze obliczeniowej (cloud computing), w przypadku których normą jest posiadanie szeregu podmiotów zależnych dedykowanych do prowadzenia centrów przetwarzania danych, rozlokowanych równomiernie na całym świecie.

Wiążące reguły korporacyjne są mechanizmem zbudowanym w oparciu o istniejące rozwiązania prawne, w szczególności możliwość wydawania decyzji zezwalających na transfer danych do państw trzecich. Przedmiotem oceny ze strony organu nadzoru nie jest jednak pojedyncza umowa łącząca dwie strony, ale zestaw dokumentów korporacyjnych, wiążących i stosowanych w obrębie określonej grupy kapitałowej. Reguły korporacyjne powinny spełniać określone warunki wskazane w opublikowanych wytycznych Grupy Roboczej Art. 29, aby na ich podstawie organ nadzoru mógł uznać adekwatność zaproponowanych środków ochrony do przepisów obowiązujących na terenie UE. Nie zmienia to jednak faktu, że cały mechanizm jest oparty na samoregulacji, a z uwagi na brak jego sformalizowania w przepisach dyrektywy stosowanie i akceptowanie BCR było niezależną decyzją państw członkowskich. Rodziło to ryzyko pojawienia się różnej interpretacji przyjętych zasad przez poszczególne оргany nadzoru, co znacząco ograniczyłoby praktyczną przydatność tego mechanizmu jako środka do regulowania transferu danych przez międzynarodowe korporacje.

⁴⁹² B. Fisher, Wiążące reguły i wzajemne uznawanie w nowelizacji OchrDanOsobU z 2015 r. oraz wspieranie efektywnego funkcjonowania tego instrumentu, [w:] Aktualne problemy prawnej ochrony danych osobowych 2015, Monior Prawniczy 2015, nr 6, s. 1042.
W okresie obowiązywania dyrektywy 95/46 nie wszystkie krajowe organy nadzoru przystąpiły do wy pracowanej przez Grupę Roboczą Art. 29 procedury wzajemnego uznawania, zgodnie z którą BCR zaakceptowane przez wiodący organ nadzoru nie wymagały oddzielnej weryfikacji w pozostałych państwach członkowskich, w których działalność prowadziła wnioskująca grupa kapitałowa. Według danych Komisji, do procedury przystąpiły organy nadzorcze z 21 państw członkowskich – w grupie tej nie ma polskiego GIOD0\textsuperscript{493}. Zgodnie z art. 48 ust. 2 pkt 2 ustawy o ochronie danych osobowych decyzja GIOD0 nie jest wymagana w odniesieniu do stosowania BCR, jeżeli zostały one wcześniej zatwierdzone przez Generalnego Inspektora. Jeżeli wiążące reguły korporacyjne były wcześniej przedmiotem rozstrzygnięcia organu nadzoru innego państwa należącego do EOG, GIOD0 jest zobowiązany do przeprowadzenia konsultacji z tym organem jednak nie musi podtrzymywać jego rozstrzygnięcia w wydanej decyzji\textsuperscript{494}.

Wiążące reguły korporacyjne stały się skutecznym mechanizmem zapewniania zgodności z europejskimi przepisami o ochronie danych osobowych przez ponadnarodowe koncerny działające w skali globalnej. Wśród podmiotów, które skorzystały z tej możliwości, znajdują się największe instytucje finansowe (Mastercard, ING Bank, Citigroup), koncerny przemysłowe (ArcelorMittal, Airbus, Siemens), telekomunikacyjne (Deutsche Telekom), firmy sektora farmaceutycznego (GlaxoSmithKline, Novartis) czy IT (OVH, Salesforce, BMC Software)\textsuperscript{495}.

Z tego powodu mechanizm ten został uwzględniony w pracach nad ogólnym rozporządzeniem. Zgodnie z motywem 110. rozporządzenia 2016/679 grupa przedsiębiorców powinna móc korzystać z zatwierdzonych wiązących reguł korporacyjnych przy międzynarodowym przekazywaniu danych z Unii do organizacji w tej samej grupie pod warunkiem, że w takich regulach korporacyjnych są ujęte wszystkie podstawowe zasady i egzekwowalne prawa zapewniające odpowiednie zabezpieczenia na potrzeby przekazywania danych osobowych lub na potrzeby określonych kategorii przekazów danych osobowych. Postulat ten znalazł rozwinięcie w ustępatach art. 43 rozporządzenia, który stanowi nowość w porównaniu z dyrektywą 95/46. Prawodawca w art. 43 ust. 1 wskazał, że BCR mogą być przedmiotem zatwierdzenia przez krajowe organy ochrony danych osobowych, pod warunkiem że są prawnie wiążące, mają zastosowanie do wszystkich podmiotów grupy przetwarzającej dane i przez każdego z nich są stosowane, a także że wyraźnie przyznają

\textsuperscript{493} Approval of binding corporate rules, http://cli.re/6Ye1YQ.

\textsuperscript{494} Por. decyzja GIOD0 z 22 lipca 2016, DESiWM/DEC-638/16, s. 3.

\textsuperscript{495} Lista organizacji dla których zakończono realizację procedury BCR EU: http://cli.re/Gp9pRq.
podmiotom danych egzekwowalne prawa. Nadto w przepisie ust. 2 wskazano listę 14 elementów, które powinny zostać określone w opracowanych regułach. Zawiera ona zarówno wymagania korporacyjne (w tym opis struktury grupy, dane kontaktowe, wskazanie podmiotów odpowiedzialnych, zadania inspektora ochrony danych), opis stosowanych mechanizmów nadzoru i kontroli, procedury skargowej, jak i odniesienie do szczegółowych praw podmiotów danych.


4.5.3.4. Inne podstawy prawne międzynarodowego transferu danych

Zarówno przepisy dyrektywy 95/46, jak również rozporządzenia 2016/679 określają katalog dopuszczalnych odstępstw, pozwalających na przekazanie danych do państwa trzeciego nawet w sytuacji, gdy nie jest spełniona żadna z pozytywnych przesłanek transferu danych (takie jak zatwierdzone wiążące reguły korporacyjne, standardowe klauzule umowne czy decyzja indywidualna organu nadzoru), a państwo trzecie nie zostało uznane za zapewniające odpowiedni stopień ochrony. Odstępstwa te – jak wszystkie inne mogące prowadzić do ingerencji w prawa podstawowe – należy interpretować w sposób wąski. Przede wszystkim transfer danych jest możliwy w oparciu o jednoznaczną zgodę podmiotu danych. Występujące w dyrektywie wymaganie jednoznacznej zgody (art. 26 ust. 1 pkt a) zostało uzupełnione w rozporządzeniu koniecznością poinformowania osobę o ryzyku, z jakim wiąże się proponowane wyrażenie zgody (art. 49 ust. 1 pkt a rozporządzenia). W dalszej kolejności przekazanie danych może być uzasadnione z uwagi na zawarcie lub wykonanie umowy z podmiotem danych lub osobą trzecią, jeżeli jest to w interesie podmiotu danych, jak również może być konieczne dla zapewnienia żywotnych interesów podmiotu danych lub być niezbędne ze względu na ważne względy interesu publicznego. Przy czym w art. 49 ust. 4 doprecyzowano, że interes publiczny musi być uznany w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator. Nie stanowi zatem przesłanki uzasadniającej
przekazanie danych do państwa trzeciego interes bezpieczeństwa publicznego tego państwa, jeżeli nie spełnia on przywołanych wyżej kryteriów. Wniosek ten jest zgodny z tezą TSUE zawartą w wyroku Schrems, a dodanie wskazanego przepisu rozstrzyga ewentualne niejasności, które mogły powstać przy interpretacji wydanych przez KE decyzji o adekwatności zabezpieczeń, w szczególności decyzji 2016/1250 dotyczącej Stanów Zjednoczonych. Ostatnią z przesłanek uzasadniających realizację transferu danych jest konieczność ustalenia, dochodzenia lub ochrony roszczeń (art. 49 ust. 1 pkt e).

Rozporządzenie uzupełniono o klauzulę dodatkową, mającą zastosowanie w sytuacjach szczególnych. Zgodnie z nią, jeżeli nie spełnione zostały żadne z wprowadzonych w przepisach wcześniejszych przesłanki do realizacji transferu danych oraz nie zachodzi żadna z okoliczności wskazanych w zamkniętym katalogu odstępstw określonym w art. 45 ust. 1, administrator może zrealizować transfer pod warunkiem, że jest on jednorazowy, dotyczy ograniczonej liczby osób oraz jest niezbędny ze względu na ważny prawnie i uzasadniony interes realizowany przez administratora, wobec którego nadrzędnego charakteru nie mają interesy ani prawa i wolności podmiotów danych. W takim przypadku dodatkowo administrator musi spełnić obowiązki informacyjne zarówno względem podmiotów danych, jak i organu nadzorczego. Jest to nowa podstawa przekazania danych, nieznana wcześniej na gruncie przepisów dyrektywy 95/46. Biorąc pod uwagę zastrzeżenie, że niezbędnym warunkiem zastosowania tej klauzuli jest instnienie ważnego i prawnie uzasadnionego interesu administratora, wobec którego charakteru nadrzędnego nie mają prawa podmiotów danych, stwierdzić należy, że w obecnym stanie prawnym jest to rozwiązanie mające bardzo ograniczone możliwości zastosowania. Zwłaszcza, że zgodnie z art. 49 ust. 3 tryb ten nie może być zastosowany do działalności prowadzonej przez organy publiczne w ramach wykonywania przysługujących im uprawnień. Prowadzi to do wniosku, że klauzula dodatkowa nie może znaleźć zastosowania w obszarze bezpieczeństwa publicznego, obrony czy bezpieczeństwa narodowego.

Ponieważ rozporządzenie jest aktem prawa stosowanym wprost, konieczne stało się uzupełnienie przepisów o uregulowanie dotyczące możliwości wprowadzenia przez państwa członkowskie uzupełniających regulacji na poziomie krajowym. W tym zakresie, zgodnie z art. 46 ust. 5, prawo Unii lub prawo państwa członkowskiego może z uwagi na ważne względy interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

496 Zgodnie z ugruntowanym orzecznictwem TSUE w obszarze interpretacji ingerencji w prawa podstawowe wskazane obszary przynależą władzy publicznej (por. np. C-73/07, p. 41).
Warunkiem wprowadzenia takiego ograniczenia jest jednak brak decyzji stwierdzającej odpowiedni stopień ochrony. Przepisy prawa krajowego nie mogą zatem prowadzić do ograniczenia możliwości realizacji transferów danych przeprowadzanych na podstawie ważnej decyzji KE stwierdzającej adekwatność zabezpieczeń. Z uwagi na zastosowaną redakcję przepisu niejasności budzi, czy ograniczenia takie mogą zostać skutecznie wprowadzone w odniesieniu do innych form transferu danych, w szczególności realizowanych w oparciu o standardowe klauzule umowne oraz wiążące reguły korporacyjne. Problem ten może zostać rozstrzygnięty w wyniku odpowiedzi przez TSUE na pytanie prejudycjalne, które zostanie zadane przez irlandzki Wysoki Sąd (ang. *High Court*) w związku z zawisłą przed nim sprawą – dotyczącą możliwości kwestionowania przez organy nadzoru transferów realizowanych w oparciu o standardowe klauzule umowne. Postępowanie⁴⁹⁷, prowadzone z wniosku irlandzkiego urzędu ochrony danych, ma na celu ustalenie, poprzez zadanie pytania prejudycjalnego do TSUE, ważności decyzji KE dotyczących standardowych klauzul umownych oraz uprawnień organów nadzoru do kontroli transferów realizowanych w oparciu o takie klauzule. Ponieważ według stanu na dzień 20 marca 2017 sprawa jest cały czas procedowana na etapie krajowym w Irlandii, należy oczekiwać że ew. rozstrzygnięcie TSUE zapadnie nie szybciej niż w 2018-2019 roku.

4.5.4. Niezależny nadzór i mechanizmy spójności

4.5.4.1. Definicja i zakres niezależności krajowych organów nadzorczych

Na gruncie unijnych przepisów o ochronie danych wprowadzenie skutecznych gwarancji w obszarze ochrony danych osobowych od początku było wiązane z funkcjonowaniem niezależnego nadzorcy. Już w wytycznych Parlamentu Europejskiego z 8 maja 1979 roku wskazywano na potrzebę powołania przez każde państwo członkowskie „niezależnego organu, posiadającego odpowiednie kadry oraz finansowanie, w celu monitorowania stosowania na jego obszarze działania norm Wspólnoty oraz przepisów krajowych je implementujących”⁴⁹⁸. Obowiązek wprowadzenia mechanizmu nadzorczego nie został uwzględniony w Konwencji 108, w której nie określono obowiązku utworzenia organu nadzorczego, ograniczając się do wskazania na konieczność wyznaczenia organu koordynującego współpracę międzynarodową w zakresie współpracy między stronami

⁴⁹⁷ *Hight Court (Commercial Division)*, sprawa *Data Protection Commissioner v. Facebook Ireland Limited & Maximilian Schrems*, sygn. 2016/4809P.

⁴⁹⁸ Rezolucja PE z dn. 8 maja 1979…, Dz.U. WE z 1979 Nr C 140, s. 38, p. 10.
traktatu\textsuperscript{499}. Dopiero wraz z wprowadzeniem Protokołu dodatkowego do Konwencji z 8 stycznia 2001\textsuperscript{500} wprowadzono obowiązek powołania przez każdą ze stron umowy jednego lub więcej niezależnych organów nadzoru oraz wyposażenia ich w uprawnienia dochodzeniowe i interwencyjne, jak również prawo do angażowania się w postępowania prawne lub informowanie właściwych organów sądowych o naruszeniach przepisów prawa krajowego.

Należy podkreślić, że i potrzeba powołania organu nadzorczego, i nadanie mu cech niezależności zostały uwzględnione w dyrektywie 95/46 już od pierwszego projektu KE opublikowanego w 1990 roku. Wskazywano, że obowiązek państw członkowskich w obszarze nadzoru stosowania przepisów o ochronie danych osobowych powinien wyraźnie realizować się realizacją dwóch zadań: powołania niezależnego organu nadzoru oraz wyposażenia go w kompetencje interwencyjne i śledcze\textsuperscript{501}. Ostatecznie zatwierdzonej wersji dyrektywy doprecyzowano zakres tych uprawnień w odniesieniu do wykonywanych operacji przetwarzania danych oraz nadzoru nad pracą administratorów danych. Ponadto umocowano organy nadzoru do pozywania lub powiadamiania organów sądowych o faktach naruszenia przepisów krajowych, stanowiących implementację dyrektywy. Obowiązek ustanowienia niezależnego regulatora umocowanego do podejmowania wiążących decyzji nadzorczych w zakresie przetwarzania danych osobowych odzwierciedla także prawnopubliczną rolę ustanowionych przepisów. W rezultacie ochronę danych osobowych w rozumieniu standardów europejskich należy rozumieć jako przynależność zarówno do dziedziny prawa prywatnego (wzajemne relacje pomiędzy administratorami a podmiotami danych, regulowane stosunkami umownymi kształtowanymi pomiędzy nimi), jak i prawa publicznego (regulacyjna rola powołanego nadzorcy, wkraczająca w swobodę kształtowania umów pomiędzy podmiotami funkcjonującymi na rynku).

Zgodnie z art. 28 ust. 1 dyrektywy 95/46 państwa członkowskie zostały zobowiązane do zapewnienia funkcjonowania jednego lub więcej organów władzy publicznej. Prawodawca przewidział zatem, aby funkcje nadzorcze były sprawowane przez kilka podmiotów – co jest modelem do dzisiaj stosowanym w niektórych państwach i stanowi cechę charakterystyczną państw federacyjnych (np. Niemcy, Stany Zjednoczone).

Kwestia niezależności organów nadzoru nigdy nie budziła wątpliwości na gruncie legislacji i wynikała wprost z przyjętej redakcji art. 28 ust. 1 („organy postępują w sposób

\textsuperscript{499} Art. 13 ust. 1 Konwencji Nr 108 (Dz.U. 2003 Nr 3, poz. 25).
\textsuperscript{501} Komunikat Komisji Europejskiej z 13 września 1990…, CELEX: 51990DC0314, s. 42.
całkowicie niezależny przy wykonywaniu powierzonych im funkcji”). W nauce prawa pojęcie niezależności organu władzy publicznej należy rozumieć dwojako\(^{502}\). Po pierwsze, jako niezależność od podmiotów nadzorowanych, a więc cecha pozwalająca na zachowanie obiektywizmu we wprowadzanych rozstrzygnięciach. W rozumieniu szerszym niezależność obejmuje także brak wpływu innych organów władzy publicznej na podejmowane decyzje i działania. Ponieważ implementacja przepisów dyrektywy w zakresie formy, umocowania i kompetencji organów nadzoru doprowadziła do pojawienia się rozbieżności pomiędzy przepisami krajowymi państw członkowskich, kwestia ta stała się przedmiotem analizy ze strony Komisji, a następnie serii skarg wniesionych do TSUE w oparciu o art. 258 TFUE. Dopiero tezy zawarte w orzeczeniach wydanych przez Trybunał kilkanaście lat po wprowadzeniu dyrektywy w życie pozwoliły na ugruntowanie i ujednolicenie rozumienia sposobu i granic interpretacji niezależności organów ochrony danych osobowych.

Już w pierwszej z badanych spraw, skierowanej przeciwko Niemcom, Trybunał wskazał, że przymiotnik „niezależny” zastosowany w odniesieniu do organu publicznego oznacza zwykle status, który zapewnia danemu organowi możliwość w pełni swobodnego działania, z wyłączeniem jakichkolwiek instrukcji czy nacisków\(^{503}\). Niezależność nie ma przy tym na celu przyznania organom czy ich pracownikom szczególnego statusu, lecz wzmocnienie ochrony osób i instytucji, których dotyczą decyzje tych organów. W takim rozumieniu zapewnienie niezależności organów jest jednym z mechanizmów zabezpieczających prawidłową realizację dyrektywy, a przez to praw i gwarancji w niej określonych. Tym samym Trybunał przychylił się do interpretacji niezależności w ujęciu szerszym, a więc dotyczącym nie tylko braku powiązań z organami nadzorowanymi, ale całkowitym brakiem zewnętrznych nacisków mogących nadawać kierunek decyzji nadzorczych. W takim rozumieniu samo już tylko zagrożenie możliwości wpływu politycznego na decyzje ustanowionych organów nadzoru jest wystarczającą przeszkodą w niezależnym wykonywaniu przez nie zadań\(^{504}\). Jak podkreślił rzecznik generalny J. Mážak, niezależność nie przekreśla możliwości ustanowienia jakiejkolwiek kontroli\(^{505}\). W szczególności wyłączenie spod wpływu władzy wykonawczej nie prowadzi do ograniczenia możliwości ustanowienia kontroli parlamentarnej czy sądowej.

\(^{502}\) Bardziej rozbudowany, wieloaspektowy model opisu i oceny niezależności został zaproponowany przez F. Gilardi w Policy credibility and delegation to independent regulatory agencies: a comparative empirical analysis, Journal of European Public Policy 2002, nr 12, s. 873.

\(^{503}\) Wyrok TSUE z 9.03.2010 w sprawie Komisja v. Niemcy, sygn. C‑518/07.

\(^{504}\) Ibidem, p. 36.

\(^{505}\) Opinia rzecznika generalnego Jána Mazáka przedstawiona 22.10.2009, sygn. C-518/07, p. 29.
W sprawie Komisja v. Austria\textsuperscript{506} Trybunał wywiódł z niezależności organu nadzoru także potrzebę pozostawania nie tylko członków kierownictwa, ale i wszystkich pracowników poza wpływem innych urzędów władzy wykonawczej. Przejawem takiego wpływu może być w szczególności podległość wynikająca z przynależności do określonego działu administracji centralnej lub związana z zaszeregowaniem wynikającym z krajowych przepisów o pracownikach administracji. Niedopuszczalne jest też wprowadzenie bezwarunkowego uprawnienia dla administracji rządowej żądania informacji na temat dowolnych aspektów funkcjonowania organu nadzoru\textsuperscript{507}.

Sprawy przeciwko Niemcom i Austrii dotyczyły głównie kompetencji władzy wykonawczej oraz relacji pomiędzy administracją rządową a ustanowionym organem nadzoru. Z kolei w sprawie Komisja v. Węgry\textsuperscript{508} rozpatrzona została skarga dotycząca przyjęcia krajowych przepisów ustawowych prowadzących do naruszenia niezależności organu wynikającej z art. 28 ust. 1 dyrektywy. Trybunał ocenił, na ile prawodawca krajowy może dowolnie kształtować ramy funkcjonowania i sposób działania organu nadzoru. Ponieważ dyrektywa nie określa struktury, organizacji organów nadzorczych oraz wymagań w zakresie kadencji osób kierujących, państwa członkowskie dysponowały swobodą w kształtowaniu tych zagadnień. Trybunał zauważył, że gdyby powyższe uprawnienia obejmowały także możliwość skracania kadencji organu nadzorczego na mocy nowo wprowadzonych środków ustawodawczych, odmiennych od przepisów wcześniej istniejących, to zagrożenie skróceniem kadencji ciążące na owym organie podczas wykonywania jego funkcji mogłoby prowadzić do pewnego rodzaju posłuszeństwa względem władzy politycznej, niezgodnego ze wskazanym wymogiem niezależności\textsuperscript{509}. W rezultacie obowiązek poszanowania kadencji organu stanowi jeden z wyznaczników niezależności organu nadzorczego odpowiedzialnego za monitorowanie stosowania przepisów o ochronie danych osobowych.

Uwzględniając tezy z przywołanych orzeczeń TSUE, K. Rokita postuluje, że skoro zgodnie z art. 8 ust. 3 KPP przestrzeganie zasad dotyczących ochrony danych podlega kontroli niezależnego organu, to nie jest możliwe rozdzielenie aspektu materialnego prawa od jego elementu instytucjonalnego\textsuperscript{510}.

\textsuperscript{506} Wyrok TSUE z 16.10.2012 w sprawie Komisja v. Austria, sygn. C-614/10.
\textsuperscript{507} Ibidem, p. 63.
\textsuperscript{508} Wyrok TSUE z 8.04.2014 w sprawie Komisja v. Węgry, sygn. C-288/12.
\textsuperscript{509} Ibidem, p. 54.
\textsuperscript{510} K. Rokita, \textit{Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych}, EPS 2016, nr 7, s. 6.
Wnioski z przywołanych orzeczeń TSUE zostały odzwierciedlone w przepisach rozporządzenia 2016/679. W miejsce dotychczasowego art. 28 dyrektywy, określającej organizację i uprawnienia organu nadzoru, prawodawca wprowadził cały rozdział nowej regulacji poświęcony kwestii niezależności. W przyjętych regulacjach (art. 52 ust. 1) podtrzymywano ogólną zasadę wypełniania zadań i uprawnień „w sposób w pełni niezależny”, co w szczególności oznacza pozostawanie członków organu wolnych od bezpośrednich i pośrednich wpływów zewnętrznych (art. 52 ust. 2). Ponadto personel organu powinien być wybierany wyłącznie przez organ nadzorczy i działać pod wyłącznym kierownictwem członka organu. Prawodawca wskazał, że organ powinien dysponować własnym, odrębnym budżetem, a kontrola finansowa obejmująca jego wykonanie powinna być prowadzona w sposób nienaruszający niezależności organu (art. 52 ust. 2). W porównaniu z dyrektywą w rozporządzeniu znacznie rozbudowane zostały przepisy związane z ogólnymi zasadami ustanawiania nadzorczy (art. 54), jak również warunki dotyczące wyboru oraz odwołania jego władz (art. 53). Podkreślenia wymaga znaczna rozbudowa katalogu zadań, przy czym w dużej mierze znalazły się w nim czynności wykonywane także pod rządami wcześniejszej dyrektywy (w szczególności rozpatrywanie skarg, udzielanie informacji, zatwierdzanie wiążących reguł korporacyjnych, wydawanie decyzji indywidualnych). Do nowości należą czynności związane z mechanizmami wprowadzonymi mocą rozporządzenia, w szczególności związane z certyfikacją administratorów (organ „zachęca do ustanawiania mechanizmów certyfikacji”, „dokonuje przeglądu udzielonych certyfikacji”, „opracowuje kryteria akredytacji podmiotów certyfikujących” oraz „dokonuje akredytacji”) oraz wprowadzaniem i stosowaniem kodeksów postępowania (które były znane pod rządami dyrektywy, ale w praktyce wcale niestosowane lub stosowane rzadko). Uprawnienia organów nadzorczych także uległy ewolucji i chociaż nadal koncentrują się na obszarach dochodzeniowych, interwencyjnych i procesowych, to, z uwagi na formę aktu prawnego łączącą się z jego bezpośrednią stosowalnością, te zostały uszczegółowione i częściowo rozszerzone. Rozbudowany został katalog sankcji i działań naprawczych, które można zastosować – włączając w to wydawanie ostrzeżeń, upomnień, nakazów, ograniczeń i czasowych lub bezterminowych zakazów przetwarzania danych. Nowością jest też możliwość zastosowania administracyjnej kary pieniężnej, środka znanego od lat z unijnych przepisów o ochronie konkurencji511.

511 Także prawodawca w motywie 150 ogólnego rozporządzenia wskazuje na analogie rozwiązania przyjętego w zakresie regulacji i nadzoru nad obszarem przetwarzania danych do definicji stosowanych w przepisach o ochronie konkurencji i konsumentów (art. 101 i 102 TFUE).
4.5.4.2. Współpraca międzynarodowa i mechanizm spójności

Zagadnieniem powiązanym z krajowym nadzorem nad stosowaniem przepisów o ochronie danych osobowych jest także współpraca na poziomie unijnym, ukierunkowana na zapewnienie spójności krajowych regulacji. Ponieważ projektując przepisy dyrektywy 95/46, zakładano, że europejski system ochrony danych osobowych będzie wdrażany i stosowany głównie na poziomie organów krajowych, zdecydowano, że koordynacja na szczeblu unijnym będzie ograniczona do niezależnego ciała doradczego – powołaną na mocy art. 29 dyrektywy Grupę Roboczą (ang. Art 29 Working Party, WP29). Grupa Robocza składa się z przedstawicieli poszczególnych organów nadzorczych ustanowionych w państwach członkowskich oraz UE, a także przedstawiciela Komisji. Dysponuje uprawnieniami o charakterze doradczym, dotyczącym głównie opracowywania opinii i wytycznych w zakresie stosowania poszczególnych przepisów dyrektywy oraz krajowych środków przyjętych na jej mocy, a celem jej działania jest wypracowanie jednolitego stopnia ochrony na obszarze UE. Wydawane dokumenty nie mają charakteru prawnie wiążącego, zarówno względem instytucji Unii, jak i organów nadzorczych państw członkowskich. W związku z tym zajęcie przez Grupę stanowiska w określonej sprawie nie skutkowało per se ustaleniem obowiązującej interpretacji przepisów lub praktyki organów nadzoru. Ograniczenie to nie zmniejszyło jednak znaczenia i dorobku Grupy dla rozwoju, ukształtowania oraz stosowania prawnych środków ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Opinie wydawane przez Grupę były brane pod uwagę zarówno przez instytucje UE, państwa członkowskie, a także organy nadzoru powołane przez te państwa. Miały istotny wpływ na kształtowanie prawa Unii w zakresie interpretacji unijnych przepisów o ochronie danych osobowych512. Grupa obok opiniowania spraw bieżących wydała szereg wytycznych w kwestiach związanych z nowymi zagrożeniami dla ochrony prywatności, w tym wskazujących na potrzebę dostosowania istniejących regulacji do pojawiających się technik gromadzenia i przetwarzania danych513. Brała również aktywy udział w pracach nad ramami reformy europejskich przepisów, w wyniku której przyjęto rozporządzenie 2016/679514. W rezultacie nie można przecenić dorobku Grupy dla ewolucji europejskiego

512 Zob. np. wyroki TSUE w sprawach T-194/04 (p. 79); opinie rzeczników generalnych w sprawach C-275/06 (p. 33), C-201/14 (p. 68), C-13/16 (p. 64).
513 Zob. np. opinia 05/2012 dotycząca przetwarzania w chmurze (WP 196), opinia 08/2014 dotycząca rozwoju Internetu Rzeczy (WP 223), opinia 01/2015 dotyczącego aspektów ochrony prywatności w odniesieniu do używania dronów (WP 231).
514 Poza aktywnym udziałem w pracach związanych z opracowaniem i przyjęciem rozporządzenia, WP29 przygotowała także liczne dokumenty dotyczące wdrożenia i zasad stosowania rekompensacji – zob. np.
myślenia o ochronie danych osobowych, a oceny tej w żaden sposób nie umniejsza wyłącznie doradczy charakter wypracowanych przez nią dokumentów.

Wraz z rozpoczęciem stosowania rozporządzenia 2016/679 Grupa Robocza art. 29 zostanie zastąpiona przez nowo powołane ciało – Europejską Radę Ochrony Danych (EROD). Skład Rady ma być podobny do wcześniej działającej Grupy i obejmie szefów organów nadzorczych działających w państwach członkowskich, Europejskiego Inspektora Ochrony Danych, nieposiadającego prawa głosu przedstawiciela Komisji. Wraz z rozszerzeniem kompetencji Rady zdecydowano o jej zinsytualizowaniu poprzez nadanie jej osobowości prawnej (art. 68 ust. 1). Oznacza to, że Rada – inaczej niż wcześniej Grupa Robocza – będzie organem UE. Zadania wykonywane przez EROD będą stanowiły rozwinięcie wcześniejszych kompetencji Grupy, w szczególności związanych z pełnieniem funkcji konsultacyjnej i doradczej w zakresie stosowania wiążących reguł korporacyjnych, standardowych klauzul umownych czy decyzji o adekwatności zabezpieczeń. Ponadto Rada będzie realizowała nowe zadania, związane ze stosowaniem i nadzorowaniem środków ochrony danych wprowadzonych mocą rozporządzenia (akredytacja podmiotów certyfikujących, opracowywanie wytycznych dla mechanizmów certyfikacji, wydawanie opinii dotyczących decyzji opartych na profilowaniu itp.). Rada w zakresie realizowanych zadań nie będzie posiadała funkcji zwierzchnich nad krajowymi organami nadzoru, jej rola ograniczy się do wydawania wytycznych, zaleceń i określania najlepszych praktyk.

Zmianą o fundamentalnym znaczeniu jest jednak wprowadzenie mocą art. 63 nowego mechanizmu spójności, służącego wypracowaniu wspólnych zasad ochrony danych na terenie Unii oraz rozwiązywaniu sporów w zakresie stosowanie przepisów przez różne krajowe оргany nadzorcze. W tym celu Rada zostanie wyposażona w uprawnienie podejmowania wiążących decyzji, mających zastosowanie do wszystkich krajowych organów nadzoru. Uprawnienie Rady będzie ograniczone do dwóch przypadków. Pierwszy to rozstrzyganie sporu pomiędzy organem, którego sprawa dotyczy, a wiodącym organem nadzorczym w przypadku realizacji procedury zatwierdzania wiążących reguł korporacyjnych w odniesieniu do administratora działającego w więcej niż jednym państwie członkowskim. Drugi przypadek dotyczy pominięcia lub nieuwzględnienia obowiązkowej opinii Rady w procesie wydawania określonych w art. 64 ust. 1 decyzji przez organ krajowy, którego skutki mogą odnosić się także do innych państw członkowskich – a więc w szczególności zatwierdzania standardowych klauzul umownych, wydania decyzji indywidualnej (zewolenia na

wytyczne dla inspektorów bezpieczeństwa informacji (WP243 rev1) czy dotyczące wyznaczania wiodącego organiz nadzoru zgodnie z RODO (WP244 rev1).
stosowanie określonych klauzul umownych), zatwierdzenia wiążących reguł korporacyjnych czy zatwierdzenia kryteriów akredytacji podmiotu lub podmiotu certyfikującego.

W obu przypadkach prawodawca określił wymóg podjęcia decyzji Rady większością dwóch trzecich głosów, a więc bardziej restrykcyjny niż stosowany w sprawach ogólnych (zwykła większość głosów). Możliwość podjęcia przez Radę decyzji prawnie wiążących jest nowym mechanizmem, który w zamierzeniu prawodawcy ma zapewnić spójne stosowanie rozporządzenia oraz ułatwić i skrócić procedurę administracyjną związaną z wydawaniem decyzji nadzorczych względem międzynarodowych administratorów. Niewątpliwie utworzenie Europejskiej Rady stanowi nowy etap w integracji nadzoru nad rynkiem przetwarzania danych, który niewykluczone, że docelowo doprowadzi do utworzenia wspólnego, unijnego nadzorcy.

4.5.4.3. Organy regulacyjne w obszarze ochrony prywatności w łączności elektronicznej

Odrębnym zagadnieniem, wymagającym szerszego omówienia, jest funkcjonowanie organów nadzorczych powołanych na mocy europejskich przepisów o ochronie prywatności w łączności elektronicznej, w szczególności dyrektywy 2002/58. Jak wskazano we wcześniejszych rozdziałach, wskazany akt stanowi lex specialis w obszarze ochrony danych osobowych, co w szczególności oznacza, że w obszarach nieuregulowanych przepisami dyrektywy 2002/58 stosuje się europejskie przepisy o ochronie danych osobowych (wcześniej dyrektywa 95/46, obecnie rozporządzenia 2016/679). To wzajemne i silne powiązanie obu norm prawnych znajduje także odzwierciedlenie w obszarze organów nadzoru i mechanizmów spójności. W motywach przyjęcia dyrektywy 2002/58 wskazano na przydatność w interpretacji jej postanowień dorobku wypracowanego przez Grupę Roboczą Art. 29\textsuperscript{515}. W przeciwieństwie do przepisów o ochronie danych dyrektywa 2002/58 w pierwotnej treści nie wymagała powołania niezależnych organów nadzorczych. Zamiast tego jest w niej mowa o krajowych „organach regulacyjnych”, które powinny dysponować odpowiednimi uprawnieniami i środkami niezbędnymi do prowadzenia dochodzeń, w tym uprawnieniami do uzyskiwania wszelkich istotnych informacji, których mogą potrzebować, aby monitorować i egzekwować przestrzeganie przepisów krajowych przyjętych zgodnie z dyrektywą\textsuperscript{516}. Kwestia niezależności organów regulacyjnych może być natomiast

\textsuperscript{515} Motyw 48. dyrektywy 2002/58.
\textsuperscript{516} Art. 15a ust. 3 dyrektywy 2002/58.
wywiedziona z przepisów dyrektywy 2002/21 (tzw. dyrektywa ramowa), dotyczącej wspólnych ram regulacyjnych sieci i usług łączności elektronicznej. Zgodnie z motywami jej przyjęcia państwa członkowskie powinny zapewnić niezależność krajowych organów regulacyjnych, aby umożliwić im wydawanie decyzji w sposób bezstronny. Zgodnie z art. 3 ust. 2 omawianej dyrektywy niezależność krajowych organów regulacyjnych rozumiana jest jako prawne i funkcjonalne oddzielenie od wszelkich organizacji udostępniających sieci, urządzenia lub usługi łączności elektronicznej. Jest to zatem niezależność w rozumieniu węższym, dotyczącym tylko podmiotów nadzorowanych. W wyniku dokonania okresowego przeglądu funkcjonowania regulacji unijnych składających się na ramy regulacyjne w dziedzinie sieci i usług łączności elektronicznej wprowadzono na mocy dyrektywy 2009/140 nowelizację przepisów dyrektywy 2002/21, skutkującą rozszerzeniem zakresu niezależności organów regulacyjnych. Środkiem do osiągnięcia tego celu było wprowadzenie nowych regulacji prowadzących do zapewnienia ochrony organowi regulacyjnemu podczas wykonywania swoich zadań przed inercją zewnętrzną lub naciskami politycznymi, które mogłyby zagrozić niezależności wydawanych przez niego ocen w sprawach, którymi się zajmuje. W rezultacie zgodnie z wprowadzonym nowym przepisem art. 3a dyrektywy ramowej, „organy regulacyjne odpowiedzialne za regulację rynku ex ante lub rozstrzyganie sporów działają niezależnie i nie występują o instrukcje do żadnego innego podmiotu ani nie przyjmują takich instrukcji w związku z wykonywaniem tych zadań”. Jest to zatem definicja znaczeniowo równoważna przyjętej na gruncie dyrektywy 95/46 – dlatego tezy omówionych wcześniej wyroków TSUE dotyczących niezależności organów ochrony danych osobowych (wydanych na gruncie dyrektywy 95/46) mają także zastosowanie w odniesieniu do organów regulacyjnych wykonujących działania nadzorcze w obszarze ochrony prywatności na rynku łączności elektronicznej (dyrektywa 2002/58).

Kontynuując prace związane z reformą europejskich przepisów o ochronie danych, Komisja przedstawiła projekt nowego rozporządzenia, mającego zastąpić dyrektywę 2002/58. W opublikowanym projekcie Komisja zaproponowała, aby funkcje regulacyjne związane z

517 Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (CELEX: 32002L0021, Dz. Urz. UE z 2002 Nr L 108, s. 33).
519 Dyrektywa Parlamentu Europejskiego i Rady 2009/140/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywy 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, 2002/19/WE w sprawie dostępu do sieci i usług łączności elektronicznej oraz wzajemnych połączeń oraz 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (CELEX: 32009L0140, Dz. Urz. UE z 2009 Nr L 337, s. 37).
520 Motyw 13. dyrektywy 2009/140.
ochroną prywatności w łączności elektronicznej były wykonywane przez krajowe organy ochrony danych osobowych\textsuperscript{521}. Jest to zasadnicza zmiana względem obecnie funkcjonującego w wielu krajach (także Polsce) modelu, w którym nadzór nad monitorowaniem obowiązków związanych z ochroną prywatności w łączności elektronicznej jest sprawowany kompleksowo przez organ regulacyjny właściwy do usług telekomunikacyjnych (w Polsce – Prezes Urzędu Komunikacji Elektronicznej). Przyjęcie propozycji Komisji oznaczałoby, że funkcje te zostaną przekazane do krajowych organów ochrony danych, przyczyniając się tym samym do stworzenia skonsolidowanego nadzoru nad obszarem ochrony danych oraz prywatności w cyberprzestrzeni. W opinii Komisji takie rozwiązanie prowadziłoby do zapewniania pełnej spójności z rozporządzeniem 2016/679\textsuperscript{522}. Propozycja spotkała się jednak z krytyką niektórych państw członkowskich, co zostało odnotowane we wstępnej opinii Rady na temat omawianego projektu\textsuperscript{523}.

4.5.5. 	extit{Ochrona prywatności w łączności elektronicznej}

Od początku wprowadzania europejskie regulacje związane z obszarem ochrony danych osobowych oraz ochrony prywatności w łączności elektronicznej były wzajemnie powiązane. Pakiet propozycji przygotowany przez Komisję i opublikowany w 1990 roku, w którym zaprezentowano pierwszy projekt dyrektywy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych (późniejsza dyrektywa 95/46), zawierał także propozycję dyrektywy w obszarze ochrony prywatności w sektorze publicznych usług telekomunikacyjnych (późniejsza dyrektywa 97/66).

Powodem dla wprowadzenia oddzielnego aktu prawnego w zakresie ochrony prywatności w łączności elektronicznej był postęp techniczny związany z rozwojem cyfrowych usług telefonicznych, w szczególności związanych z technologią ISDN (\textit{Integrated Services Digital Network}). Usługi ISDN były świadczone za pośrednictwem standardowych łączy telekomunikacyjnych, jednak dzięki wykorzystaniu cyfrowych protokołów komunikacji pozwalały na zaoferowanie i dostarczanie użytkownikom wielu nowych, wcześniej nieznanych usług telekomunikacyjnych – takich jak identyfikacja numeru wywołującego, obsługa skrzynek głosowych po stronie operatora telekomunikacyjnego czy przekazywanie

\textsuperscript{521} Art. 18 ust. 1 przedstawionego przez KE projektu rozporządzenia zastępującego dyrektywę 2002/58 (CELEX: 52017PC0010).
\textsuperscript{522} Motyw 38. przedstawionego przez KE projektu rozporządzenia zastępującego dyrektywę 2002/58 (CELEX: 52017PC0010).
\textsuperscript{523} Council of European Union, \textit{Regulation on Privacy and Electronic Communications – Progress report...}, 9324/17, op. cit., s. 5.
wiadomości tekstowych (będących de facto prekursorem znanych z telefonii mobilnej wiadomości SMS). Ponadto wprowadzenie infrastruktury cyfrowej pozwoliło na oferowanie usług telekomunikacyjnych abonentom przez podmioty niebędące operatorami (właścicielami) sieci telekomunikacyjnej. Pojawienie się dostawców usług jako samodzielnego uczestnika rynku telekomunikacyjnego wymagało doprecyzowania wzajemnych relacji i obowiązków pomiędzy nimi a operatorami infrastruktury, także w obszarze bezpieczeństwa świadczonych usług, którego elementem jest zapewnienie poufności transmisji. Nowe możliwości związane z wykorzystania usług cyfrowych rodziły też obawy pod kątem ochrony prywatności – w szczególności związane z możliwością gromadzenia i przetwarzania przez dostawców usług oraz operatorów telekomunikacyjnych rozbudowanego zestawu informacji dodatkowych na temat abonentów i sposobów korzystania przez nich usług, włączne z możliwością rejestrowania czy innego przechwytywania informacji przekazywanych za pośrednictwem sieci telekomunikacyjnej. Warto pokreślić, że pomimo znacznego rozwoju technologii obawy te są aktualne i nadal odzwierciedlają zagrożenia i ryzyka związane z wykorzystywaniem nowoczesnych usług telekomunikacyjnych.

Dyrektywa 97/66 nakładała trzy najważniejsze obowiązki związane z ochroną prywatności w publicznych sieciach telekomunikacyjnych:

- bezpieczeństwo (art. 4) – nakaz wdrożenia środków technicznych i organizacyjnych przez dostawców usług oraz operatorów infrastruktury potrzebnych do zapewnienia bezpieczeństwa świadczonych usług, z uwzględnieniem możliwości technicznych, kosztów ich wprowadzenia oraz występujących ryzyk;

- poufność komunikacji (art. 5) – obowiązek zapewnienia przez państwa członkowskie za pośrednictwem przepisów prawa krajowego poufności komunikacji w publicznych sieciach oraz publicznie dostępnych usługach telekomunikacyjnych; w szczególności zakaz słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, za wyjątkiem realizacji przewidzianych w prawie wyłączeń określonych w art. 14;

- przetwarzanie danych o wykorzystaniu usług (art. 6) – informacje gromadzone i przetwarzane przez dostawcę usług lub infrastruktury telekomunikacyjnej związane z użytkownikami muszą być zanonimizowane lub usuwane
niezwłocznie po zakończeniu połączenia, za wyjątkiem uzasadnionych potrzeb związanych z rozliczaniem usług.

Powyższe trzy wymagania i wynikające z nich zasady stały się podstawą dla funkcjonującego w UE modelu ochrony prywatności w łączności elektronicznej. W praktycznie niezmienionej postaci zostały odzwierciedlone w późniejszych aktach prawnych, w tym w dyrektywie 2002/58 oraz projekcie nowego rozporządzenia, którego projekt został przedstawiony przez KE w styczniu 2017 roku.

Prawodawca uregulował także w przepisach dyrektywy 97/66 szereg innych elementów, związanych z świadczeniem cyfrowych usług telekomunikacyjnych – takich jak możliwość ograniczenia przez abonenta przekierowań przychodzących na numer jego terminalu (art. 10), zakres informacji udostępnianych w tradycyjnych lub elektronicznych książkach telefonicznych (art. 11) czy zakaz używania automatycznych systemów wykonujących połączenia bez wcześniejszej i wyraźnej zgody abonentów, na których terminale połączenia takie byłyby realizowane (art. 12).

Z uwagi na stosunkowo wąski zakres przedmiotowy regulacji – obejmujący wyłącznie publicznie dostępne usługi świadczone za pośrednictwem publicznych sieci telekomunikacyjnych (w szczególności sieci ISDN oraz sieci komórkowych) – oraz biorąc pod uwagę dynamiczny postęp technologiczny w usługach komunikacji cyfrowej, spowodowany między innymi rozwojem sieci Internet, wkrótce po przyjęciu dyrektywy konieczne było przeprowadzenie jej gruntownej nowelizacji. W szczególności praktyczną trudność stanowiło ustalenie granic stosowania dyrektywy z uwagi na interpretację terminu „publicznie dostępny” w kontekście usługi i sieci telekomunikacyjnej. Niejasności wiązały się też z samą definicją usługi telekomunikacyjnej w brzmieniu przedstawionym w art. 2 pkt d dyrektywy. Niektóre z nich stały się przedmiotem orzeczeń TSUE. W sprawie UPC Nederland BV Trybunał uznał, że usługa polegająca na dostarczaniu pakietu programów radiowych i telewizyjnych drogą kablową, za którą wystawiany jest rachunek obejmujący zarówno koszty transmisji, jak i wynagrodzenie stacji nadawczych oraz opłaty na rzecz organizacji zbiorowego zarządzania prawami autorskimi w związku z rozpowszechnieniem treści utworów, wchodzi w zakres pojęcia „usługa łączności elektronicznej”. W efekcie usługi świadczona przez operatorów sieci kablowych zostały objęte zakresem stosowania dyrektywy 97/66. Z kolei w sprawie ze skargi Komisji przeciwko Holandii Trybunał wypowiedział się

Wyrok TSUE z 7.11.2003 w sprawie UPC Nederland BV, sygn. C-518/11, p. 47.
w zakresie możliwości stosowania wyjątków od reguły ustanowionej w art. 6 dyrektywy (nakaz ograniczonego wykorzystania danych dotyczących użycia usług zawierających informacje o abonentach)\textsuperscript{525}. Wyroki te, chociaż dotyczą nieaktualnego stanu prawnego, nie tracą na aktualności z uwagi na funkcjonowanie w obowiązujących obecnie przepisach (w szczególności dyrektywie 2002/58) analogicznych do badanych przez Trybunał rozwiązań prawnych.

W przyjętej 12 lipca 2002 roku dyrektywie 2002/58 dostosowano wprowadzony w przepisach dyrektywy 97/66 model ochrony prywatności do aktualnych postępów technicznych oraz form komunikacji, coraz szerzej wykorzystywanych przez abonentów. Jak wskazał prawodawca, konieczność zmiany dyrektywy 97/66 wynikała z rozwoju rynku i technologii w usługach łączności elektronicznej i była podyktowana zapewnieniem równego poziomu ochrony danych osobowych i prywatności użytkowników dostępnych publicznie usług łączności elektronicznej, bez względu na zastosowane technologie. Stąd główny nacisk położono na zmianę definicji i terminologii – w szczególności na zastąpienie odniesień do sieci i usług „telekomunikacyjnych” wskazaniem na sieci i usługi „łączności elektronicznej”.

W ten sposób zakresem przepisów objęte zostały nie tylko połączenia głosowe czy usługi dodane świadczone z wykorzystaniem infrastruktury operatorów telekomunikacyjnych, ale również zyskujące wówczas na popularności usługi dostępu do Internetu czy poczty elektronicznej. Co do zasady utrzymano trzy podstawowe obowiązki nałożone na dostawców usług oraz infrastruktury komunikacyjnej – związane z zapewnieniem bezpieczeństwa przetwarzania, zachowaniem poufności komunikacji oraz ograniczeniem wykorzystania danych dotyczących abonentów, z tą różnicą, że z uwagi na zmianę zakresu podmiotowego dyrektywy obowiązki te były adresowane do szerszego kręgu podmiotów.

W wyniku okresowego przeglądu ram regulacyjnych dotyczących sieci i usług łączności elektronicznej\textsuperscript{526}, realizowanego przez Komisję, którego celem było w szczególności określenie potrzeby zmian w świetle rozwoju techniki i sytuacji rynkowej, zaproponowano przyjęcie pakietu zmian do istniejących dyrektyw, między innymi dyrektywy 2002/58. W rezultacie przyjętej 25 listopada 2009 dyrektywy 2009/136 istniejące obowiązki wynikające z dyrektywy 2002/58 zostały doprecyzowane i dostosowane do aktualnego rozwoju rynku łączności elektronicznej. Z punktu widzenia użytkowników najczęściej zauważaną zmianą było dodanie w art. 5 ust. 3 obowiązku uzyskiwania zgody ona

\textsuperscript{525} Wyrok TSUE z 24.06.2004 w sprawie Komisja v. Holandia, sygn. C-350/02.

\textsuperscript{526} Pod terminem tym wprawie UE należy rozumieć pięć aktów prawnych (dyrektyw), wskazanych między innymi w motywie 1. dyrektywy 2009/136 (CELEX: 32009L0136).
przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym. Biorąc pod uwagę powszechne wykorzystywanie w serwisach internetowych tzw. plików cookies, przyjęta nowelizacja dyrektywy wiązała się z nałożeniem na wydawców treści internetowych obowiązku informowania o stosowanej polityce prywatności w odniesieniu do plików cookies oraz uzyskiwaniu zgody użytkownika na gromadzenie i zapisywanie tych danych na jego urządzeniu końcowym (np. komputerze osobistym). Do dzisiaj informacja na ten temat jest obowiązkowym elementem każdego serwisu internetowego, którego wydawca jest zobowiązany do stosowania przepisów dyrektywy 2002/58.

Oddzielne zagadnienie stanowi jednak ocena, czy mechanizm ten należy uznać za skuteczny i efektywny w podnoszeniu świadomości użytkowników oraz zmniejszaniu zagrożeń dla ich prywatności. Wiele przesłanek wskazuje, że tak nie jest. W pierwszej kolejności należy zauważyć, że masowo realizowany obowiązek informacyjny (wyświetlanie podobnie wyglądających okienek na każdej odwiedzanej stronie internetowej) – jakkolwiek służy realizacji obowiązku prawnego – nie prowadzi do zwiększenia świadomości użytkowników co do zakresu informacji przetwarzanych na ich temat. Użytkownicy często nie czytają polityk prywatności w odniesieniu do plików cookie, ograniczają się do mechanicznego akceptowania ich treści, aby móc szybciej rozpocząć interakcję z przeglądaną stroną internetową. Z drugiej strony wydawcy treści stosują często generyczne polityki, zbyt ogólne i niedostosowane do specyfiki stosowanych czynności przetwarzania. W efekcie użytkownik nie otrzymuje wystarczających informacji, aby podjąć świadomą decyzję w zakresie wyrażenia zgody na gromadzenia określonych kategorii informacji na swój temat i zapisywania ich w plikach cookies. Realizacja obowiązków informacyjnych w zakresie plików cookies nie spełniła także swojej funkcji w zakresie ograniczenia stosowania technik profilowania użytkowników, bowiem rozwój techniki spowodował, że nawet z pozoru nieistotne i niewrażliwe informacje zapisane w pliku cookies (o zakresie których został poinformowany użytkownik) mogą być w dalszym etapie w wyniku stosowania zaawansowanych algorytmów korelacji danych wykorzystane do stworzenia rozbudowanego profilu zachowania i preferencji użytkownika, daleko wykraczającego poza zakres informacji przechowywanych w pliku cookies. Realizacja obowiązku wynikającego z art. 5 ust. 3 dyrektywy 2002/58 zwiększyła świadomość użytkowników końcowych na temat

527 Więcej informacji na temat plików cookies, w tym ich typów oraz znaczenia, w: S. Piątek, Prawne warunki stosowania cookies, IKAR 2015, nr 6, s. 6.
528 Por. także uwagi Grupy Roboczej Art. 29 przedstawione w opinii 3/2016 (WP 214), s. 11.
powszechności i ilości przetwarzanych na ich temat informacji przez wydawców treści internetowych. Przyczyniła się także do upowszechnienia wiedzy na temat istnienia technik ochrony prywatności w cyberprzestrzeni jak i stała się impulsem do rozwoju mechanizmów bezpieczeństwa w przeglądarkach internetowych oraz innych narzędzi informatycznych skutkujących zwiększeniem poziomu prywatności użytkowników sieci Internet.

Istotnym zagadnieniem związanym z funkcjonowaniem dyrektywy 2002/58 oraz mającym bezpośredni wpływ na realizację gwarancji związanych z ochroną prywatności jest kwestia prawnego uregulowania w państwach członkowskich możliwości stosowania retencji danych. Pod terminem tym należy rozumieć obowiązek czasowego zatrzymania przez dostawcę usług lub operatora telekomunikacyjnego danych związanych ze sposobem korzystania z usług (w szczególności – w przypadku połączeń głosowych – takich informacji, jak numery wywoływane, czas połączenia, informacja o komunikujących się stronach). Celem gromadzenia tych danych jest ułatwienie prowadzenia postępowań związanych z wykrywaniem i ściganiem najpoważniejszych przestępstw czy realizacją podstawowych funkcji państwa, takich jak zapewnienie porządku czy bezpieczeństwa publicznego. Co do zasady – zgodnie z art. 6 ust. 1 dyrektywy – dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu. Prawodawca przewidział jednak w art. 15 ust. 1 możliwość stosowania przez państwa członkowskie wyjątku od tej zasady, motywowanego względami bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego czy zapobiegania przestępstwom, ich dochodzenia, wykrywaniu lub karaniu. W szczególności przepis ten pozwala na uchwalanie krajowych środków ustawodawczych wprowadzających ogólny obowiązek zatrzymania danych na określony czas.\footnote{Por. także rozważania na temat ogólnego obowiązku retencji danych w prawodawstwie polskim – rozdział 8.4.3 (s. 351).}

Uszczegółowieniem (lex specialis) zasad w zakresie retencji danych była przyjęta 15 marca 2006 roku dyrektywa 2006/24, w której przyjęto jako zasadę obowiązek stosowania niezróżnicowanego (dotyczącego wszystkich abonentów) obowiązku przechowywania danych dotyczących korzystania z usług przez okres nie krótszy niż 6 oraz nie dłuższy niż 24 miesiące. Dodatkowo w dyrektywie wskazano szczegółowy zakres informacji, jaki powinien być gromadzony – z podziałem na usługi telefonii stacjonarnej i komórkowej oraz usługi dostępu internetowego, poczty elektronicznej i telefonii internetowej.
Wprowadzenie dyrektywy 2006/24 miało doprowadzić do ujednolicenia krajowych przepisów związanych z retencją danych, dlatego też – podobnie jak w przypadku dyrektywy 2002/58 – jako przepis kompetencyjny wskazano art. 100a TFUE (obecnie 104 TFUE), dotyczący harmonizacji rynku wewnętrznego. Od początku wprowadzenia dyrektywy retencyjnej nałożenie obowiązku przechowywania danych oraz zakres gromadzonych danych budziły zastrzeżenia niektórych państw członkowskich i organizacji zajmujących się ochroną praw człowieka. Efektem tych wątpliwości były sprawy zawisłe przed Trybunałem Sprawiedliwości – w których kolejno kwestionowano ważność dyrektywy retencyjnej z uwagi na wydanie jej w oparciu o błędną podstawę prawną, jak i jej zgodność z przepisami wyższego rzędu (w szczególności dyrektywą 2002/58 oraz art. 7 i 8 KPP). Chociaż Trybunał uznał, że podstawa formalna wprowadzenia dyrektywy retencyjnej była prawidłowa i wiązała się z funkcjonowaniem rynku wewnętrznego⁵³⁰, to stwierdził także nieuzasadnioną i nieproporcjonalną ingerencję zastosowanego środka w prawa podstawowe oraz gwarancje wynikające z art. 7 i 8 KPP⁵³¹. W efekcie Trybunał uznał, że prawodawca unijny przekroczył swoje kompetencje i orzekł o nieważności dyrektywy.

W kolejnych sprawach kierowanych do Trybunału kwestionowana była też zgodność z prawem UE krajowych mechanizmów retencji danych przewidujących obowiązek ogólnego i niezróżnicowanego gromadzenia informacji o wykorzystaniu usług telekomunikacyjnych. W precedensowym orzeczeniu Tele2 Trybunał wskazał, że art. 15 ust. 1 dyrektywy 2002/58 stoi na przeszkodzie istnieniu przepisów krajowych zakładających uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej⁵³². Trybunał podkreślił, że ogólny obowiązek zatrzymania danych nie może być pogodzony z poszanowaniem zasady proporcjonalności, wynikającej z art. 15 ust. 1 dyrektywy⁵³³.

Dyrektywa 2002/58 stanowi jeden z kluczowych elementów europejskiego modelu ochrony prywatności w cyberprzestrzeni. Wprowadzone mocą jej postanowień obowiązki, nakazy, prawa i gwarancje przyczyniły się do zwiększenia ochrony jednostek zarówno przed zagrożeniami horyzontalnymi (ochrona przed niechcianymi informacjami, wykorzystywanie usług telekomunikacyjnych do celów marketingowych, gromadzeniem

⁵³⁰ Wyrok TSUE z 10.02.2009 w sprawie Irelandia v. PE i Radzie, sygn. C-301/06, p. 85-94.
⁵³¹ Wyrok TSUE z 8.04.2014 w sprawie Digital Rights Ireland, sygn. C-293/12 i C-594/12, p. 69.
⁵³² Wyrok TSUE z 21.12.2016 w sprawie Tele2, sygn. C-293/12 i C-594/12, p. 112.
⁵³³ Por. rozważania nt. zasady proporcjonalności na tle EKPC (s. 65), KPP (s. 74) oraz Konstytucji (s. 91).
rozbudowanego zbioru informacji na temat użytkowników usług), jak i wertykalnymi (w odniesieniu do ogólnego obowiązku retenции danych).

Istniejące przepisy nie są jednak doskonałe, w szczególności w niewystarczający sposób obejmują nowoczesne środki komunikacji realizowane za pośrednictwem sieci Internet, które w literaturze przedmiotu określa się terminem usług OTT (ang. over-the-top)\(^\text{534}\). Obejmują one swoim zasięgiem szeroki zestaw usług, począwszy od usług głosowych VoIP (ang. Voice over IP), komunikatorów internetowych czy mediów strumieniowych. Cechą wspólną wszystkich tych rozwiązań jest korzystanie z Internetu jako medium transmisyjnego. W efekcie stosowany w dyrektywie 2002/58 podział na dostawców publicznie dostępnych usług łączności elektronicznej oraz operatorów publicznej sieci łączności okazuje się niepełny, bowiem dostawcy usług OTT nie należą do żadnej z tych kategorii. Jednocześnie biorąc pod uwagę, że obecnie z rozwiązań tego typu korzystają miliardy użytkowników na świecie, a także setki milionów w obrębie UE, istnienie tego typu luki prawnej musi prowadzić do wniosku, że funkcjonujące regulacje powinny być znówelizowane. Problem ten zauważyła również Komisja Europejska, wskazując, że „dyrektywa [2002/58 – przyp. autora] nie nadąża za rozwojem technologicznym, co skutkuje brakiem ochrony komunikacji przekazywanej za pośrednictwem nowych usług”\(^\text{535}\). W rezultacie Komisja przedstawiła projekt nowego rozporządzenia mającego zastąpić dyrektywę 2002/58. Z uwagi na trwającą procedurę legislacyjną ostateczny kształt nowej regulacji i termin jej wprowadzenia w życie nie jest jednak w tym momencie znany\(^\text{536}\).

4.5.6. Współpraca policyjna i sądowa w sprawach karnych

Zgodnie z zasadą przyznającą wynikającą z art. 5 TUE\(^\text{537}\) Unia dysponuje jedynie takimi kompetencjami, jakie zostały jej wprost przyznane w traktatach. Istniejące przed reformą Lizbońską przepisy prawa pierwotnego wyłączały określone obszary działalności państw spod zakresu stosowania prawa unijnego (wspólnotowego) – w szczególności dotyczyło to działań wymienionych w tytule V i VI TUE\(^\text{538}\), a więc związanych między

\(^{534}\) Por. rozważania nad zakresem definicji OTT przedstawione w analizie przygotowanej na zlecenie Parlamentu Europejskiego, *Over-the-Top (OTTs) players: Market dynamics and policy challenges*, PE 569.979, www.europarl.europa.eu/supporting-analyses, s. 21 i n.
\(^{535}\) Por. przyczyny i cele wniosku wskazane w projekcie KE rozporządzenia zastępującego dyrektywę 2002/58, CELEX 52017PC0010, s. 2.
\(^{536}\) Szersze omówienie projektu wraz z krytycznymi uwagami Rady oraz WP29 przedstawiano w rozdziale 4.2 (s. 131).
\(^{537}\) Przed reformą Lizbońską art. 5 TWE.
\(^{538}\) W brzmieniu TUE obowiązującym do zmian wprowadzonych reformą Lizbońską (por. wersja skonsolidowana Traktatu, Dz. Urz. UE z 2006 Nr C 321E, s. 1).
innymi z obszarami bezpieczeństwa publicznego, obronności oraz współpracy w zakresie prawa karnego. Brak przyznania Unii kompetencji w tych obszarach stał na przeszkodzie wypracowaniu i przyjęciu wspólnych regulacji z wykorzystaniem ogólnych zasad stanowienia prawa wtórnego, np. w oparciu o mechanizm dotyczący harmonizacji rynku wewnętrznego. W rezultacie przepisy dyrektywy 95/46 nie obejmowały działalności podejmowanych przez państwa w zakresie organów ścigania oraz wymiaru sprawiedliwości, w tym takich działań, jak gromadzenie i przetwarzanie danych na potrzeby wykrywania i zapobiegania przestępczości, jak również prowadzenia postępowań przygotowawczych, ścigania czynów zabronionych oraz wykonywania kar.

Środkiem zbliżania ustawodawstw w obszarze współpracy w sprawach karnych, przewidzianym w prawie pierwowzorowym przed reformą lizbońską, była możliwość wydawania przez Radę UE podejmowanych jednomyślnie decyzji ramowych w trybie określonym w art. 34 TUE. Decyzje takie wiązały państwa członkowskie w odniesieniu do rezultatu, który miał być osiągnięty, pozostawiały jednak organom krajowym swobodę wyboru formy i podejmowanych środków. Nie mogły także wywoływać skutku bezpośredniego. Mechanizm ten został wykorzystany do wydania decyzji ramowej 2008/977 z dnia 27 listopada 2008 w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. Zakresem stosowania decyzji były objęte czynności przetwarzania, jeżeli dane miały zostać przekazywane poza granicę państwa członkowskiego. Zakresem przedmiotowym nie objęto zatem całego obszaru przetwarzania danych w sprawach karnych, a tylko kwesię współpracy międzynarodowej i transgranicznego przetwarzania danych. To zasadnicze ograniczenie powodowało, że trudno uznać omawianą decyzję ramową jako uzupełnienie lub przeniesienie ogólnych zasad przetwarzania danych osobowych wynikających w szczególności z dyrektywy 95/46, na organy policyjne i wymiar sprawiedliwości państw członkowskich.

W zakresie przepisów materialnych w decyzji ramowej zastosowano wybrane regulacje dyrektywy 95/46. W szczególności wprowadzony model ochrony danych osobowych opierał się na tych samych podstawowych zasadach przetwarzania (zasada legalności, proporcjonalności i celowości). Znacznie ograniczone zostały obowiązki informacyjne oraz prawa podmiotu danych. Mocą decyzji nie powołano żadnego organu doradczego, podobnego do Grupy Roboczej Art. 29, który mógłby pomóc w wypracowaniu

539 Por. treść motywu 13. dyrektywy 95/46.
540 Por. treść art. 3 ust. 2 tiret 1 dyrektywy 95/46.
541 Wersja skonsolidowana Traktatu, Dz. Urz. UE z 2006 Nr C 321E, s. 1.
wspólnego podejścia do interpretacji i wdrażania poszczególnych przepisów decyzji we wszystkich państwach członkowskich. Ponadto, jak podkreśliła w późniejszych analizach Komisja, praktyczne stosowanie decyzji wiązało się z trudnością związaną z nie zawsze łatwym rozróżnieniem pomiędzy przetwarzaniem mającym charakter czysto wewnętrzny oraz przetwarzaniem transgranicznym.\(^{542}\)

Wprowadzone wraz z reformą lizbońską zmiany traktatowe pozwoliły na objęcie przepisami prawa UE obszaru przetwarzania danych osobowych w zakresie współpracy policyjnej i sądowej. Możliwość taka została już zasygnalizowana w deklaracji 21 dołączonej do Akta końcowego konferencji międzyparlamentarnej, która przyjęła Traktat z Lizbony.\(^{543}\) We wczesnych dokumentach dotyczących planowanej reformy przepisów o ochronie danych osobowych Komisja Europejska sygnalizowała możliwość objęcia obszaru współpracy w sprawach karnych projektowanym ogólnym rozporządzeniem o ochronie danych.\(^{544}\) Biorąc pod uwagę trudności w wypracowaniu jednolitego i spójnego modelu ochrony danych, obejmującego specyfikę funkcjonowania organów policyjnych i sądowych we wszystkich państwach członkowskich, okazało się, że bardziej właściwą formą ustawodawczą w tym obszarze jest dyrektywa. W rezultacie 25 stycznia 2012 roku Komisja Europejska przedstawiła projekt dyrektywy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, która po zatwierdzeniu w procedurze legislacyjnej została przyjęta jako dyrektywa 2016/680.\(^{545}\)

---

\(^{542}\) Zob. np. komunikat KE „Całościowe podejście…”, COM (2010) 609, s. 15.

\(^{543}\) W konsekwencji wprowadzenia reformy lizbońskiej zmodyfikowano założenia traktatowe związane z ramami funkcjonowania Unii Europejskiej. Odstąpiono od funkcjonującego wcześniej modelu integracji w obrębie trzech filarów, czego efektem było przebudowanie i rozszerzenie przepisów kompetencyjnych UE w zakresie współpracy policyjnej i sądowej w sprawach karnych oraz uchylenie przepisów tytułu VI TUE. W szczególności rozszerzono listę kompetencji dzielonych (niewyłącznych) UE o prawa do przestrzeni wolności, bezpieczeństwa i sprawiedliwości (art. 4 ust. 2 pkt j TUE). Wprowadzono też odrębny przepis kompetencyjny (art. 16 ust. 2 TFUE) stanowiący podstawę do przyjmowania unijnych aktów ustawodawczych w obszarze ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez państwa członkowskie w wykonywaniu działań wpływających w zakres zastosowania prawa Unii.

\(^{544}\) Deklaracja w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej (Dz. Urz. UE z 2012 Nr C 326, s. 347).

\(^{545}\) Komunikat KE „Całościowe podejście…”, COM (2010) 609, s. 16.

\(^{546}\) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (CELEX: 32016L0680, Dz. Urz. UE z 2016 Nr L 119 s. 89).
Z uwagi na nowy – z perspektywy prawa UE – obszar regulacji, określono stosunkowo długi okres na przeprowadzenie implementacji do krajowego porządku prawnego. Zgodnie z art. 18 ust. 1 państwa członkowskie mają czas na wprowadzenie przepisów ustawowych, wykonawczych i administracyjnych do 25 maja 2018 – jest to więc termin zbliżny z rozpoczęciem stosowania przepisów ogólnego rozporządzenia o ochronie danych.

Rozwiązania szczegółowe przyjęte w dyrektywie 2016/680 bazują na rozwiązaniach wprowadzonych w rozporządzeniu 2016/679. Jest to zrozumiałe, zwłaszcza biorąc pod uwagę, że oba akty były procedowane jednocześnie. Dlatego w dyrektywie wykorzystano podobny zestaw definicji, podstawowych zasad przetwarzania, praw podmiotów danych oraz obowiązków realizowanych przez administratorów danych. Z uwagi na specyfikę przetwarzania danych przez organy policyjne oraz wymiaru sprawiedliwości szereg rozwiązań pochodzących z rozporządzenia musiało zostać przebudowanych lub zmodyfikowanych. W odmienny sposób określono legalne podstawy przetwarzania, wskazując, że przetwarzanie jest zgodne z prawem w zakresie, w jakim jest ono niezbędne do wykonywania zadań realizowanych przez właściwy organ w celach określonych w art. 1 ust. 1 dyrektywy. Istnienie podstawy prawnej oraz zgodność tej podstawy z celami przetwarzania wskazanymi w art. 1 ust. 1 jest więc jedynym i niezbędnym warunkiem do gromadzenia i przetwarzania danych. Co oczywiste, w przypadku działalności organów ścigania oraz wymiaru sprawiedliwości dane nie muszą być gromadzone za dobrowolną zgodą podmiotu danych.

Przyjęty model częściowo przypomina rozwiązanie po raz pierwszy zaproponowane w początkach lat siedemdziesiątych dwudziestego wieku w rekomendacjach Rady Europy, w których wskazano zgodę jako najważniejszą podstawę przetwarzania danych w sektorze prywatnym, a istnienie podstawy prawnej jako warunku koniecznego do przetwarzania danych w sektorze publicznym. W dyrektywie przyjęto szeroki zakres praw podmiotu danych, zbliżony do zdefiniowanego w ogólnym rozporządzeniu, natomiast rozbudowano listę przesłanek uzasadniających odmowę wykonania danego żądania przez uprawnione organy. Ponadto wprowadzono odmienne regulacje w zakresie ograniczenia prawa dostępu, które w szczególności może być motywowane dobrem toczącego się postępowania.

547 Dalsze informacje nt. rezolucji Komitetu Ministrów RE nr 73/22 oraz nr 74/29 przedstawiono w rozdziale 3.2 (s. 99).
548 Por. np. wskazane w art. 16 ust. 2 dyrektywy 2016/680 przesłanki ograniczające w części lub całości obowiązek udzielenia informacji o odmowie sprostowania lub usunięcia danych.
urzędowego lub sądowego, postępowania przygotowawczego, wykrywania i ścigania czynów zabronionych czy ochroną bezpieczeństwa publicznego.


Dyrektwy zawiera definicję poważnej przestępczości oraz wprowadza w tym zakresie zamknięty katalog przestępstw (załącznik II). Należy zauważyć, że jest to odmienne rozwiązanie od zastosowanego wcześniej, np. w dyrektywie 2006/24 (dyrektywa retencyjna), gdzie zamiast wprowadzać definicję terminu poważnej przestępczości prawodawca uniarny zdecydował się odwołać do wewnętrznych przepisów państw członkowskich. Ponieważ pojęcie takie nie zostało zdefiniowane w przepisach prawnokarnych większości państw członkowskich, a przynależy bardziej do języka polityki, precyzyjne wyznaczenie jego zakresu nie było prostym zadaniem. Wykaz załączony do dyrektywy 2016/681 obejmuje

549 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przechodu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (CELEX: 32016L0681, Dz.U. UE z 2016 Nr L 119 s. 132).
550 Art. 1 ust. 1 dyrektywy 2006/24.
poza przestępstwami powszechnie kwalifikowanymi jako najpoważniejsze (zorganizowana przestępczość, handel ludźmi, przestępczość narkotykowa, wykorzystywanie dzieci)\(^{552}\), także przestępczość komputerową i cyberprzestępczość.

Zgodnie z art. 12 ust. 1 gromadzone dane mogą być przechowywane przez okres pięciu lat, przy czym po sześciu miesiącach od ich przekazania powinny zostać poddane depersonalizacji polegającej na maskowaniu informacji mogących posłużyć do bezpośredniej identyfikacji pasażera.

Z uwagi na trwający nadal okres \textit{vacatio legis} aktu ocena zgodności zasad retencji danych z gwarancjami wynikającymi z KPP – zwłaszcza w zakresie adekwatności (konieczności) i proporcjonalności wprowadzonej ingerencji w sferę ochrony prywatności – nie mogła być dotychczas przedmiotem badania przez Trybunał Sprawiedliwości. Wydaje się, że w przypadku omawianej dyrektywy prawodawca zastosował się do wniosków płynących z orzeczeń TSUE w sprawach \textit{Digital Rights Ireland} oraz \textit{Tele2}, w szczególności związanych z ograniczeniem zakresu gromadzonych danych oraz kontrolą ich przepływu pomiędzy wyznaczonymi, uprawnionymi jednostkami. W literaturze przedmiotu wskazuje się jednak na niejasności związane ze zgodnością mechanizmu obowiązkowej retencji danych w odniesieniu do wszystkich pasażerów z art. 52 w zw. z art. 7 i 8 KPP\(^{553}\). Wątpliwości te mogą być zasadne, zwłaszcza uwzględniając, że zgodnie z dyrektywą przetrzymywane mają być dane dotyczące osób niemających żadnych – nawet odległych czy pośrednich – powiązań z poważnymi przestępstwami. Analogiczna obserwacja poczyniona w sprawach \textit{Digital Rights Ireland}\(^{554}\) oraz \textit{Tele2}\(^{555}\) doprowadziła TSUE do wniosku, że analizowane regulowania nie wymagały istnienia żadnego związku między danymi, których zatrzymywanie nakazywały, a zagrożeniem dla bezpieczeństwa publicznego – co z kolei prowadziło do wniosku, że badane środki naruszały zasadę proporcjonalności, a w konsekwencji były niezgodne z art. 52 KPP. Obawy te podzielił Europejski Inspektor Ochrony Danych Osobowych w swojej opinii dotyczącej projektu dyrektywy, formułując pytanie o „konieczność i proporcjonalność zatrzymywania identyfikowalnych danych wszystkich pasażerów na okres pięciu lat”\(^{556}\).

\(^{552}\) Por. np. katalog przestępstw, których popełnienie lub podejrzenie uzasadnia zastosowania środka w postaci kontroli i utrwalania treści rozmów telefonicznych – art. 237 §3 kpk.


\(^{554}\) Wyrok TSUE z 8.04.2014 w sprawie \textit{Digital Rights Ireland Ltd}, sygn. C-293/12 i C-594/12, p. 58.


\(^{556}\) Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania (CELEX: 52011XX0622(02), Dz. Urz. UE z 2011 Nr C 181 s. 24).
Chociaż nie wiadomo, czy Trybunał podzieli te obawy i czy uzna je za wystarczające do zakwestionowania ważności przepisów dyrektywy 2016/681, a nawet czy kwestia badania zgodności postanowień dyrektywy z prawem pierwotnym UE (w szczególności KPP) będzie w ogóle przedmiotem rozważań Trybunału, to przedstawione wątpliwości powinny zostać odpowiednio uwzględnione w trakcie implementacji postanowień dyrektywy do krajowego porządku prawnego. Na rolę prawodawcy krajowego w kształtowaniu ostatecznych przepisów w zakresie przetwarzania danych PNR wskazuje także RPO w swoim piśmie z 20 lutego 2017 roku skierowanym do Minister Cyfryzacji.

4.6. Umowy międzynarodowe UE a ochrona prywatności

4.6.1. Wprowadzenie

Wraz z przyjęciem reformy lizbońskiej, osobowość prawna UE została explicite wskazana w art. 47 TUE. We wcześniejszym stanie prawnym uznawano, że podmiotowość prawnomiędzynarodowa Unii wynikała z konieczności realizacji kompetencji przypisanych jej w traktatach.

Podstawowy przepis regulujący zakres zdolności traktatowej UE odnaleźć można w art. 216 TFUE, zgodnie z którym Unia może zawierać umowy z jednym lub z większą liczbą państw trzecich lub organizacji międzynarodowych, jeżeli spełniony jest jeden z następujących warunków:

- przewidują to traktaty;
- zawarcie umowy jest niezbędne do osiągnięcia, jednego z celów, o których mowa w traktatach;
- zawarcie umowy jest przewidziane w prawnie wiążącym aktie Unii;
- zawarcie umowy może mieć wpływ na wspólne zasady lub zmienić ich zakres.

Pierwsza przesłanka nie powinna budzić niejasności i związana jest z sytuacją, gdy państwa członkowskie określiły możliwość przystąpienia do określonej umowy międzynarodowej bezpośrednio w prawie pierwotnym. Przykładem może być prawo (a zgodnie z dominującym w piśmiennictwie poglądem – obowiązek) przystąpienia UE do EKPC (art. 6 ust. 2 TUE). Pozostałe przesłanki pozwalające na zawarcie umowy międzynarodowej wymagają odniesienia jej planowanego zakresu do kompetencji Unii,

559 L. Garlicki, Przystąpienie UE..., op. cit., s. 15.
określonych w traktatach. Unia ma wyłączną kompetencję do zawierania umów międzynarodowych, jeżeli jej zawarcie jest niezbędne do umożliwienia Unii wykonywania jej wewnętrznych kompetencji lub w zakresie, w jakim ich zawarcie może wpływać na wspólne zasady lub zmieniać ich zakres. Innymi słowy, możliwość zawierania umów międzynarodowych dotyczących dziedzin, w których UE posiada wyłączone kompetencje (art. 3 ust. 1 TFUE), ma tylko Unia, a państwa członkowskie pozbawione są możliwości podejmowania własnych autonomicznych działań, a podjęcie takich działań będzie postrzegane jako naruszenie prawa unijnego\textsuperscript{560}. Natomiast w odniesieniu do ostatniej ze wskazanych przesłanek, tj. gdy zawarcie umowy może mieć wpływ na wspólne zasady lub zmienić ich zakres, to zgodnie z ugruntowanym orzecznictwem TSUE istnienie wyłącznej kompetencji zewnętrznej UE wynika z ryzyka naruszenia przez zobowiązania międzynarodowe wspólnych zasad Unii lub naruszenia ich zakresu, ale tylko wówczas, gdy zobowiązania te należą do dziedziny stosowania rzeczonych zasad\textsuperscript{561}. W takim przypadku państwa członkowskie nie mogą, poza ramami instytucji Unii, podjąć takich zobowiązań i to nawet przy braku ewentualnej sprzeczności między tymi zobowiązaniami i wspólnymi zasadami Unii\textsuperscript{562}.

Każdy z powyższych przypadków wiąże się także z różną jurysdykcją TSUE w zakresie oceny zgodności umowy międzynarodowej oraz jej interpretacji w kontekście prawa UE. TSUE ma wyłącznie uprawnienie do badania umów realizujących kompetencje wyłączne, a także traktatów wielostronnych w zakresie, w jakim analizowane przepisy nie odnoszą się do kompetencji wyłącznych państw. Natomiast TSUE nie posiada uprawnień do badania aktów prawnomiędzynarodowych, zawartych przez państwa członkowskie i niedotykających zakresu prawa UE\textsuperscript{563}.

Co do zasady umowy zawarte przez Unię wiążą instytucje UE oraz państwa członkowskie (art. 216 ust. 2). Od momentu wejścia w życie umowa stanowi integralną część porządku prawnego Unii\textsuperscript{564}. W systemie prawa UE umowy międzynarodowe umieszczone są pomiędzy traktatami, z którymi muszą być zgodne, a zwykłymi aktami ustawodawczymi (normami prawa wtórnego).

\textsuperscript{560} M. Niedźwiedź, P. Mostowik, Wspólnota Europejska jako strona umów międzynarodowych w dziedzinie prawa prywatnego międzynarodowego. Uwagi na tle opinii Trybunału Sprawiedliwości WE w sprawie I/03, Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego, vol. VII, A.D. MMIX, s. 74.
\textsuperscript{561} Wyrok TSUE z 4.09.2014 w sprawie Komisja i Parlament v. Radzie, sygn. C-114/12, p. 68.
\textsuperscript{562} Ibidem, p. 71.
\textsuperscript{563} Wyrok TSUE z 4.05.2010 w sprawie TNT Express Nederland BV, sygn. C-533/08, p. 61.
\textsuperscript{564} Wyrok TSUE z 30.04.1974 w sprawie R. & V. Haegeman, sygn. 181-73 p. 5; także wyrok C-366/10, p. 73.
Odrębnym zagadnieniem jest wzajemna relacja w krajowych systemach prawnych zobowiązań wynikających z aktów prawnomiedzynarodowych, których stroną jest bezpośrednio państwo członkowskie do traktatów, zawartych przez UE. Zgodnie z art. 351 TFUE postanowienia traktatów nie naruszają praw i obowiązków wynikających z umów międzynarodowych zawartych przed datą akcesji (w przypadku państw-założycieli, przed datą wejścia w życie traktatów rzymskich, tj. 1 stycznia 1958). Umawiające się strony nie wskazały w traktatach żadnego okresu przejściowego, w którym umowy tego typu powinny być zrewidowane i dostosowana do prawa UE, poprzestając na sformułowaniu, że „w zakresie, w jakim umowy te nie są zgodne z traktatami, dane państwo lub państwa członkowskie zastosują wszelkie właściwe środki w celu wyeliminowania stwierdzonych niezgodności”.

4.6.2. Transgraniczna wymiana informacji o pasażerach

Wykorzystanie danych dotyczących przeletu pasażera (ang. passenger name record, PNR) do celów egzekwowania prawa staje się coraz powszechniejsze i jest coraz częściej postrzegane jako standardowy i konieczny aspekt działań w zakresie egzekwowania prawa. Rekordy PNR są gromadzone przez linie lotnicze i zawierają nie tylko dane osobowe pasażerów (ang. Advanced Passenger Information, API), ale również szereg dodatkowych informacji – takich jak informacja o posiadanych wizach, osobach towarzyszących w podróży, nadanych bagażach, informacje o przynależności do programu lojalnościowego, przydzielonym miejscu w samolocie czy wymaganiach żywieniowych. Dane te są potrzebne operatorom lotniczym do realizacji świadczonej usługi, muszą być także przekazywane innym podmiotom, od których zależne jest prawidłowe wykonanie kompleksowej usługi przewozu pasażerskiego. Dostęp do informacji PNR stanowi przydatne źródło danych dla służb kontroli granicznej, pozwalając one bowiem na odpowiednio wczesne przeprowadzenie weryfikacji (ang. screening) osób, które zamierzają przekroczyć granicę. Dane takie mogą być również gromadzone w celu późniejszej analizy, co pozwala na identyfikowanie osób powiązanych z osobami podejrzewanymi o popełnienie najpoważniejszych przestępstw. Według zaprotokołowanych zeznań przedstawicieli Departamentu Bezpieczeństwa Wewnętrznego USA złożonych przed Podkomitetem ds. Zwalczania Terroryzmu i Wywiadu Izby Reprezentantów USA, analiza danych PNR pozwalała na identyfikowanie około 1750 spraw.

565 Grupa Robocza Art. 29, Opinia 7/2010 dotycząca komunikatu Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przeletu pasažera (PNR) państwowom trzecim, WP 178, s. 2.
każdego roku, a także okazała się pomocna w wielu najbardziej znanych dochodzeniach związanych z terroryzmem po 11 września 2001. Dostęp do danych PNR i przekazywanie ich państwom trzecim od lat budzi niepokój organizacji oraz ekspertów zajmujących się problematyką ochrony prywatności. Jak zauważa J. Laskowski, daleko posunięta swoboda w dysponowaniu danymi wrażliwymi obywateli, wymienianych pomiędzy instytucjami i służbami specjalnymi w celu walki z poważną przestępczością, może tworzyć dość duże pole do nadużyć, a nawet powodować łamanie praw człowieka. Ten sam mechanizm, który może być wykorzystany do celów bezpieczeństwa publicznego, może również znaleźć zastosowanie jako środek inwigilacji dużej części społeczeństwa. Dlatego kontrola nad zakresem i sposobem gromadzenia, przetwarzania i udostępniania danych PNR od lat stanowi przedmiot pogłębionych analiz i dyskusji.

W wyroku Parlament v. Rada TSUE rozstrzygnął, że międzynarodowa wymiana danych PNR jest elementem współpracy w obszarze bezpieczeństwa publicznego, co w stanie prawnym obowiązującym przed reformą lizbońską oznaczało konieczność skorzystania ze środków ustawodawczych właściwych dla tytułu VI traktatu. Wniosek taki wykluczał

566 Written Testimony of David Heyman, Mary Ellen Callahan and Thomas L. Bush before US House Of Representatives, Committee On Homeland Security, Subcommittee On Counterterrorism And Intelligence, homeland.house.gov/files/Testimony%20DHS_0.pdf, s. 2.

567 J. Laskowski, Problemy ochrony danych wrażliwych we współpracy antyterrorystycznej UE i USA, w: Amerykański system ochrony praw człowieka pod red. J. Jaskierni, Wydawnictwo Adam Marszałek 2015, s. 560-561.


Tłem sporu były nowo wprowadzone przepisy o kontroli granicznej, przyjęte w Stanach Zjednoczonych po wydarzeniach 11 września 2001, nakładające na przewoźników lotniczych wykonujących połączenia do Stanów Zjednoczonych lub z tego obszaru konieczność zapewnienia organom celnym elektronicznego dostępu do danych zawartych w automatycznych systemach rezerwacji i kontroli wylotów. Z uwagi na znaczenie ruchu lotniczego pomiędzy UE a USA Komisja i Rada postulowały szybkie uregulowanie przedmiotowej kwestii, przy czym Komisja proponowała wydanie decyzji o adekwatności zabezpieczeń w oparciu o art. 25 dyrektywy 95/46 w odniesieniu do traktatu przeznaczonego do celów bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa, a także w ramach działalności państwa w zakresie prawa karnego (wyrok TSUE z 30.05.2006 w sprawie Parlament v. Rada, sygn. C-317/04, p. 59). Komisja nie mogła zatem wydać decyzji o adekwatności zabezpieczeń, bowiem dyrektywa, która stanowiła podstawę do jej wydania, nie miała zastosowania do spraw dotyczących obszaru bezpieczeństwa publicznego. Z kolei w odniesieniu do decyzji Rady TSUE wskazał – w sposób analogiczny – że wybrany przepis kompetencyjny, tj. art. 95 TWE (obecnie art. 104 TFUE), odpowiadający się do harmonizacji rynku wewnętrznego i zbliżania ustawodawstw, nie znajdował zastosowania w obszarze współpracy policyjnej i sądowej, a także w sprawach karnych (Parlament v. Rada…. p. 63-70).
możliwość zastosowania środków prawnych związanych z harmonizacją rynku wewnętrznego, co de facto oznaczało, że jedynym sposobem udostępnienia tych danych innym państwom są akty prawnomеждуnarodowe.

W rezultacie wszystkie kolejne porozumienia UE z państwami trzecimi, których przedmiotem było przekazywanie i przetwarzanie danych PNR, formalizowane były w postaci umów międzynarodowych. W latach 2006-2010 UE zawarła trzy tego typu umowy – ze Stanami Zjednoczonymi, Kanadą i Australią. W 2010 roku Komisja wydała komunikat w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażyra państwom trzecim570, w którym wskazała konieczność zawarcia nowych umów, uwzględniających nowe ramy prawne po reformie Lizbońskiej571.

Negocjacje dotyczące zawarcia poszczególnych umów były prowadzone jednocześnie, przy czym umowa z Australią została zawarta 14.07.2012 roku572, ze Stanami Zjednoczonymi 11.08.2012573, a umowa z Kanadą została zatwierdzona przez Radę, ale nie weszła w życie z uwagi na skierowany przez Parlament wniosek do TSUE o wydanie opinii w trybie art. 218 ust. 11 TFUE574.

Wszystkie umowy zbudowane zostały w podobny sposób – w szczególności zawierają w treści wszystkie uregulowania związane z określeniem celu, zakresu i sposobu przetwarzania przekazywanych danych. Co do zasady dane mogą być przetwarzane przez wyznaczone оргany państwowe wyłącznie do celów zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości międzynarodowej. W przypadku umowy z Australią przestępstwa terrorystyczne zostały enumeratywnie wymienione, pozostawiając jednak niesprecyzowaną kategorię „powojnej przestępczości międzynarodowej”. Z kolei w umowie z USA zdefiniowano obie kategorie, jednak zamiast wskazać zamknięty katalog przestępstw, strony wskazały przesłanki (okoliczności) wskazujące na podejrzenie popełnienia czynu o charakterze terrorystycznym lub powojnej przestępczości. Ponadto w

571 Rezolucja Parlamentu Europejskiego z 11.11.2010 w sprawie globalnego podejścia do przekazywania krajom trzecim danych dotyczących przelotu pasażyra (PNR) oraz zaleceń Komisji dla Rady dotyczących upoważnienia do podjęcia negocjacji między Unią Europejską a Australią, Kanadą i Stanami Zjednoczonymi, P7_TA(2010)0397, p. 3.
572 Umowa między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służby celnej i granicznej danych dotyczących przelotu pasażyra (danych PNR), CELEX: 22012A0714(01), Dz. Urz. UE z 2012 Nr L 186, s. 4.
573 Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażyra oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, CELEX: 22012A0811 (01), Dz. Urz. UE z 2012 Nr 215, s. 5.
574 Zob. także Rezolucja Parlamentu Europejskiego z dnia 25 listopada 2014 r. w sprawie zasięgniecia opinii Trybunału Sprawiedliwości na temat zgodności z traktatami Umowy między Kanadą a Unią Europejską w sprawie przekazywania i przetwarzania danych dotyczących przelotu pasażyra (PNR), P8_TA(2014)0058.
obu umowach określono wyjątki pozwalające na przetwarzanie danych obywateli UE także do innych celów oraz przez inne organy. W przypadku umowy z Australią wyjątki te zostały ograniczone do sytuacji związanych z jednostkowym dostępem do danych związanym z nadzorem nad działalnością administracji publicznej, w tym złożeniem skargi i dochodzeniem praw (art. 3 ust. 5). Natomiast w umowie ze Stanami Zjednoczonymi dopuszczono kolejny wyjątek – związany z decyzją sądu. W rzeczywistości zapis ten może znacząco osłabiać cały system ochrony danych obywateli UE, z uwagi na obowiązujące w Stanach Zjednoczonych przepisy pozwalające na masowe gromadzenie danych przez upoważnione organy w oparciu o postanowienia sądu wydane na podstawie ustawy FISA575 (Foreign Intelligence Surveillance Act), bez wiedzy i możliwości złożenia skargi ze strony zainteresowanych osób576. Problem ten był już podnoszony między innymi w orzecznictwie TSUE jako dowód, że Stany Zjednoczone nie zapewniają ochrony prywatności na poziomie adekwatnym do prawa UE577.

W obu umowach zdefiniowano także prawa podmiotów danych, obowiązki upoważnionych organów związane z przetwarzaniem danych oraz środki odwoławcze i nadzorcze. Przy czym w umowie z Australią wskazano, że nadzór jest realizowany przez niezależny organ – komisarza ds. informacji (art. 10 ust. 1). W przypadku umowy z USA funkcję tę pełni wyznaczona komórka powołana w strukturach organu upoważnionego do przetwarzania danych, dlatego w tym przypadku nie można mówić o spełnieniu warunku nadzoru przez „niezależny organ” w rozumieniu prawa UE i orzeczeń TSUE578. W żadnej z umów nie określono uprawnień krajowych organów nadzoru państw członkowskich ani żadnych instytucji UE (w szczególności EIOD) do przeprowadzania kontroli czy inspekcji prawidłowości realizacji zawartych porozumień. Jest to kolejna uwaga, która może wskazywać na niezgodność omawianych traktatów – a w szczególności umowy z USA – z prawem UE, między innymi z art. 8 ust. 3 KPP.

Kolejnym obszarem będącym przedmiotem regulacji jest możliwość przekazywania danych PNR dotyczących obywateli UE do innych agend rządowych. Także w tym zakresie zastosowano różne rozwiązania – w umowie z USA ograniczono się do wskazania mało precyzyjnych przesłanek uzasadniających przekazanie danych (art. 16), podczas gdy w

575 Ustawa federalna USA z dn. 25 października 1975 o prowadzeniu wywiadu elektronicznego na obszarze Stanów Zjednoczonych (Foreign Intelligence Surveillance Act); sygn. 95-511, publikacja 50 U.S.C. §1801
577 Omówienie wyroku w sprawie Schrems: rozdział 2.4.3, s. 77.
578 Kwestia niezależności organu nadzoru w europejskich przepisach o ochronie danych została omówiona w rozdziale 4.5.4 (s. 173).
umowie z Australią sprecyzowano zamkniętą listę organów rządowych, do których informacje takie mogą być przekazane (art. 18 ust. 1). Co jednak ważniejsze, w porozumieniu z Australią wprost wskazano, że dane mogą być udostępniane wyłącznie w indywidualnych przypadkach, chyba że zostały zdepersonalizowane. Brak takiego zapisu w umowie USA może być interpretowany jako możliwość przekazywania wszystkich informacji na potrzeby dalszego gromadzenia, przetwarzania i analizy przez inne, niewymienione w treści umowy agencje rządu USA. Brak wiedzy na temat podmiotów przetwarzających informacje, miejsca ich przetwarzania, sposobu i celu przetwarzania wzmacnia wątpliwości w zakresie zgodności umowy z USA z normami prawa UE.

Odrębnym zagadnieniem, także odmiennie uregulowanym w obu traktatach, jest kwestia dozwolonego okresu przechowywania przekazanych danych. W porozumieniu z Australią wskazano, że co do zasady dane PNR mogą być zatrzymywane nie dłużej niż przez pięć lat (art. 16 ust. 1), przy czym po trzecim roku powinny być zdepersonalizowane za pomocą maskowania wybranych danych osobowych. Maskowanie stanowi operację odwracalną, dlatego w tym wypadku nie można mówić o anonimizacji. Stosując terminologię wprowadzoną w ogólnym rozporządzeniu o ochronie danych, maskowanie jest formą pseudonimizacji. W umowie z USA wskazano również pięcioletni okres przechowywania danych, przy czym po upływie sześciu miesięcy dane podlegają maskowaniu (błędnie określonym w umowie jako forma anonimizacji). Po upływie pięciu lat dane przenoszone są do tzw. bazy archiwalnej na okres nieprzekraczający dziesięciu lat. Dane zgromadzone w bazie archiwalnej nadal mogą być przywrócone do formy pozwalającej na identyfikację osoby, jednak może to nastąpić w szczególnych przypadkach. Dopiero po upływie pięcioletniego okresu dane podlegają trwałej anonimizacji (uniemożliwiającej przeprowadzenie identyfikacji osoby). W rezultacie dane przekazywane do USA mogą być przechowywane i przetwarzane przez okres łącznie piętnastu lat. Biorąc pod uwagę, że przekazywanie danych PNR dotyczy wszystkich pasażerów (a nie tylko mających jakikolwiek związek z terroryzmem czy poważną przestępczością), trudno uznać ten środek za konieczny czy proporcjonalny w rozumieniu przepisów europejskich. Kolejne niejasności są związane z możliwością i zakresem przetwarzania danych wrażliwych – w umowie z Australią uwzględniono zakaz przetwarzania tego typu danych, a w przypadku ich przekazania razem z innymi danymi PNR nakaz ich trwałego usunięcia (art. 8). Z kolei w umowie z USA uwzględniono istnienie ogólnego automatycznego mechanizmu filtrowania danych.

579 Różnicę pomiędzy pseudonimizacją a anonimizacją omówiono na stronie 133.
wrażliwych (art. 6 ust. 1), jednak jednocześnie przewidziano szereg odstępstw pozwalających na wykorzystanie tych informacji i ich przetwarzanie, przy czym nie jest to warunkowane od uzyskania wcześniej zgody niezależnego organu (art. 6 ust. 3).

Przedstawione powyżej porównanie wskazuje na szereg różnic pomiędzy dwiema umowami międzynarodowymi zawartymi przez UE z partnerami zagranicznymi w podobnym okresie, mających za przedmiot ten sam obszar regulacji. Oczywiste i znaczące różnice pomiędzy szczegółowością zobowiązań państw trzecich w zakresie stosowania środków i gwarancji związanych z ochroną przekazywanych danych pasażerskich budziły uzasadnione wątpliwości nie tylko organizacji zajmujących się ochroną prywatności, ale i instytucji UE uczestniczących w procesie negocjowania i zawierania wymienionych umów. W szczególności interesujące są uwagi Europejskiego Inspektora Ochrony Danych, który w oparciu o ugruntowane orzecznictwo ETPC i TSUE wskazał na szereg niezgodności w proponowanej treści umów, w szczególności porozumienia z USA, z prawem UE. Inspektor podkreślił zbyt szeroki zakres przekazywanych informacji, brak precyzyjnie określonego celu przetwarzania, niedopuszczalne przetwarzanie informacji wrażliwych czy zbyt długi okres przechowywania danych. Podobne niejasności zgłaszane były przez Parlament Europejski i w efekcie − z uwagi na ich nieuwzględnienie zarówno w umowie z USA, jak i Australią − stały się przyczyną wystąpienia przez PE z wnioskiem o wydanie opinii przez TSUE w zakresie zgodności planowanej umowy z Kanadą z prawem UE. Dodatkową, nie mniej istotną przyczyną wystąpienia z wnioskiem o wydanie opinii były wątpliwości na temat zgodności z prawem UE w zakresie mechanizmów retencji danych z uwagi na argumenty przedstawione przez Trybunał w niedawno wówczas wydanym orzeczeniu w sprawie Digital Rights Ireland, w którym stwierdzono nieważność dyrektywy retencyjnej. Projekt umowy wynegocjowany z Kanadą zawierał zbliżone rozwiązania do zastosowanych w przyjętych umowach ze Stanami Zjednoczonymi i Australią, w szczególności:

− brak zamkniętego katalogu przestępstw terrorystycznych i poważnej przestępczości, zamiast tego określenie przesłanek uzasadniających uznanie określonego zdarzenia za tego typu przestępstwo (art. 3 ust. 2 i 3) − rozwiązanie podobne do przyjętego w umowie ze Stanami Zjednoczonymi;

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji Rady w sprawie podpisania umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przechowywania danych w Departamencie Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (Dz. Uzg. UE z 2012 Nr C 35, s. 16).

Zob. także omówienie wyroku w sprawie DRI: rozdział 2.4.3, s. 75.

Szersze informacje nt. dyrektywy retencyjnej na stronie 187 i n.

możliwość wykorzystania danych PNR w innym celu niż do celów przeciwdziałania terroryzmowi oraz poważnej przestępczości, w szczególności do ochrony żywotnych interesów jakiejkolwiek osoby, ale także w wykonaniu postanowienia lub nakazu sądu krajowego (art. 3 ust. 4-5); możliwość przetwarzania danych PNR na podstawie decyzji sądu krajowego w innym celu niż pierwotnie wskazany w umowie transferowej może prowadzić do utraty realnej kontroli nad zakresem i sposobem przetwarzania danych; rozwiązanie takie zostało zastosowane w umowie ze Stanami Zjednoczonymi (brak takiej klauzuli w umowie z Australią),

możliwość przetwarzania danych szczególnie wrażliwych (art. 8) w sposób i zakresie podobnym do rozwiązań przyjętych w umowie ze Stanami Zjednoczonymi;

przechowywanie danych (retencja) przez okres pięciu lat przy jednoczesnym maskowaniu wybranych danych (imię i nazwisko) po 30 dniach od ich otrzymania oraz maskowaniu dalszych informacji po dwóch latach od ich otrzymania; rozwiązanie zbliżone do umowy z Australią.

Rozpatrując wniosek o wydanie opinii na temat zgodności umowy Kanadą z prawem UE, konieczne jest w pierwszej kolejności rozstrzygnięcie kwestii, czy przekazywanie danych PNR do państw trzecich w celu wykrywania i zapobiegania najpoważniejszym przestępstw, ale w odniesieniu do wszystkich podróżnych, jest w ogóle środkiem proporcjonalnym w rozumieniu orzecznictwa TSUE i ETPC. Dopiero odpowiedź na to pytanie pozwala na przeprowadzenie głębszej analizy, pozwalającej na wyznaczenie dopuszczalnego zakresu przekazywanych danych, a także formy oraz czasu ich przetwarzania. Należy pamiętać, że EIOD, opiniując każdy z projektów umów, zgłaszał szereg zastrzeżeń o stosowanych w nich rozwiązaniach (np. pięcioletniego okresu retencji danych584), jak i poddał „w wątpliwość konieczność i proporcjonalność systemów danych dotyczących przelotu pasażera oraz masowego przekazywania danych PNR państwom trzecim”585.

584 Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji Rady w sprawie zawarcia umowy między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR), Dz. Urz. UE z 2011 Nr C 322, p. 2.7.

585 Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie wniosków dotyczących decyzji Rady w sprawie zawarcia i podpisania umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera, Dz. Urz. UE z 2014 Nr C 51, p II.3.
W wydanej 8 września 2016 roku opinii\textsuperscript{586} rzecznik generalny P. Mengozzi w dużej części potwierdził obserwacje EIOD oraz PE w zakresie zgodności projektowanej umowy z Kanadą z prawem UE. W szczególności wymienił uregulowania, które w przedstawionym projekcie są sprzeczne z KPP, w związku z czym stoją na przeszkodzie zatwierdzeniu umowy w analizowanym brzmieniu. Rzecznik zauważył, że niedopuszczalne jest uwzględnienie możliwości rozszerzenia celu i zakresu przetwarzania przekazanych danych, w szczególności prowadzące do możliwości ich przetwarzania w obszarze innym niż zapobieganie przestępstwom terrorystycznym i poważnym przestępstwom międzynarodowym. Ponadto wskazał na potrzebę wprowadzenia zakazu przetwarzania przez państwa trzecie danych PNR zawierających dane wrażliwe. Podkreślił też jako nieakceptowany pięcioletni termin przechowywania (retencji) danych przy jednoczesnym braku wykazania związku tego środka z celem umowy dotyczącym bezpieczeństwa publicznego.

W wydanej 26 lipca 2017 roku opinii\textsuperscript{587} Trybunał nie zakwestionował co do zasady możliwości transgranicznego przekazywania danych PNR. Co więcej, potwierdził, że zastosowanie takiego środka jest uzasadnione celem interesu ogólnego Unii\textsuperscript{588}. Jednocześnie jednak wskazał na szereg przypadków dowodzących nieproporcjonalności przyjętych rozwiązań, skutkujących niezgodnością projektowanej umowy z prawem UE. Trybunał podzielił stanowisko rzecznika generalnego w zakresie zbyt ogólnego wskazania zakresu danych, które mają być przekazywane. Podkreślił także, że uregulowania prowadzące do możliwości przekazywania danych szczególnie wrażliwych oraz dalszego ich przetwarzania przez organy państwa trzeciego prowadzą do naruszenia art. 52 ust. 1 KPP\textsuperscript{589}. Trybunał zgłosił także szereg innych zastrzeżeń, podzielając tym samym omówione wcześniej wątpliwości EIOD. W konsekwencji, stwierdzając niezgodność opiniowanego projektu z prawem UE, Trybunał wskazał minimalne warunki konieczne do spełnienia, aby umowa ta nie prowadziła do naruszenia prawa UE w zakresie prawa do prywatności (art. 7 KPP), ochrony danych osobowych (art. 8 KPP) oraz była zgodna zasadą proporcjonalności (art. 52 ust. 1 KPP)\textsuperscript{590}.

W konsekwencji – zgodnie z art. 218 ust. 11 TFUE – projektowana umowa nie może być zawarta w obecnej, wynegocjowanej formie. Chociaż opinia dotyczy wyłącznie umowy

\textsuperscript{586} Opinia rzecznika generalnego Stefano Mengozzi przedstawiona 8 września 2016, sygn. 1/15, ECLI:EU:C:2016:656.
\textsuperscript{587} Opinia TSUE 1/15 z 26.07.2017 (ECLI:EU:C:2017:592).
\textsuperscript{588} Ibidem, p. 151.
\textsuperscript{589} Ibidem, p. 167.
\textsuperscript{590} Ibidem, p. 232.3.
UE – Kanada i nie prowadzi automatycznie do uznania porozumień zawartych ze Stanami Zjednoczonymi oraz Australią za nieważne, to jednak biorąc pod uwagę podobne zarzuty, jakie można sformułować w odniesieniu do obu wymienionych traktatów, stwierdzenie ich nieważności wydaje się kwestią nieodległej przyszłości.

Niezależnie od kwestii polityki UE w zakresie umów międzynarodowych dotyczących danych PNR Unia podejmuje także działania związane ze współpracą policyjną obejmującą właściwe organy państw członkowskich. Celem tych działań jest zapewnienie jednakowych procedur i schematów działania, między innymi w obszarze gromadzenia, przetwarzania, analizowania i wymiany istotnych informacji (art. 87 ust. 2 lit a TFUE). Wyraz realizacji tego celu stanowi przyjęta 27 kwietnia 2016 dyrektywa 2016/681, która uzupełnia unijną reformę danych w obszarze gromadzenia, wymiany i przetwarzania danych PNR przez państwa członkowskie. Z uwagi na bliskie i wzajemne powiązanie regulacji wewnętrznych UE (dyrektywa 2016/681) z aktami prawno Międzynarodowymi (umowy z państwami trzecimi w zakresie danych PNR), wnioski zawarte w opinii 1/2015 będą miały zastosowanie nie tylko do zawartych lub projektowanych umów międzynarodowych, ale również przepisów wewnętrznych, w szczególności sposobu interpretacji i implementacji przywołanej dyrektywy.

4.6.3. Umowa ramowa UE – USA w sprawie ochrony danych osobowych w obszarze współpracy policyjnej i sądowej

Jednym z obszarów, który od lat stanowi obszar napięć w bliskiej współpracy gospodarczej i politycznej UE – USA, jest kwestia różnego spojrzenia na obszar praw podstawowych w zakresie granic ochrony prywatności jednostki i gwarancji związanych z ochroną jej danych osobowych. Problem ten jest szczególnie wyraźny w zakresie dynamicznie rozszerzającej się współpracy gospodarczej, której warunkiem jest coraz częściej swobodny przepływ danych osobowych. Model wymiany danych osobowych z UE do partnerów w USA, oparty na programie „Tarcza prywatności” (wcześniej „Bezpieczna przystań”) budzi uzasadnione wątpliwości w zakresie jego zgodności z prawem UE. Współpraca w obszarze bezpieczeństwa publicznego, w szczególności walki z terroryzmem i najpoważniejszymi przestępstwami – chociaż jest istotnym celem zarówno USA, jak i UE – również napotyka na trudności, zwłaszcza w zakresie zabezpieczenia przekazywanych danych

591 Szersza analiza dyrektywy 2016/681 została przedstawiona na stronie 193.
592 Por. wcześniejsze rozważania dotyczące Tarczy prywatności oraz wskazaną tam literaturę (s. 164).
obywateli UE i zapewnienia podmiotom danych praw i gwarancji, porównywalnych do tych, z których mogą korzystać w oparciu o przepisy unijne.

Wraz z reformą lizbońską, skutkującą odejściem od funkcjonującego wcześniej podziału na trzy filary współpracy, wprowadzono jednolity model funkcjonowania UE, pozwalający na rozpoczęcie nowego etapu w rozmowach z USA w obszarze wzajemnych relacji dotyczących transferu danych osobowych. Dodatkowym impulsem były wyroki TSUE, odnoszące się wprost do kwestii współpracy z USA (np. unieważnienie decyzji 2000/520 dot. programu „Bezpieczna przystań”) lub pośrednio, poprzez kwestionowanie legalności ważnych mechanizmów, szeroko stosowanych przy przetwarzaniu danych przez rząd USA (np. kwestia hurtowego i nieograniczonego przechwytywania danych, stosowanie obowiązku retencji danych itp.). W efekcie już od 2009 roku PE postulował rozpoczęcie negocjacji nowej umowy, której celem byłoby określenie wspólnych ram w zakresie ochrony transferowanych danych osobowych w związku ze współpracą policyjną i sądową. Konsekwencją było uzgodnienie i zatwierdzenie przez Radę UE 2 grudnia 2016 umowy międzynarodowej z USA w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ścięganiem czynów zabronionych. Umowa weszła w życie wraz z jej publikacją w oficjalnym publikatorze UE w dniu 10 grudnia 2016.

W zamierzeniach KE nowa umowa miała pomóc uzupełnić lukę w prawodawstwie USA w obszarze prawa do ochrony danych osobowych. Wraz z nadaniem KPP mocy równej traktatom ochrona danych została uznana za prawo podstawowe w UE. W systemie prawnym USA brakuje analogicznej regulacji. Amerykańska konstytucja nie definiuje wprost prawa do prywatności, jak i do ochrony danych osobowych, a na poziomie przepisów federalnych nie wprowadzono całościowego modelu ochrony danych przetwarzanych w celach publicznych i

593 Zob. np. rezolucja Parlamentu Europejskiego z dnia 26 marca 2009 r. w sprawie stanu stosunków transatlantyckich po wyborach prezydenckich w USA, P6_TA (2009)0193.
594 Decyzja Rady (UE) 2016/2220 z dnia 2 grudnia 2016 r. dotycząca zawarcia w imieniu Unii Europejskiej Umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ścięganiem czynów zabronionych (CELEX: 32016D2220, Dz. Urz. UE z 2016 Nr L 336 s. 1).
595 Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ścięganiem czynów zabronionych (CELEX: 22016A1210(01), Dz. Urz. UE z 2016 Nr L 336 s. 3).
596 W systemie prawnym USA ochrona prywatności została wywiedziona z gwarancji przewidzianych w Czwartej Poprawce do Konstytucji USA w drodze precedensów sądowych ustanowionych przez Sąd Najwyższy; por. orzeczenie Sądu Najwyższego USA z 7.06.1965 w sprawie Griswold v. Connecticut, 381 U.S. 479 (1965); zob. także rozdział 1.2 (s. 23).
prywatnych, w sposób podobny do obowiązującego w Unii czy wynikającego z rekomendacji organizacji międzynarodowych\textsuperscript{597}.

Traktat, nazywany też „umową parasolową” lub „umową ramową”, dotyczy określenia wspólnych zasad przetwarzania danych, przy czym sama umowa nie jest podstawą do transferu żadnych zbiorów danych z UE do USA\textsuperscript{598}. Przyjęto rozwiązanie, że uzgodnione przepisy powinny stanowić wspólny zbiór zasad stosowany, gdy dane są przekazywane na podstawie innej umowy szczegółowej zawartej między stronami. Jednocześnie zasady określone w umowie ramowej powinny być stosowane bez uszczerbku dla regulacji uzgodnionych w konkretnych umowach szczegółowych. Umowa parasolowa jest więc lex generalis w zakresie współpracy UE – USA w odniesieniu do ochrony danych osobowych przekazywanych w sprawach karnych. Oznacza to w szczególności, że nie dotyczy ona i nie wprowadza nowych regulacji dla transferów gospodarczych (np. realizowanych w wyniku realizacji programu „Tarcza prywatności”).

Umowa posłużyła do przeniesienia na grunt zobowiązań prawnomiędzynarodowych najważniejszych regulacji UE w zakresie ochrony danych – począwszy od podstawowych definicji (informacje osobowe, przetwarzanie, właściwy organ), poprzez określenie praw podmiotu danych, obowiązków administratora, w tym zasady odpowiedzialności, na mechanizmach kontroli i nadzoru skończone. W porozumieniu uregulowano wiele kwestii związanych z przetwarzaniem danych osobowych, które były wcześniej przyczyną sporów i niejasności pomiędzy stronami. Komisja zwróciła w szczególności uwagę na wprowadzenie\textsuperscript{599}:

- zasady ograniczonego użycia danych – nakazującej wykorzystanie danych wyłączenie w zakresie celu ich przekazania, tj. zapobiegania, wykrywania i ścięgania przestępczości;
- ograniczeń w dalszym przekazywaniu danych – w przypadku przekazania danych do państwa trzeciego, konieczne jest uzyskanie zgody właściwego organu, który pierwotnie zaakceptował przekazanie danych;
- zasad związanych z retencją danych – w których wskazuje się na przechowywanie danych nie dłużej, niż jest to potrzebne do realizacji celów przetwarzania; okresy

\textsuperscript{597} Problemy dy systemu prawnego Stanów Zjednoczonych została szerzej omówiona w rozdziale 6.4.5 (s. 280).
\textsuperscript{598} Art. 1 ust. 3 umowy parasolowej, CELEX: 22016A1210(01).
retenacji mają być jawne i publikowane, a decyzje związane z ich określeniem powinny uwzględniać prawa podmiotów danych;

- prawa dostępu i poprawienia danych;

- mechanizmów informowania w przypadku wycieku informacji właściwych organów strony przekazującej informacje, a w przypadku, gdy jest to zasadne – także podmiotów danych;

- prawa do dochodzenia przez obywateli UE odszkodowania w przypadku naruszenia ich praw przed sądami federalnymi w USA.

Szerszego omówienia wymaga ostatni ze wskazanych obszarów regulacji, związany z prawem do skorzystania ochrony sądowej przed sądami amerykańskimi. Brak istnienia dostępnej i skutecznej możliwości dochodzenia praw przez obywateli UE był jednym z powodów uznania przez TSUE, że Stany Zjednoczone nie zapewniają odpowiedniego stopnia ochrony w rozumieniu europejskich przepisów o ochronie danych osobowych. Jak zauważył Trybunał, „samo istnienie skutecznej kontroli sądowej służącej zapewnieniu poszanowania przepisów prawa Unii jest nierozumelnie związane z istnieniem państwa prawa”601. Istniejące przepisy prawa federalnego USA wiązały możliwość dochodzenia praw związanych z naruszeniem zasad przetwarzania danych osobowych z posiadaniem obywatelstwa lub statusu rezydentu w Stanach Zjednoczonych. Regulacja ta, wynikająca z przepisów ustawy Privacy Act z 1972 roku, nie została zmieniona, chociaż była wielokrotnie krytykowana i wskazywana jako prowadząca do braku symetrii we wzajemnych relacjach UE – USA (prawo UE zakłada możliwość skorzystania z ochrony sądowej niezależnie od posiadania obywatelstwa UE)603.

Przepisami implementującymi zobowiązanie prawnomiędzynarodowe wynikające z omawianej umowy w prawie USA była uchwalona w 2015 roku ustawa Judicial Redress Act604. Weszła ona w życie 1 lutego 2017 roku, a jej podstawowym celem jest rozszerzenie kręgu osób uprawnionych z Privacy Act na obywateli innych państw lub regionalnych organizacji ekonomicznych, których lista ma być okresowo aktualizowana przez Biuro Prokuratora Generalnego USA. Strona amerykańska nie zdecydowała się na rozszerzenie

600 Wyrok TSUE z 6.10.2015 w sprawie Schrems, sygn. C-362/14, p. 97.
601 Ibidem, p. 95.
603 Szersze omówienie przepisów Privacy Act w: A. Czubik, Prawo do prywatności..., op. cit., s. 193-195.
kręgu osób uprawnionych z Privacy Act, a zamiast tego przyjęła odrębny akt ustawowy wskazujący, że obywatele państw spełniających określone w przepisie kryteria mogą korzystać z prawa do dochodzenia przed sądem rekompensaty finansowej (odszkodowania) na zasadach takich samych jak obywatele amerykańscy z ustawy Privacy Act.

Pamiętając o tle niniejszych rozważań – a więc zapewnieniu obywateli UE skutecznej ochrony sądowej w zakresie odpowiadającym prawu UE – uznać trzeba, że rozwiązanie przyjęte w Judicial Redress Act, a przez to i w umowie parasolowej UE – USA nie prowadzi do realizacji tego celu. W pierwszej kolejności należy wskazać, że ustawa Judicial Redress Act ogranicza krąg podmiotów zobowiązanych do wybranych, wskazanych przez rząd USA, agencji rządowych. Na aktualnej liście, opublikowanej przez Biuro Prokuratora Generalnego 27 stycznia 2017 roku605, znajdują się cztery agencje federalne oraz dziewięć biur stanowiących jednostki organizacyjne innych agencji – głównie związanych z kontrolą skarbową oraz nadzorem nad rynkiem finansowym. Na liście nie uwzględniono Agencji Bezpieczeństwa Narodowego (NSA) ani innych podmiotów realizujących kwestionowane prawnie programy masowej inwigilacji. Ponadto przepisy Judicial Redress Act nadają obywatelom państw trzecich tylko niektóre z praw zagwarantowanych w Privacy Act dla obywateli i rezydentów amerykańskich. W szczególności są ograniczone do możliwości dochodzenia finansowego odszkodowania. Poza zakresem unormowania jest możliwość zainicjowania postępowania służbowego czy karnego wobec osób odpowiedzialnych za naruszenie przepisów. W efekcie w literaturze przedmiotu zwraca się uwagę, że aby umowa parasolowa UE – USA prowadziła do zapewniania obywatelom UE ochrony sądowej w USA podobnej do dostępnej w Unii, Judicial Redress Act powinien nie tylko zrównywać prawa obywateli UE z prawami rezydentów i obywateli USA, ale nawet nadawać im szersze uprawnienia niż wynikające z Privacy Act606. Ponieważ rozwiązanie takie prowadzioby do zapewnienia skuteczniejszej ochrony w zakresie praw podstawowych obywatelom państw trzecich niż obywatelom własnym, postulat ten jest w oczywisty sposób nierealizowalny w żadnym demokratycznym państwie prawa.

Na płaszczyźnie terminologicznej zauważa się odwołanie w preambule umowy do zasad proporcjonalności i konieczności jako podstaw określania zasadności przetwarzania danych osobowych. Umowa parasolowa jest jedynym dokumentem normatywnym zawartym pomiędzy UE a USA, w którym Stany Zjednoczone uznały korzystanie z zasady

605 Departament Sprawiedliwości USA, Attorney General Order No. 3824–2017, Judicial Redress Act of 2015; Attorney General Designations, Federal Register t. 82, nr 13, s. 7860.
606 D. Bender: The Judicial Redress Act: A Path To Nowhere, iapp.org/news/a/the-judicial-redress-act-a-path-to-nowhere/
proporcjonalności w odniesieniu do celowości przetwarzania danych osobowych. Nie zmienia to faktu, że preambuła jest jedynym miejscem, gdzie takie odwołanie uwzględniono. W przepisach szczegółowych, dotyczących np. retencji danych czy obowiązków administratora danych, zasada proporcjonalności nie została już wymieniona.

Z kolei EIOD wskazał w opublikowanej opinii na brak formalnego wpisania zakazu masowego przekazywania danych wrażliwych oraz konieczność doprecyzowania, że wykładnia dotycząca stosowania praw i gwarancji wynikających z umowy będzie się odbywała z uwzględnieniem zasad konstytucyjnych UE, w szczególności wynikających z art. 16 TFUE oraz art. 7 i 8 KPP. Także europejskie i amerykańskie organizacje zajmujące się ochroną prywatności zgłosiły szereg zastrzeżeń w zakresie praktycznej skuteczności zawartej umowy.

Z uwagi na krótki okres obowiązywania zarówno umowy parasolowej, jak i ustawy Judicial Redress Act brakuje weryfikowalnych danych, na bazie których można ocenić przydatność i skuteczność nowych przepisów w rozszerzeniu i wzmocnieniu praw i gwarancji podmiotów danych w odniesieniu do danych przekazanych do przetwarzania z Unii Europejskiej do Stanów Zjednoczonych.

4.7. Podsumowanie

Przez ostatnie dwadzieścia lat europejskie regulacje w zakresie ochrony prywatności w cyberprzestrzeni ewoluowały, odzwierciedlając nie tylko postęp techniki w przetwarzaniu informacji oraz rozwój rynku i usług IT, ale przede wszystkim potrzebę i oczekiwania społeczne co do bardziej skutecznej ochrony przed ingerencją w życie prywatne.

Kształt dzisiejszego modelu ochrony danych jest skutkiem podejmowania zarówno przez instytucje UE, jak również państwa członkowskie działań w trzech najważniejszych obszarach: (i) wzmacniania praw podstawowych na poziomie traktatów; (ii) stopniowego rozszerzania zakresu przedmiotowego i podmiotowego prawa UE; (iii) zwiększania stopnia harmonizacji i integracji poprzez wprowadzenie unijnych aktów prawnych (rozporządzenia w miejsce dyrektyw, dyrektywy w miejsce decyzji wykonawczych).

607 Streszczenie opinii wstępnej Europejskiego Inspektora Ochrony Danych w sprawie Umowy pomiędzy Stanami Zjednoczonymi Ameryki a Unią Europejską o ochronie danych osobowych dotyczących zapobiegania przestępstwom kryminalnym, prowadzenia dochodzeń w ich sprawie, wykrywania i ścigania (Dz. Urz. UE z 2016 C 186, s. 4), p. 56
608 Ibidem, p. 58.
 Każda ze wskazanych płaszczyzn rozwoju legislacji realizowana była systematycznie przez wiele lat iangażowała różne instytucje UE, a zsumowany wysiłek przyczynił się do wyprawowania najbardziej kompleksowego modelu ochrony prywatności na świecie i to w odniesieniu do organizacji ponadnarodowej.

Wraz z rozpoczęciem stosowania ogólnego rozporządzenia, Unia będzie musiała zwiększyć działania związane z propagowaniem i zapewnianiem stosowania wysokich standardów w relacjach z państwami trzecimi. Źaden model ochrony danych osobowych nie będzie skuteczny, jeżeli nie będzie stosowany we wszystkich miejscach, gdzie informacje te są przetwarzane. Dlatego przepisy UE nie mogą pomijać tego aspektu i muszą być stosowane także przez usługodawców i podwykonawców zagranicznych, świadczących usługi lub przetwarzających informacje na zlecenie. Niewykluczone, że wynikający z prawa UE i wzmacniany orzeczeniami TSUE wysoki reżim ochrony danych osobowych w pewnym momencie stanie na przeszkodzie w dalszym rozwoju międzynarodowej współpracy gospodarczej, a więc realizacji de facto pierwotnego celu ustanowienia Wspólnot Europejskich. Już samo to – w chwili obecnej – jedynie potencjalne zagrożenie w najpełniejszy sposób obrazuje ewolucję, jaką przebyła UE od organizacji o czysto gospodarczych aspiracjach do struktury stojącej na straży poszanowani praw podstawowych.

Działania UE związane ze wzmocnieniem europejskich standardów ochrony danych osobowych spotykają się również z krytyką. W szczególności podkreśla się, że budowanie skutecznego modelu ochrony danych o zasięgu wyłącznie regionalnym, a nie globalnym nie jest możliwe i stanowi działanie iluzoryczne611. Unii trudno w chwili obecnej poszukiwać politycznych partnerów do rozmowy na temat stworzenia wspólnej przestrzeni ochrony danych osobowych o zasięgu ponadregionalnym. Dotychczasowe próby tego typu działań, podejmowane w oparciu o Konwencję nr 108 RE, nie powiodły się – chociaż zarówno Unia, jak i Stany Zjednoczone sygnowały chęć przystąpienia do traktatu, działania te nie zostały zrealizowane. Unia oraz – co oczywiste – państwa członkowskie, chcą wspierać dalsze procesy budowania gospodarki opartej na wiedzy i informacji, muszą skoncentrować się na ujednoliceniu wewnętrznego rynku przetwarzania danych w oparciu o nowo wprowadzona i planowane rozporządzenia, a relacje zewnętrzne realizować z wykorzystaniem wspólnych aktów prawnomiędzynarodowych.

Dzięki reformie lizbońskiej i odejściu od koncepcji działania w trzech filarach możliwa stała się budowa na poziomie Unii jednolitego modelu ochrony danych

611 C. Kuner, Reality and Illusion….., op. cit., s. 4.
obejmującego wszystkie formy integracji, nie tylko współpracy gospodarczej. Coraz wyraźniej widać, że i prawo UE, i orzeczenia TSUE w zakresie ochrony prywatności i zakresu dopuszczalnej ingerencji w to prawo prowadzą nieuchronnie do kolizji z interesami polityczno-gospodarczymi niektórych państw członkowskich. Problem ten jest doskonale widoczny na tle środka o kwestionowanej legalności – ogólnej retencji danych. W tym kontekście Unia coraz bardziej zaczyna przybierać kompetencje wiązane historycznie z organizacjami ochrony praw człowieka, w szczególności EKPC. Z perspektywy ochrony praw podstawowych to zarówno szansa, jak i zagrożenie. Szansa, ponieważ silne i uzupełniające się wzajemnie więzy łączące państwa europejskie z EKPC i UE przyczyniają się do skuteczniejszej ochrony praw jednostek. Zagrożenie, bo oparcie europejskiego modelu ochrony praw podstawowych na EKPC612 będzie stanowiło kolejną przeszkodę w ewolucji systemu ochrony prywatności w cyberprzestrzeni w strukturę o zasięgu ponadregionalnym.

612 Należy pamiętać, że zawarte w traktatach oraz KPP odniesienie do interpretacji praw i gwarancji wypracowanych na tle stosowania EKPC wiąże nie tylko przy interpretacji przepisów prawa wewnętrznego, ale również umów międzynarodowych zawieranych przez UE.
Rozdział 5. Uregulowania szczegółowe w prawie polskim

5.1. Wprowadzenie

Dotychczasowe rozważania związane z prawnym zakresem ochrony prywatności w cyberprzestrzeni obejmowały w dużej mierze przepisy konstytucyjne oraz prawnomiędzynarodowe. Omówione w rozdziale 3 systemy ochrony praw człowieka, wprowadzające do katalogu praw podstawowych ochronę prywatności – takie jak MPPOP, EKPC czy KPP – jako ratyfikowane akty międzynarodowe stanowią część krajowego porządku prawnego. Oczywiście dotyczy to także aktów ustawowych UE, omówionych w rozdziale 4. Co więcej, od 25 maja 2018 roku, wraz z rozpoczęciem stosowania ogólnego rozporządzenia o ochronie danych i utratą mocy przez dotychczasową ustawę o ochronie danych osobowych uzasadnione będzie stwierdzenie, że z perspektywy polskiego systemu prawnego najważniejsze normy określające zakres i treść prawnej ochrony prywatności – obok przepisów konstytucyjnych – mają źródło w aktach międzynarodowych. Prawo unijne w powszechnym rozumieniu traktowane jest jako uzupełniające i ujednolicające prawodawstwo wewnętrzne państw członkowskich. W przypadku ochrony danych osobowych, wraz z wprowadzeniem rozporządzenia, stanie się ono jednak podstawową regulacją – zarówno w obszarze prawa prywatnego, jak i publicznego – definiującą zasady i sposoby przetwarzania danych, a także obowiązki administratorów oraz uprawnienia organów nadzoru. W efekcie zasadne wydaje się przeanalizowanie planowanych zmian dostosowujących polskie prawodawstwo do zastąpienia krajowej ustawy prze z unijne rozporządzenie. Tym bardziej, że zmiana ta wiąże się też z koniecznością nowelizacji przez ustawodawcę wielu aktów prawnych stanowiących lex specialis względem ustawy o ochronie danych osobowych. Ponieważ w wielu przypadkach w ogólnym rozporządzeniu nie delegowano państwu członkowskim uprawnień pozwalających na stanowienie przepisów szczegółowych, działania związane z dostosowaniem prawodawstwa do nowego rozporządzenia będą w sposób nieunikniony wiązały się również z koniecznością wprowadzenia zmian w wielu ustawach, w których takie wyjątki dotychczas były stosowane.

Byłoby jednak błędem przyjęcie, że w efekcie wprowadzenia ogólnego rozporządzenia rola krajowego prawodawcy zostanie sprowadzona wyłącznie do wydawania aktów delegowanych i wykonawczych. Ogólne rozporządzenie przyczyni się do ujednolicenia zasad funkcjonujących na europejskim rynku cyfrowym, jednakże zakres nowej regulacji nie obejmuje wszystkich obszarów związanych z ochroną prywatności. Przywołując rozważania
przedstawione w rozdziale 1.3, nietrafne byłoby stawianie równości pomiędzy ochroną danych osobowych a prywatnością. Nawet po wejściu w życie ogólnego rozporządzenia istnieje bardzo wiele dziedzin życia – mających wpływ na sferę prywatności jednostek – które nie będą regulowane przez nowe prawo unijne. Można je podzielić na trzy grupy:

- obszary, dla których ogólne rozporządzenie nie stanowi wyłącznej regulacji krajowej;
- obszary regulowane przez przepisy krajowe stanowione w wykonaniu innych norm prawa UE (w szczególności – dyrektyw);
- obszary znajdujące się poza zakresem istniejących regulacji unijnych, w tym związane z dziedzinami wyłączonymi z prawa UE.

Do pierwszej grupy należą wszystkie przepisy, do przyjęcia których krajowy ustawodawca jest uprawniony na podstawie norm kompetencyjnych zawartych w ogólnym rozporządzeniu. Przykładem może być wprowadzenie dodatkowych warunków, w tym ograniczeń, w odniesieniu do przetwarzania danych genetycznych, biometrycznych lub dotyczących zdrowia (art. 9 ust. 3 rozporządzenia). Wśród norm kompetencyjnych można wyróżnić przepisy, które państwa członkowskie mogą przyjąć dla uszczegółowienia regulacji zawartych w ogólnym rozporządzeniu (por. art. 6 ust. 2) oraz takie, których wprowadzenie jest obowiązkowe (np. art. 51 ust. 1).

Do kolejnej grupy należą przepisy ustanowione w wykonaniu innych norm prawa UE. Przykładem mogą być regulacje stanowiące transpozycję dyrektywy 2002/58. Chociaż KE zapoczątkowała prace legislacyjne związane z przyjęciem nowego rozporządzenia dotyczącego bezpieczeństwa łączności elektronicznej, to dopóki akt taki nie zostanie wypracowany i zatwierdzony, podstawową regulacją w tym obszarze pozostaje dyrektywa 2002/58 oraz krajowe przepisy ją implementujące. Chociaż prawodawca unijny przewidział w art. 95 rozporządzenia brak nałożenia dodatkowych obowiązków na podmioty zobowiązanych do stosowania norm wynikających z dyrektywy 2002/58, to w praktyce niezgodność obu aktów może prowadzić do szeregu trudności w ich stosowaniu. Temat ten zostanie szerzej omówiony w dalszej części rozdziału.

Problem taki nie powinien występować w przypadku zgodności pomiędzy przepisami ustawowymi stanowiącymi wykonanie dyrektywy 2016/680 oraz ogólnym rozporządzeniem. Przyczyną jest naturalnie fakt, że obie wskazane regulacje zostały przygotowane jako element tej samej reformy unijnych przepisów o ochronie danych, są zatem ze sobą zbieżne zarówno w warstwie terminologicznej, jak i szczegółowych rozwiązań prawnych. Wdrożenie dyrektywy 2016/680 może wiązać się jednak z inną trudnością – według dotychczasowych
przepisów ustawa o ochronie danych osobowych nie reguluje gromadzenia i przetwarzania danych przez uprawnione organy (np. służby specjalne). Dlatego problemem nie będzie zapewnienie zgodności nowej ustawy implementującej dyrektywę 2016/680 z ogólnym rozporządzeniem, ale wprowadzenie rozwiązań prawnych w obszarze do tej pory niepodlegającym regulacjom ustawowym. Także ten aspekt realizacji reformy przepisów o ochronie danych wydaje się interesującym zagadnieniem.

Do ostatniej, trzeciej grupy należą obszary oddziałujące na sferę prywatności jednostek, ale jednocześnie niepodlegające istniejącym przepisom UE lub w ogóle wyłączone z zakresu stosowania prawa UE. W takich przypadkach prawodawca ma największą swobodę w stanowieniu przepisów krajowych. Przykładem mogą być regulacje dotyczące niektórych tajemnic prawnie chronionych, np. związanych z wykonywaniem zawodów prawniczych. Profesjonalni pełnomocnicy dysponują informacjami przynależnymi do sfery życia prywatnego ich klientów. Nie zawsze są to jednak informacje, które można zakwalifikować jako dane osobowe. Informacje te są także przetwarzane w systemach informatycznych i de facto są narażone na te same zagrożenia i ryzyka co inne zbiory zawierające dane wrażliwe. Dlatego warto przyjrzeć się standardowi ochrony tajemnicy zawodów prawniczych wynikającemu z polskich przepisów na tle wzorców funkcjonujących w innych krajach, a także wprowadzonemu w ogólnym rozporządzeniu. W szczególności interesujące może być przeanalizowanie, na ile reżim ochrony wyznaczany przez polskie przepisy prowadzi do zabezpieczenia informacji przetwarzanych w ramach e-usług prawnych oraz nowoczesnych form komunikacji pomiędzy pełnomocnikami a ich klientami.

5.2. Wpływ reformy przepisów UE na prawo krajowe

5.2.1. Wycofywane rozwiązania prawne

Przyjęta 27 sierpnia 1997 roku, a więc ponad dwadzieścia lat temu, ustawa o ochronie danych osobowych na trwałe wpisała się w krajowe prawodawstwo. Należy pamiętać, że w czasach, gdy ustawa była procedowana, dopiero co przyjęta Konstytucja RP nie została jeszcze zatwierdzona w referendum, Polska nie była członkiem UE, jak i nie przystąpiła do Konwencji 108 RE. Już tylko z powodu zmiany otoczenia prawnego zrozumiałe jest zatem, że ustawa musiała być kilkukrotnie nowelizowana. Dodatkowo, wraz ze wzrostem świadomości i potrzeb społecznych w obszarze ochrony danych osobowych, rosla znaczenie nowej regulacji.
Nie dziwi więc, że wprowadzenie ogólnego rozporządzenia zastępującego przepisy krajowe stanowi duże wyzwanie związane z przebudowaniem istniejącego prawodawstwa. Chociaż obecny kształt ustawy stanowi transpozycję prawa UE, w szczególności dyrektywy 95/46, to jednak luz decyzyjny związany z możliwością doboru własnych środków spowodował, że niektóre z rozwiązań przyjętych w polskim prawie to rozwiązania unikalne i niestanowiące bezpośredniego przełożenia wymagań dyrektywy.

Jednym z najważniejszych tego typu elementów, mających jednocześnie istotne znaczenie z punktu widzenia tematyki niniejszej pracy, jest wprowadzone na podstawie delegacji ustawowej wskazanej w art. 39a uodo rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Rozporządzenie uszczegóławia przepisy ustawy o wymagania dotyczące sposobu prowadzenia czynności przetwarzania oraz zakres niezbędnej dokumentacji, w tym opisującej użyte środki techniczne. Najważniejszym obszarem regulacji jest jednak katalog podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące przetwarzaniu danych osobowych. Prawodawca zdecydował się na określenie trzech kategorii systemów (§6 rozporządzenia) i wskazanie dla każdej z nich minimalnych wymagań, które administrator powinien spełnić:

- **poziom podstawowy** – stosowany w przypadku przetwarzania danych osobowych nienależących do danych wrażliwych w systemie, który nie jest podłączony do publicznej sieci informatycznej (Internetu);
- **poziom podwyższony** – stosowany w przypadku przetwarzania danych wrażliwych w systemie niepodłączonym do publicznej sieci informatycznej;
- **poziom wysoki** – stosowany niezależnie od zakresu przetwarzanych danych osobowych, jeżeli co najmniej jedno urządzenie systemu informatycznego połączone jest z siecią publiczną (Internetem).

Chociaż w rozporządzeniu wskazano katalog zabezpieczeń dla każdej z kategorii systemów, ich wybór trudno uznać za kompleksowy. Dla przykładu jedyne techniczne wymaganie, które musi spełnić system informatyczny zaklasyfikowany do poziomu podwyższonego w porównaniu z poziomem podstawowym, to obsługa nieskomplikowanej polityki hasłowej na potrzeby realizacji procesu uwierzytelniania użytkowników (hasło składające się z „co

---

613 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dn. 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).
najmniej z 8 znaków, zawierające małe i wielkie litery oraz cyfry lub znaki specjalne”). Już w czasach, gdy rozporządzenie było przyjmowane, nie odzwierciedlało ani wytycznych branżowych w zakresie bezpieczeństwa systemów IT (tzw. hardeningu\textsuperscript{614}), ani uznawanych standardów międzynarodowych dotyczących zarządzania bezpieczeństwem informacji (np. BS 7799\textsuperscript{615}).

Biorąc pod uwagę, że poziom wysoki określony w rozporządzeniu obejmuje wszystkie systemy podłączone do Internetu, dziwi zupełny brak uszczegółowienia wymagań dla tej grupy w aspekcie rozproszonego przetwarzania informacji (np. poprzez rozdzielenie obowiązków dla administratora i przetwarzającego). Jakkolwiek w 2004 roku przetwarzanie w chmurze obliczeniowej\textsuperscript{616} nie rozwinięło się jeszcze do kształtu znanego obecnie, to nawet przy zastosowaniach klient – serwer\textsuperscript{617} powszechnym zjawiskiem było powierzanie przetwarzania podmiotom trzecim (np. w postaci usług hostingu).


\textsuperscript{614} Hardering jest techniką podnoszenia bezpieczeństwa systemów IT poprzez zmianę jego konfiguracji z wykorzystaniem zewnętrznych standardów lub rekomendacji (np. pochodzących od producenta lub organizacji branżowych). Hardering prowadzi do skuteczniejszego wykorzystania istniejących w danym środowisku informatycznym mechanizmów bezpieczeństwa (np. w systemie operacyjnym, zarządzania bazodanowym, serwerze aplikacyjnym itp.).


\textsuperscript{616} Wyjaśnienie znaczenia przetwarzania w chmurze dla ochrony prywatności – zob. rozdział 6.1 (s. 248).

\textsuperscript{617} Omówienie koncepcji przetwarzania w modelu klient-serwer w rozdziale 6.3.4 (s. 256).
tylko dlatego, że ten drugi system nie był podłączony do Internetu. Błędne założenia stojące u podstaw przyjęcia rozporządzenia spowodowały, że w praktyce dokument ten nie stanowił dla przedsiębiorców elementu uwzględnianego w mechanizmach zarządzania ryzykiem IT. Fakt, że przez ponad czternaście lat nie zdecydowano się na odejście od przyjętego modelu, należy ocenić krytycznie. Niezależnie od tego, co było przyczyną takiego zaniechania, przez ponad dekadę obszar bezpieczeństwa systemów informatycznych przetwarzających dane osobowe był w Polsce pozbawiony adekwatnych regulacji, co miało negatywny wpływ na poziom bezpieczeństwa przetwarzanych danych, było także niekorzystne z punktu widzenia przedsiębiorców – ponoszących ryzyko prowadzonych operacji przetwarzania. Dlatego trzeba ocenić pozytywnie, że wraz z wejściem w życie ogólnego rozporządzenia nastąpi uchylenie rozporządzenia wykonawczego MSWiA, a w miejscu sztywnych kryteriów klasyfikowania systemów i wybiórczych zabezpieczeń dla każdego z nich wprowadzone zostaną mechanizmy oceny i zarządzania ryzykiem wynikające z art. 35 rozporządzenia.

Podobnie wycofane zostaną inne rozporządzenia wydane w oparciu o delegację ustawową – w szczególności związane z przyjęciem ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej618. Wprowadzona wówczas „deregulacja”619 przepisów ustawy o ochronie danych osobowych skutkowała wycofaniem niektórych oraz modyfikacją innych obowiązków nakładanych na administratorów danych. W konsekwencji odstąpiono np. od obowiązku wyznaczania Administratora Bezpieczeństwa Informacji (ABI), czy potrzeby rejestracji zbiorów danych w GIODO. Przez wiele lat rejestracja zbiorów danych w GIODO była wskazywana jako jeden z głównych obowiązków związanych ze stosowaniem ustawy. Jednocześnie trudno było wskazać na praktyczne korzyści związane z realizacją tego zadania – w szczególności prowadzących do zwiększenia bezpieczeństwa przetwarzania albo możliwości skuteczniejszego wykonywania zadań przez GIODO. Wraz z uchyleniem art. 36 ust. 3620 (obowiązek wyznaczenia GIODO) oraz wprowadzeniem art. 43 ust. 1a (brak obowiązku rejestracji zbiorów danych jeżeli powołano ABI) prawodawca przyjął model, w którym wyznaczenie ABI przez przedsiębiorcę miało być jego prawem, a nie obowiązkiem. Wyznaczenie osoby do pełnienia funkcji ABI z perspektywy administratora mogło być korzystne, bowiem związane z nim skutek w postaci

---

618 Ustawa z dn. 7 listopada 2014 o ułatwieniu wykonywania działalności gospodarczej (Dz. U. z 2014 r. poz. 1662).
619 Zob. uzasadnienie do rządowego projekt ustawy o ułatwieniu wykonywania działalności gospodarczej, druk sejmowy 2606 (VII kadencja).
620 W miejsce przepisu uchylonego wprowadzono art. 36a ust. 1 oraz uzupełniające art. 36b.
braku konieczności rejestracji zbiorów danych w GIODO\textsuperscript{621}. Nowelizacja z 2015 została różnie przyjęta zarówno przez praktyków, jak i przedstawicieli doktryny. Z jednej strony wskazywano na uproszczenie mechanizmów biurokratycznych związanych z ochroną danych (podkreślana w projekcie zmian funkcja deregulacyjna), z drugiej – na brak wizji prawodawcy związanej z dalszą ewolucją przepisów.


5.2.2. Projektowany zakres nowej ustawy o ochronie danych

Przepisy ogólnego rozporządzenia pozostawiają państwom członkowskim pewien margines uznania, pozwalający na doprecyzowanie i dostosowanie niektórych przepisów do uwarunkowań lokalnych. Polski projektodawca zdecydował się na przeprowadzenie prac dostosowawczych poprzez wypracowanie projektów dwóch ustaw:

- ustawy o ochronie danych osobowych – nowego aktu, zastępującego dotychczasową ustawę (nazywaną w dalszej części rozdziału także „ustawą merytoryczną”)\textsuperscript{622};
- ustawy dostosowującej przepisy szczegółowe funkcjonujące w obszarze przetwarzania danych osobowych (nazywana w dalszej części rozdziału także „ustawą wprowadzającą”)\textsuperscript{623}.

\textsuperscript{621} Nie dotyczyło to sytuacji, w której administrator zamierzał przetwarzać dane wraźliwe.
\textsuperscript{622} Projekt z dn. 16.03.2018 ustawy o ochronie danych osobowych, http://cli.re/G9Y4re.
Projekt pierwszej ze wskazanych ustaw został opublikowany 28 marca 2017 roku i – w opinii projektodawcy, którym jest Minister Cyfryzacji – jego przyjęcie będzie prowadziło do „zapewnienia pełnej skuteczności normom przewidzianym w rozporządzeniu 2016/679”, ponadto umożliwi obywatelom „skuteczniejsze egzekwowanie ochrony ich danych osobowych – w tym poprzez przyśpieszenie postępowania w sprawach naruszeń”624. Projekt przekazany do konsultacji publicznych został podzielony na jedenaście rozdziałów, wprowadzających kolejno: przepisy ogólne, regulacje dotyczące inspektorów ochrony danych, akredytacji i certyfikacji, powołania funkcji Prezesa Urzędu Ochrony Danych Osobowych, zagadnienia związane z postępowaniem w sprawie naruszenia przepisów o ochronie danych osobowych, europejską współpracę administracyjną, postępowanie kontrolne, administracyjne kary pieniężne, odpowiedzialność cywilną oraz karną.

Zdecydowana większość przepisów ma charakter regulacji administracyjnoprawnych i określa sposób wykonywania uprawnień i kompetencji wynikających z ogólnego rozporządzenia. Przedstawiony projekt nie odnosi się do nowych praw i obowiązków wynikających z ogólnego rozporządzenia. Co oczywiście, ustawa krajowa nie może powielać regulacji rozporządzenia, jak i wprowadzać norm z nim niezgodnych. Projektodawca mógł jednak wykorzystać możliwość (i potrzebę) zmiany ustawy do osadzenia regulacji wynikających z ogólnego rozporządzenia w krajowym porządku prawnym. Przykładem mogą być działania rządu brytyjskiego, który pracując nad reformą krajowych przepisów (Data Protection Act, DPA), od początku założył, że ich funkcją ma być ułatwienie implementacji i stosowania ogólnego rozporządzenia625 oraz zapewnienie stosowania regulacji wynikających z rozporządzenia do wszystkich zbiorów danych, a nie tylko objętych zakresem stosowania prawa UE.

Analizując szczegółowe propozycje, w obszarze uregulowań dotyczących praw podmiotów danych należy zwrócić uwagę na dyskutowaną możliwość obniżenia granicy wieku, po przekroczeniu którego nie ma konieczności uzyskiwania zgody opiekunów prawnych na przetwarzanie danych osoby niepełnoletniej. Zgodnie z ogólną normą wskazaną w art. 8 ust. 1 rozporządzenia jest to 16 lat. Prawodawca unijny przewidział możliwość wprowadzenia niższej granicy wiekowej w prawodawstwie państw członkowskich. W art. 5 projektu ustawy merytorycznej z 8.02.2018 ustalono tę granicę na 13 lat (minimalny wiek

dopuszczony w ogólnym rozporządzeniu). Przyjęcie takiej zmiany prowadziłoby więc do ograniczenia reżimu prawnego związanego z przetwarzaniem danych osób niepełnoletnich. Projektodawca tłumaczy swoją propozycję faktem, że art. 15 k¢ stanowi, że osoba, która ukończyła 13 lat, ma ograniczoną zdolność do czynności prawnych. Z tego faktu projektodawca wyprowadził wniosek, że skoro dziecko po przekroczeniu 13 lat może rozporządzać swoim zarobkiem czy zawierać umowy w drobnych bieżących sprawach życia rodzinnego, może także świadomie wyrazić zgodę na przetwarzanie danych osobowych. Z poglądem tym nie można się zgodzić. Czym innym jest dokonywanie drobnych zakupów, a czym innym zawieranie skomplikowanych umów, składających się często z wielu dokumentów oraz obejmujących różne jurysdykcje. Skoro według opublikowanych badań Eurostatu, wśród Europejczyków korzystających z Internetu aż 40% nie zdecydowało się na przechowywanie plików z wykorzystaniem usług online właśnie z uwagi na obawy o prywatność, to trudno uznać, że 13-letnie dziecko będzie mogło w sposób kompleksowy dokonać analizy zawieranej umowy oraz jej długofalowej konsekwencji dla ochrony własnej prywatności. Pamiętając, że od wielu lat dzieci są jedną z najbardziej pożądanymi grup docelowych przez reklamodawców, zaproponowana regulacja prowadzi do narażenia 13-latków na ryzyko związane z profilowaniem. Legalne profilowanie zainteresowań i potrzeb 13-letnich dzieci może skutkować kierowaniem do nich indywidualnych reklam i innych treści, co poza decyzjami zakupowymi może wpłynąć na ich prawidłowy rozwój poprzez kształtowanie postaw i oczekiwań.

Przepis art. 5 w omawianym brzmieniu został usunięty z treści projektu ustawy merytorycznej, opublikowanej w dniu 3.03.2018 roku. Chociaż nie są znane przyczyny wprowadzenia tej zmiany, to rozsądne jest przyjęcie, że projektodawca uwzględnił argumenty dotyczące potrzeby zapewnienia dzieciom większej ochrony w korzystaniu z cyberprzestrzeni.

Z przedstawionego projektu wynika ponadto, że projektodawcy nie zdecydowali się na skorzystanie z delegacji pozwalającej na ograniczenie możliwości skutecznego wyrażenia zgody przez podmiot danych na przetwarzanie danych szczególnie wrażliwych (określonych w art. 9 ust. 1). Prawodawca unijny wskazał, że prawodawstwo państwa członkowskiego może przewidywać, iż osoba, której dane dotyczą, nie może uchylić zakazu związanego z

---

626 Zob. wyniki badania Eurostatu omówione na s. 250.  
628 Z analizy procesu legislacyjnego wynika, że zmiana została wprowadzona w trakcie prac w Komitece do Spraw Europejskich w okresie luty/marzec 2018. Weryfikacja listy zgłoszonych uwag oraz uzgodnień międzyresortowych nie pozwoliła wskazać podmiotu wnioskującego o usunięcie art. 5 z projektu udro w wersji z 8.02.2018, nie jest także znane przedstawione uzasadnienie dla wprowadzenia tej zmiany.
przetwarzaniem danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także danych biometrycznych, genetycznych oraz informacji o stanie zdrowia\[629\]. Wydaje się zasadne wprowadzenie do przepisów krajowych nieważności czynności prawnej polegającej na wyrażeniu zgody na przetwarzanie danych wrażliwych w celach komercyjnych przynajmniej w przypadku, gdy zgoda jest udzielana w imieniu osoby niepełnoletniej.

Nowością zawartą w projekcie, w porównaniu z wcześniejszymi przepisami krajowymi, jest jednoinstancyjność postępowania przed organem nadzoru. W dotychczasowym stanie prawnym wobec decyzji GIODO strona mogła wnieść wniosek do Prezesa Urzędu o ponowne rozpatrzenie sprawy (art. 21 ust 1). Środek ten nie był jednak sensu stricto odwołaniem\[630\]. Dopiero w przypadku wyczerpania ścieżki administracyjnej możliwe było wniesienie skargi do sądu administracyjnego\[631\]. Wraz z nowelizacją przepisów ustawy – Prawo o postępowaniu przed sądami administracyjnymi\[632\] wprowadzono nową treść art. 52 §3, zgodnie z którą, jeżeli stronie przysługuje prawo do zwrócenia się o ponowne rozstrzygnięcie sprawy, może wnieść skargę do sądu administracyjnego bez skorzystania z tego prawa. Zatem zmiana przepisów o postępowaniu przed sądami administracyjnymi dała stronom szerszy wybór mechanizmów ochrony prawnej – mogą zarówno skorzystać z wniosku o ponowne rozpatrzenie sprawy, jak i złożyć skargę w sądzie administracyjnym.

5.2.3. Zmiany innych aktów prawnych

Nowelizacja i aktualizacja kilkudziesięciu aktów ustawowych, w których przewidziano odmienne tryby przetwarzania danych osobowych niż wynikające z ustawy o ochronie danych osobowych, obok wprowadzenia nowych regulacji, nieznanych wcześniej na

\[629\] W przypadku polskiego prawodawstwa skutek nieważności może wynikać z ogólnych norm kodeksu cywilnego dotyczących nieważności czynności prawnej (np. sprzeczność z zasadami współżycia społecznego - art. 58 §2 kc). Innym przykładem jest możliwość wprowadzenia przez ustawodawcę zastrzeżonej formy ad somelinitatem dla czynności związanej z udzieleniem zgody na przetwarzanie określonych kategorii danych lub w określonych celach. Jak wskazała WP29, „na przykład w przypadku ubiegania się o kartę umożliwiającą dostęp do dokumentacji medycznej państwa członkowskiego mogą postanowić, że osoby fizyczne rejestrujące się za pośrednictwem Internetu muszą korzystać z konkretnego rodzaju podpisu elektronicznego. Wybór taki zagwarantuje wyraźną zgodę, dając również administratorowi danych większą pewność, że będzie w stanie wykazać, iż osoba fizyczna udzieliła zgody” (źródło: Opinia WP29 w sprawie definicji zgody, WP187, s. 29).


\[631\] Ibidem, Nb 10.

\[632\] Ustawa z dn. 30 sierpnia 2002 – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2017 r. poz. 1369 ze zm.).
gruncie dyrektywy 95/46, będzie stanowiła największe wyzwania dla legislatorów, ale i – a może przede wszystkim – dla podmiotów zobowiązanych do stosowania przepisów.

Polski ustawodawca przez dwadzieścia lat funkcjonowania ustawy o ochronie danych zdecydował się na wprowadzenie szeregu odmiennych przepisów szczegółowych. Środek ten był stosowany do stanowienia norm doprecyzowujących regulacje wynikające z ustawy o ochronie danych, ale równie często do tworzenia odmiennych reżimów prawnych, dedykowanych do określonych celów, branż lub zastosowań. W ten sposób polskie przepisy o ochronie danych osobowych stały się zbiorem wielu powiązanych ustaw i aktów wykonawczych do nich. Nierzadko *lex specialis* były stanowione w ważnych obszarach, mających istotne znaczenie z punktu widzenia ochrony danych osobowych. Przykładem może być usta wa o świadczeniu usług drogą elektroniczną, w której w rozdziale 4 określono zasady ochrony danych osobowych. Zgodnie art. 16 ust. 1 ustawy dla przetwarzania danych osobowych w związku ze świadczeniem usług drogą elektroniczną stosuje się przepisy uodo, o ile przepisy tej ustawy nie stanowią inaczej. Biorąc pod uwagę istotną rangę regulacji, dotyczącej usług elektronicznych, oraz fakt, że w momencie przyjmowania ustawy o świadczeniu usług drogą elektroniczną ustawa o ochronie danych już istniała, nie jest zrozumiałe, dlaczego prawodawca zdecydował się na wprowadzenie w obu ustawach odmiennych przepisów, a nawet jeżeli uznał, że takie działanie jest konieczne i uzasadnione, przez kilkanaście lat nie przeprowadził prac ujednolicających i nie przeniósł właściwych przepisów do uodo.

Podobne regulacje, wprowadzające odmienny reżim przetwarzania, znajdują się w kilkunastu dalszych ustawach – między innymi kodeksie pracy, prawie bankowym, prawie ubezpieczeniowym, ustawie o ochronie zdrowia czy ustawie o działalności kulturalnej. W niektórych z nich prawodawca zastosował nawet odmienną terminologię, utrudniającą odniesienie wprowadzanych obowiązków do przepisów ustawy o ochronie danych osobowych. Według oceny Ministerstwa Cyfryzacji, przygotowanie reformy ochrony danych osobowych wymagało przeglądu ponad 140 ustaw z punktu widzenia konieczności ich zmian\(^{633}\), przy czym w przepisach projektu ustawy wprowadzającej przewidziano nowelizację 133 ustaw sektorowych. W poszczególnych branżach jako obszary wymagające podjęcia decyzji merytorycznych przez właściwe resorty wskazano:

- profilowanie w sektorze bankowym i ubezpieczeniowym,
- zmianę zasad gromadzenia danych osobowych pracowników,

---

– postępowanie sądowo-administracyjne w sprawach ochrony danych osobowych\cite{634}.

Warto przypomnieć, że sposób przeprowadzenia nowelizacji obowiązujących ustaw ma kluczowe znaczenie z punktu widzenia zachowania zasady pewności prawa. Rozporządzenie UE stanowi w polskim porządku prawnym akt o randze ponadustawowej, a w efekcie w przypadku braku ujednolicenia zasad powstaje ryzyko, że w obiegu prawnym nadal będą znajdowały się uregulowania niemające mocy prawnej z uwagi na ich niezgodność z przepisami wyższego rzędu.

Omawianie szczegółowych propozycji zmian dostosowujących ustawy sektorowe znajduje się poza zakresem niniejszej rozprawy. Z uwagi na trwający proces legislacyjny propozycje zawarte w projekcie ustawy mogą być jeszcze zmienione. Ponadto w zdecydowanej większości zakres planowanych zmian sprowadza się do usunięcia odniesienia do przepisów uchylanej ustawy o ochronie danych i wprowadzeniu w to miejsce odpowiednich przepisów ogólnego rozporządzenia.

5.3. Wybrane przepisy szczegółowe

W tej części pracy przeanalizowano Hasaną wybrane przepisy związane z ochroną różnych aspektów informacji dotyczących życia prywatnego jednostki – dane medyczne, informacje powierzane pełnomocnikom prawnym oraz dane telekomunikacyjne. Wybór ten nie jest przypadkowy i został podejrzane przez zażądanie przedstawienia, w jaki sposób krajowy prawodawca reguluje obszary związane z ochroną prywatności, znajdujące się w różnej relacji z prawodawstwem unijnym. Kwestia przetwarzania danych medycznych to obszar lex specialis względem europejskich przepisów o ochronie danych (w szczególności ogólnego rozporządzenia). Przepisy krajowe, zachowując zgodność z normami unijnymi, mogą więc prowadzić do przyznania jednostkom większej ochrony. Z kolei tajemnica zawodów prawniczych to obszar nieregulowany prawem UE, a zatem prawodawca krajowy może dowolnie (w granicach przewidzianych ustawą zasadniczą i wiążącymi normami prawnomiędzynarodowymi) kształtować zakres i granicę przyznanej ochrony. Większa swoboda decyzyjna wiąże się jednak z większym ryzykiem wprowadzenia odmiennych norm przez poszczególne państwa, także w obrębie państw członkowskich UE. Z kolei ostatni badany obszar – tj. prawodawstwo związane z tajemnicą telekomunikacyjną – jest

\cite{634} M. Kawecki, Wdrożenie do porządków prawnych państw członkowskich ogólnego rozporządzenia o ochronie danych: Polska perspektywa, http://cli.re/6ZY9mr, s. 5-6.

Przedstawione rozważania pozwolą więc na wskazanie faktycznej funkcji i roli krajowego prawodawcy w stanowieniu przepisów zmierzających do ochrony prywatności w cyberprzestrzeni. Nawet bowiem przy przyjęciu tezy postulowanej w niniejszej pracy – zmierzającej do wykazania, że tylko rozwiązania prawnomеждуnarodowe mogą prowadzić do skutecznej ochrony prywatności w cyberprzestrzeni – to i tak konieczne jest uznanie, że skuteczne wdrożenie niektórych regulacji będzie wymagało bardziej elastycznego podejścia, dopuszczającego uszczegółowienie norm w przepisach krajowych. Zasadne wydaje się zatem pytanie, czy obecnie – mając szerokie możliwości wprowadzania norm kształtujących zakres i granice ochrony prywatności – prawodawca potrafi wprowadzać spójne i jasne regulacje prowadzące do tego celu.

5.3.1. Informacje o stanie zdrowia

Jednym z sektorów, dla którego w polskim systemie wprowadzono szczegółowe uregulowania w zakresie gromadzenia, przetwarzania i udostępniania danych, jest branża ochrony zdrowia. Funkcjonujące przepisy stanowią rozwinięcie norm ogólnych – wynikających z nadal obowiązującej ustawy o ochronie danych osobowych (transpozycja dyrektywy 95/46), a w przyszłości – przepisów ogólnego rozporządzenia. Informacje o zdrowiu, w szczególności związane z chorobami, schorzeniami czy świadczeniami medycznymi, są powszechnie traktowane jako przynależące do danych wymagających szczególnej ochrony. Potrzeba ta była rozpoznana już na gruncie dyrektywy 95/46 poprzez włączenie danych dotyczących zdrowia do katalogu informacji wrażliwych, wymienionych w art. 8 ust. 1 – z czym wiązano domyślny zakaz ich przetwarzania. Konsekwencją było także ich uwzględnienie w przepisie art. 27 ust. 1, definiującym bardziej rygorystyczne warunki przetwarzania.

W tym miejscu należy pokrótce przedstawić wątpliwości związane z samym terminem „dane o stanie zdrowia”. Na gruncie dyrektywy 95/46 nie zdefiniowano tego pojęcia. Nie
został on też uszczegółowiony w przepisach ustawy o ochronie danych osobowych. Ogólność pojęcia prowadzi do niejasności dotyczących zakresu informacji, jaki powinien korzystać ze szczególnej ochrony. Czy tylko dokumentacja wytworzoną w ramach świadczonych usług medycznych? Czy informacją o stanie zdrowia jest już sam fakt korzystania z określonych usług, które mają charakter usług medycznych (np. wizyty u okulisty)?

Idąc dalej – czy w erze aplikacji mobilnych program zainstalowany w telefonie komórkowym, generujący na podstawie aktywności użytkownika zestawienia dotyczące jego stanu zdrowia, można uznać za przetwarzający dane wrażliwe w rozumieniu art. 8 ust. 1 dyrektywy i art. 27 ust. 1 uodo? Powyższe obserwacje prowadziły do wyrażanych w doktrynie wątpliwości, czy już sama informacja, że dana osoba znajduje się w dobrym zdrowiu – w określonych warunkach – może być uznana jako wymagająca zastosowania reżimu przewidzianego dla danych wrażliwych.

Do dalszych trudności interpretacyjnych prowadzi uwzględnienie w katalogu informacji wrażliwych, obok danych dotyczących stanu zdrowia, także informacji o nałogach. Termin ten również nie został rozwinięty w krajowym prawodawstwie, a jednocześnie wykracza poza zakres danych wrażliwych wskazanych na gruncie dyrektywy 95/46. W efekcie nie jest zatem jasne, czy sama informacja o tym, że konkretna osoba pali papierosy, jest już wystarczająca, aby oczekiwać zastosowania reżimu związanego z przetwarzaniem danych wrażliwych.

Ostatnim z pojęć istotnych dla omawianej problematyki jest „dokumentacja medyczna”. Termin ten zastosowano w art. 25 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (dalej: upp)636. W art. 25 ust. 1 ustawy zdefiniowano, że w skład dokumentacji medycznej wchodzą co najmniej: (1) dane pozwalające na ustalenie tożsamości pacjenta, (2) oznaczenie podmiotu udzielającego świadczeń zdrowotnych, (3) opis stanu zdrowia pacjenta lub udzielonych mu świadczeń zdrowotnych oraz (4) data sporządzenia. Dokumentacja medyczna może się przy tym dzielić się na indywidualną (dotyczącą konkretnej osoby) lub zbiorczą (odnoszącą się do ogółu lub określonych grup pacjentów). Co więcej, zgodnie z §6 ust. 1 rozporządzenia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania w przypadku dokumentacji prowadzonej w postaci papierowej pierwsza strona dokumentacji indywidualnej musi zawierać oznaczenie pacjenta, a kolejne...

---

635 P. Barta, P. Litwiński, Komentarz do art. 27, Nb 5, [w:] Ustawa o ochronie danych osobowych, CH Beck 2016.
636 Ustawa z dn. 6 listopada 2008 o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2017 r. poz. 1318 ze zm.).
637 Rozporządzenie Ministra Zdrowia z dn. 9 listopada 2015 w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015 r. poz. 2069).
strony – co najmniej jego imię i nazwisko. W przypadku prowadzenia dokumentacji elektronicznej wskazany sposób oznaczania musi być zastosowany do każdej strony wydruku.

Z faktu, że niezbędnym elementem dokumentacji jest wskazanie danych identyfikujących tożsamość pacjenta, można dojść do wniosku, że dokumentacja medyczna zawsze obejmuje dane osobowe – a więc w całości mieści się w pojęciu dane o stanie zdrowia w rozumieniu uodo. Byłoby to jednak niepoprawne uogólnienie. Przykład dokumentacji indywidualnej, która nie zawiera danych osobowych w rozumieniu uodo, stanowi dokumentacja medyczna osoby zmarłej. Jak wskazał GIODO w szeregu wydanych decyzji, zakresem stosowania ustawy nie są objęte dane osób zmarłych, ponieważ w takim przypadku nie jest spełniony warunek określony w art. 6 ust. 1 uodo638.

Nie jest zatem prawdą, że dokumentacja medyczna zawsze musi być przetwarzana zgodnie z ustawą o ochronie danych osobowych. Dlatego nie można powiedzieć, że jest podzioborem danych o stanie zdrowia w rozumieniu uodo.

Do dalszych nieporozumień może prowadzić zamienne stosowanie terminów „dane medyczne” oraz „dokumentacja medyczna”. O ile drugie ze wskazanych pojęć zostało zdefiniowane na gruncie krajowych przepisów, to często w literaturze przedmiotu przedstawiane są rozważania związane z ochroną danych medycznych. Dane medyczne mają szeroki zakres znaczeniowy i odnoszą się nie tylko do informacji o osobach. Jak zauważył M. Kamiński, za „dane medyczne trzeba bowiem uznać zarówno dane osobowe pacjentów, jak i np. dane o ilości opakowań leku znajdujących się w szpitalu”640. Termin ten jest jednak – błędnie – stosowany w niektórych regulacjach dla określenia podzbioru danych osobowych (por. art. 21 ust. 2 pkt 2 ustawy – Prawo lotnicze641).

Podsumowując, na gruncie przepisów krajowych wprowadzono trzy powiązane terminy:

- **dane o stanie zdrowia** – wprowadzone w przepisach o ochronie danych (w tym ustawie o ochronie danych osobowych, także dyrektywie 95/46 oraz rozporządzeniu 2016/679);
- **dokumentacja medyczna** – stosowane w przepisach regulujących przetwarzanie dokumentacji zawierającej informacje medyczne, w tym dotyczące stanu zdrowia;

---

638 Decyzja Generalnego Inspektora Ochrony Danych Osobowych z dnia 11 czerwca 2012 (DOLiS/DEC-520/12/35884,35886), s. 2.
639 Por. np. tytuły opracowań wskazanych w przypisach 640 oraz 643.
640 M. Kamiński, *Powierzenie przetwarzania osobowych danych medycznych a perspektywy prowadzenia dokumentacji medycznej w postaci elektronicznej*, PME 2008, nr 8, s. 7.
641 Ustawa z dn. 3 lipca 2002 – Prawo lotnicze (Dz.U. z 2017 r. poz. 959 ze zm.).
– *dane medyczne* – termin stosowany w różnych innych przepisach sektorowych, między innymi w ustawie Prawo lotnicze.


Należy pamiętać o konieczności interpretowania terminu dane osobowe w granicach stosowania ustawy – a więc w zakresie wynikającym z art. 2 ust. 1 uudo. Oznacza to, że aby określona informacja była przetwarzana w szczególnym reżimie ustawowym określonym dla danych o stanie zdrowia, musi jednocześnie być przetwarzana w kontekście pozwalającym na identyfikację podmiotu danych. Dane medyczne, które nie odnoszą się do konkretnego pacjenta i nie pozwalają na przeprowadzenie identyfikacji, nie będą korzystały z ochrony wynikającej z art. 27 ust. 1 ustawy. Dlatego należy uznać, że poszczególne pojęcia – dane medyczne, dokumentacja medyczna oraz dane o stanie zdrowia – tworzą zbiór częściowo wspólny. Można wskazać przykłady informacji, które będą stanowiły wyłącznie dokumentację medyczną, takie, które będą stanowiły wyłącznie informację o stanie zdrowia (ale nie dokumentację medyczną), oraz takie, które będą należały do obu zbiorów. Podobnie zależności występują w odniesieniu do trzeciego terminu – a więc danych medycznych. Dlatego w doktrynie spotyka się stosowanie terminów utworzonych poprzez złączenie powyższych pojęć – np. „*dane osobowe medyczne*”643. W efekcie, w ocenie M. Jagielskiego, w polskich aktach prawnych pojawił się pełen wachlarz możliwych relacji pomiędzy pojęciami „*dane medyczne*”, „*dane o stanie zdrowia*” oraz „*dane osobowe*”644.

Przenosząc powyższe rozważania na grunty krajowych przepisów, należy omówić wymagania prawne, jakie zostały wprowadzone w celu zapewnienia prawidłowego przetwarzania dokumentacji medycznej oraz odnieść te wymagania do przepisów o ochronie danych osobowych – a w szerszym ujęciu także do ochrony prywatności. Z uwagi na zakres niniejszej pracy implikujący ukierunkowanie rozważań na przetwarzanie informacji w postaci elektronicznej, w pierwszej kolejności należy omówić przepisy przywołane wcześniej ustawy


o prawach pacjenta i Rzeczniku Praw Pacjenta. Co do zasady, zgodnie z art. 24 ust. 1 podmiot udzielający świadczeń zdrowotnych jest zobowiązany do zapewnienia ochrony danych zawartych w dokumentacji medycznej. Jednocześnie osoby wykonujące zawód medyczny oraz czynności pomocnicze przy udzielaniu świadczeń zdrowotnych są obowiązane do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z wykonywaniem zadań (art. 25 ust. 3). Ustawa wskazuje zatem dane medyczne jako objęte tajemnicą zawodową, określając jednocześnie krąg osób zobowiązanych do zachowania ich w poufności.

Co do zasady podmiot udzielający świadczeń medycznych może zawrzeć umowę na powierzenie przetwarzania (art. 31 ust. 1 uodo). Poza spełnieniem warunku wynikającego z przepisów o ochronie danych osobowych (forma pisemna) podmiot medyczny musi dodatkowo zapewnić sobie prawo do kontroli zgodności przetwarzania z zawartą umową. Z uwagi na brak wystarczającego dostosowania uodo do specyfiki przetwarzania w chmurze, zarówno na gruncie uodo, jak i upp, nie określono dodatkowych zabezpieczeń proceduralnych, jakie powinny być zastosowane w przypadku chęci skorzystania z tej formy przetwarzania. Prawdą jest, że wraz z rozpoczęciem stosowania ogólnego rozporządzenia wskazana luka prawna zostanie częściowo usunięta. Biorąc jednak pod uwagę wcześniejsze rozwiązania na temat pojęć dane medyczne, dokumentacja medyczna oraz dane dotyczące stanu zdrowia, wydaje się zasadne, aby krajowy prawodawca zapewnił zgodność przepisów poprzez wskazane, że każdy przypadek powierzenia do przetwarzania zbioru obejmującego dokumentację medyczną musi być realizowany w sposób zgodny z przepisami o ochronie danych osobowych. Prawodawca może też rozważyć, czy nie wprowadzić dalszych zabezpieczeń związanych z przetwarzaniem danych wrażliwych, np. poprzez wymaganie, że czynności przetwarzania takich danych mogą być zlecone wyłącznie podmiotom podlegającym prawu UE oraz na potrzeby przetwarzania mającego miejsce na obszarze Unii.

Obok przepisów upp regulacje związane z przetwarzaniem dokumentacji medycznej zostały uwzględnione w ustawie o systemie informacji w ochronie zdrowia (dalej: usioz). W przepisie art. 2 ust. 6 ustawy wprowadzono definicję „elektronicznej dokumentacji medycznej”, którym jest dokument elektroniczny umożliwiający usługobiorcy uzyskanie świadczenia opieki zdrowotnej lub stanowiący dokumentację medyczną indywidualną (z wyłączeniem skierowań) wytworzoną w postaci elektronicznej. Ustawa wprowadza przepisy

645 Ustawa z dn. 28 kwietnia 2011 o systemie informacji w ochronie zdrowia (Dz.U. z 2016 r. poz. 1535 ze zm.).
rozszerzające zakres danych, jaki może być przetwarzany w systemach informacji o ochronie zdrowia (art. 4 ust. 3).

Wymagania związane z prowadzeniem dokumentacji w wersji elektronicznej zostały również uregulowane w rozporządzeniu Ministra Zdrowia646, wydanym na podstawie delegacji ustawowej wskazanej w art. 30 upp. W szczególności w §80 rozporządzenia wskazano kryteria pozwalające na uznanie, że system teleinformatyczny może być wykorzystywany do prowadzenia dokumentacji medycznej w postaci elektronicznej. Należy oczekiwać, że znaczenie przetwarzania dokumentacji elektronicznej będzie rosło w czasie z uwagi na planowane na 1 stycznia 2018 wycofanie możliwości prowadzenia dokumentacji w wersji papierowej647.

Na tle powyższych rozważań – zwłaszcza dotyczących rozumienia granic pojęcia „informacje o stanie zdrowia” – nie jest jasne, czy i w jakim zakresie prawnej ochronie na podstawie istniejących przepisów podlegają dane o kodzie genetycznym oraz dane biometryczne. Obie terminy mają oczywisty związek ze sfereą prywatności jednostki. Zarówno dane biometryczne, jak i związane z kodem genetycznym przy odpowiedniej wiedzy i zastosowanej technice pozwalają na jednoznaczną identyfikację osoby. Ponadto analiza kodu genetycznego pozwala na poznanie wielu informacji związanych z predyspozycjami zdrowotnymi (np. większym ryzykiem zachorowania na określone choroby), ale także na wnioskowanie związane z pochodzeniem etnicznym. Ponadto kod genetyczny ma istotną cechę, o fundamentalnym znaczeniu z punktu widzenia ochrony prywatności – unikalność połączona z brakiem możliwości modyfikacji. Jednostka może podjąć działania związane ze zmianą wszystkich innych rodzajów danych osobowych (w tym danych adresowych, ale także imienia i – po spełnieniu dodatkowych warunków – nazwiska). Także identyfikatory nadane przez органы publiczne (takie jak PESEL) w określonych sytuacjach mogą być zmienione, a w przypadku braku takiej możliwości jednostka może przestać ich używać (np. zmienić kraj zamieszkania). Kod genetyczny jest unikalny i nierozwalalnie związany z daną osobą. Zatem jego ujawnienie lub przetwarzanie poza zakresem udzielonej zgody może potencjalnie prowadzić do poważnego zagrożenia dla prywatności. Potrzeba wprowadzenia ograniczeń prawnych w związku z gromadzeniem i przetwarzaniem informacji genetycznych została już

646 Rozporządzenie Ministra Zdrowia z 9.11.2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015 r. poz. 2069 ze zm.).
647 Art. 56 ust. 1 ustawy o systemie informacji w ochronie zdrowia.
zauważona na forum międzynarodowym już w 2003 roku, czego najlepszym wyrazem było przyjęcie Międzynarodowej Deklaracji UNESCO w sprawie danych genetycznych648.

Przepisy krajowej ustawy o ochronie danych wymieniają dane o kodzie genetycznym w katalogu danych wrażliwych (art. 27 ust. 1). Jak wskazuje się w literaturze przedmiotu, ponieważ treść przepisu wykracza poza wymogi przewidziane w dyrektywie 95/46, fakt uwzględnienia danych genetycznych w katalogu danych wrażliwych jest kwestionowana przez instytucje UE649. Ponadto jak zauważa D. Krekora-Zając, wprowadzony w ustawie termin „kod genetyczny” nie jest tożsamy z pojęciem „danych genetycznych”, co z kolei może prowadzić do niejasności związanych z zakresem informacji objętych ochroną650. Zarówno krajowa ustawa, jak i dyrektywa 95/46 nie wymieniają danych biometrycznych w katalogu informacji dodatkowych szczegółów, ustawy i dyrektywy 95/46 nie wymieniają danych biometrycznych w katalogu danych wrażliwych (art. 27 ust. 1). Ponadto informacje o stanie zdrowia zostały szczegółowo omówione w motywie 35 rozporządzenia.

Rozpoczęcie stosowania ogólnego rozporządzenia nie będzie skutkowało uchyleniem albo ograniczeniem krajowych przepisów szczegółowych, ustanowionych w obszarze przetwarzania dokumentacji medycznej. Zgodnie z art. 9 ust. 4 rozporządzenia państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, biometrycznych lub dotyczących zdrowia. Oznacza to, że państwa nie mogą wprowadzać przepisów skutkujących

zmniejszeniem rygorów przetwarzania wynikających z ogólnego rozporządzenia. Mogą jednak stanowić prawo nakładające dodatkowe warunki czy zasady przetwarzania.

Dlatego po wejściu w życie ogólnego rozporządzenia w obiegu prawnym pozostaną omówione wyżej regulacje zawarte w ustawach o prawach pacjenta oraz systemu informacji w ochronie zdrowia, a także w wydanych przepisach wykonawczych. Wydaje się zatem zasadne, aby prowadząc prace związane z reformą krajowych przepisów o ochronie danych, prawodawca zapewnił ujednolicenie stosowanych definicji oraz środków zabezpieczeń z regulacjami dotyczącymi przetwarzania danych medycznych, tak aby zmniejszyć ryzyko niespójności pomiędzy wymaganiami przewidzianymi w obu grupach aktów prawnych.\footnote{651}

5.3.2. Tajemnica adwokacka

Tajemnicą zawodową o szczególnym znaczeniu w systemie prawnym państw demokratycznych jest tajemnica zawodów prawniczych, zwłaszcza tajemnica obrończa. O ile bowiem ochrona innych tajemnic zawodowych ustanawiana jest w celu zabezpieczenia słusznych interesów osób, których dane są przetwarzane, to co do zasady w przypadku tajemnicy obrończej faktycznym cel jej ustanowienia stanowi wzmocnienie ustrojowych zasad będących fundamentem państwa demokratycznego. Dodatkowego znaczenia tym rozważaniom nadaje fakt, że prawo UE co do zasady nie reguluje kwestii tajemnic zawodowych, pozostawiając ten obszar prawodawstwu krajowemu. Dlatego dalszej analizy wymaga, na ile krajowy prawodawca zapewnił dostosowanie reżimu przetwarzania tajemnicy zawodów prawniczych do definicji, form i zakresu wynikających z unijnych przepisów o ochronie danych.

Na wstępie należy wprowadzić podstawowe definicje – w szczególności precyzyjnie określić, czym jest tajemnica zawodów prawniczych. W Polsce funkcjonuje kilka zawodów regulowanych, których wykonywanie wiąże się ze świadczeniem usług prawnych lub sprawowaniem funkcji w wymiarze sprawiedliwości. Z uwagi na zakres niniejszej pracy – odnoszący się do kwestii ochrony prywatności w cyberprzestrzeni – dalsze rozważania skoncentrowane zostaną na zawodzie adwokata.

Podstawę prawną zachowania tajemnicy przez członków korporacji adwokackiej (a więc adwokatów i aplikantów adwokackich) stanowi art. 6 ustawy – Prawo o adwokaturze 651

\footnote{651 W projekcie ustawy wprowadzającej (zob. przypis 623, s. 219) projektodawca nie przewidział realizacji tego postulatu. W obecnym kształcie proponowanych zmian nowelizacja ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta koncentruje się na zapewnieniu podstawy prawnnej do przetwarzania danych przez Rzecznika, a nie kwestii ujednolicenia terminologii i zasad ochrony różnych typów informacji przetwarzanych w ramach świadczenia usług medycznych (art. 87 ustawy wprowadzającej).}
(dalej: upa)\textsuperscript{652}, zgodnie z którym adwokat obowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej (art. 6 ust. 1), a obowiązek ten nie może być ograniczony w czasie (art. 6 ust. 2). Analogiczny przepis można odnaleźć w art. 3 ust. 3 i 4 ustawy o radcach prawnych.\textsuperscript{653} Przedstawiona definicja jest szeroka i obejmuje wszystkie informacje, niezależnie od ich formy, a także sposób uzyskania, w posiadaniu których znalazł się pełnomocnik w związku z wykonywaną pracą. Dalsze uszczegółowienie zakresu przedmiotowego tajemnicy znalazło rozwinięcie w przepisach Zbioru Zasad Etyki Adwokackiej i Godności Zawodu (dalej: Kodeks), zgodnie z którymi tajemnicą objęte są też wszystkie wiadomości, notatki i dokumenty dotyczące sprawy uzyskane od klienta oraz innych osób, niezależnie od miejsca, w którym się znajdują (§19 ust. 3). Należy przy tym zaznaczyć, że zgodnie z wyrokiem NSA z 21 września 1998 tajemnicą adwokacką nie są objęte dane personalne klienta i ogólna informacja (wiedza) o rodzaju świadczonej na jego rzecz usługi prawnej\textsuperscript{655}.

Kwalifikowaną formą tajemnicy prawniczej (adwokackiej i radcowskiej) jest tajemnica obrończa. Materialnie odnosi się do tego samego zakresu informacji, ale związana jest z reprezentacją w sprawach karnych. O ile zarówno tajemnica prawnicza, jak i obrończa mają charakter bezwzględną (\textit{erga omnes}), to w przypadku tej drugiej zastosowanie znajduje dodatkowo przepis art. 178 kpk wykłuczający możliwość przesłuchania ustanowionego w sprawie obrońcy. Jak zauważył SN, „z tych samych względów w toku przeszukania nie wolno zatrzymać pism lub innych dokumentów obejmujących okoliczności związane z wykonywaniem przez adwokata funkcji obrońcy, niezależnie od tego czy wykonuje on tą funkcję w sprawie, której dotyczy przeszukanie, czy w innej, przy czym samo oświadczenie obrońcy o takim charakterze dokumentów jest wiązące dla organu dokonującego przeszukania”\textsuperscript{656}.

W efekcie tajemnica obrończa ma nie tylko charakter powszechnie obowiązujący, ale również ścisły w tym rozumieniu, że żaden organ – w tym sąd – nie ma możliwości zwolnienia z obowiązku jej dotrzymania. Wyjątek stanowi spełnienie przesłanki wskazanej w ...

\textsuperscript{652} Ustawa z dn. 26 maja 1982 – Prawo o adwokaturze (Dz.U. z 2016 r. poz. 1999 ze zm).
\textsuperscript{653} Ustawa z dn. 6 lipca 1982 o radcach prawnych (Dz.U. z 2016 r. poz. 233 ze zm.).
\textsuperscript{654} Obwieszczenie NRA z dn. 11 grudnia 2011 r. w sprawie ogłoszenia jednolitego tekstu Zbioru zasad etyki adwokackiej i godności zawodu (Kodeksu etyki adwokackiej), https://goo.gl/XXsGQH.
\textsuperscript{656} Postanowienie SN z 26.10.2011, sygn. I KZP 12/11, OSNKW 2011, nr 10, poz. 90.
art. 180 § 2 kpk, tj. niezbędność dla dobra wymiaru sprawiedliwości oraz brak możliwości ustalenia faktów na podstawie innego dowodu niż przesłuchanie obrońcy\(^{657}\).

Zakres ochrony prawnej związanej z tajemnicą obrończą jest wyraźnie większy niż związany z innymi tajemnicami prawnie chronionymi (por. np. wcześniejsze rozważania dotyczące ochrony tajemnicy zawodów medycznych). Ponadto, co potwierdzają orzeczenia SN, cechą szczególną tajemnicy obrończej jest również brak możliwości zwolnienia z obowiązku jej zachowania przez klienta. W ten sposób wyrażane jest przekonanie, że tajemnica obrończa ustanowiona została nie tylko w celu ochrony interesu prywatnego, ale i dobra wymiaru sprawiedliwości\(^{658}\).

Wydaje się zatem uzasadnione, że ustanowienie tak silnego reżimu ochrony powinno znaleźć odzwierciedlenie w określeniu minimalnych zabezpieczeń wymaganych dla przetwarzania tego typu informacji w postaci elektronicznej.

Zgodnie z §19 ust. 5 Kodeksu adwokat posługujący się w pracy zawodowej komputerem lub innymi środkami elektronicznego utrwalania danych obowiązany jest stosować oprogramowanie i inne środki zabezpieczające dane przed ich niepowołanym ujawnieniem\(^{659}\). W przypadku korzystania z elektronicznych środków przekazu (np. poczty elektronicznej, przesyłania dokumentów za pośrednictwem internetowych repozytoriów plików) konieczne jest zachowanie szczególnej ostrożności oraz uprzedzenie klienta o ryzyku związanym z zachowaniem poufności przy wykorzystaniu tych środków (§19 ust. 6 Kodeksu). Z kolei w stanowisku przedstawionym przez Ośrodek Badań, Studiów i Legislacji KRRP w sprawie zapytania w przedmiocie tajemnicy zawodowej radcy prawnego

\(^{657}\) Istnieje spór w doktrynie co do praktycznego znaczenia wskazanego przepisu. Wskazywana jest niezgodność z normą art. 6 ust. 3 upa, zgodnie z którą „adwokata nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnnej lub prowadząc sprawę”. W ocenie J. Warylewskiego w trwającej dyskusji nad określeniem, która z ustaw jest lex specialis, co ma kluczowe znaczenie dla wskazania normy wiążącej w tej sytuacji (zasada lex specialis derogat legi generali), zaczyna przeważać stanowisko o względnym charakterze tajemnicy adwokackiej (zob. J. Warylewski, Tajemnica adwokacka i odpowiedzialność karna za jej naruszenie (ujawnienie), Palestra 2011, nr 5-6, s. 11). Jako argument przemawiający za taką interpretacją wskazywana jest okoliczność, że obowiązek zachowania tajemnicy nie został przez ustawodawcę wprowadzony w interesie adwokatów, lecz w interesie osób, które korzystają z ich usług. Z kolei M. Warchoł, wiceminister sprawiedliwości, w marcu 2017 roku stwierdził, że „pomiędzy przepisem art. 180 § 2 k.p.k. a art. 6 ust. 3 Prawa o adwokaturze zachodzi pozorna sprzeczność. Powinna być ona rozstrzygnięta poprzez uznanie, że ten pierwszy przepis stanowi lex specialis” (zob. Przepisy o tajemnicy adwokackiej nie będą modyfikowane – odpowiedź MS na interpelację, Rzeczpospolita, 22.03.2017, https://goo.gl/1Eiv8D).

\(^{658}\) Jak ponadto stwierdził Sąd, nieskuteczność zwolnienia z obowiązku zachowania tajemnicy przez klienta skutkuje także negatywnymi konsekwencjami dla pełnomocnika w przypadku zastosowania się do takiej dyspozycji: „Złożenie przez radę prawnego zeznań z uwagi na prośbę klienta w procesie karnym bez uprzedniego zwolnienia go od jej zachowania przez sąd prowadzący to postępowanie, bez wątpienia zatem oznaczało naruszenie tajemnicy zawodowej, a przez to i świadome, zawinionie, nienależyte wykonywanie obowiązków przez obwinionego jako radę prawnego. Postanowienie SN z 15.11.2012, sygn. SDI 32/12, Legalis 549636.

\(^{659}\) Analogicznie art. 23 ustawy o radach prawnych.
wyjaśniono, że „ochrona dotyczy wszystkich dokumentów objętych tajemnicą zawodową radcy prawnego, niezależnie od ich formy. Obejmuje ona zatem zarówno dokumenty w formie tradycyjnej (pisma), jak i dokumenty elektroniczne. W wypadku danych przechowywanych na twardym dysku komputera zapisanym nośnikiem informacji jest ten właśnie dysk. Z kolei w wypadku danych kopiowanych z serwerów poczty elektronicznej zapisanym nośnikiem jest serwer”.

Oddzielnym zagadnieniem jest korzystanie przez adwokata bądź prawnika z usług przetwarzania informacji świadczonych przez podmioty zewnętrzne – dostawców usług poczty elektronicznej, hostingu (np. przesyłanie danych z formularzy online), a także szerokiego spektrum usług przetwarzana w chmurze. W takim wypadku konieczne jest uwzględnienie przepisów o ochronie danych osobowych. O ile jednak prawodawstwo związane z gromadzeniem i przetwarzaniem danych osobowych szczegółowo określa obowiązki administratora danych i warunki, jakie należy spełnić w celu powierzenia przetwarzania danych podmiotowi trzeciemu, to regulacje ustawowe wynikające z ustawy – Prawo o adwokaturze nie nakładają żadnych dodatkowych obowiązków. Regulacje takie można odnaleźć w Kodeksie, w szczególności w §19 ust. 4, zgodnie z którym adwokat powinien zobowiązać swoich współpracowników i personel oraz wszelkie osoby zatrudnione przez niego podczas wykonywania działalności zawodowej do przestrzegania obowiązku zachowania tajemnicy zawodowej. W rezultacie co do zasady tajemnica adwokacka, chociaż ma charakter publicznoprawny, a więc i skutek erga omnes, to wiąże inne podmioty (np. usługodawców) tylko wtedy, gdy zostaną do tego zobowiązani przez adwokata. Jest to nietypowe rozwiązanie, skutkujące ograniczeniem odpowiedzialności podwykonawców względem osób, których dane są przetwarzane. O ile bowiem w omawianej wcześniej ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, na mocy art. 24 ust. 3, osoby wykonujące czynności pomocnicze, w tym związane z utrzymaniem i zapewnieniem bezpieczeństwa systemów informatycznych, są ustawowo zobowiązane do zachowania tajemnicy, to w przypadku informacji zawierających tajemnicę adwokacką – zobowiązanie takie ma charakter prywatnoprawny. Kodeks zawodowy korporacji adwokackiej nie stanowi źródła prawa dla osób nienależących do tej korporacji, a zgodnie z wyrokiem WSD z 22.02.2014 nawet

660 Stanowisko OBSiL Krajowej Rady Radców Prawnych z dnia 30 października 2015 r. w sprawie zapytania w przedmiocie tajemnicy zawodowej radcy prawnego, Biblioteka Prawa Samorządu Radców Prawnych, http://bibliotekakirp.pl/items/show/480, s. 5.

niedopelnienie przez adwokata obowiązku wynikającego z §19 ust. 4 nie może skutkować jego odpowiedzialnością dyscyplinarną662.

Przepisy ustawy – Prawo o adwokaturze odzwierciedlają technologicznie wczesne lata dziewięćdziesiąte dwudziestego wieku i w efekcie są znacząco niedostosowane do dzisiejszych realiów rynku związanych z wykonywaniem zawodu. Dlatego pilnym postulatem de lege ferenda powinno być znowelizowanie upa poprzez dodanie zapisu rozszerzającego krąg podmiotów zobowiązanych do zachowania tajemnicy na wszystkie osoby (fizyczne i prawne), które uczestniczą w wykonywaniu czynności pomocniczych – w tym związanych ze świadczeniem usług informatycznych. Oczywiście obowiązek dochowania tajemnicy można wywodzić na gruncie innych przepisów – w szczególności art. 266 §1 kk – jednak wydaje się rozsądne, aby zwłaszcza w obszarze tajemnicy obraźliwej, prawodawca usunął wszelkie wątpliwości co do zakresu zobowiązania tajemnicą w odniesieniu do podmiotów świadczących usługi dla adwokatów. Tym bardziej, że celem postulowanej nowelizacji nie jest zapobieganie celowemu ujawnieniu informacji tylko zwiększenie standardów związanych z przetwarzaniem danych.

Bierność korporacji prawniczych w tym zakresie jest niezrozumiała, tym bardziej że od kilku lat wskazana problematyka stanowi przedmiot intensywnych badań ze strony Rady Adwokatur i Stowarzyszeń Prawniczych Europy (CCBE). Rada w swojej analizie już w 2002 roku podjęła temat ochrony tajemnicy zawodów prawniczych w chmurze obliczeniowej663. Ogólne uwagi dotyczące ryzyk związanych z chmurą obliczeniową zostały odniesione do realiów związanych z wykonywaniem zawodów prawniczych. Dlatego też CCBE podkreśliła rolę nie tylko wyboru właściwego prawa czy jurysdykcji, ale również opracowała podsumowanie prezentujące zabezpieczenia prawne związane z ochroną tajemnicy adwokackiej funkcjonujące w poszczególnych państwach członkowskich UE664. Jak wykazano, z uwagi na brak regulacji UE w tym obszarze, w poszczególnych państwach zakres ochrony znacznie się różni, powodując, że dokumenty elektroniczne zawierające ten sam zakres informacji mogą być różnie chronione w zależności od wybranego prawa właściwego.

662 „Materialnoprawną podstawą odpowiedzialności dyscyplinarnej musi być przepis rangi ustawowej, a kryterium tego nie spełnia uchwała wprowadzająca Zbiór Zasad Etyki Adwokackiej i Godności Zawodu, będąca aktem wewnętrznym organu samorządu zawodowego adwokatury”, orzeczenie Wyższego Sądu Dyscyplinarnego z 22.02.2014, sygn. WSD 95/13.


Analizy CCBE zawierają także listę zabezpieczeń proceduralnych, jakie powinny być uwzględniony w zawieranych umowach z podwykonawcami, w wykonaniu których przetwarzane będą dane stanowiące tajemnicę zawodową. Zdaniem CCBE, poza kwestią wskazania prawa i sądu właściwego do rozstrzygania sporów w umowie określone powinny zostać między innymi: kwestia własności danych oraz wyłącznego dostępu do nich, zakaz korzystania z podwykonawców bez uzyskania wcześniejszej zgody usługobiorcy, miejsce fizycznej lokalizacji serwerów, prawo do kontroli i audytu przestrzegania zapisów umownych, zasady przetwarzania danych osobowych zgodne z krajowymi wymaganiami obowiązującymi usługobiorcę, kary umowne oraz zakres odpowiedzialności usługodawcy w przypadku naruszenia poufności informacji

Opracowania CCBE szczegółowo prezentują również szereg praktycznych technologii, jakie mogą być zastosowane przez prawników, jak i standardów międzynarodowowych (np. ISO/IEC 27001) oraz branżowych (dokumenty NIST) dotyczących poprawienia poziomu bezpieczeństwa przetwarzanych informacji. Dlatego powinny one stanowić punkt wyjścia do rozważenia wprowadzenia odpowiednich standardów branżowych przez polskie korporacje prawnicze. Temat ten zyskuje na znaczeniu zwłaszcza w związku z wprowadzeniem w Polsce, będących uzasadnione niejasności co do zgodności z prawem krajowym i międzynarodowym, znowelizowanych przepisów rozszerzających uprawnienia służb specjalnych w zakresie prowadzenia inwigilacji elektronicznej

Podsumowując, niezależnie od potrzeby wypracowania wspólnych regulacji na poziomie unijnym – skutkujących nadaniu tajemnicy zawodów prawniczych takich samych gwarancji, zwłaszcza w zakresie ochrony przed ingercją ze strony władzy publicznej, ale również nakładających obowiązek odpowiedniego zabezpieczenia informacji przez osoby i podmioty uczestniczące w ich przetwarzaniu (np. zagranicznych dostawców usług informatycznych) – konieczne wydaje się wzmocnienie reżimu ochrony przewidzianego w prawie krajowym. Inaczej bowiem, z braku wspólnych regulacji publicznonaprawnych (obejmujących podmiot zobowiązany, stopień ochrony związany z przetwarzaniem tajemnic zawodów prawniczych (w tym tajemnicą obrończą) w systemach informatycznych

665 M. Rojszczak, Ochrona tajemnicy adwokackiej a usługi świadczone w chmurze obliczeniowej, Studia Prawnicze 2017, nr 2, s. 158.
666 Temat szczegółowo omówiony w rozdziale 8.4.3 (s. 351). Przywołując rozważania dotyczące znowelizowanej treści ustawy o Policji (oraz analogicznych przepisów w pozostałych ustawach regulujących funkcjonowanie innych służb specjalnych), należy wskazać, że ustawodawca nie przewidział zakazu objęcia czynnością inwigilacyjnymi wynikającymi z art. 20c (a więc prowadzonymi bez kontroli sądowej) osób wykonujących zawody prawnicze.
usługodawców w głównej mierze związany będzie z konkretnymi zapisami kontraktowymi lub świadomością osób uczestniczących w wykonaniu umowy.

5.3.3. Tajemnica telekomunikacyjna

Omwiane przepisy stanowią rozwinięcie i transpozycję dyrektywy 2002/58 oraz innych przepisów prawa UE związanego z bezpieczeństwem łączności elektronicznej. Zgodnie z art. 288 TFUE dyrektywa wiąże państwa co do celu, pozostawiając im swobodę wyboru podjętych środków. Dlatego celem niniejszego punktu nie jest omawianie wymagań dotyczących bezpieczeństwa łączności elektronicznej funkcjonujących na terenie UE667, ale wskazanie różnic pomiędzy prawem UE a prawem krajowym – zarówno w zakresie przepisów nieprawidłowo zaimplementowanych, jak i wprowadzonych norm krajowych niemających odpowiednika w prawie UE. Ponieważ rozważania związane z funkcjonowaniem w polskim porządku prawnym ogólnego obowiązku retencji danych (art. 180a ustawy – Prawo telekomunikacyjne668, dalej: pr. tel.) oraz uprawnienia organów zostały przedstawione w rozdziale 8.4.3 (s. 352), zagadnienia te nie będą omawiane w niniejszym punkcie.

Zakres przedmiotowy tajemnicy telekomunikacyjnej został określony w art. 159 ust. 1 pr. tel. i obejmuje:

- dane dotyczące użytkownika,
- treść indywidualnych komunikatów,
- dane transmisyjne (metadane),
- dane o lokalizacji,
- dane o próbach uzyskania połączenia, w tym dane o nieudanych próbach połączenia.

Porównując powyższe zestawienie z prawem UE, można zauważyć, że pierwsze cztery pozycje znajdują odpowiedniki w dyrektywie 2002/58 – zwłaszcza w art. 4 ust. 1 (dane o użytkowniku), art. 5 ust. 1 (treść komunikacji oraz dane transmisyjne, nazywane na gruncie dyrektywy „danymi o ruchu”) i art. 9 (dane o lokalizacji inne niż dane transmisyjne). W przypadku ostatniego punktu – tj. danych o próbach uzyskania połączenia – należy rozważyć, dlaczego ustawodawca zdecydował się na jego wyodrębnienie z grupy danych transmisyjnych. Pierwotną przyczyną było dostosowanie do terminologii wprowadzonej w

667 Problematyka ta została omówiona w rozdziale 4.4.2 (s. 138).
668 Ustawa z dn. 16 lipca 2004 – Prawo telekomunikacyjne (Dz.U. z 2016 r. poz. 1489 ze zm.).
dyrektywie 2006/24 (dyrektywa retencyjna), w szczególności do definicji „nieudanej próby połączenia”\(^{669}\). Pozostawienie jednak wskazanego przepisu w obrocie prawnym, także po orzeczeniu przez TSUE nieważności dyrektywy retencyjnej każe rozważyć możliwe implikacje dla zakresu tajemnicy telekomunikacyjnej oraz czytelności całej normy prawnej wynikającej z art. 159 ust. 1 pr. tel.

Zgodnie z przyjętą na gruncie dyrektywy 2002/58 definicją „dane o ruchu oznaczają wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi”. Jednocześnie w motywie 15. dyrektywy wskazano, że mogą one także „obejmować dane odnoszące się do wyznaczania trasy, długości, czasu lub pojemności komunikatu, zastosowanego protokołu, lokalizacji terminala nadawcy lub odbiorcy, sieci, w której komunikat powstaje lub zostaje przerwany, początku, końca lub długości połączenia”.

Jeżeli przyjąć, że dane transmisyjne muszą być związane z komunikatem, to informacje przesyłane przez sieć w ramach próby nawiązania połączenia nie stanowią danych transmisyjnych – a w konsekwencji zastosowane na gruncie pr. tel. rozróżnienie jest prawidłowe. Z drugiej strony, jeżeli uznać, że komunikat – a więc treść merytoryczna przekazu – może być wyrażony w inny sposób, np. samą próbą nawiązania połączenia, to dane o ruchu wymieniane w sieci telekomunikacyjnej w związku z tym zdarzeniem również powinny być objęte tajemnicą telekomunikacyjną. Zastosowana w pr. tel. redakcja przepisu rozwiązuje te niejasności i prowadzi do uznania, że wszystkie dane transmisyjne, także te związane z nieudanymi próbami nawiązania połączenia, powinny być chronione w taki sam sposób.

Krąg podmiotów zobowiązananych obejmuje nie tylko przedsiębiorców uczestniczących w wykonywaniu działalności telekomunikacyjnej, ale i podmioty z nimi współpracujące (art. 160 ust. 1). Co więcej, przedsiębiorca telekomunikacyjny ponosi odpowiedzialność za naruszenie tajemnicy przez podmioty działające w jego imieniu (art. 162 ust. 2). W art. 159 ust. 3 wskazano ponadto, że pod pojęciem naruszenia tajemnicy należy rozumieć nie tylko przypadki skutkujące jej ujawnieniem, ale i przetwarzaniem treści albo danych bez podstawy ustawowej. W rezultacie należy uznać, że prawodawca określił szeroki zakres podmiotów zobowiązanych oraz enumeratywne przypadki, w których przetwarzanie danych objętych tajemnicą telekomunikacyjną jest dopuszczalne.

Zgodnie z art. 15a ust. 2 dyrektywy państwa członkowskie zostały zobowiązane do ustanowienia organu krajowego uprawnionego do nadzorowania przestrzegania oraz nakazywania zaprzestania naruszeń przepisów wprowadzonych w drodze implementacji dyrektywy. W przypadku polskiej ustawy prawodawca zdecydował się na przyznanie takich uprawnień ministrowi właściwemu do spraw informatyzacji oraz Prezesowi Urzędu Komunikacji Elektronicznej (art. 189 ust. 1). Jednocześnie wskazał Prezesa UKE jako organ regulacyjny w dziedzinie rynku usług telekomunikacyjnych i pocztowym (art. 190 ust. 1). Biorąc pod uwagę, że zakres tajemnicy telekomunikacyjnej obejmuje także dane osobowe oraz uwzględniając uprawnienia GIODO związane z nadzorem nad prawidłowością przestrzegania przepisów o ochronie danych, oczywiste jest, że część zadań nadzorczych i kontrolnych związanych z prawidłowością ochrony tajemnicy telekomunikacyjnej wykonuje także organ właściwy do ochrony danych osobowych. Prawodawca wprost wskazał uprawnienia GIODO w redakcji przepisów art. 174a-d, przy czym art. 174a dotyczący przypadków naruszenia bezpieczeństwa danych osobowych stanowi bezpośrednią transpozycję art. 4 ust. 3 dyrektywy 2002/58.

W tym miejscu warto przypomnieć wcześniejsze rozważania związane z wymaganiem niezależności organu nadzorczego, także w kontekście orzecznictwa TSUE („wyłączenie spod jakiegokolwiek wpływu z zewnątrz mogącego nadawać kierunek decyzjom”670), dla rozwiązań przyjętych w polskim prawodawstwie. O ile bowiem przepisy UE wymagają zapewnienia przez ustawodawstwo państw członkowskich niezależności zarówno organom nadzorczym powołanym w obszarze ochrony danych, jak i łączności elektronicznej, to uzasadnione są wątpliwości, czy krajowe przepisy realizują ten wymóg w odniesieniu do Prezesa UKE. W szczególności niejasności mogą być związane z trybem powołania zastępców Prezesa – o ile w przypadku GIODO zastępca Generalnego Inspektora jest powoływany przez ten sam organ, który powołuje Generalnego Inspektora (czyli – zgodnie z art. 12a ust. 1 uodo – przez Sejm), to zastępcy Prezesa UKE są powoływani przez ministra właściwego do spraw informatyzacji (art. 190 ust. 8 pr. tel.). Kolejne różnice pojawiają się w zakresie sposobu nadania statutu urzędowi, za pośrednictwem którego organ wykonuje swoje zadania. W przypadku Generalnego Inspektora statut Biura GIODO nadaje Prezydent w drodze rozporządzenia (art. 13 ust. 3 uodo), w przypadku Prezesa UKE – minister właściwy do spraw informatyzacji (art. 193 ust. 3 pr. tel.). Porównanie tych różnic oraz zestawienie ich z orzecznictwem TSUE (w

szczegółności z wyrokami w sprawach C-518/07, C-614/10 i C-288/12 – zob. rozdział 4.5.4) pozwala na sformułowanie poniższych wniosków:

- w przepisach prawa krajowego odmiennie uregulowano kwestię niezależności GIODO oraz Prezesa UKE; wymagana dla organu ochrony danych „całkowita niezależność” nie została zapewniona w przypadku regulatora rynku telekomunikacyjnego.

- w odniesieniu do ochrony danych osobowych w sektorze łączności danych pojawia się dualizm nadzorczy (GIODO/Prezes UKE) - ten sam obszar może być kontrolowany przez instytucje posiadające różne umocowanie w zakresie niezależności podejmowanych decyzji.

powołany w miejsce GIODO. Propozycja ta została – jeszcze przed formalnym przedstawieniem przez Minister Cyfryzacji – krytycznie oceniona przez GIODO671.

Wraz z rozpoczęciem stosowania ogólnego rozporządzenia oraz wejściem w życie projektowanej ustawy o ochronie danych osobowych, różnice dotyczące niezależności organu właściwego do ochrony danych osobowych (GIODO/PUODO) oraz nadzorującego sektor łączności elektronicznej (PUKE) mogą się jeszcze powiększyć. Przyczyną jest planowane nadanie PUODO swobody w kształtowaniu organizacji Urzędu (art. 47 ust. 3 projektu uodo), a także zmieniony – względem obowiązującego – tryb powoływania i odwoływania zastępców Prezesa.

Zgodnie z art. 37 ust. 1 projektu uodo Prezes Urzędu może wykonywać swoje zadania przy pomocy do trzech zastępców. W aktualnej wersji projektu ustawy (z dnia 16 marca 2018), ich powoływanie jest samodzielnym uprawnieniem Prezesa, które może być wykonywane z jego własnej inicjatywy oraz bez konieczności przeprowadzania konsultacji zewnętrznych. We wcześniejszych projektach672. Ministerstwo Cyfryzacji proponowało, aby powoływanie dwóch zastępców następowało na wniosek ministra właściwego do spraw informatyzacji, a jednego na wniosek ministra właściwego do spraw wewnętrznych. W takim przypadku, zastępcy Prezesa byliby wskazywani de facto bez jego udziału. Rozwiązanie to budziło poważne zastrzeżenia w zakresie zgodności z prawem UE, zwłaszcza dotyczące niezależności organu nadzoru od wpływów władzy wykonawczej673. Problem ten został zauważony w procedurze opiniowania projektu przez RPO674. W efekcie propozycja Ministerstwa Cyfryzacji została odrzucona w trakcie uzgodnień międzyresortowych. Jednocześnie jednak wskazano, że Ministerstwo Cyfryzacji oraz Ministerstwo Spaw Wewnętrznych i Administracji postulują przywrócenie trybu powoływania zastępców na ich wniosek – ale po przeprowadzeniu konsultacji z KE w zakresie zgodności tej koncepcji z prawem UE675.

---

672 Por treść art. 31 ust. 2-7 projektu z dn. 3.03.2018 ustawy o ochronie danych osobowych, http://cli.re/GZeQX8.
673 Problematyka ta została szeroko omówiona w rozdziale 4.5.4.1.

Bierność polskiego prawodawcy może w niektórych przypadkach skutkować korzystnymi rozwiązaniami z punktu widzenia funkcji ochronnej dla użytkowników. Przykładem może być anonimizacja danych, która jak wyjaśniono wcześniej pozwala na wyłączenie lub ograniczenie stosowania przepisów o ochronie danych. Możliwość taka wynika z przepisów dyrektywy 95/46 (por. motyw 26.), stanowiącej jej implementację krajowej ustawy o ochronie danych osobowych (art. 2 ust. 3) oraz przepisów nowego ogólnego rozporządzenia (por. motyw 26.). Z uwagi na włączenie danych osobowych abonentów w zbiór informacji objętych tajemnicą telekomunikacyjną, wyjaśnienia wymagają konsekwencje z jakimi wiąże się zastosowanie technik anonimizacji także na gruncie prawa telekomunikacyjnego. W szczególności w pr. tel. brakuje przepisu o skutku analogicznym do art. 2 ust. 3 uodo, a więc prowadzącego na ograniczenie zakresu stosowania reżimu określonego ustawą wobec zbioru danych poddanego anonimizacji. Co więcej, obowiązująca treść przepisu art. 162 ust. 1 pr. tel. stoi na przeszkodzie, aby wykorzystać dane objęte

---

676 Zob. omówienie OTT na s. 189.
677 Z definicji komunikatu wskazanej w art. 2 pkt 17 pr. tel., M. Rogalski wywodzi wniosek, że zakresem tajemnicy jest objęta „treść (...) przesyłana za pomocą głosu, w sposób tekstowy, np. poprzez komunikator internetowy, e-mail, kodowany albo niekodowany”. Należy jednak zauważyć, że obowiązek ten dotyczy przedsiębiorcy telekomunikacyjnego, a nie usługodawcy świadczącego usługi OTT. Jest to istotne rozróżnienie, ważne przy omawianiu zagadnienia zakresu podmiotowego tajemnicy telekomunikacyjnej. Cytat za: M. Rogalski, Tajemnica telekomunikacyjna i ochrona danych użytkowników końcowych, [w:] „Prawo telekomunikacyjne”, LEX 2011.
tajemnicą telekomunikacyjną – nawet po ich anonimizacji – w celach innych niż związane z realizacją usługi świadczonej dla użytkownika lub wskazanych w przepisie rangi ustawowej.

W doktrynie prezentowane są poglądy, że powyższa obserwacja prowadzi do wniosku o niepełnej implementacji do krajowego systemu prawnego przepisów dyrektywy 2002/58⁶⁸⁰. Pogląd taki może wydawać się zasadny, zwłaszcza uwzględniając, że w treści dyrektywy 2002/58 kilkukrotnie wskazywana jest możliwość zastosowania anonimizacji jako alternatywy dla usunięcia danych (np. dane o ruchu – art. 6 ust. 1, dane o lokalizacji – art. 9 ust. 1). W efekcie postuluje się wyłączenie z zakresu tajemnicy telekomunikacyjnej danych dotyczących użytkowników będących osobami fizycznymi, co prowadziłoby do ograniczenia reżimu ochronnego tajemnicy telekomunikacyjnej do typowych danych transmisyjnych (w tym lokalizacyjnych). Wskazuje się przy tym na potrzebę dopuszczenia anonymizacji danych transmisyjnych jako ekwiwalentu ich usuwania, co z kolei powinno pozwolić na ich anonimizację i dalsze wykorzystanie przez przedsiębiorców telekomunikacyjnych. Jakkolwiek przedstawiona propozycja jest interesująca i warta rozważenia, to należy zwrócić uwagę na jej zauważalne mankamenty. Po pierwsze, prawodawca unijny nie wymaga uwzględnienia możliwości anonimizacji danych, a jedynie zaznacza przydatność tej techniki i wskazuje ją jako alternatywę dla usunięcia danych (por. treść motywów 9, 26 i 28 oraz art. 6 ust. 1 i art. 9 ust. 1 dyrektywy 2002/58). Dlatego wydaje się, że krajowy prawodawca, nie przewidując możliwości anonimizacji, działał w granicach wynikających ze swobody wyboru formy i środków określonych w art. 288 TFUE. Sama anonimizacja jest techniką o ograniczonym zastosowaniu praktycznym, zwłaszcza w odniesieniu do dużych zbiorów danych (a takie są w posiadaniu operatorów telekomunikacyjnych). Wydaje się zasadne, aby przetwarzanie tych danych, nawet w przypadku ich anonimizowania, nie podlegało zwolnieniu z reżimu wynikającego z przepisów o ochronie tajemnicy telekomunikacyjnej – zwłaszcza biorąc pod uwagę możliwości techniczne związane z Big Data oraz ponowną identyfikacją podmiotów danych. W tym przypadku interes przedsiębiorców telekomunikacyjnych nie powinien być uznany za ważniejszy od uzasadnionych względów ochrony prywatności jednostek (por. art. 7 pkt f dyrektywy 95/46 i art. 6 ust. 1 pkt f ogólnego rozporządzenia). Wyodrębnienie danych osobowych („danych dotyczących użytkownika”) ze zbioru stanowiącego tajemnicę telekomunikacyjną jest koncepcją ciekawą i alternatywną względem przedstawionej wcześniej, związanej z przypisaniem funkcji nadzorczych nad obszarem tajemnicy telekomunikacyjnej do organu odpowiedzialnego za regulacje związane z

---

ochroną danych osobowych. Należy jednak zwrócić uwagę, że jej zastosowanie może prowadzić do zaledwie pozornego rozdzielenia zbioru stanowiącego tajemnicę telekomunikacyjną od zbioru danych osobowych. W codziennym funkcjonowaniu operatorów telekomunikacyjnych dane należące do obu tak zdefiniowanych zbiorów byłyby i tak przetwarzane łącznie. Co więcej, z uwagi na istniejące orzecznictwo TSUE część danych przesyłowych musiałaby zostać zakwalifikowana jako dane osobowe. W konsekwencji wydaje się, że nie ma możliwości faktycznego rozdzielenia tych dwóch zbiorów, tak aby móc wprowadzić bardziej elastyczne formy przetwarzania związane z danymi transmisyjnymi. Przy obecnym stanie możliwości technicznych, zbiór danych (metadanych) dotyczących aktywności użytkownika (w tym także geolokalizacja urządzenia abonenckiego czy czasy logowań do sieci) powinny być przetwarzane i zabezpieczane tak jak dane osobowe.

Na zakończenie warto omówić niejasności związane z interpretacją przepisów ustawy – Prawo telekomunikacyjne w zakresie jej zgodności z ogólnym rozporządzeniem. Zgodnie z art. 95 co do zasady rozporządzenie nie nakłada dodatkowych obowiązków na osoby fizyczne i prawne w zakresie, w jakim podlegają szczegółowym regulacjom ustanowionych w wyniku implementacji dyrektywy 2002/58. Nie dotyczy to jednak przepisów ustawowych, które nie stanowią transpozycji dyrektywy. Takie przepisy powinny być zgodne z ogólnym rozporządzeniem. W wydanym stanowisku KPP Lewiatan zwraca uwagę na uzasadnione wątpliwości, czy zakres tajemnicy telekomunikacyjnej – wykraczający poza wymagany dyrektywą 2002/58 – nie wymaga dostosowania w taki sposób, aby nie prowadził do kolizji z przepisami ogólnego rozporządzenia.

5.4. Podsumowanie

Z przedstawionej w niniejszym rozdziale analizy wynika, że działania krajowego prawodawcy związane ze wzmacnianiem funkcji ochronnej stanowionych rozwiązań prawnych w dziedzinie ochrony prywatności należy uznać za niewystarczające. Prace związane z implementacją ogólnego rozporządzenia de facto ograniczają się do usunięcia nieścisłości i wycofania nieaktualnych aktów prawnych. W ten sposób nie wykorzystuje się możliwości przeprowadzenia głębszej reformy regulacji, wychodzących także naprzeciw postulatom zawartym w projekcie nowej regulacji o bezpieczeństwie w łączności.

681 Uwagi dotyczące zmian w prawie krajowym koniecznych w związku z przyjęciem rozporządzenia w sprawie ochrony danych osobowych, KPP Lewiatan 18.07.2016, https://goo.gl/aX7RDf, s. 8.
elektronicznej. Z drugiej strony prawodawca nie rozwija regulacji krajowych niepodlegających standaryzacji w ramach prawa UE.

Biernej postawy ustawodawcy nie można jednak zaobserwować w zakresie stanowienia nowych przepisów wzmacniających uprawnienia inwigilacyjne służb, czego efektem jest znaczne ograniczenie gwarancji związanych z ochroną prywatności w Polsce682. Dlatego wydaje się, że przyczyną braku nowelizacji czy wzmacniania przepisów ochronnych nie jest brak wizji czy strategii władz polskich. Wręcz przeciwnie, uzasadniony wydaje się pogląd, że działania takie są skutkiem zmiany orientacji rządu oraz większości parlamentarnej w zakresie roli i znaczenia w prawodawstwie krajowym ochrony praw podstawowych, w tym także prawa do prywatności.


Wniosek związany z niewystarczającą aktywnością władzy publicznej może być też odniesiony do działalności krajowego organu nadzoru do spraw ochrony danych osobowych. Nie bez przyczyny organ ten został na gruncie przepisów krajowych i europejskich umocowany w sposób szczególny, w pełnej niezależności od władzy wykonawczej. W efekcie należałoby oczekiwać większej inicjatywy w zakresie krytycznej oceny istniejącej legislacji, ale również wskazywania kierunków doskonalenia prawodawstwa krajowego. Jako przykład można wskazać działania podejmowane przez brytyjski organ nadzoru ICO

682 Szczegółowe rozważania na temat krajowych przepisów inwigilacyjnych przedstawiono w rozdziale 8.4.3 (s. 351).
683 Przykładem mogą być działania władz Rosji na tle stosowania EKPC oraz uznawania orzeczeń ETPC. W 2005 roku przyjęto przepisy krajowe prowadzące do ograniczenia skuteczności prawomocnych wyroków Trybunału (zob. rozdział 8.4.1, s. 350). W ten sposób – działając de facto niezgodnie z prawem międzynarodowym – podważono gwarancje związane z możliwością ochrony praw przed instytucjami międzynarodowymi. Z drugiej strony, rosyjski ustawodawca przyjął przepisy prowadzące do utrudnienia lub uniemożliwienia korzystania z technicznych środków ochrony prywatności (zob. rozdział 8.3.4, s. 359). W efekcie z jednej strony Rosja nie stosuje się do prawodawstwa związanego z europejską konwencją (w tym wyroków ETPC), z drugiej – wprowadza kolejne przepisy prowadzące do dalszej ingerencji państwa w prawa jednostki.
(Information Commissioner’s Office), który przygotowuje rozbudowane analizy związane z różnymi aspektami ochrony prywatności w cyberprzestrzeni – w tym dotyczące stosowania monitoringu wizyjnego\textsuperscript{684}, analityki Big Data\textsuperscript{685} czy monitorowania sieci Wi-Fi\textsuperscript{686}. Każde z tych zagadnień odnosi się do ważnego i aktualnego problemu w obszarze ochrony prywatności, dla którego dopiero dyskutowana jest potrzeba wprowadzenia odpowiednich regulacji. GIODO nie realizuje podobnych działań na rynku krajowym\textsuperscript{687}.

Przyjęcie ogólnego rozporządzenia nie powinno być postrzegane jako rozwiązanie problemów dotyczących niewystarczającej jakości stanowienia oraz stosowania prawa na poziomie krajowym. Oczywiście, dzięki bezpośredniej skuteczności oraz prymatowi prawa UE normy wynikające z rozporządzenia przyczynią się do wzmocnienia mechanizmów ochronnych i regulacyjnych związanych z poszanowaniem prywatności w Polsce. Rolą prawa UE nie jest jednak zastępowanie prawa krajowego, ale jego uzupełnianie i ujednolicanie na płaszczyźnie wspólnego rynku wewnętrznego. Prawodawca krajowy zawsze będzie miał duży wpływ na kształtowanie swobód wynikających z traktatów i prawa międzynarodowego w relacjach wewnętrznych, a zaniechania lub celowe działania z jego strony mogą prowadzić do skutecznego ograniczenia praw przynależnych jednostkom.

\textsuperscript{684} In the picture: A data protection code of practice for surveillance cameras and personal information, ICO, 9.06.2017, http://cli.re/6DDDK6.
\textsuperscript{685} Big data, artificial intelligence, machine learning and data protection, ICO, 18.08.2017, http://cli.re/67YbyX.
\textsuperscript{686} Wi-Fi location analytics, ICO, 16.02.2016, http://cli.re/6VWJey.
CZĘŚĆ 2. OCHRONA PRYWATNOŚCI W DOBIE SPOŁECZEŃSTWA INFORMACYJNEGO – WYBRANE ZAGADNIENIA

Rozdział 6. Przetwarzanie danych w modelu chmury obliczeniowej

6.1. Wprowadzenie

Jednym z ważniejszych aspektów ochrony prywatności w cyberprzestrzeni jest zachowanie autonomii informacyjnej jednostki, rozumiane jako prawo do decydowania o zakresie udostępnianych innym informacji na swój temat. W świecie cyfrowym przejawem autonomii jest prawo do publikowania, modyfikowania lub usuwania treści z domeny publicznej (np. informacji czy zdjęć z serwisów społecznościowych). Autonomia informacyjna nie będzie jednak pełna, jeżeli jednostka zostanie pozbawiona kontroli nad obiegem informacji – przez co należy w szczególności rozumieć brak skutecznych środków pozwalających jej na kształtowanie kręgu osób mających dostęp do informacji. Problem kontroli dostępu do informacji nie przejawia się wyłącznie w limitowaniu liczby jej zamierzonych odbiorców. Formą nadzoru jest także posiadanie wiedzy i kontrolowanie przekazywania danych do przetwarzania przez usługodawcę (np. operatora e-usługi świadczonej w Internecie). Problem ten można podsumować w następujący sposób: aby kontrolować prywatność informacji w cyberprzestrzeni, nie wystarczy wiedzieć, komu została udostępniona, ale i komu informacje te udostępnili operator wykorzystywanej e-usługi. Istotnym problemem utrudniającym realizację tego uprawnienia jest złożoność systemów przetwarzania danych oraz trudność w zrozumieniu i odniesieniu terminologii technicznej i prawniczej, stosowanej w regulaminach korzystania z portali internetowych, do faktycznych zagrożeń związanych z ochroną prywatności i danych osobowych. W szczególności problem ten jest aktualny w przypadku coraz popularniejszej formy przetwarzania danych, jaką jest przetwarzanie w chmurze (ang. cloud computing). Jest to rozwiązanie stosowane obecnie powszechnie i w odniesieniu do szerokiego spektrum usług dostępnych w Internecie (jak usługi poczty elektronicznej, składowania plików, mediów strumieniowych, portale społecznościowe itp.). Przetwarzanie w chmurze jest szybszą, tańszą, bardziej niezawodną i efektywniejszą formą udostępniania globalnych serwisów internetowych. Wiąże się również z nowymi zagrożeniami i ryzykami dla prywatności przetwarzanych informacji. Rozpatrzmy następujący przykład:
Użytkownik korzystając zakłada konto dostępowe w prowadzonym przez krajowego przedsiębiorcę portalu internetowym, oferującym usług z zakresu profilaktyki zdrowia. W ramach uzupełnienia swojego profilu użytkownik przekazuje dobrowolnie informacje, które są potrzebne z uwagi na funkcjonalność e-usługi: w tym dane osobowe, adresowe, a także informacje na temat stanu zdrowia. Administrator danych zapewnił, że informacje te nie będą przekazywane innym podmiotom bez wiedzy użytkownika, za wyjątkiem podwykonawców świadczących usługi techniczne utrzymania portalu.

Administrator korzysta z usług jednego z wiodących globalnych dostawców usług przetwarzania w chmurze. Dostawca ten posiada 20 centrów przetwarzania danych, zlokalizowanych w 15 krajach, także poza obszarem UE – między innymi w Stanach Zjednoczonych i Chinach. Sposób organizacji procesu przetwarzania powoduje, że dane użytkownika są jednocześnie dostępne we wszystkich centrach danych, co radykalnie zmniejsza ryzyko niedostępności w przypadku awarii.

Użytkownik korzystając z dostępnej online usługi potwierdza, że jego dane zostały ujawnione w jednym z wielu mających miejsce w ostatnich latach incydentów bezpieczeństwa. Może w ten sposób określić przedsiębiorcę, któremu wykradziono dane, ale nie wie, czy i jaka relacja łączyła tę firmę z operatorem usługi, z której korzysta, oraz jakie ma prawa w związku z zaistniałym naruszeniem – zwłaszcza biorąc pod uwagę, że ujawnienie danych miało miejsce w Brazylii.

Powyższy opis – jakkolwiek przedstawia sytuację hipotetyczną – zawiera istniejące usługi, formy przetwarzania i zagrożenia. Także w Polsce funkcjonują e-usługi związane z pośrednictwem w wyszukiwaniu usług medycznych, w których ramach których użytkownicy mają możliwość udostępniania informacji o stanie zdrowia. Istnieją również wyspecjalizowane portale będące de facto wyszukiwarkami pozwalającymi na sprawdzenie, czy dane osobowe określonej osoby zostały ujawnione w jednym z wycieków danych. Wiodącą tego typu usługę oferuje serwis „Have I been pwned”, w którego bazie według stanu na 22 marca 2018 roku

---


689 Serwis Have I been pwned (https://havebeenpwned.com) zawiera informacje ujawnione w efekcie najpoważniejszych włamań do portali internetowych w ostatnich latach – między innymi bazie użytkowników MySpace (ponad 359 mln kont), LinkedIn (ponad 160 mln kont) czy Adobe (ponad 150 mln kont). Zawiera także dane pochodzące z wykryzionej bazy użytkowników największego rosyjskiego serwisu
zgromadzono informacje na temat 4,9 mld kont użytkowników ujawnionych w efekcie kradzieży danych z 273 portali internetowych.

Według badań Eurostatu, w 2014 roku ponad 20% badanych korzystało z usług przechowywania plików w chmurze obliczeniowej. Jako przyczynę korzystania z tego typu usług 59% respondentów wskazywało na łatwość w dostępie do danych z dowolnego urządzenia lub lokalizacji. Taka sama liczba badanych uznała, że przechowywanie danych w chmurze ułatwia ich udostępnianie, a 55% wskazało na aspekty ochrony przed utratą danych składowanych lokalnie. Z drugiej strony, badania Eurostatu wykazały, że duża część ankietowanych, chociaż używała Internetu, to nie potrafiła zdefiniować, czym są usługi przetwarzania w chmurze i w związku z tym wskazać, czy z nich korzysta (26%). Z kolei 40% korzystających z Internetu i świadomych istnienia usług przechowywania danych w chmurze jako przyczynę niekorzystania z tych usług wskazało obawy związane z bezpieczeństwem lub prywatnością.

Usługi przetwarzania w chmurze nie są kierowane wyłącznie do użytkowników indywidualnych czy biznesowych. Coraz częściej są wykorzystywane przez podmioty publiczne – także w zakresie przetwarzania informacji dotyczących obywateli. W efekcie nawet jeżeli technologia ta nie jest wybierana przez użytkowników z uwagi na obawy związane z ochroną prywatności, może okazać się, że dotyczące ich dane i tak są przetwarzane w usługach cloud computingu w efekcie korzystania z takich usług przez podmioty publiczne.

Rozważania związane z charakterem usług świadczonych w chmurze obliczeniowej i ryzykami, jakie się z nimi wiążą, mają więc bardzo praktyczny wymiar prawny – zrozumienie, z wykorzystaniem jakich środków kształtować stosunki umowne z operatorami usług świadczonych w modelu chmury obliczeniowej, aby zwiększyć kontrolę nad

**Podstawowe źródła**


691 Wskaźnik ten wynosił 35% w grupie 16-24 lata

udostępnianymi informacjami, a w konsekwencji zapewnić skuteczność praw i gwarancji wynikających z krajowego porządku prawnego.

6.2. Hipotezy badawcze

Przystępując do omówienia charakteru usług przetwarzania w chmurze, konieczne jest wstępne określenie najważniejszych hipotez badawczych – odzwierciedlających kontekst zdefiniowanej we wstępie głównej tezy niniejszej pracy:

1) Uregulowanie stosunków umownych cloud computingu wyłącznie regulacjami prawa prywatnego (swoboda zawierania umów) prowadzi do nierównomiernej ochrony praw użytkowników, których dane podlegają przetwarzaniu.

2) Przepisy prawa krajowego są niewystarczającą ochroną danych przekazywanych do dostawców usług chmury obliczeniowej.

3) Prawo UE oraz konwencje regionalne (w szczególności EKPC oraz Konwencja 108 RE) przyczyniają się do zwiększenia gwarancji związanych z ochroną prywatności, nie prowadzą jednak do kompleksowego rozwiązania wszystkich zagrożeń wynikających z globalnego charakteru usług przetwarzania w chmurze.

4) Przekazanie danych usługodawcy, który korzysta z usług przetwarzania w chmurze, może prowadzić do naruszenia zasady „uzasadnionego oczekiwania prywatności”.

6.3. Charakterystyka zjawiska

6.3.1. Definicja usług przetwarzania w chmurze

Wprowadzenie terminu „chmura obliczeniowa” w odniesieniu do sposobu przetwarzania danych jest związane ze sposobem graficznego opisu publicznych sieci informatycznych (w szczególności – Internetu) na schematach technicznych. Tradycyjnie sieci takie są reprezentowane właśnie przez symbol (grafikę) chmury, co z jednej strony jest wystarczające, aby zaprezentować wzajemne połączenia pomiędzy opisywaną siecią a Internetem, a z drugiej – obrazuje fakt, że struktura Internetu jest zbyt skomplikowana, aby ją odzwierciedlać na jakimkolwiek schemacie.

Zgodnie z najczęściej przywoływano w literaturze definicją formalną, wprowadzoną przez NIST, chmurę obliczeniową można określić jako sposób dostępu poprzez sieć
komputerową do współdzielonych i łatwo konfigurowalnych zasobów obliczeniowych (sieci, serwerów, aplikacji czy usług), które na żądanie i dynamicznie mogą być przydzielane i zwalniane, przy równoczesnym minimalnym zaangażowaniu obsługi technicznej. Definicja ta określa najważniejszą cechę chmury – jest nią separacja infrastruktury od usługi na niej świadczonej. Gdy wynajmuje się zasoby od dostawcy w modelu chmury obliczeniowej, definiowane są najważniejsze parametry jakościowe usługi (moc obliczeniowa, czas dostępu, przepustowość łączy itp.), a nie konkretne elementy infrastruktury IT, które zostaną udostępnione. Co więcej, najczęściej usługobiorca nie wie, z wykorzystaniem jakich zasobów i gdzie zlokalizowanych świadczona będzie jego usługa.

Omawiając terminologię, wskazać należy, że pojęcie użytkownika używane w odniesieniu do przetwarzania w chmurze nie zawsze powinno być łączone z usługobiorcą cloud computingu. Użytkownikiem w potocznym rozumieniu jest odbiorca usługi końcowej, podczas gdy użytkownikiem (usługobiorcą) cloud computingu od strony formalnej może być operator usługi świadczonej dla użytkownika. W takim rozumieniu dostawca usług przetwarzania w chmurze jest podwykonawcą usługodawcy internetowego, z usług którego korzysta użytkownik końcowy. Rozróżnienie to jest istotne i ma szczególne znaczenie przy rozważaniach prawnych, ponieważ pozwala na zdefiniowanie stron poszczególnych stosunków umownych oraz środków ochrony prawnej, które każda z nich (użytkownik, usługodawca internetowych, dostawca usługi przetwarzania w chmurze obliczeniowej) może i powinna uwzględnić w zawieranych umowach.

Obecnie wszystkie główne usługi internetowe korzystają z różnych form cloud computingu, wliczając w to najważniejsze usługi firm takich jak Google, Amazon czy Dropbox. Każdy użytkownik, logując się na swoje konto pocztowe w jednym z popularnych serwisów online (np. globalny GMail czy Outlook 365, ale także usług oferowanych przez krajowych dostawców, takich Home.pl czy Nazwa.pl), korzysta z infrastruktury technicznej udostępnionej w chmurze.

6.3.2. Podział ze względu na zasady współkorzystania (modele implementacyjne)

W praktyce pod pojęciem przetwarzania w chmurze rozumieć należy kilka różnych form świadczenia usługi, z którymi wiąże się różny wpływ usługobiorcy na techniczny


694 Jak dowodzi P. Schwartz, model przetwarzania w chmurze okazał się dużym sukcesem ekonomicznym – rynek cloud computingu był już w 2010 roku wyceniany na ponad 40 mld USD, a do 2020 roku oczekuje się, że wartość ta przekroczy 240 mld USD. P. Schwartz, Information privacy..., op. cit., s. 1627.
sposób świadczenia usługi. Cechą odróżniającą wskazane poniżej modele są odmienne zasady współkorzystania z tych samych zasobów przez różnych usługobiorców.\textsuperscript{695}

- **Chmura publiczna** (ang. *public cloud*) – najbardziej popularny model świadczenia *cloud computing*, zakładający współdzielenie zasobów pomiędzy wielu użytkowników oraz brak ograniczeń co do sposobu i formy przetwarzania danych w zakresie udostępnionej infrastruktury. Użytkownik, korzystając z usług chmury publicznej, nie wie zatem, w jakich dokładnie lokalizacjach będą przetwarzane jego dane, a także z wykorzystaniem jakie infrastruktury. Chmura publiczna pozwala na minimalizację kosztów oraz optymalizację parametrów usług. Jest najczęściej wykorzystywana do oferowania masowych, stypizowanych usług dla szerokiego grona odbiorców (np. usługi poczty elektronicznej, przechowywania plików, media strumieniowe). Z uwagi na brak możliwości indywidualnej modyfikacji parametrów świadczonych usług (wykorzystanie wzorców umów) z punktu widzenia użytkownika końcowego wiąże się jednak z największymi ryzykami w zakresie ochrony prywatności.

- **Chmura prywatna** (ang. *private cloud*) – w takim wariancie chmura obliczeniowa jest projektowana i eksploatowana przez jeden lub grupę podmiotów na wyłączność. Zasoby infrastrukturalne – zarówno informatyczne (procesory, macierze dyskowe, urządzenia sieciowe), jak i organizacyjne (np. fizyczne, odseparowane miejsca przetwarzania danych) – są dedykowane do obsługi określonego klienta i nie są współdzielone z innymi usługobiorcami. W takim przypadku najczęściej wszystkie elementy implementacyjne rozwiązania (konfiguracja środowiska IT, jego wydajność, lokalizacja geograficzna) jest szczegółowo uzgadniana pomiędzy usługodawcą i usługobiorcą. Rozwiązanie to, ze względu na swoje koszty, znajduje praktyczne zastosowanie do obsługi dużych podmiotów, często korporacji międzynarodowych.

- **Chmura hybrydowa** (ang. *hybrid cloud*) – model łączący cechy chmury publicznej oraz prywatnej i zazwyczaj realizowany z wykorzystaniem obu wskazanych technologii; typowym przykładem zastosowania chmury hybrydowej jest wykorzystywanie chmury publicznej do przechowywania informacji ogólnodostępnych, podczas gdy dane wrażliwe są gromadzone i przetwarzane w chmurze prywatnej. Rozwiązanie takie jest tańsze niż korzystanie wyłącznie z

chmury prywatnej, a jednocześnie pozwala na eliminację jednego z podstawowych ryzyk prawnych związanych z chmurą publiczną – przetwarzania danych poza granicami jurysdykcji właściwej dla usługobiorcy.

- Chmura dedykowana/wspólna (ang. community cloud) – szczególny przykład chmury hybrydowej, tworzony w oparciu o określone wymagania regulacyjne lub prawne. Przykładem może być chmura dedykowana utworzona przez brytyjski rząd na potrzeby obsługi podmiotów z sektora publicznego (G-Cloud). Chmury dedykowane są tworzone w określonym celu, mają wskazany krąg odbiorców oraz zasady przetwarzania. Prawidłowo zaimplementowane pozwalają na odnoszenie korzyści z modelu przetwarzania w chmurze (zmniejszenie kosztów względem zakupu własnej infrastruktury, zwiększenie wydajności i wskaźników dostępności) przy jednoczesnym ograniczeniu lub wyeliminowaniu ryzyk prawnych (funkcjonowanie chmur hybrydowych w ramach istniejącego reżimu prawnego).

W praktyce użytkownicy indywidualni mają możliwość skorzystania z usług świadczonych w chmurze publicznej. Model przetwarzania w chmurze prywatnej i hybrydowej wiąże się z dużymi kosztami, dlatego korzystają z niego głównie przedsiębiorcy i podmioty publiczne. Z tego powodu w dalszych rozważaniach przedstawiona zostanie analiza głównie zagrożeń związanych z korzystaniem z chmury publicznej, podczas gdy charakterystyka innych modeli implementacyjnych będzie przeprowadzana uzupełniająco.

6.3.3. Podział ze względu na udostępnione zasoby (modele usługowe)

Oddzielnym sposobem klasyfikacji usług świadczonych w chmurze obliczeniowej jest podział ze względu na udostępnione zasoby. Jak wskazano wcześniej, cechą wspólną usług świadczonych w chmurze jest udostępnienie zasobów informatycznych przez podmiot zewnętrznzy. Z uwagi na zamierzone przez usługobiorcę cele przetwarzania oraz dostosowanie do nich środowiska informatycznego wyróżnić można następujące modele usługowe:

- **Software as a Service** (SaaS) – w którym usługobiorca (użytkownik) otrzymuje dostęp do kompleksowej usługi, składającej się zarówno z warstwy technicznej (procesory, macierze dyskowe, lączę danych), jak i aplikacyjnej uruchomionej i działającej w oparciu o zasoby sprzętowo-programowe usługodawcy. W takim przypadku usługobiorca korzysta z udostępnionej mu funkcjonalności systemu informatycznego na warunkach i w zakresie wynikającym z
zaakceptowanego regulaminu (wzorca umowy). Przedmiotem umowy nie jest zatem udostępnienie infrastruktury technicznej, ale subskrypcja konkretnej aplikacji uruchomionej i w całości działającej z wykorzystaniem infrastruktury usługodawcy 696.

- **Platform as a Service (PaaS)** – w którym przedmiotem świadczenia usługi jest udostępnienie infrastruktury informatycznej usługodawcy, z wykorzystaniem której usługobiorca może tworzyć, rozwijać i eksploatować własne programy użytkowe (aplikacje) działające na udostępnionym środowisku aplikacyjnym. W takim wariancie umowa także można być zawarta z wykorzystaniem wzorca, jeżeli jej przedmiotem są stypizowane elementy konfiguracji środowiska IT (np. serwery o standardowych parametrach).

- **Infrastructure as a Service (IaaS)** – w której usługobiorca otrzymuje dostęp do środowiska IT usługodawcy, oferującego uzgodnione wcześniej parametry przetwarzania (np. moc obliczeniową, przepustowość łączności sieciowych, powierzchnię dyskową, ale i np. gwarantowane wskaźniki dostępności).

Podobnie jak w przypadku omówionych wcześniej modeli implementacyjnych, także w przypadku modeli usługowych z każdym z typów wiążą się różne ryzyka prawne oraz możliwe skutki dla bezpieczeństwa (w szczególności – prywatności 697) przetwarzanych informacji. Popularne wśród użytkowników indywidualnych usługi świadczone w chmurze publicznej realizowane są w modelu usługowym SaaS. Dlatego w dalszych rozważaniach najwięcej uwagi zostanie poświęcone analizie ryzyk prawnych związanych z tym modelem usługowym.

---

696 Przykładem może być usługa Office 365 udostępniana przez firmę Microsoft, pozwalająca na korzystanie z produktów pakietu Microsoft Office z dowolnego komputera i w dowolnym miejscu na świecie z wykorzystaniem standardowej przeglądarki internetowej, bez konieczności posiadania dodatkowych licencji i instalowania dedykowanego oprogramowania na komputerze klienckim.

6.3.4. Odniesienie do modelu klient-serwer

W modelu klient – serwer użytkownik zazwyczaj zнал i mógł określić miejsce przetwarzania danych. Nawet jeżeli usługodawca korzystał z podwykonawców, to określenie podmiotów mających dostęp do danych, a także miejsce ich przetwarzania nie stanowiło problemu. W przypadku usług świadczonych w chmurze zadanie to może być już bardziej skomplikowane, a w niektórych przypadkach wręcz niemożliwe. Nie wynika to ze skomplikowania technicznego usługi cloud computingu, ale z charakteru jednej z jej najważniejszych cech – przetwarzania rozproszonego. W modelu cloud computingu dane użytkownika mogą być – i zazwyczaj są – przechowywane i dostępne w różnych centrach przetwarzania, co jednak nie oznacza, że we wszystkich jednocześnie. Działając w oparciu o odpowiednie algorytmy, następuje automatyczna optymalizacja wykorzystania zasobów, polegająca między innymi na dystrybucji danych do centrów przetwarzania oferujących najlepsze parametry świadczenia usług. Jest to proces cykliczny i zautomatyzowany. Realizując żądanie użytkownika (np. dostęp do określonego pliku), jego realizacja może za każdym razem przebiegać inaczej i angażować inne serwery pośredniczące po stronie dostawcy usługi chmurowej. W efekcie za każdym razem faktyczna operacja przetwarzania może odbywać się w innej lokalizacji, a nawet w innym państwie. Co więcej, decyzja o tym, jakie zasoby zostaną wykorzystane do realizacji żądania użytkownika, podejmowana jest automatycznie i w momencie pojawienia się tego żądania. Efekt działania algorytmów optymalizacyjnych nie zależy wyłącznie od treści żądania, ale również od aktualnego obciążenia poszczególnych zasobów, wskaźników dostępności sieci itp. Zatem w przypadku dostępu do danych zgromadzonych w chmurze publicznej i z wykorzystaniem modelu SaaS uzyskujemy zasobów w chmurze publicznej i z wykorzystaniem modelu SaaS użytkownik nie ma żadnej możliwości przewidzenia ani wpływu na to, w jaki sposób jego żądanie zostanie zrealizowane przez usługodawcę. Co jednak ważniejsze, także dostawca nie ma takiej możliwości, ponieważ cały proces jest realizowany automatycznie i bezobsługowo. Celem jest optymalizacja wykorzystania zasobów i zmniejszenie kosztów przetwarzania – wprowadzanie ręcznego sterowania czy podejmowania decyzji byłoby przeszkodą dla możliwości realizacji tak określonego celu.

Co więcej, operatorzy chmur publicznych często rezerwują sobie prawo do korzystania z podwykonawców w celu zapewnienia potrzebnej infrastruktury IT. W takim wypadku istnieje możliwość, że proces przetwarzania będzie realizowany z wykorzystaniem zasobów firm trzecich (dalszych podwykonawców), które w szczególnym przypadku mogą stanowić odrębną usługę chmury obliczeniowej.
6.3.5. Wirtualizacja

Oddzielnym zagadnieniem, wymagającym ogólnego nakreślenia w celu zrozumienia ryzyk prawnych związanych z przetwarzaniem w chmurze, jest technologia wirtualizacji. Od strony technicznej wirtualizacja stanowi w istocie sposób funkcjonowania systemów operacyjnych, dzięki którym możliwe stało się zbudowanie modelu przetwarzania w chmurze. Prawdziwe jest zatem stwierdzenie, że bez wirtualizacji nie ma cloud computingu i każda chmura obliczeniowa korzysta z wirtualizacji.

Wirtualizacja jest techniką logicznego rozdzielenia warstwy infrastruktury technicznej (procesory, przestrzeń dyskowa, pamięć operacyjna) od warstwy programowej (w szczególności – systemu operacyjnego). Działanie standardowego komputera kontroluje jeden system operacyjny. Na komputerze może być zainstalowanych kilka systemów, ale w danej chwili uruchomiony jest jeden. System ten ma bezpośredni dostęp do podzespołów komputera, takich jak procesor czy dysk twardy. Wirtualizacja pozwala na jednoczesne działanie na tym samym komputerze kilku systemów operacyjnych. Systemy są od siebie odseparowane i działają niezależnie, korzystając z zasobów sprzętu za pośrednictwem dedykowanego środowiska nazywanego „wirtualizatorem”. Wirtualizator emuluje zasoby sprzętowe dla poszczególnych środowisk (systemów klienckich), w ten sposób uruchomione jednocześnie systemy operacyjne mogą działań równolegle, korzystając z tych samych zasobów.

Z wirtualizacją, a przez to i z usługami cloud computingu, związane są również potencjalnie negatywne konsekwencje dla poufności przetwarzanych informacji. Ponieważ od strony technicznej wirtualizator pośredniczy w przekazywaniu wszelkich informacji ze środowisk przetwarzających do warstwy sprzętu, na której przetwarzanie się odbywa, jest także miejscem w którym może następować niezauważone i niedające się wykryć przez użytkownika z poziomu systemu wirtualnego przechwytywanie danych. Przechwytywanie to może być konsekwencją udanego włamania do środowiska informatycznego (np. poprzez zainstalowanie tzw. root kita), ale również celowym działaniem podmiotu przetwarzającego. Jest to ryzyko immamentnie związane z technologią wirtualizacji, o którym trzeba pamiętać i uwzględniać wszędzie tam, gdzie dane są powierzane w usłudze świadczonej w chmurze.
6.4. Analiza prawna

6.4.1. Najważniejsze ryzyka związane z przetwarzaniem w chmurze obliczeniowej

Powyższe rozważania prowadzą do wniosków, że z usługami świadczonymi w modelu chmury obliczeniowej wiąże się liczne ryzyka, które w przypadku braku zastosowania odpowiednich rozwiązań prawnych (kontraktowych czy publicznoprawnych) mogą wpłynąć na osłabienie gwarancji związanych z ochroną prywatności. Wśród zagadnień o największym znaczeniu praktycznym należy wymienić:

- problem wskazania właściwego prawa oraz jurysdykcji,
- wiedzę o podmiotach i lokalizacjach przetwarzania danych,
- ustalenia dotyczące własności danych,
- prawa podmiotów danych i możliwość ich skutecznej ochrony prawnej,
- zakres i charakter odpowiedzialności dostawcy usługi,
- postępowanie w przypadku zakończenia świadczenia usługi.

Ponadto przetwarzanie w chmurze cechują także ryzyka typowo techniczne, związane z rozdzieleniem miejsca przetwarzania i prezentowania wyników – należą do nich w szczególności:

- awaria infrastruktury technicznej: przerwy w połączeniu w wyniku zdarzeń losowych, cyberataki itp.,
- przeciążenie łączy: słaba przepustowość, znaczny wzrost transferu danych (audio, wideo, spam itp.), ale i ograniczenia wynikające z najpopularniejszego schematu adresowania (IP v4),
- przeciążenie serwerów: łączenie zasobów i wynikający z niego możliwe przeciążenie wykorzystania zasobów, skutkujące niedostępnoscia usług.

O ile zagrożenia technologiczne mogą zostać rozwiązane poprzez wprowadzanie nowych i udoskonalanie istniejących rozwiązań technicznych, o tyle ryzyka prawne – w szczególności związane z ochroną prywatności – wymagają szerszego omówienia oraz podjęcia działań systemowych, zmierzających do ich rozwiązania poprzez wprowadzenie odpowiednich norm prawnych. Za wyjątkiem zagadnienia właściwej jurysdykcji pozostałe punkty wymagają omówienia zarówno z perspektywy prawa UE, jak i USA. Przepisy unijne, w szczególności rozporządzenie 2016/679, posłużą do omówienia skuteczności zabezpieczeń

698 Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie chmur obliczeniowych w Europie (opinia z inicjatywy własnej), Dz.U. UE z 2012 nr C 24, s. 10.
przyjętych w europejskim modelu przetwarzania danych w odniesieniu do ryzyk związanych z chmurą obliczeniową. Z kolei analiza prawodawstwa Stanów Zjednoczonych będzie stanowiła uzupełnienie wcześniejszych rozważań o kwestie wzajemnej kompatybilności modelów ochrony funkcjonujących w UE i USA, zwłaszcza w odniesieniu do danych przekazywanych do centrów przetwarzania prowadzonych przez przedsiębiorców amerykańskich. Przyczyną zastosowania takiego podejścia wynika z faktu, że znaczna część głównych dostawców usług przetwarzania w chmurze – szczególnie oferowanych dla klientów indywidualnych – to podmioty zarejestrowane w Stanach Zjednoczonych699. Jak wskazuje KE, według stanu z maja 2016 roku, na UE przypada tylko 4% całkowitej kapitalizacji największych platform internetowych700. Kluczowe zatem jest określenie, na ile prawo UE zabezpiecza użytkowników europejskich przed wskazanymi wcześniej ryzykami nie tylko w przypadku, gdy ich dane są przetwarzane na terenie Unii, ale i w przypadku ich przekazywania do podwykonawców w państwach trzecich.

6.4.2. Charakter prawny i definicja umowy przetwarzania w chmurze

W pierwszej kolejności należy zdefiniować przedmiot, strony oraz ewentualne wymagania co do formy omawianych umów701. Najczęściej przedmiotem umów SaaS jest czasowe i niewyłączne udostępnienie (subskrypcja) dostępu do aplikacji, uruchomionej i utrzymywanej na infrastrukturze dostawcy. Dostęp do aplikacji odbywa się za pośrednictwem przeglądarki internetowej lub innego klienta programowego, udostępnionego przez dostawcę. Powstaje zatem pytanie – czy każda subskrypcja usługi internetowej wiąże się z korzystaniem z usługi w modelu SaaS, a zwłaszcza w chmurze publicznej? Jest to pytanie nietrywialne i dużej mierze wiąże się ze sposobem implementacji usługi po stronie usługodawcy. Odpowiedź utrudnia brak powszechnie uznanej prawnej definicji usług przetwarzania w chmurze. Bazując na terminologii wprowadzonej przez NIST, przyjść można, że każda umowa, której przedmiotem jest udzielenie użytkownikowi niewyłącznego dostępu do skalowanej usługi świadczonych publicznie, jest umową przetwarzania w chmurze publicznej.

699 W zestawieniu zawierającym informacje o usługach internetowych posiadających co najmniej 100 mln aktywnych użytkowników znajduje się jeden przedsiębiorca posiadający siedzibę główną na terenie UE (firma Sulake, operator serwisu Habbo). Na pierwszych dziesięciu pozycjach znajduje się poza tym sześć korporacji zarejestrowanych w Stanach Zjednoczonych, dwie w Chinach i jedna w Rosji. Źródło: https://en.wikipedia.org/wiki/List_of_social_networking_websites.


701 W dalszych rozważaniach, jeżeli nie zostanie zaznaczone inaczej, z umową na usługę przetwarzania w chmurze utożsamiana będzie umowa, której przedmiotem jest świadczenie usług w modelu SaaS/chmura publiczna.
Jeżeli ponadto użytkownik nie zarządza oraz nie kontroluje infrastruktury informatycznej, na której jest uruchomiona usługa, można mówić o umowie na przetwarzanie w modelu SaaS. Tak sformułowane definicje obejmują szeroki zakres usług świadczonych w Internecie. W praktyce usługi SaaS/chwura publiczna obejmują popularne zastosowania konsumenckie – takie jak poczta elektroniczna (np. Google GMail, Yahoo! Mail), oprogramowanie biurowe (Microsoft Office 365, Google Docs), przechowywanie i przetwarzanie plików (Dropbox, Google Drive, Microsoft OneDrive, Box), zdjęcia (Flickr, Google Photos), media strumieniowe (YouTube, Vimeo), portale społecznościowe (Facebook, LinkedIn) udostępnianie muzyki (Spotify) czy filmów na żądanie (Netflix). W wielu ze wskazanych przypadkach usługi chmury publicznej są wykorzystywane przez usługodawcę jako narzędzie do realizacji usługi, przy czym od strony formalnej usługa jest zbudowana na innej chmurze udostępnianej przez podwykonawcę. Przykładem może być Box, serwis internetowy udostępniający popularną usługę do przechowywania i współdzielenia plików. Usługa SaaS – którą jest Box – jest świadczona w oparciu o usługę Amazon Cloud w modelu w modelu IaaS. Zatem firma Box (dostawca usługi) udostępnia swój produkt w oparciu o inną usługę świadczoną w chmurze obliczeniowej. Przykład ten obrazuje, w jaki sposób usługi świadczone w chmurze mogą być budowane warstwami i zależne od siebie – w szczególności, że usługi SaaS często korzystają z innych usług udostępnionych w modelu IaaS lub PaaS.

Usługa przetwarzania danych w chmurze obliczeniowej nie została zdefiniowana w przepisach Kodeksu cywilnego ani innych przepisach krajowych. Jest zatem usługą nienazwaną, do której stosuje się art. 750 kc – zgodnie z którym do umów o świadczenie usług, które nie są uregulowane innymi przepisami, stosuje się odpowiednio przepisy o zleceniu.

Z uwagi na swój charakter usługa cloud computing jest zawsze świadczona na odległość, przy czym jej cechą charakterystyczną jest możliwość automatycznego uruchomienia w oparciu o elektroniczne zamówienie otrzymane od usługobiorcy. Ta cecha – nazywana w angielskojęzycznej literaturze self-service (samoobsługę) lub on-demand service (usługa na żądanie) – podkreśla jej w pełni elektroniczny charakter oraz, z uwagi na brak ręcznego (manualnego) procesu obsługi zamówienia, na konieczność oparcia się na wzorcach umów (umowach adhezyjnych) stanowiących element automatycznego procesu obsługi zamówień.

702 Dla użytkowników w UE usługodawcą jest Box.com Ltd.
Usługa *cloud computing* stanowi więc usługę świadczoną drogą elektroniczną. Zgodnie z definicją wprowadzoną w art. 2 pkt 4 ustawy o świadczeniu usług drogą elektroniczną⁷⁰³ pod pojęciem usługi świadczonej drogą elektroniczną należy rozumieć usługę realizowaną bez jednocześnie obecności stron (a zatem na odległość) poprzez przekaz danych na indywidualne żądanie usługobiorcy, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy – Prawo telekomunikacyjne. Usługa *cloud computing* jest także usługą świadczoną elektronicznie w węższym znaczeniu, wprowadzonym w ustawie o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym⁷⁰⁴. W szczególności spełnia przesłankę pozytywną do uznania jej za usługę świadczoną elektroniczną (art. 4 ust. 1) oraz nie spełnia przesłanek negatywnych (art. 4 ust. 2). W szczególności nie jest usługą o charakterze materialnym oraz nie polega na dystrybucji jakichkolwiek treści na informatycznych nośnikach danych.

Jak wskazano wcześniej, usługi *cloud computing* mogą być świadczone zarówno dla konsumentów, jak i innych podmiotów. W przypadku pierwszej grupy usługobiorców dodatkowego uwzględnienia wymagają przepisy ustawy o prawach konsumenta⁷⁰⁵ – w szczególności związane z obowiązkami przedsiębiorcy w umowach zawieranych poza lokalem przedsiębiorstwa lub na odległość (art. 12 i nast.). Przepisy ustawy określają szczegółowy reżim związany z procesem oferowania, zawarciem umowy, obowiązkami informacyjnymi, prawem odstąpienia oraz skutkami niedotrzymania poszczególnych wymagań ze strony przedsiębiorcy. Znaczenie szczegółowego trybu związanego z zawieraniem umów z konsumentami zostało podkreślone przepisem art. 26 ustawy, zgodnie z którym w przypadku konfliktu z przepisami ustawy o świadczeniu usług drogą elektroniczną stosuje się przepisy ustawy o prawach konsumenta.

Umowy *cloud computing* są zatem umowami, do których stosuje się przepisy o zleceniu. Jednocześnie są umowami o świadczenie usług drogą elektroniczną, a także – jeżeli zostały zawarte z konsumentem – mogą być regulowane szczegółowym reżimem wynikającym z ustawy o prawach konsumenta.

Z uwagi na swoją powszechność oraz zachowanie bezobsługowej obsługi zamówień umowy na usługi przetwarzania w chmurze często zawierane są z wykorzystaniem wzorca akceptowanego przez usługobiorcę w trakcie procesu rejestracji realizowanej za

---

⁷⁰³ Ustawa z 18 lipca 2002 o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 nr 144, poz. 1204 ze zm.).
⁷⁰⁴ Ustawa z 5 lipca 2002 o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. z 2002 nr 126, poz. 1068).
⁷⁰⁵ Ustawa z 30 maja 2014 o prawach konsumenta (Dz.U. z 2014, poz. 827 ze zm.).
pośrednictwem odpowiednio przygotowanego formularza internetowego. Nie praktykuje się zawierania umów w formie pisemnej oraz możliwości negocjacji lub modyfikacji zapisów umowy poza ustalonymi wcześniej przez usługodawcę zakresem – ograniczonym do wyboru predefiniowanych wariantów świadczonej usługi. Na gruncie polskich przepisów cywilistycznych taki sposób zawierania umowy nie prowadzi do dochowania formy pisemnej ani elektronicznej czynności prawnej. Jeżeli użytkownik usługi nie otrzymuje w trwałej postaci na nośniku elektronicznym kopii regulaminu (np. załączonego do wiadomości e-mail), a usługodawca w ten sam sposób oświadczenia woli usługobiorcy, umowa nie jest także zawarta z zachowaniem formy dokumentowej. W przepisach nie zastrzeżono wymaganej formy wymaganej dla umowy przetwarzania w chmurze obliczeniowej. Jest to oczywiście, biorąc pod uwagę, że jak wskazano wcześniej, jest to umowa nienazwana, łącząca cechy zlecenia, umowy świadczonej elektroniczne oraz zawartej na odległość. Umowa jest zatem ważna niezależnie od zachowania formy szczególnej, chyba że strony umówiły się inaczej (art. 76 kc). Warto jednak pamiętać, że jeżeli usługodawca planuje wykorzystywać usługę przetwarzania w chmurze do realizacji czynności, dla których ustawodawca określił szczególny reżim prawny, ważność umowy może być oceniana z uwzględnieniem celu jej zawarcia, a więc z odniesieniem do przepisów szczegółowych. Przykładem może być umowa powierzenia przetwarzania danych osobowych, która zgodnie z art. 31 ust. 1 ustawy o ochronie danych osobowych musi być zawarta w formie pisemnej. Umowy przetwarzania w chmurze zawierane elektroniczne z wykorzystaniem wzorca nie spełniają tego wymagania, dlatego nie powinny być podstawą do przekazywania danych osobowych przez administratora innym podmiotom.

Ponadto zgodnie z art. 384 §4 kc szczególne znaczenie ma fakt udostępnienia wzorca umowy usługobiorcy przed zawarciem umowy w taki sposób, aby mógł on wzorcować ten przechowywać i odtwarzać w zwykłym toku czynności. Jak bowiem podkreśla się w doktrynie, niedoręczne wzorcowanie powoduje, że wzorcowie nie wiąże adresata.\footnote{P. Miklaszewicz, \textit{Komentarz do art. 384 KC}, p. 16, \textit{[w:] Kodeks cywilny. Komentarz} pod red. K. Osajda, CH Beck 2017.}

6.4.3. Prawo właściwe i jurysdykcja dla umów przetwarzania w chmurze

Z perspektywy ochrony prywatności kluczowym zagadnieniem problemowym związanym z przetwarzaniem w chmurze obliczeniowej jest możliwa do wystąpienia trudność w określeniu właściwego systemu prawnego, jakiemu podlega umowa z dostawcą usługi.
Przedstawione wcześniej rozważania zakładają, że umowa będzie podlegała prawu polskiemu – co w przypadku usług świadczonych w modelu chmury obliczeniowej nie jest oczywiste, zwłaszcza biorąc pod uwagę, że w większości usługi takie są oferowane przez przedsiębiorców zagranicznych. Wysokie standardy ochrony prywatności w cyberprzestrzeni wynikające z europejskich przepisów o ochronie danych mogą nie mieć zastosowania w przypadku zawarcia umowy przewidującej stosowanie systemu prawnego państwa trzeciego. Dlatego przed oceną skuteczności istniejących przepisów publicznoprawnych należy ustalić zakres ich stosowania w przypadku, gdy usługodawca prowadzi działalność gospodarczą z terenu innego państwa.

Zgodnie z art. ust. 1 ustawy o świadczeniu usług drogą elektroniczną świadczenie usług podlega prawu państwa EOG, na którego terytorium usługodawca ma miejsce zamieszkania lub siedzibę. Jeżeli usługa jest świadczona przez przedsiębiorcę nieposiadającego siedziby na terenie EOG, zastosowanie znajduje art. 28 ustawy – Prawo prywatne międzynarodowe, regulujący zobowiązania umowne i wskazujący na rozstrzygające znaczenie rozporządzenia 593/2008 w sprawie prawa właściwego dla zobowiązań umownych (tzw. Rozporządzenie Rzym I). Zgodnie z art. 1 ust. 1 rozporządzenia stosuje się je do zobowiązań umownych w sprawach cywilnych i handlowych powiązanych z prawem różnych państw. Prawo wskazane przez rozporządzenie stosuje się bez względu na to, czy jest ono prawem państwa członkowskiego (art. 1 ust. 4). Co do zasady i jeżeli strony nie umówili się inaczej, umowa o świadczenie usług podlega prawu państwa, w którym usługodawca ma miejsce zwykłego pobytu (art. 4 ust. 1 pkt b). Wyjątkiem są umowy z konsumentami, które podlegają prawu państwa, w którym konsument ma miejsce zwykłego pobytu, jednakże pod warunkiem że przedsiębiorca:

1) wykonuje swoją działalność gospodarczą lub zawodową w państwie, w którym konsument ma miejsce zwykłego pobytu, lub
2) w jakikolwiek sposób kieruje taką działalność do tego państwa lub do kilku państw z tym państwem włącznie a umowa wchodzi w zakres tej działalności.

W praktyce jednak umowy cloud computing zawierają klauzulę wyboru prawa i w ten sposób rozstrzygająca dla określenia prawa właściwego jest wola samych stron. Art. 3 ust. 1 rozporządzenia Rzym I stanowi, że umowa podlega prawu wybranemu przez strony, jeżeli

707 Ustawa z dn. 4 lutego 2011 – Prawo prywatne międzynarodowe (Dz.U.z 2011 Nr 80, poz. 432).
708 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Dz.Urz.UE. z 2008 Nr L 177, s. 6).
709 Na tym tle należy przypomnieć rozważania przedstawione przy omówieniu wyroku TSUE w sprawie Weltimmo związane z przesłankami uzasadniającymi uznanie, że przedsiębiorca prowadzi działalność gospodarczą w kontekście danego państwa członkowskiego – zob. s. 137.
wybór prawa jest dokonany wyraźnie lub w sposób jednoznaczny wynika z postanowień umowy lub okoliczności sprawy, przy czym strony mogą dokonać wyboru prawa właściwego dla całej umowy lub tylko dla jej części. Zdaniem J. Gołaczyńskiego, przesłanki zawarcia i ważności klauzuli wyboru prawa powinny zasadniczo podlegać ocenie prawa wybranego przez strony dla ich stosunku zobowiązaniowego. Przy czym jak zauważa A. Jaroszek, dla ważności umowy nie ma znaczenia, czy strony znają treść przepisów prawa wybranego: „Zakłada się, że jeśli strony wybraly określone prawo, to chcą działać w ramach prawa prawdopodobnie im najbliższego. Wybrane prawo będzie także właściwe dla oceny powstania, treści i wygaśnięcia zobowiązania”. Należy jednak pamiętać, że nawet w przypadku zastosowania klauzuli wyboru prawa (art. 3 ust. 1 rozporządzenia) w przypadku umów zawartych z konsumentem zastosowanie znajdzie art. 6 ust. 2, zgodnie z którym wybór prawa nie może prowadzić do pozbawienia konsumenta ochrony przyznanej mu na podstawie przepisów, których nie można wyłączyć w drodze umowy według prawa właściwego dla miejsca jego zwykłego pobytu.

Do powyższej kwestii nawiązuje orzeczenie SN w sprawie I CSK 555/13, w którym Sąd orzekł, że zamieszczenie we wzorze umowy konsumenckiej postanowienia przewidującego zastosowanie prawa obcego dla konsumenta, a właściwego dla twórcy wzorca, stanowi klauzulę niedozwoloną w rozumieniu art. 385 § 1 kc – a w konsekwencji skutki tego postanowienia nie wiązą konsumenta. Sąd uznał, że wprowadzenie klauzuli prowadzi do nieuzasadnionego naruszenia równowagi stron oraz „stawia twórcę wzorca umowy w sytuacji wyjątkowo uprzywilejowanej w stosunku do konsumenta, któremu klauzula ta została narzucona”. Co więcej, uznał, że zastosowane w rozporządzeniu Rzym I postanowienia szczególne dla umów zawieranych z konsumentami nie wykluczają uznania tych klauzul za niezgodne na gruncie przepisów krajowych. Ponadto – zdaniem Sądu – w praktyce zaakceptowane modelu wprowadzanego przez art. 6 ust. 2 wymagałyby znajomości przez konsumenta obcego systemu prawnego. Dopiero w trakcie ewentualnego sporu okazałoby się, które konkretnie przepisy prawa z poszczególnych systemów znajdują zastosowanie w badanej sprawie. Dlatego w ocenie SN takie ukształtowanie stosunku umownego jest niezgodne z dobrymi obyczajami i dlatego nie może prowadzić do skutecznego związania konsumenta.

710 J. Gołaczyński, Prawo prywatne międzynarodowe, CH Beck 2015, Nb 240, s. 184.
711 A. Jaroszek, Wagaśność wyboru, [w]: Prawo właściwe dla umów konsumenckich zawieranych przez Internet, Oficyna 2009.
712 Wyrok SN z 17.09.2014, sygn. I CSK 555/13, OSNC 2015, nr 7-8, poz. 94.
Wskazane orzeczenie spotkało się z krytycznym przyjęciem doktryny. W szczególności zaznaczano jego niezgodność z normami wyższego rzędu (zwłaszcza rozporządzeniem Rzym I) oraz brak uwzględnienia specyfiki umów zawieranych w Internecie. W konsekwencji sygnalizowano, że przyznanie konsumentowi zbyt daleko posuniętej ochrony doprowadzi do utrudnienia prowadzenia działalności gospodarczej oraz – z punktu widzenia przedsiębiorców zagranicznych – sprawi, że świadczenie usług dla użytkowników zlokalizowanych w Polsce będzie wiązało się z niedekwatawnymi kosztami będącymi następstwem konieczności dostosowywania globalnej usługi do lokalnych regulacji. Jak zauważają M. Kolasiński i M. Świerczyński, w praktyce stanowisko SN może prowadzić także do pogorszenia prawnej sytuacji konsumentów poprzez pozbawienie ich „możliwości powołania się na te przepisy prawa obcego, które przyznają im dalej idące uprawnienia, niż te przewidziane w prawie polskim”.

Do ustalenia wspólnej linii orzeczniczej na obszarze UE przyczyniły się niedawno wydany wyrok TSUE w sprawie Amazon EU Sàrl. Zadane Trybunałowi pytanie prejudycjalne dotyczyło zagadnienia zgodności z prawem UE (w szczególności z dyrektywą 93/13, regulującą kwestię nieuczciwych warunków w umowach konsumenckich) umowy adhezyjnej zawartej drogą elektroniczną pomiędzy przedsiębiorcą a konsumentem, przewidującej wybór prawa państwa członkowskiego właściwego dla siedziby przedsiębiorcy. Trybunał na wstępie przypomniał, że zgodnie z art. 3 ust. 1 dyrektywy 93/13 postanowienie umowy, które nie było indywidualnie negocjowane, jest niedozwolone, jeśli stoi w sprzeczności z wymogami dobrej wiary, powoduje znaczącą nierównowagę między wynikającymi z umowy prawami i obowiązkami stron ze szkodą dla konsumenta. Jednocześnie podkreślił jednak, że samo stosowanie klauzuli wyboru prawa obcego w umowach z konsumentami nie jest a priori niezgodne z prawem UE. Rozstrzygające znaczenie ma treść klauzuli, a w szczególności konieczność poinformowania konsumenta o tym, iż korzysta on również, na podstawie art. 6 ust. 2 rozporządzenia Rzym I, z ochrony zapewnianej mu przez bezwzględnie wiązające przepisy prawa, które byłoby właściwe w braku tej klauzuli.

Wydanie orzeczenia w sprawie Amazon EU Sàrl prowadzi zatem do braku

---

713 Por. np. M. Jagielska, A. Kunkiel-Kryńska, Wybór prawa jako klauzula abuzywna w umowach konsumenckich zawieranych przez Internet, IKAR 2016, nr 3, s. 4.
716 Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (CELEX 31993L0013, Dz.U.WE z 1993 Nr L 95, s. 29).
717 Wyrok TSUE w sprawie C-191/15, op. cit., p. 71.
aktualności tez zawartych w wyroku analizowanym wcześniej wyroku SN. Należy oczekiwać, że pogląd wyrażony przez TSUE – prowadzący do uznania ważności klauzuli wyboru prawa także w umowach zawieranych z konsumentami – stanie się rozstrzygający w wyrokowaniu spraw zawisłych przed krajowymi sądami.

Odrębnym zagadnieniem jest kwestia wyboru sądu właściwego do rozstrzygania ewentualnych sporów pomiędzy stronami. Podobnie jak w przypadku wyboru prawa strony mogą dokonać wyboru jurydykcyjnego, a w przypadku braku wskazania stosuje się przepisy ogólne. W polskim systemie prawnym zastosowanie w takim przypadku znajdują przepisy części IV KPC, wskazujące na konieczność wystąpienia jednego z łączników warunkujących zastosowanie jurydykcyjnej krajowej. Do podstawowych należą łączniki podmiotowe wskazane w art. 1103 kpc, tj. miejsce zamieszkania, zwykłego pobytu lub siedziby powoda na terenie Polski. Do jurydykcyjnej krajowej należą też sprawy wynikające z umów, jeżeli powodem jest konsument, który poza posiadaniami miejsca zamieszkania lub miejsca zwykłego pobytu na terenie Polski w Polsce podjął czynności niezbędne do zawarcia umowy. W przypadku umów cloud computing zastosowanie znaleźć może również przepis art. 1103718, rozszerzający jurydykcyję krajową o sprawy dotyczące zobowiązań wynikających z czynności prawnej, która została wykonana albo ma być wykonana na terenie Polski. W tym przypadku potencjalna trudność w zastosowaniu wskazanej normy może wiązać się ze wskazanym w przepisie odniesieniem terytorialnym, które w przypadku umów dotyczących przetwarzania w chmurze może podlegać różnym interpretacjom718. Wszystkie omówione powyżej łączniki prowadzą do możliwości wskazania tzw. jurydykcyjnej fakultatywnej (a więc nie wyłącznej) sądów polskich, która może być wyłączena poprzez ustanowienie przez strony umowy o jurydykcyję sądów prawa obcego (art. 1105 ust. 1). Umowa taka jest ważna, jeżeli została zawarta na piśmie – przy czym zgodnie z art. 1105 wymaganie to jest spełnione, jeżeli wynika z dokumentu podpisanego przez strony lub z wymienionych między nimi pismach albo oświadczeniach złożonych za pomocą środków porozumiewania się na odległość, które pozwalają utrwalić ich treść. Przywołane przepisy kodeksu postępowania cywilnego nie znajdą zastosowania do określania jurydykcyjnej właściwej według przepisów rozporządzenia 1215/2012719.

718 W zależności od interpretacji oraz sytuacji faktycznej miejscem wykonania umowy może być lokalizacja centrum danych, gdzie wykonywane są operacje przetwarzania danych; miejscem może być także lokalizacja komputera usługobiorcy, który korzystając z usługi pobiera lub wysyła dane do przetwarzania.
719 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurydykcyjnej i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (CELEX: 32012R1215, Dz.Urz.UE z 2012 Nr L 351, s. 1).
Podsumowując dotychczasowe rozważania, wskazać należy, że co do zasady prawo właściwe dla usługi *cloud computingu* będzie określane względem siedziby usługodawcy, natomiast jurysdykcja względem miejsca zamieszkania lub siedziby powoda. Z uwagi na brak szczegółowych rozwiązań prawnych związanych z regulacją umów przetwarzania w chmurze usługobiorcy pragnący zagwarantować możliwość stosowania prawa krajowego lub jurysdykcji sądów krajowych w przypadku rozstrzygania sporów powinni uwzględnić odpowiednie zapisy na etapie zawierania umowy. Postulat ten jest najczęściej niemożliwy do spełnienia z uwagi na fakt, że jednym z podstawowych założeń *cloud computingu* jest automatyczne (bezobsługowe) zawieranie umowy przez usługodawcę na podstawie zamówienia przesłanego przez usługobiorcę. Umowy tego typu nie są negocjowane i bazują na standardowych wzorcach (regulaminach) opracowanych i udostępnionych przez usługodawcę, które są akceptowane przez usługobiorcę na etapie rejestrowania usługi. W rezultacie w przypadku gdy w umowie uwzględniono klauzulę wyboru prawa oraz umowę o jurysdykcję, przepisy te będą rozstrzygające dla określenia zasad rozstrzygania ewentualnych sporów między stronami. W odniesieniu do umów o przetwarzanie danych w chmurze obliczeniowej konsekwencją może być ograniczenie praw lub gwarancji, także związanych z ochroną prywatności, których zakres jest inaczej definiowany przedmiotowo lub podmiotowo w systemie prawnym państwa trzeciego.

Poddanie umowy prawu właściwemu dla siedziby usługodawcy może prowadzić do znacznego utrudnienia usługobiorcy oceny skutków podejmowanej czynności prawnej. Brak zastosowania przepisów funkcjonujących w systemie prawnym usługobiorcy odnosi się nie tylko do przepisów prawa prywatnego (ocena ważności, zakres swobody zawierania umów, odpowiedzialność kontraktowa i deliktowa), ale również do możliwości stosowania norm wynikających z przepisów publicznoprawnych (w polskim porządku prawnym – np. skargi do organu ochrony konsumentów), co oznacza, że usługobiorcy może nie przysługiwać w ogóle lub przysługiwać w ograniczonym zakresie możliwość skorzystania ze środków ochrony prawnej przewidzianych we właściwym dla niego systemie prawnym.

Z uwagi na globalny charakter świadczonych usług, ich dostawcy stosują w udostępnianych wzorcach dodatkowe zapisy mające odzwierciedlić uwarunkowania poszczególnych ryków docelowych. Zapisy te mogą dodatkowo utrudnić analizę postanowień umowy nawet w zakresie ustalenia właściwego systemu prawnego czy jurysdykcji. Dla przykładu firma Facebook we wstępie do regulaminu świadczenia usług

---

720 Warunki świadczenia poszczególnych analizowanych usług zostały wskazane w przypisie 728 (s. 272).
wskazuje, że oryginał umowy został sporządzony w języku angielskim i w przypadku jakichkolwiek rozbieżności pomiędzy angielskojęzyczną treścią a jej przekладem obowiązuje wersja w języku angielskim. Z kolei firma Dropbox zamiast precyzyjnie zdefiniować usługodawcę określa warunki, jakie trzeba przeanalizować, aby stwierdzić, z kim umowa została zawarta.

Zdefiniowanie usługodawcy (a w ten sposób i prawa właściwego dla zawieranej umowy) kryteriami miejsca zamieszkania usługobiorcy jest powszechną praktyką stosowaną także przez innych dostawców analizowanych usług. Rozwiązanie to nie dosyć, że jest nieczynne, to jeszcze nie uwzględnia konsekwencji wynikającej ze zmiany miejsca zamieszkania przez użytkownika w tracie trwania umowy. Z kolei firma Microsoft w warunkach świadczenia usług wskazała usługodawcę nie w odniesieniu do miejsca zamieszkania usługobiorcy, ale w zależności od korzystania z płatnych wersji usług – użytkownik mieszkający w Europie i korzystający z bezpłatnych usług zawiera umowę z Microsoft Corporation (podmiot prawa Stanów Zjednoczonych), natomiast przy korzystaniu z usług płatnych umowa jest zawierana z Microsoft Ireland Operations Limited (podmiot prawa Irlandii). W efekcie umowa tego samego użytkownika, zamieszkanego na terenie UE, korzystającego z tej samej usługi informatycznej (np. usługi przechowywania plików takiej jak Microsoft OneDrive) może podlegać prawu Stanów Zjednoczonych lub kraju jego zamieszkania – w zależności, czy korzysta z usługi w wersji bezpłatnej czy płatnej.

Szczegółowe zestawienie dotyczące prawa i sądów właściwych dla rozstrzygania sporów w umowach dotyczących wiodących usług świadczonych w chmurze obliczeniowej zaprezentowano w tabeli 1 (s. 276). Z zaprezentowanego porównania wyłania się wniosek, że usługodawcy korzystają z przywileju kształtowania stosunku prawnego – także w zakresie preferowania wskazywania prawa i jurysdykcji właściwej dla ich siedziby. Z uwagi na zmiany wprowadzone w ogólnym rozporządzeniu o ochronie danych warunki korzystania z usług są stopniowo dostosowywane do potrzeb usługodawców. Z uwagi na zmiany wprowadzone w ogólnym rozporządzeniu o ochronie danych warunki korzystania z usług są stopniowo dostosowywane do potrzeb usługodawców.

721 Informacja wprowadzająca do warunków świadczenia usług firmy Facebook (zob. przypis 728): „Niniejsza umowa została sporządzona w języku angielskim (USA). W przypadku jakichkolwiek rozbieżności pomiędzy niniejszą umową w języku angielskim a jej przekładem obowiązuje wersja w języku angielskim. Zwracamy uwagę, że Rozdział 16 zawiera zmiany warunków ogólnych dotyczące użytkowników spoza Stanów Zjednoczonych”.

722 „Niniejsze Warunki korzystania z usługi („Warunki”) obejmują korzystanie z usług, oprogramowania klienta i stron internetowych oraz dostęp do nich („Usługi”). Jeśli mieszkasz poza granicami Stanów Zjednoczonych Ameryki, Kanady i Meksyku („Ameryka Północna”), Twoja umowa zawarta jest z Dropbox International Unlimited Company, a jeśli mieszkasz w Ameryce Północnej, Twoja umowa zawarta jest z Dropbox, Inc.”. Zob. tabelę 1 oraz przypis 728.

do potrzeby uwzględnienia właściwości prawa europejskiego w odniesieniu do użytkowników korzystających z usług z terenu UE.

Cechą wspólną usługodawców mających siedzibę w Stanach Zjednoczonych jest oparcie wzorców umów na terminologii i rozwiązaniach prawnych wynikających z prawa amerykańskiego i systemu common law. Przykładem mogą być regulacje związane z zakresem (wyłączeniem) odpowiedzialności kontraktowej lub prawem do przekazywania danych innym podmiotom, jeżeli będzie to realizowało interes usługodawcy. Standardem są też zapisy związane z prawem jednostronnej zmiany warunków umowy przez usługobiorcę w trybie i na warunkach nieznanych w polskich przepisach. Przykładem mogą być warunki korzystania z usług Google724:

Konsekwencją stosowania takich klauzul jest możliwość wprowadzenia dowolnych modyfikacji zarówno w umowie, jak i wszelkich warunkach dodatkowych, regulowanych w innych porozumieniach zawartych pomiędzy stronami. Możliwość stosowania takich rozwiązań prawnych także w umowach z konsumentami jest bezpośrednią konsekwencją oparcia umowy na systemie prawnym państwa trzeciego, bowiem w przypadku zastosowania krajowych rozwiązań prawnych taka regulacja umowna – jako klauzula abuzywna – byłaby uznana za nieważną na podstawie art. 385\(^1\) §1 w zw. z art. 385\(^3\) pkt 23 kc.

Odmienne podejście, zasługujące na wyróżnienie, zostało zastosowane w umowie regulującej korzystanie z usługi Spotify725. W umowie precyzyjnie wskazano prawo właściwe oraz jurysdykcję z podziałem na poszczególne państwa (w tym Polskę). Umowa ponadto precyzyjnie wskazuje dane identyfikacyjne usługodawcy oraz administratora bezpieczeństwa informacji.

Co do zasady, we wszystkich analizowanych umowach usługodawcy nie wskazali podmiotów, którym powierzają przetwarzanie danych swoich użytkowników. Ograniczają się do wskazania, że dane są przetwarzane w centrach danych rozlokowanych w różnych państwach i podległych różnym jurysdykcjom. Użytkownicy nie są informowani, jakie są to państwa ani jakie podmioty mają dostęp do ich danych726. Z kolei w polityce prywatności usługi Dropbox ograniczono się do wskazania, że „aby świadczyć usługi, możemy

---

725 Zob. przypis 728 (s. 272).
przechowywać, przetwarzać i przekazywać informacje w USA i lokalizacjach na całym świecie – w tym również poza twoim krajem” 727.

Chociaż warunki świadczenia usługi Spotify są równie ogólne w zakresie wskazania państw, do których dane mogą być przekazane w celu dalszego przetwarzania, to administrator usługi zgodnie z prawdą informuje o możliwych konsekwencjach przetwarzania danych w różnych jurysdykcjach dla zakresu praw przysługujących użytkownikom: „Informacje gromadzone na terenie EOG i Szwajcarii mogą np. zostać przesłane i przetworzone przez określone powyżej podmioty zewnętrzne zlokalizowane w krajach innych niż kraje EOG i Szwajcaria, gdzie może Ci przysłużyć mniej praw dotyczących Twoich informacji”.

Podsumowując, należy wskazać, że problem wyboru prawa właściwego ma fundamentalne znaczenie dla zakresu praw i gwarancji związanych z ochroną prywatności przy korzystaniu z usług online. Teza ta jest szczególnie prawdziwa w odniesieniu do usług przetwarzania w chmurze, bowiem poza kwestią odmiennych regulacji prawnych państwa trzeciego uwidoczniony zostaje problem możliwości oraz nieznanych warunków przekazywania danych użytkowników do dalszego przetwarzania przez podwykonawców usługobiorców zlokalizowanych w państwach trzecich. Globalny charakter usług cloud computing powoduje, że dane są jednocześnie przetwarzane w wielu centmach danych rozmieszczonych na całym świecie – powszechnie stosowany w umowach opartych na prawie amerykańskim standard braku informowania użytkowników o podmiotach (podwykonawcach) przetwarzających dane powoduje, że mogą oni utracić realny wpływ i kontrolę nad udostępnianiem i obiektem informacji. Nawet gdyby usługobiorca był poinformowany o podmiotach (centmach danych), w których przetwarzane są jego informacje, to w przypadku, gdy lista na mogłaby być jednostronnie zmieniana – jej przydatność dla oceny ryzyk związanych z ochroną prywatności byłaby ograniczona. Co więcej, nawet przyjmując, że usługodawca nie mógłby dokonać jednostronnej zmiany warunków umowy w zakresie wykazu miejsce przetwarzania informacji, to biorąc pod uwagę konieczność szczegółowej analizy wielu systemów prawnych, określenie wynikowego zestawu praw i gwarancji przysługujących użytkownikowi w obszarze ochrony prywatności w każdej z jurysdykcji, w której przetwarzane są jego informacje, byłaby zadaniem w praktyce niewykonalnym. Stąd wniosek, że rozproszony charakter działania usług w modelu chmury obliczeniowej przy jednoczesnej możliwości dalszego podzlecania przetwarzania do

kolejnych podmiotów oraz braku jednakowych, powszechnie obowiązujących we wszystkich systemach prawnych, w których następuje przetwarzanie norm prawa publicznego (*erga omnes*), prowadzi do znacznego ograniczenia możliwości skutecznej ochrony praw przez usługobiorcę. Tylko wprowadzenie jednakowych i tak samo interpretowanych norm prawa związanych z ochroną prywatności w cyberprzestrzeni we wszystkich państw, w których zlokalizowane są centra przetwarzania danych, spowoduje, że prawa usługobiorcy nie zostaną ograniczone i będą mogły być skutecznie egzekwowalne niezależnie od miejsca powstania naruszenia.

Aby powyższe wnioski były kompletne, problem prawa właściwego i jurysdykcji należy dodatkowo przeanalizować przez pryzmat ogólnego rozporządzenia o ochronie danych osobowych, które nie zawsze i nie w pełni znajduje odzwierciedlenie w treści warunków korzystania z usług publikowanych przez zagranicznych usługodawców.
Tabela 1. Informacja na temat prawa właściwego i jurysdykcji zawarta w umowach na usługi świadczone w chmurze obliczeniowej

<table>
<thead>
<tr>
<th>Grupa usług</th>
<th>Usługa/produkt</th>
<th>Siedziba usługodawcy</th>
<th>Prawo właściwe</th>
<th>Jurysdykcja</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poczta elektroniczna</td>
<td>Google GMail</td>
<td>Stany Zjednoczone</td>
<td>Stany Zjednoczone (prawo stanu Kalifornia w Stanach Zjednoczonych)</td>
<td>Stany Zjednoczone (sąd federalny lub stanowy właściwy dla siedziby usługodawcy)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yahoo Mail!</td>
<td></td>
<td>Stany Zjednoczone (obsługa użytkowników z EU przez spółkę zależną z siedziby w Irlandii)</td>
<td></td>
<td>Irlandia</td>
</tr>
<tr>
<td>Pakiet biurowy</td>
<td>Microsoft Office 365</td>
<td>Usługi bezpłatne – Stany Zjednoczone</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stany Zjednoczone</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Przechowywanie plików</td>
<td>Dropbox</td>
<td>Stany Zjednoczone</td>
<td>Stany Zjednoczone (prawo stanu Kalifornia w Stanach Zjednoczonych)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Przechowywanie zdjęć</td>
<td>Flickr</td>
<td>Stany Zjednoczone (obsługa użytkowników z UE przez spółkę zależną z siedziby w Irlandii)</td>
<td></td>
<td>Irlandia</td>
</tr>
</tbody>
</table>

728 Przy opracowaniu tabeli wykorzystano warunki świadczenia usług aktualne na dzień 21.07.2017 i dotyczące użytkowników rejestrujących usługi z obszaru Polski.

Odnośniki do regulaminów świadczenia usług (wzorców umów):
- Dropbox: https://www.dropbox.com/privacy#terms,
- Vimeo: https://vimeo.com/terms#general_provisions,
- Spotify: https://www.spotify.com/pl/legal/end-user-agreement/#s24,
- Netflix: https://help.netflix.com/legal/termsofuse,
- LinkedIn: https://www.linkedin.com/legal/user-agreement,
- Facebook: https://www.facebook.com/legal/terms/update,
- Microsoft: https://www.microsoft.com/pl-pl/servicesagreement/,
<table>
<thead>
<tr>
<th>Media strumieniowe</th>
<th>Youtube</th>
<th>Stany Zjednoczone</th>
<th>Stany Zjednoczone (prawo stanu Kalifornia w Stanach Zjednoczonych)</th>
<th>Stany Zjednoczone (sąd federalny lub stanowy właściwy dla siedziby usługodawcy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vimeo</td>
<td></td>
<td>Stany Zjednoczone</td>
<td>Stany Zjednoczone (prawo stanu Nowy Jork w Stanach Zjednoczonych)</td>
<td>Stany Zjednoczone (sąd federalny lub stanowy właściwy dla siedziby usługodawcy)</td>
</tr>
<tr>
<td>Portale społecznościowe</td>
<td>Facebook</td>
<td>Stany Zjednoczone</td>
<td>Stany Zjednoczone (prawo stanu Kalifornia w Stanach Zjednoczonych)</td>
<td>Stany Zjednoczone (sąd federalny lub stanowy właściwy dla siedziby usługodawcy)</td>
</tr>
<tr>
<td>LinkedIn</td>
<td></td>
<td>Stany Zjednoczone</td>
<td>Irlandia</td>
<td>Irlandia</td>
</tr>
<tr>
<td>Snapchat</td>
<td></td>
<td>Stany Zjednoczone</td>
<td>Prawo Anglii i Walii</td>
<td>Sąd właściwy dla siedziby usługodawcy</td>
</tr>
<tr>
<td>Udostępnianie muzyki</td>
<td>Spotify</td>
<td>Szwecja</td>
<td>Szwecja</td>
<td>Polska</td>
</tr>
<tr>
<td>Wideo na żądanie</td>
<td>Netflix</td>
<td>Stany Zjednoczone</td>
<td>Holandia</td>
<td>Brak wskazania</td>
</tr>
</tbody>
</table>
6.4.4. Chmura obliczeniowa z perspektywy przepisów europejskich

Prawo UE, stanowiąc normy o zasięgu ponadnarodowym i regionalnym, przyczyniło się do skutecznego rozwiązania niektórych z wcześniej omówionych problemów – w szczególności dotyczących ryzyk związanych z wyborem prawa właściwego dla siedziby usługodawcy oraz trudnością w skutecznej ochronie praw podmiotów danych w odniesieniu do działań zagranicznych przedsiębiorców. Powstanie spójnego rynku wewnętrznego, także w obszarze przetwarzania danych, na którym obowiązują te same regulacje publicznoprawne, spowodowało, że użytkownicy mogą swobodnie korzystać z usług oferowanych przez podmioty prowadzące działalność z terenu innych krajów UE bez obaw o naruszenie swoich praw czy zakresu ochrony prywatności. Chmura obliczeniowa jest jednak technologią w pełni wykorzystującą potencjał cyberprzestrzeni, także związany ze swobodną, globalną wymianą informacji. Stąd też rozwiązania prawne o charakterze ponadnarodowym, ale tylko regionalnym de facto przenoszą problem prawa właściwego oraz skuteczności mechanizmów ochrony praw jednostki z poziomu relacji pomiędzy systemami prawnymi poszczególnych państw na poziom relacji pomiędzy systemem prawnym UE a prawodawstwem państw trzecich (nienależących do UE/EOG). Prawdziwe jest zatem stwierdzenie, że o ile przepisy unijne przyczyniły się do zbudowania jednolitego rynku w obrębie państw członkowskich, to problemy związane z wymianą danych z innymi państwami w znacznej części pozostały nierozwiązane.

Przepisy dyrektywy 95/46 były formułowane w czasach, gdy nie było technicznej możliwości realizacji usług cloud computingu oraz rynku globalnego przetwarzania danych. Stąd też próba objęcia istniejącymi regulacjami nowego fenomenu technicznego napotykała szereg trudności interpretacyjnych. Problemy te stały się jedną z przyczyn podjęcia prac legislacyjnych związanych z opracowaniem nowego rozporządzenia o ochronie danych. Ogólne rozporządzenie w zamyśle projektodawców miało zatem być europejską odpowiedzią na globalny rynek przetwarzania informacji i pojawiające się w nim ryzyka dla ochrony prywatności729. W szczególności zarówno Komisja Europejska, jak i inne instytucje UE oraz uczestnicy procesu legislacyjnego podkreślali znaczenie przyjętych rozwiązań dla regulacji rynku przetwarzania danych w chmurze730. Najważniejsze zagadnienia, które stały się przedmiotem dyskusji i regulacji rozporządzenia, dotyczą:

1) problemu zakresu terytorialnego,

729 Por. rekomendacje dotyczące projektowanego rozporządzenia przez WP29 w opinia 05/2012 na temat przetwarzania danych w chmurze obliczeniowej, WP 196, https://goo.gl/ZDi2XH, s. 26-27.
2) zakresu stosowania wyłączenia związanego z przetwarzaniem na cele prywatne,
3) możliwości podzlecania przetwarzania danych oraz różnym zakresem obowiązków administratora danych i przewarzającego dane,
4) możliwości dochodzenia praw przez podmioty danych w odniesieniu do przedsiębiorców nieposiadających siedziby ani oddziału na terenie UE,
5) możliwości praktycznego stosowania przepisów UE poza granicami Unii (perspektywa przetwarzającego dane).

Warto zauważyć, że wskazane wyżej problemy nie są unikalne tylko dla rozwiązań przetwarzania w chmurze, w rzeczywistości dotyczą wszystkich usług świadczonych za pośrednictwem Internetu. Ich wspólnym mianownikiem jest bowiem globalny transfer danych. Usługi chmury obliczeniowej uwypuklają znaczenie tych zagrożeń, ponieważ międzynarodowy transfer danych oraz przetwarzanie rozproszone, w którym uczestniczy wielu podwykonawców, to najważniejsze cechy, bez których usługi te nie mogą być poprawnie realizowane.

Zgodnie z zaproponowanym w ogólnym rozporządzeniu modelem zasięgiem stosowania europejskich przepisów o ochronie danych obecni są przedsiębiorcy, którzy spełniają co najmniej jeden z poniższych warunków:
- przetwarzają dane na terenie Unii;
- prowadzą działalność na terenie Unii, nawet jeżeli dane nie są przetwarzane na terenie Unii,
- nie prowadzą działalności na terenie Unii, ale oferują swoje usługi podmiotom danych w Unii.

Pierwszy przypadek jest oczywisty i dotyczy sytuacji, w której dane są przetwarzane w centrach danych zlokalizowanych w Unii. Warto zauważyć, że w takim przypadku przedsiębiorca niejako z definicji prowadzi działalność na terenie Unii. Scenariusz ten jest jasny i nie budzi wątpliwości, a zakres regulacji jest znany z dyrektywy 95/46.

Dwa kolejne przypadki prowadzą do rozszerzenia zakresu podmiotowego rozporządzenia i mają bezpośrednio zastosowanie w odniesieniu do usług przetwarzania w chmurze. Objęcie zakresem wszystkich czynności przetwarzania w związku z działalnością prowadzoną przez przedsiębiorcę niezależnie od faktycznego miejsca przetwarzania (art. 3 ust. 1 rozporządzenia) skutkuje obowiązkiem zachowania reżimu wynikającego z europejskich przepisów także poza obszarem UE i również przez podwykonawców, którym administrator powierzył przetwarzanie. Należy jednak zwrócić uwagę, że co do zasady zobowiązany z art. 1 jest przedsiębiorca (administrator lub podmiot przetwarzający)
posiadający jednostkę organizacyjną w Unii. Odpowiedzialność podmiotów, którym zlecił przetwarzanie, wynika z relacji kontraktowych pomiędzy administratorem a jego podwykonawcami. Podwykonawcy z państw trzecich nie są więc na mocy art. 1 objęci zakresem regulacji rozporządzenia. Zatem odpowiedzialność za naruszenie zobowiązań publicznoprawnych ponosi zlecający, a nie podmiot, który naruszenia się dopuścił. Ma to o tyle istotne znaczenie, że w przypadku przetwarzania w chmurze istnieje wielopoziomowa hierarchia firm podwykonawczych i w praktyce administrator ma ograniczoną wiedzę na temat dalszych podwykonawców (w terminologii przepisów europejskich nazywa się ich *subprocesorami*, w odróżnieniu od bezpośrednich podwykonawców – których określa się *procesorami*).

Ostatni ze wskazanych przypadków stosowania europejskich przepisów o ochronie danych dotyczy przedsiębiorców, którzy nie prowadzą działalności na terenie Unii, jednak oferują swoje usługi użytkownikom z terenu UE (art. 3 ust. 2 pkt a rozporządzenia). Zgodnie z orzecznictwem TSUE przesłankę wystarczającą do uznania, że usługa jest oferowana na obszarze Unii, stanowi w szczególności opracowanie strony internetowej w języku powszechnie używanym w dowolnym z państw członkowskich lub obsługa płatności w walucie lokalnej. W przypadku usług realizowanych w chmurze obliczeniowej – świadczonych z definicji na odległość i kierowanych do szerokiego kręgu odbiorców – rozstrzygające znaczenie może mieć treść regulaminu świadczenia usług (umowy pomiędzy usługodawcą a usługobiorcą). Jeżeli regulamin nie zawiera żadnych ograniczeń i wyłączeń w zakresie terytorialnego zakresu korzystania z usługi lub też bezpośrednio (w treści regulaminu) lub pośrednio (poprzez np. udostępnienie regulaminu w języku usługobiorcy) potwierdza możliwość korzystania z usługi w jakimkolwiek państwie członkowskim UE, uzasadniają one wady o spłaceniach przesłanki objęcia czynności przetwarzania realizowanych w ramach tej usługi europejskimi przepisami o ochronie danych. Przywołując wcześniejszą analizę wybranych usług *cloud computingu*, wskazać należy, że wszystkie wymienione w tabeli 1 (s. 276) usługi spełniają tak zdefiniowane kryterium. Uznanie, że przedsiębiorca zagraniczny ma obowiązek stosować przepisy europejskie w zakresie czynności związanych z przetwarzaniem danych użytkowników z UE, prowadzi do wniosku, że także jego podwykonawcy muszą stosować te przepisy. Rozporządzenie 2016/679 ma w efekcie bardzo szeroki zakres stosowania, wykraczając poza granice geograficzne UE – zwłaszcza uwzględniając, że główne usługi świadczone w chmurze obliczeniowej są świadczone przez przedsiębiorców z państw trzecich (głównie Stanów Zjednoczonych).
Istotną cechą usług świadczonych w chmurze obliczeniowej jest mnogość podwykonawców. Dane są przetwarzane w sposób rozproszony geograficznie, ale często również przez różne podmioty na podstawie zawartych umów. Postanowienia kontraktowe regulują zasady i formy przetwarzania, a także służą rozliczaniu kosztów wzajemnych usług. Jednocześnie relacje te są mało przejrzyste z punktu widzenia podmiotów danych, a często i samych administratorów. W efekcie powstaje ryzyko utraty kontroli nad obiektem informacji oraz miejsc ich przetwarzania. Z uwagi na brak aktów prawnomiedzynarodowych, które mogłyby służyć jako źródło norm *erga omnes* w tym zakresie, prawodawca unijny zdecydował się wprowadzić własny system budowania relacji i odpowiedzialności pomiędzy podmiotami przetwarzającymi dane. Jest to nowe rozwiązanie, nieznane wcześniej na gruncie dyrektywy 95/46, stąd będzie podlegało uważnej ocenie w pierwszym okresie stosowania rozporządzenia. Podstawę do określenia obowiązków podmiotów przetwarzających stanowi art. 28 rozporządzenia. Wszystkie podmioty zaangażowane w przetwarzanie danych muszą być zobowiązane do przestrzegania przepisów rozporządzenia, a umowa, na mocy której odbywa się przetwarzanie, musi podlegać prawu UE lub prawu państwa członkowskiego. Podmioty przetwarzające nie mogą samodzielnie decydować o dalszych podwykonawcach bez uprzedniej zgody administratora. Administrator ma zatem pełną odpowiedzialność wobec administratora podmiotów przetwarzających informacje w jego imieniu. W przypadku, gdy dalszy podwykonawca (*subprocesor*) nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora spoczywa na pierwotnym (głównym) podmiocie przetwarzającym (*procesorze*). Ponieważ prawo właściwe dla wszystkich czynności przetwarzania to prawo UE, podmiot danych może korzystać ze wszystkich środków ochrony wynikających z przepisów – zarówno na ścieżce publiczno-prawnej (administracyjnej), jak i cywilnej – i to przed organami właściwymi dla jego miejsca zamieszkania.

W praktyce duża część administratorów i podmiotów przetwarzających dane posiada siedziby i prowadzi działalność poza obszarem UE. W odniesieniu do ich działalności możliwość stosowania środków ochrony prawnej mogła być częściowo ograniczona, zwłaszcza w zakresie wniosków czy żądań kierowanych bezpośrednio do administratorów. Dlatego prawodawca wprowadził w rozporządzeniu jeszcze jedno nowe rozwiązanie – konieczność ustanowienia w UE odpowiednio umocowanego przedstawiciela przez administratorów i podmioty przetwarzające, nie mające siedziby w Unii (a więc podlegające
przepisom rozporządzenia na mocy art. 2 rozporządzenia)\textsuperscript{731}. Zgodnie z art. 27 ust. 3 przedstawiciel musi mieć siedzibę na terenie UE oraz musi być upoważniony do kontaktu w sprawach związanych z zapewnieniem przestrzegania rozporządzenia organy nadzorcze i podmioty danych.

Przedstawiony powyżej model regulacji usług \textit{cloud computing} w europejskich przepisach o ochronie danych – na który składają się rozszerzony zakres terytorialny przepisów, wymóg stosowania prawa UE w relacjach pomiędzy podmiotami uczestniczącymi w przetwarzaniu oraz konieczność wyznaczenia przedstawiciela – ma na celu zapewnienie wysokich standardów ochrony danych osobowych w odniesieniu do danych użytkowników UE niezależnie od geograficznego miejsca, w którym przetwarzane są ich dane i niezależnie od przepisów wynikających z lokalnego prawodawstwa. Podejście to, aczkolwiek ambitne i zmierzające do podniesienia standardów ochrony w cyberprzestrzeni, ma kilka istotnych wad, które należy wskazać.

W pierwszej kolejności należy pamiętać, że wszystkie podmioty uczestniczące w przetwarzaniu w chmurze funkcjonują w określonej przestrzeni prawnej. Przepisy o ochronie danych, w różnym zakresie i różnej formie, funkcjonują także poza Unią – o czym w dyskusji nad europejską reformą nie zawsze pamiętano. Trudno założyć, że w przypadku kolizji norm przedsiębiorca zagraniczny odrzuci przepisy prawa krajowego – którym wprost podlega – i zacznie stosować sprzeczne regulacje europejskie, wynikające ze zobowiązań umownych, które na siebie przyjął. Usługi przetwarzania w chmurze nie są dedykowane wyłącznie dla mieszkańców z obszaru Unii. Z definicji mają charakter uniwersalny i – w większości przypadków – globalny. Wypełnienie przepisów rozporządzenia oznaczałoby, że albo dane wszystkich użytkowników (niezależnie od kraju ich pochodzenia) będą przetwarzane zgodnie z reżimem przepisów europejskich, albo dostawca zmuszony będzie do przygotowania oddzielnych środowisk przetwarzania informacji dedykowanych tylko do obsługi użytkowników z UE. Oba rozwiązania wydają się tam samo mało prawdopodobne. Dlatego, aby uniknąć tego typu problemów, niektórzy dostawcy usług przetwarzania w chmurze już obecnie zapewniają obsługę swoich europejskich klientów wyłącznie przez centra danych zlokalizowane w UE. Takie rozwiązanie jest możliwe do zastosowania tylko w przypadku mniejszych e-usług. W przypadku usług o zasięgu globalnym doprowadziłoby \textit{de facto} do stworzenia formuły „europejskiego Internetu”, stojącego w pewnym zakresie w opozycji do Internetu światowego. \textit{Europejski Internet} wprowadzałby wyższe standardy ochrony danych,
ale jednocześnie przepływ i wymiana informacji z systemami zagranicznymi byłaby utrudniona. Prawodawca europejski nie miał takiego zamieru, więc koncepcję tę należy odrzucić.


Powyższa obserwacja ukazuje największą słabość wprowadzonego w rozporządzeniu modelu ochrony danych przetwarzanych przez przedsiębiorców zagranicznych, jakim jest brak środków prawnych dyscyplinujących do przestrzegania przepisów europejskich. W skrajnym przypadku przedsiębiorca z państwa trzeciego może nie ustanowić przedstawiciela w UE i nie stosować prawa UE nawet w odniesieniu do użytkowników z Unii. W takim przypadku, jakkolwiek przepisy zostaną w oczywisty sposób naruszone, podmiot danych oraz organy nadzoru nie będą dysponowały skutecznym środkiem oddziaływania na zachowanie zagranicznego przedsiębiorcy. Teoretycznie rozwiązania można szukać w próbie blokowania dostępu do takich usług z obszaru UE, jednak w praktyce rozwiązanie takie po pierwsze są trudne w implementacji, a po drugie budżet obu podmiotów prawo do informacji związane z możliwością cenzorowania w ten sposób treści udostępnianych w Internecie. Skoro zatem brak jest publicznoprawnych mechanizmów oddziaływania na

732 Rozwiązanie tego typu zostało wprowadzone do polskiego porządku prawnego wraz z nowelizacją ustawy o grach hazardowych z dn. 15.12.2016 (Dz.U. z 2017 r. poz. 88). Na mocy art. 15f ust. 1 ustawy minister
przedsiębiorstw zagranicznych, ich dostosowanie się do norm europejskich będzie wynikało wyłącznie z poszanowania przepisów obowiązujących na rynku, na którym chcą działać. W wielu przypadkach tak rozumiana „dobra wola” to jednak zbyt mało, aby można było mówić o pełnej skuteczności przepisów.

Kolejnym – powiązanym – problemem jest brak możliwości oceny, czy przedsiębiorcy zagraniczni wdrożyli skuteczne i zgodne z prawem mechanizmy bezpieczeństwa związane z podejmowanymi czynnościami przetwarzania. W przypadku przetwarzania mającego miejsce na terenie UE istnieje możliwość przeprowadzenia działań kontrolnych przez organ nadzoru (por. art. 58 ust. 1 rozporządzenia). W odniesieniu do podmiotów zagranicznych funkcję taką może pełnić wyłącznie audytor wskazany przez administratora (art. 28 ust. 3 pkt h rozporządzenia), jednak czynności przez niego podejmowanie nie korzystają z ochrony państwa i nie zmierzają do oceny zobowiązań prawnopublicznych. Mają zatem inny charakter – i podobnie jak w przypadku stosowania przepisów europejskich – wynikają wyłącznie ze zobowiązań kontraktowych, które przyjął na siebie.

Z powodu braku możliwości oparcia regulacji na normach erga omnes (w tym wypadku – aktach prawnomiędzynarodowych) prawodawca unijny zdecydował się rozszerzyć zakres stosowania przepisów europejskich poprzez obowiązkowe stosowanie prawa UE we wszystkich czynnościach przetwarzania i uzależnić od tego możliwość przekazania danych do podmiotów zagranicznych. Chociaż jest to model ciekawy i nowatorski to wydaje się się, że w znacznym zakresie ma charakter deklaratywny i będzie trudny do zastosowania w praktyce.

6.4.5. Chmura obliczeniowa z perspektywy prawa USA

Przyjmując za punkt odniesienia model funkcjonujący w UE – na który składają się normy wynikające z traktatów, aktów prawa wtórnego jak i orzecznictwa TSUE – podejście do prawnej ochrony prywatności w Stanach Zjednoczonych charakteryzuje:

- brak konstytucyjnych gwarancji dla ochrony danych osobowych oraz ograniczone prawo do ochrony prywatności,
- rozproszony charakter ustawowych przepisów o ochronie danych, wprowadzanych sektorowo w nie zawsze spójny sposób,

Prawo USA jest w kontrastie do europejskiego modelu, gdzie na szczeblu unijnym istnieją uniwersalne przepisy w zakresie ochrony danych. W Stanach Zjednoczonych istnieje wiele lokalnych przepisów ochrony prywatności, a rola państwa jest ograniczona. Wiele z tych przepisów jest konfliktowne, co powoduje niejednolitość i niejednolitość wykonania w różnych stanach.
– brak jednego organu nadzoru oraz funkcji ombudsmana,
– niejednolity system prawny (prawo stanowe i federalne), w którym te same kwestie mogą być realizowane w odmienny sposób przez poszczególnych legislatorów.

Najważniejszą różnicą pomiędzy modelem UE a USA, mającą fundamentalne znaczenie dla ukształtowania amerykańskiego systemu prawnego, jest brak nadania ochronie danych osobowych rangi prawa podstawowego. Co więcej, Konstytucja USA nie definiuje wprost także prawa do ochrony prywatności. Zakres prawnej ochrony prywatności jest związany z orzecznictwem Sądu Najwyższego USA stanowiącym wykładnię stosowania Czwartej Poprawki do Konstytucji, dotyczącej nietykalności osobistej i materialnej oraz zakazującej przeprowadzania nieuzasadnionych rewizji lub zatrzymań. Brak odpowiednich norm konstytucyjnych nie może być także uzupełniony wiążącymi aktami prawa międzynarodowego w sposób podobny do roli realizowanej przez EKPC w systemie prawnym państw europejskich. Chociaż Stany Zjednoczone przystąpiły do MPPOP, to na skutek zastrzeżeń zgłoszonych w procesie ratyfikacji, normy Paktu nie mają skutku bezpośredniego w systemie prawnym USA. Wskutek braku umocowania ochrony danych osobowych w przepisach konstytucyjnych w Stanach Zjednoczonych nie wprowadzono publiczнопrawnych mechanizmów ochrony na wzór rozwiązań stosowanych w państwach europejskich. W literaturze przedmiotu podkreślą się natomiast wiodące znaczenie prawa do informacji i wolności wypowiedzi jako kluczowych wartości konstytucyjnych, co prowadzi także do ograniczania prawa do prywatności.

Badając problematykę gwarancji konstytucyjnych mających zastosowanie do ochrony danych przetwarzanych w chmurze, należy zwrócić uwagę na dwie istotne doktryny prawne, stosowane od lat w orzecnictwie Sądu Najwyższego i mające fundamentalne znaczenie z punktu widzenia ochrony użytkowników przed nieuprawioną ingerencją w sferę prywatności.

Pierwszą z nich jest test uzasadnionego oczekiwania prywatności (ang. reasonable expectation of privacy)\(^{736}\), zdefiniowany po raz pierwszy w sprawie *Katz v. Stany Zjednoczone*\(^{737}\). Zgodnie z nim ustalenie, czy ingerencja ze strony władzy publicznej w sferę prywatności jest uzasadniona, przeprowadza się dwuetapowo. W pierwszej kolejności sąd powinien ocenić, czy analizowane zdarzenie w subiektywnej ocenie jednostki naruszyło jej oczekiwania prywatności. Dopiero jeżeli odpowiedź na pierwsze pytanie jest twierdząca, sąd powinien rozważyć, czy oczekiwania to było obiektywnie uzasadnione, a więc czy „społeczeństwo jest gotowe, aby uznać je za uzasadnione”\(^{738}\). Ponieważ obszar subiektywnych odczuć jednostki nie podlega prostej ocenie, w amerykańskiej judykатурze przyjmuje się, że zasadniczy element testu stanowi wyważenie tego, co obiektywnie można uznać za „uzasadnione”\(^{739}\).

Drugą ważną doktryną, wyznaczającą granice ochrony wynikające z Czwartej Poprawki jest zasada trzeciej strony (ang. third party doctrine). O ile test uzasadnionego oczekiwania prywatności powała na rozszerzenie zakresu ochrony w odniesieniu do okoliczności, które w powszechnym odczuciu związane są z ochroną sfery prywatności, to doktryna trzeciej strony służy do wyłączenia spod ochrony sytuacji, w których jednostka sama przyczyniła się do ujawnienia informacji. Zgodnie z zasadą trzeciej strony, po raz pierwszy wprowadzoną w sprawie *Hoffa v. Stany Zjednoczone*\(^{740}\), jeżeli jednostka sama i dobrowolnie przekazała informacje podmiotowi zewnętrznemu, nie może żądać ochrony przed ujawnieniem tych informacji władzy publicznej. Nie ma przy tym znaczenia zakres kontraktowych zobowiązań lub innych uzgodnień pomiędzy stronami dla faktu możliwości pozyskania takich informacji przez organy władzy publicznej bez konieczności przestrzegania trybu wynikającego z Czwartej Poprawki. Przekazanie informacji trzeciej stronie prowadzi do

---


\(^{738}\) Ibidem, s. 361.


braku możliwości uznania, że jednostka posiada uzasadnione oczekiwanie prywatności w związku z treścią przekazanych informacji. Zasada trzeciej strony, zgodnie z wyrokami Sądu Najwyższego, znalazła zastosowanie w odniesieniu do danych bankowych (dostęp do wyciągów bankowych) czy telekomunikacyjnych (dostęp do danych billingowych) – w uogólnieniu wszędzie tam, gdzie dane były dobrowolnie udostępniane i przetwarzane przez podmioty zewnętrzne w związku z prowadzeniem przez nie działalności gospodarczej. W konsekwencji w opisanych przypadkach organy ścigania i wymiaru sprawiedliwości mogą uzyskiwać żądane informacje nie w oparciu o nakaz sądowy (ang. warrant), czyli w trybie wynikającym z Czwartej Poprawki, ale na podstawie postanowienia wydanego przez wnioskujący organ (ang. subpoena). W wyroku Couch v. Stany Zjednoczone Sąd Najwyższy wskazał na trzy przesłanki, które muszą zostać łącznie spełnione, aby można było zastosować zasadę trzeciej strony: (1) informacje muszą zostać dobrowolnie przekazane (2) do podmiotu trzeciego, który (3) wykorzystuje je w rama chmur. W doktrynie istnieją różne oceny, czy użytkownicy mogą posiadać uzasadnione oczekiwanie prywatności w odniesieniu do usług przetwarzanych w modelu chmury obliczeniowej – zwłaszcza wobec faktu, że dobrowolnie przekazują dane podmiotom zewnętrznym. Dominuje pogląd o możliwości odniesienia gwarancji wynikających z Czwartej Poprawki do usług cloud computingu. Stanowisko to wspiera wyrok wyrok Katz v Stany Zjednoczone, w którym SN wskazał, że konstytucja co do zasady chroni ludzi, a nie miejsca. Choć zasady to dotyczyło konkretnego stanu faktycznego (zakresu ochrony prywatności w odniesieniu do korzystania z publicznych aparatów telefonicznych), to ma oczywiste zastosowanie także do przechowywania danych z wykorzystaniem zasobów zewnętrznych usługodawców. Z kolei w wyroku Stany Zjednoczone v. Warshak federalny Sąd Apelacyjny uznał, że Czwarta Poprawka obejmuje także treść informacji przechowywanych w wersji elektronicznej (w tej konkretnej sprawie –

742 Wyrok Sądu Najwyższego USA z 20.06.1979, sprawa Smith v. Maryland, sygn. 442 U.S. 735 (1979).
745 Wyrok SN w sprawie Stany Zjednoczone v. Katz, op. cit., s. 351.
wiadomości e-mail). Łącząc powyższe wnioski można uznać, że ochrona konstytucyjna powinna dotyczyć danych przechowywanych w chmurze obliczeniowej.

Z drugiej jednakże strony nie sposób pominać faktu, że powierzenie danych podmiotowi trzeciemu – zwłaszcza na warunkach pozwalających na dostęp do tych danych i ich wykorzystanie w celach prowadzonej działalności gospodarczej – prowadzi do zniesienia możliwości powoływania się na zasadę uzasadnionego oczekiwania prywatności. W tym zakresie rozstrzygające znaczenie może mieć treść regulaminów świadczenia usług, a w szczególności zakres dostępu do danych użytkownika przyznany usługodawcy oraz ograniczenia związane z ustalonymi celami przetwarzania. I tak dla przykładu Google w warunkach korzystania z usługi przewiduje możliwość wykorzystania danych użytkownika (np. wiadomości e-mail) w celu dostosowania treści wyświetlanych przez siebie reklam. Z kolei Dropbox wyraźnie zastrzega, że jedynym celem przetwarzania danych jest świadczenie usług w granicach określonych w zawartej umowie. Odmiennie podejście zastosował Snap (operator serwisu Snapchat), który w warunkach korzystania z usługi wskazał, że użytkownik udziela przedsiębiorcy licencji na wykorzystanie udostępnianych materiałów. Oznacza to, że operator serwisu może wykorzystywać treści publikowane przez użytkowników do własnych celów.

Jak widać z powyższego zestawienia, nie jest możliwe generalne odniesienie zasady trzeciej strony do usług świadczonych w chmurze obliczeniowej bez skonkretyzowania analizowanej usługi. Od szczegółowych zapisów kontraktowych wynikających z zatwierdzonego regulaminu wynika zakres czynności, jakie w odniesieniu do udostępnionych danych może podjąć usługodawca. Jeżeli regulamin nie zezwala na wykorzystanie danych w innym celu niż związany z realizacją umowy, w szczególności na ich wykorzystanie komercyjne przez usługodawcę, nie zostaną spełnione wszystkie przesłanki zastosowania doktryny trzeciej strony, a zatem dostęp do danych użytkownika nadal będzie korzystał z ochrony konstytucyjnej.

Powyższe rozważania należy uzupełnić dwoma istotnymi aspektami: po pierwsze wyłącznie publicznoprawnym charakterem ochrony wynikającej z Czwartej Poprawki oraz jej niewielkim praktycznym zastosowaniem w odniesieniu do cudzoziemców (osób niebędących obywatelami albo rezydentami Stanów Zjednoczonych). Treść Czwartej Poprawki wprost obejmuje wyłącznie naruszenia wertykalne, a więc mające źródło w działaniach władzy publicznej\(^\text{747}\). Norma nakłada zatem negatywny obowiązek na państwo, związany z

powstrzymaniem się od nieuzasadnionej ingerencji. Nie obejmuje obowiązków pozytywnych, związanych z wprowadzeniem regulacji wewnętrznych gwarantujących poszanowanie prywatności w relacjach horyzontalnych. Jest to fundamentalna różnica pomiędzy zakresem prawa do prywatności wynikającym z Konstytucji USA oraz z europejskich norm konstytucyjnych (prawa międzynarodowego – EKCP, prawa unijnego – KPP, ale także Konstytucji RP)⁷⁴⁸.

Drugim istotnym ograniczeniem stosowania Czwartej Poprawki jest zdefiniowanie zakresu podmiotów uprawnionych wyłącznie do obywateli i rezydentów USA. Wniosek taki wynika z orzeczenia SN w sprawie Stany Zjednoczone v. Verdugo-Urquidez⁷⁴⁹ i jest często przytaczany w literaturze przedmiotu w kontekście wskazywania ograniczonych gwarancji dla obywateli UE w zakresie prawa do poszanowania prywatności⁷⁵⁰. W efekcie praktyczne znaczenie Czwartej Poprawki w odniesieniu do ochrony danych obywateli UE przetwarzanych w systemach informatycznych amerykańskich usługodawców jest niewielkie⁷⁵¹.

Niezależnie od zakresu gwarancji konstytucyjnych związanych z ochroną prywatności prawodawstwo Stanów Zjednoczonych reguluje tę materię także na poziomie aktów rangi ustawowej. Odmienne niż w modelu europejskim w Stanach Zjednoczonych nie wprowadzono centralizowanego systemu ochrony danych opartego na reżimie prawnopublicznym. Dlatego powstały odrębne normy dotyczące przetwarzania danych w sektorze publicznym oraz prywatnym. Przepisy związane z zagrożeniami horyzontalnymi są też znacznie rozproszone i definiowane sektorowo (np. ochrona danych medycznych, telekomunikacyjnych itp.) lub rodzajem przetwarzania (np. ochrona danych przesyłanych w formie elektronicznej). Przepisy te mają różne zakres stosowania także jeżeli chodzi o ich skutki dla prawodawstwa stanowego. Dla przykładu ustawa Privacy Act⁷⁵², będąca podstawowym aktem prawnym regulującym dostęp, gromadzenie i przetwarzanie danych przez organy władzy publicznej, jako regulacja federalna nie znajduje zastosowania do

⁷⁴⁸ Szczegółowe rozważania przedstawiono w rozdziale 2 (s. 50).
⁷⁵⁰ Directorate General for Internal Policies Policy, Department C: Citizens’ Rights and Constitutional Affairs: The US legal system..., op. cit., rozdz. 2.1, s. 10.
⁷⁵² Zob. przypis 602 (s. 208).
organów władzy stanowej\textsuperscript{753}. W efekcie ustalenie faktycznego zakresu praw i gwarancji wymaga odniesienia do konkretnego stanu faktycznego i prawa właściwego dla rozstrzygnięcia danego problemu, z uwzględnieniem kluczowego w systemie \textit{common law} prawa precedensów.

Również obszar nadzoru i kontroli nie jest w USA koordynowany centralnie, w efekcie czego różne agendy rządowe wykonują działania związane z nadzorem przestrzegania przepisów dotyczących ochrony danych osobowych w nadzorowanym sektorze rynku\textsuperscript{754}. Wiodącą rolę w tym zakresie odgrywa Federalna Komisja Handlu (\textit{Federal Trade Commission}, FTC), której kompetencje w badanej dziedzinie wynikają z przepisów o ochronie konsumentów i przeciwdziałania nieuczciwym praktykom handlowym. FTC nie nadzoruje jednak wszystkich gałęzi gospodarki, nie ma też możliwości podejmowania działań w sektorze publicznym.

Podsumowując, system prawny Stanów Zjednoczonych reguluje kwestie ochrony prywatności w cyberprzestrzeni w sposób fundamentalnie odmienny od modelu europejskiego. Różnice pojawiają się już na poziomie przepisów konstytucyjnych i znajdują odzwierciedlenie zarówno w ustawodawstwie, jak i judykaturze. Prawa jednostki w odniesieniu do operacji przetwarzania w sektorze publicznym i prywatnym są gwarantowane różnymi przepisami oraz w odmiennym zakresie. Federalne przepisy ustawowe w głównej mierze wprowadzają regulacje związane z przetwarzaniem danych w sektorze publicznym, sektor prywatny pozostawiając swobodę kształtowania stosunków między stronami.

Regulacje publicznoprawne niedotykające sektora publicznego wprowadzone są uzupełniające, np. w obszarze ochrony konsumentów czy przetwarzania szczególnych kategorii danych, takich jak dane medyczne. Nie bez znaczenia jest także podkreślana w literaturze przedmiotu ochrona wolności słowa i prawa do informacji (Pierwsza Poprawka do Konstytucji\textsuperscript{755}), która wyraża się też w nadawaniu tym wartościom większej wagi niż kwestiom ochrony prywatności jednostek\textsuperscript{756}. Konsekwencją przyjętego podejścia jest

\begin{enumerate}
\item [753] Poszczególne stany mogą wprowadzać własne regulacje w tym zakresie, jednak w większości stanów przepisy takie nie zostały uchwalone. Co więcej, przepisy funkcjonujące w różnych stanach mogą różnić się od siebie oraz od regulacji federalnych.
\end{enumerate}
odmienny zakres ochrony danych przechowywanych w modelu chmury obliczeniowej wynikający z prawodawstwa UE i USA. Z uwagi na znaczenie usługodawców amerykańskich dla rynku cloud computingu problem ten może mieć zasadnicze znaczenie dla dalszego rozwoju rynku. Odpowiedzią na to zagrożenie jest wprowadzenie do ogólnego rozporządzenia o ochronie danych przedstawionych wcześniej rozwiązań prawnych prowadzących do objęcia przepisami unijnymi wszystkich podmiotów przetwarzających dane użytkowników UE, niezależnie od miejsca przetwarzania.

6.5. Podsumowanie i wnioski

Przetwarzanie danych w chmurze obliczeniowej jest nowym i stale rosnącym trendem technologicznym, stanowiącym jedno z narzędzi budowania społeczeństwa informacyjnego. Jak z każdą dynamicznie rozwijającą się technologią o powszechnym zastosowaniu praktycznym, poza szansami związane z nią także różne ryzyka i zagrożenia, również o charakterze prawnym.

Trend ten jest zauważalny nie tylko wśród przedsiębiorców, ale również organizacji publicznych. W Wielkiej Brytanii utworzono ramy świadczenia usług cloud computingu dla podmiotów administracji – tzw. G-Cloud. Rozwiązanie to polega na wyborze i zatwierdzeniu dostawców usług w chmurze, z których mogą w łatwy sposób korzystać podmioty publiczne. Sposób realizacji G-Cloud, będących w istocie połączeniem cech chmury prywatnej i wspólnej, prowadzi do zapewnienia odpowiedniego poziomu bezpieczeństwa i prywatności przetwarzanych danych, jednocześnie dostarczając możliwość korzystania usługodbiornikom publicznym z szerokiego wachlarza nowoczesnych usług świadczonych w modelu chmury obliczeniowej. Ministerstwo Cyfryzacji w maju 2017 opublikowało zamówioną przez siebie opinię prawną mającą na celu wskazanie możliwości wprowadzenia rozwiązania podobnego G-Cloud w Polsce. We wnioskach z przeprowadzonej analizy wskazano, że implementacja modelu G-Cloud w Polsce jest możliwa „w oparciu o aktualnie obowiązujące przepisy prawa

757 Por. wyniki badania Eurostatu omówione na s. 250.
oraz nie jest rozwiązaniem skomplikowanym technicznie. Należy zatem oczekiwać, że także władze polskie będą zainteresowane wprowadzeniem formuły ułatwiającej zamawianie i korzystanie z usług świadczonych w chmurze przez podmioty publiczne.


Analizy dotyczące dynamicznego rozwoju rynku usług świadczonych w chmurze obliczeniowej prowadzą do wniosku o potrzebie prawnego uregulowania kwestii prywatności i bezpieczeństwa przetwarzanych danych. Podjęte obecnie przez prawodawcę unijnego działania związane ze wzmocnieniem gwarancji przysługujących użytkownikom w korzystaniu z usług w chmurze, związane z rozszerzeniem zakresu stosowania prawa UE, zasługują na aprobatę, trudno jednak nie zauważyć, że ich praktyczna skuteczność wydaje się znacznie ograniczona. Stosowanie globalnych technik przetwarzania informacji bez uszczelkowania dla praw i gwarancji prynależnych użytkownikom wymaga, aby normy wprowadzające te prawa i gwarancje także miały zasięg globalny.

W powyższych rozważaniach przeanalizowano i potwierdzono prawdziwość wszystkich zdefiniowanych na wstępie hipotez badawczych. W szczególności już na obecnym etapie rozwoju rynku przetwarzania w chmurze można zaobserwować ujemne konsekwencje braku regulacji publiczno-prawnych wspólnych dla obu stron umowy i oparcia relacji użytkownik-usługodawca wyłącznie na rozwiązaniach kontraktowych, przybierających

---

760 Ibidem, s. 5.
761 Przykładowym produktem tego typu jest VMware Horizon, oferowany w nowym wariantie modelu chmury obliczeniowej – określonym terminem Desktop as a Service (DaaS) – por. omówienie pozostałych modeli w rozdziale 6.3.3. W modelu DaaS usługobiorca korzysta z określonej liczby wirtualnych stacji roboczych, uruchamianych na zasobach informatycznych usługodawcy zlokalizowanych w chmurze obliczeniowej.
762 Przykładem mogą być komputery Chromebook, działające pod kontrolą systemu operacyjnego Google Chrome OS. Chrome OS został zaprojektowany do wsparcia usług świadczonych w chmurze obliczeniowej w sposób, który nie wymaga instalowania lokalnych aplikacji ani przechowywania danych na komputerze użytkownika.
najczęściej postać umów adhezyjnych. Problem ten zyskuje na znaczeniu zwłaszcza w przypadku stosowania przez dostawcę usługi systemu prawnego państwa trzeciego.

Prawodawstwo Stanów Zjednoczonych z uwagi na odmienny od europejskiego model ochrony nie prowadzi do zapewnienia podstawowych praw i gwarancji osobistych na poziomie porównywalnych do wynikającego z prawa UE. Jest wątpliwe, czy problem ten może zostać skutecznie rozwiązany poprzez próbę narzucenia przedsiębiorcom amerykańskim stosowania prawa UE – zwłaszcza biorąc pod uwagę, że w przypadku usług świadczonych w chmurze rozwiązanie takie jest trudne w realizacji zarówno od strony technicznej, ale i prawnej. Dlatego należy poszukiwać innych rozwiązań – takich jak wypracowanie prawnie wiążącej umowy międzynarodowej UE – USA obejmującej wymianę danych w celach komercyjnych763, propagowania przystąpienia kluczowych partnerów UE na rynku usług cyfrowych do Konwencji RE 108 lub wypracowania nowego lub zreformowania istniejącego systemu ochrony praw podstawowych, który dostosowany zostanie do potrzeb i specyfiki cyberprzestrzeni.

763 Zob. uwagi krytyczne na temat programu Tarcza prywatności w rozdziale 4.5.3 (s. 164) oraz analiza umowy parasolowej UE – USA w rozdziale 4.6.3 (s. 205).
Rozdział 7. Analizy dużych zbiorów danych (Big Data)

7.1. Wprowadzenie

Rozwój Internetu, w szczególności możliwość zestawiania i łączenia (korelowania) informacji pochodzących z różnych zbiorów danych, doprowadziła do powstania nowego rynku usług, związanego z tworzeniem i zarządzaniem profilami użytkowników, a także opracowania zaawansowanych systemów informatycznych, pozwalających na przewidywanie trendów i odkrywanie faktów (data mining) w oparciu o informacje pochodzące z dużych baz danych.

Data mining, jako obszar zastosowania informatyki jest znany od wielu lat. Technikę tę można zdefiniować w skrócie jako pozyskiwanie nowej wiedzy z posiadanego wcześniej zbioru danych. Często środowiska tego typu wykorzystują zaawansowane algorytmy uczenia maszynowego (także sztucznej inteligencji) oraz bardzo duże zbiory danych. Celem jest lepsze wykorzystanie informacji, którą dany podmiot (najczęściej przedsiębiorca) już posiada – co w efekcie może przyczynić się do zmniejszenia kosztów działania lub zwiększenia zysków z oferowanych produktów lub usług. Upowszechnienie usług internetowych oraz pojawienie się nowego rynku usług i urządzeń mobilnych doprowadziły do globalizacji rynku zbiorów danych – coraz częściej przedmiotem obrotu stały się bazy danych, a możliwość ich agregowania i korelowania pozwalała na uzyskiwanie nowej, komercyjnie przydatnej informacji na temat badanych obszarów. W ten sposób powstał rynek określany dzisiaj jako Big Data (lub skrótowo – BD).

W literaturze nie wprowadzono jednej, powszechnie akceptowanej definicji pojęcia. P. Cohen określa Big Data jako technikę konwersji strumieni danych w precyzyjną wiedzę, cechującą się wysoką wartością poznawczą. Z kolei według I. Rubinstein Big Data to zaawansowana wersja data miningu, którą z kolei definiuje jako „nietrywialne wnioskowanie lub wydobywanie wcześniej nieznanych i przydatnych informacji ze zbioru danych”. Z kolei Grupa Robocza Art. 29 w swojej opinii podkreśla, że termin jest wykorzystywany do opisu różnych technik przetwarzania danych i odmiennych zastosowań, z których tylko część jest precyzyjnie zdefiniowana, podczas gdy inne nadal podlegają ewolucji, a niektóre dopiero

I. Rubinstein, Big Data: The End of Privacy or a New Beginning?, International Data Privacy Law 2013, t. 3, z. 2, s. 76.
mają zostać wprowadzone do użytku. B. van der Sloot i S. van Schendel w swojej pracy zebrali definicje Big Data funkcjonujące w różnych systemach prawnych na świecie.

Na potrzeby niniejszej pracy przyjęto, że Big Data to sposób prowadzenia procesów przetwarzania danych pochodzących z różnych źródeł i dotyczących różnych aspektów badanego problemu, w celu wyszukiwania trendów pozwalających na pozyskanie nowej wiedzy lub odkrycie nieoczywistych powiązań pomiędzy informacjami już posiadanymi. Często technologia BD utożsamiana jest wyłącznie z analizą danych – to błąd. Big Data to proces realizowany w czterech głównych etapach: (1) gromadzenie danych, (2) ich agregacja i korelacja, (3) analiza oraz (4) wykorzystanie wniosków. Każdy etap wiąże się z różnymi ryzykami w zakresie ochrony prywatności, dlatego sprowadzenie Big Data wyłącznie do etapu analizy skutkuje utratą z pola widzenia dużej części badanego problemu.

Analityka Big Data ta jest pomocna i skuteczna w analizowaniu dowolnych problemów badawczych. Szeroko omawianym w literaturze przykładem, gdzie analiza dużych zbiorów danych pomogła nie tylko odkryć istotną i wcześniej nieznaną wiedzę, ale w konsekwencji uratować setki, jeżeli nie tysiące, osób przed śmiercią lub poważnymi konsekwencjami zdrowotnymi, są badania dotyczące leku Vioxx. Analizy Big Data wykorzystywane są także do realizacji innych zadań o korzystnym wpływie na obszar zdrowia publicznego. Jako przykłady można podać analizy epidemiologiczne czy badania związané z korelacją wpływu szczepionek na możliwość wystąpienia innych schorzeń.

Big Data to także olbrzymi rynek profilowania użytkowników, przez co należy rozumieć tworzenie profili opisujących indywidualne cechy oraz schematy zachowań i preferencji, które mogą być wykorzystane do uzyskiwania nowej wiedzy lub prognozowania zdarzeń przyszłych. Systemy Big Data są powszechnie wykorzystywane w obszarze zdrowia publicznego.

---

766 Grupa Robocza Art. 29, Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, https://goo.gl/3ii8Au, s. 3.
769 Przeprowadzona przez szpital Kaiser Permanente analiza danych klinicznych i informacji na temat kosztów terapii Vioxx pozwoliła na powiązanie stosowania leku z 27 tys. przypadkami śmierci, jakie wystąpiły w latach 1999-2003 jako następstwo poważnych problemów z układem krążenia u pacjentów stosujących lek. Źródło: O. Tene, J. Polonetsky, Privacy in the Age of Big Data: A Time for Big Decisions, Stanford Law Review Online 2013, t. 64, s. 64.
bezpieczeństwa narodowego jako podstawowa technika służąca ujawnianiu powiązań i relacji pomiędzy osobami znajdującymi się w zainteresowaniu uprawnionych organów oraz typowaniu zdarzeń i osób, które mogą być podejrzewane o popełnienie najpoważniejszych przestępstw. Systemy te tym zatem różnią się od standardowych technik inwigilacji (opartych na przykład na rejestracji informacji i ich dalszej analizie), że celem nie jest zbieranie dowodów potwierdzających, że dana osoba jest zaangażowania w określone działania przestępcze, ale wskazywanie, które osoby z dużej badanej próby (w skrajnym przypadku – całego społeczeństwa) w takie działania mogą być zaangażowane. Przykład ten obrazuje jedną z najważniejszych cech systemów Big Data – budowanie na podstawie dużego zbioru z pozoru nieistotnych i niepowiązanych informacji wiedzy i wniosków o kluczowym znaczeniu z punktu widzenia obszaru badawczego.

W ten sam sposób systemy Big Data są wykorzystywane w zakresie profilowania użytkowników Internetu. Pozwalają w oparciu o korelację bardzo wielu, rozproszonych informacji dostarczyć konkretną wiedzę, wykraczającą poza dane znajdujące się wprost w analizowanym zbiorze\(^771\). W obszarze profilowania użytkowników systemy Big Data są najczęściej wykorzystywane do reklamy behawioralnej, a więc dostarczania użytkownikowi reklamy dedykowanej, odzwierciedlającej jego zainteresowania, potrzeby i przekonania. Analogicznie – korzystając z tych samych algorytmów i bazy wiedzy – można badać preferencje wyborcze (określić, na kogo zagłosują badane osoby), wnioskować na temat stanu zdrowia czy preferencji seksualnych – i to wyłącznie w oparciu o dane, które na temat tych osób są dostępne w publicznych źródłach internetowych. W rezultacie stosowanie technik Big Data skutkuje zatarciem różnicy pomiędzy zwykłymi danymi osobowymi a danymi

---

\(^771\) Przykładem takiego działania może być opublikowana w lipcu 2017 analiza uczestników Open’er Festival – z której wynika, że 82% osób to klienci sklepów sieci Lidl czy Biedronka, 28% osób było ostatnie 6 miesięcy za granicą, a 32% to osoby dbające o zdrowie. Są to informacje dotyczące życia prywatnego, jednak nie prowadzą one do ujawnienia danych wrażliwych. Jednak już informacja o tym, że 11% uczestników należy do mniejszości seksualnych, a 14% to kobiety starające się o dziecko, może świadczyć, że firma przetwarza dane szczególnie chronione. Tym bardziej podkreśla wymaga fakt, że powyższe analizy nie są efektem świadomego udostępnienia przez użytkowników wrażliwych informacji na swój temat, tylko zainstalowania konkretnej aplikacji na telefonie komórkowym i zezwolenia na udostępnianie jej listy wszystkich zainstalowanych przez użytkownika aplikacji oraz geolokalizacji telefonu. W ten sposób, analizując i koraelując listę zainstalowanych przez użytkownika aplikacji z informacją na temat zmiany lokalizacji telefonu w czasie oraz z informacjami pochodzącymi od innych użytkowników, a także bazą danych przedsiębiorcy, firma Selectivv – twórcą badania – mogła określić cechy indywidualne osób, takie jak przynależność seksualna (zainstalowanie programów popularnych wśród mniejszości seksualnych), chęć posiadania dziecka (zainstalowanie aplikacji takich jak PeriodTracker czy WomanLog), ale i fakt odwiedzania konkretnych miejsc (w tym wypadku – sklepów sieci Biedronka czy Lidl). O ile omawiane wyniki bazują na danych zagregowanych, to przedsiębiorca, dysponując danymi źródłowymi, posiada możliwość konkretnego wskazania, które osoby należą do każdej ze wskazanych grup użytkowników. Wyniki i opis metodyki badawczej: http://selectivv.com/opener-festival-2017-uczestnicy-smartfonow-liczba-infografika/.
wrażliwymi – pozwala bowiem na podstawie analizy tych pierwszych dostarczać wiedzy na temat tych drugich. W podobny sposób analiza Big Data może być skuteczną techniką identyfikacji podmiotów danych w zbiorze wcześniej zanonimizowanym. Oznacza to, że korelując wystarczająco dużo informacji na temat zbioru użytkowników, można przeprowadzić ich ponowną identyfikację. Należy zatem postawić pytanie o zasadność stosowania anonimizacji i pseudonimizacji jako podstawowych technik służących ochronie zbiorów danych osobowych. Podobne wątpliwości dotyczą zasadności i celowości dalszego stosowania zgody podmiotu danych jako niezbędnego (i często – wystarczającego) warunku do przetwarzania danych. Skoro Big Data pozwala wydobyć nową wiedzę ze zbioru przetwarzanych informacji, może okazać się, że podmiot danych, zezwalając na przetwarzanie ogólnych informacji na swój temat, pośrednio doprowadził też do ujawnienia danych wrażliwych na swój temat. Co więcej, wyjaśnienia wymaga także zakres udzielonej zgody do wiedzy pozyskanej z technik Big Data – w szczególności, czy nowo wydobyte informacje będące efektem działania algorytmów są objęte zakresem udzielonej przez użytkownika zgody, a jeżeli nie – to jaka jest podstawa przetwarzania tych informacji. Czy w odniesieniu do automatycznego procesu wnioskowania można mówić o nowych informacjach? I w jaki sposób odnieść do tych „informacji” (wniosków) prawa podmiotów danych (np. prawo do usunięcia danych)?

Big Data obecnie to już nie tylko technika wspomagająca prowadzenie działalności gospodarczej, tworzenie profili i obrót nimi stało się oddzielną gałęzią gospodarki. Przedsiębiorcy, określani jako „brokerzy danych”, prowadzą działalność, której głównym celem jest tworzenie i komercyjne udostępnianie profili użytkowników. Dla przykładu firma Acxiom Corporation zarządza profilami ponad 500 milionów osób, przy czym każdy z nich jest przeciwnie opisany przez około 1500 punktów danych772. Wyniki finansowe publikowane przez Acxiom wskazują, że na swojej działalności firma uzyskała w 2011 roku ponad 1 mld USD przychodu i 77 mln USD zysku. Wartości te odzwierciedlają wymiar finansowy danych gromadzonych i przetwarzanych tylko przez jeden podmiot działający na rynku Big Data. Jednocześnie wskazują na znaczenie, jakie precyzyjne dane na temat użytkowników mają dla przedsiębiorców. Przykład Acxiom każe także zastanowić się nad skutecznością prawnym mechanizmów kontrolujących gromadzenie i przekazywanie informacji do dalszego przetwarzania. Jest też przesłanką wskazującą na konieczność

przeprowadzenia dyskusji w zakresie ryzyka związanego ze sprowadzeniem cyfrowego opisu podmiotów danych do roli przedmiotów obrotu gospodarczego.


7.2. *Hipotezy badawcze*

Przenosząc powyższe wstępne rozważania dotyczące charakteru analiz Big Data, należy zdefiniować wstępne hipotezy badawcze, które będą pomocne w dalszym odniesieniu badanej problematyki do zagadnienia ochrony prywatności w cyberprzestrzeni:

1) Masowe przetwarzanie i korelowanie dużych zbiorów danych stanowi wyzwanie dla tradycyjnych regulacji prawnych dotyczących ochrony prywatności – prowadzi bowiem do ograniczenia ich skuteczności oraz efektywności, zwłaszcza w obszarze praw podmiotów danych.

2) Budowanie świadomości użytkowników oraz oparcie przetwarzania na świadomej zgodzie to niewystarczające rozwiązania w zakresie kontrolowania udostępniania informacji osobowych.

3) Dynamiczny wzrost rynku Big Data wymaga wprowadzenia nowych regulacji o charakterze publicznoprawnym dotyczących wprost stosowania technik profilowania użytkowników, tak aby uniemożliwić nieorganiczny obrót szczegółowymi informacjami na temat całej populacji.

4) Z uwagi na globalny charakter sieci Internet także zagadnienie ustanowienia prawnych norm regulujących stosowanie technik Big Data musi być traktowane jako zagadnienie o zasięgu globalnym.

7.3. Charakterystyka zjawiska

7.3.1. Najważniejsze cechy Big Data

Analizy oparte na dużych zbiorach danych pomimo wielu podobieństw do badań statystycznych przez większość badaczy uznawane są obecnie za posiadające ograniczoną przydatność jako podstawowe narzędzie badań naukowych. Pogląd ten nie zawsze był jednak dominujący.774

Badacze z rolnych dziedzin nauki wyrażali przekonanie, że gromadząc wystarczająco duży zbiór danych i zestawiając go z innymi informacjami, można po pierwsze zapewnić wiarygodność próby (przeprowadzić walidację danych) a po drugie na tak otrzymanym zestawieniu budować nietrywialne wnioski. Siłą Big Data miała więc być masowość przetwarzania. Aby zrozumieć, dlaczego przekonanie to było błędne i jakie są konsekwencje ograniczeń Big Data dla ochrony prywatności, należy wpierw omówić kilka najważniejszych i – z punktu widzenia problemu badawczego niniejszej pracy – kluczowych cech charakteryzujących tą technologię. Należą do nich:

– nieznana jakość danych,
– masowy charakter przetwarzania,
– nieprzewidywalne wyniki analizy,
– efekt przyrostowy,
– automatyczne podejmowanie decyzji,
– brak pewności co do prawdziwości wniosków.

W pierwszej kolejności należy omówić problem danych źródłowych, a w szczególności jakości tych danych. W przypadku analiz komercyjnych istotnym źródłem informacji są wiadomości publikowane przez samych użytkowników w różnych serwisach społecznościowych775. Informacje te są aktualne, publiczne dostępne oraz prezentują interakcję pomiędzy użytkownikami. Mogą zatem służyć do badania trendów oraz profilowania samych użytkowników. Błędem byłoby jednak zrównanie opinii, nawet powszechnie prezentowanej w Internecie, z obiektywną prawdą. Co więcej, nawet bardzo


775 Zob. także rozdział 7.3.2, s. 300.
duży zbiór danych, zawierający setki milionów rekordów, może nie spełniać kryteriów losowości i reprezentatywności. Duże zbiory danych tworzone na podstawie informacji zgromadzonych w Internecie są obarczone także różnymi typami błędów. Wynika to z faktu, że zbiory te najczęściej nie są moderowane i weryfikowane semantycznie, znaczeniowo czy składniowo. W efekcie konieczne jest stosowanie przed przystąpieniem do analizy mechanizmów poprawienia jakości danych (nazywanych oczyszczaniem danych, ang. data cleaning). Proces ten, co należy podkreślić, realizowany jest nie w pełni automatycznie – bowiem w oparciu o manualną weryfikację skuteczności zastosowanych algorytmów oraz ręczne usuwanie danych niewiarygodnych. Jest to o tyle istotne, że skoro dane, na których bazuje Big Data są weryfikowane i oceniane w sposób subiektywny, to wyniki analizy tych danych nie mogą zostać uznane za w pełni obiektywne. To ważna obserwacja, której znaczenie zostanie zobrazowane w dalszej części rozważań

Proces łączenia poszczególnych zbiorów danych także jest podatny na wystąpienie różnych rodzajów błędów. W efekcie nawet jeżeli takie zbiory łączy, aby uzyskać pełniejszy obraz badanego problemu, to w ten sposób nie można wyeliminować niepewności związanej z jakością poszczególnych zbiorów danych. Wprost przeciwnie, jak zauważali D. Boyd i K. Crawford, łączenie danych prowadzi do zwielokrotnienia błędów i przeinaczeń obecnych w zbiorach źródłowych.

Oddzielną kwestią związaną z jakością danych stanowiących źródło dla analiz Big Data jest znaczenie kontekstu dla prawidłowości przetwarzania. M. Mattioli podsumował ten problem, wskazując, że „dane pozbawione kontekstu mogą być także pozbawione sensu”777. W przypadku agregowania zbiorów pochodzących od zewnętrznych dostawców operator systemu Big Data może nie być świadomy kontekstu (okoliczności), w jakim dane zostały gromadzone, w efekcie nawet analiza prawidłowych danych może doprowadzić do błędnych wniosków. Co więcej, zbiory poddane procesowi poprawienia jakości przestają wiernie odzwierciedlać dane źródłowe i stanowią zaledwie ich subiektywną interpretację. Jeżeli są później przekazywane do kolejnych podmiotów, które przeprowadzają dalsze procedury agregacji, korelacji i oczyszczania danych, to w efekcie po kilku tego typu iteracjach pierwotny zbiór danych może znacząco odbiegać od jego ostatecznej formy. Konsekwencją

776 W niektórych zastosowaniach – na przykład związanych z typowaniem transakcji podejrzanych i wykrywaniem nadużyć finansowych – dane nie są poddawane oczyszczaniu. W takim wypadku nawet jeżeli dane źródłowe zawierają błędy, w takiej postaci są dalej przetwarzane. Ma to zasadnicze znaczenie dla celu przetwarzania, a więc typowania podejrzanych transakcji (np. wpisanie we wniosku kredytowym danych osoby zmarłej lub wpisanie numeru dokumentu tożsamości innej osoby, pozwala na sygnalizowanie możliwych nieprawidłowości).

jest także brak możliwości ustalenia źródła pochodzenia pierwotnych (nieprzetworzonych) danych\textsuperscript{778}.

Należy przypomnieć, że zapewnienie odpowiedniej jakości danych było już we wczesnych regulacjach prawnych wskazywane jako jeden z podstawowych obowiązków podmiotu przetwarzającego. Celem było zapewnienie, że decyzje podejmowane w oparciu o wnioski nie będą błędne, a w efekcie krzywdośną dla osoby, której dane są przetwarzane.

Powstaje zatem pytanie, czy błędy w dużych zbiorach danych – które są inherentnie związane z Big Data – mogą być skutecznie zredukowane albo wyeliminowane na etapie dalszego przetwarzania, w szczególności działania zaawansowanych algorytmów analitycznych. Cechą wspólną algorytmów działających na dużych zbiorach danych jest konieczność ich samoadaptacji i uczenia maszynowego. Oznacza to, że algorytmy te potrafiają w pewnym zakresie samodzielnie poszukiwać nowych wzorców i trendów, które nie były oryginalnie przewidziane przez programistów. Są to zatem rozwiązania posiadające cechy algorytmów heurystycznych i jak wszystkie heurystyki są niepewne i częściowo nieprzewidywalne w zakresie rezultatów działania.

W praktyce zatem algorytmy analityczne zwiększają, a nie zmniejszają niepewność w zakresie dokładności i wiarygodności wyników badań. Nieprawdziwy jest także pogląd, że wykorzystanie Big Data w zakresie badania trendów, a nie przypadków jednostkowych nie jest opisane powyższymi wadami – jeżeli algorytm nie jest w stanie prawidłowo ocenić sytuacji jednostkowej, to występujący błąd zostanie tylko zmiłokrotniony w badaniach masowych.

Cechą charakterystyczną analiz Big Data jest ukazywanie nieoczywistych trendów i zależności, które mogą budować wiedzę na temat zdarzeń przyszłych. W literaturze przedmiotu właściwość ta jest określana terminem analizy predykcyjnej (ang. predictive analysis) i ma fundamentalne znaczenie praktyczne, zwłaszcza w zastosowaniach związanych z obszarem przeciwdziałania przestępczości i bezpieczeństwa narodowego. Analiza predykcyjna ma jednak także cechy samospelniącej się teorii – wyniki badania, odpowiednio udokumentowane metodologicznie mogą skłonić jej odbiorców do podjęcia działań, które bezpośrednio lub pośrednio przyczynią się do realizacji przewidzianych

zdarzeń⁷⁷⁹. Niektórzy wskazują, że samo wykonywanie analiz na dużych zbiorach danych może prowadzić do de facto dowolnych wniosków, zależnych od oczekiwań badającego⁷⁸⁰.


Rozważania te prowadzą zatem do wniosku, że osoba chcącą zachować anonimowość w Internecie nie powinna publikować żadnych informacji w serwisach społecznościowych, nawet korzystając z pseudonimu. Efekt przyrostowy jest bezpośrednio związany z możliwością ponownej identyfikacji osób w zbiorze anonimizowanym, problemem szerzej przedstawionym w rozdziale 7.3.3.

Co do zasady głównym celem stosowania analityki Big Data jest wykorzystanie uzyskanych wniosków do podejmowania decyzji. Mogą one mieć różny charakter, począwszy od generalizacji, aż po specyficzne rozwiązania w konkretnych sytuacjach.


od decyzji całkowicie automatycznych (np. wzrost składki ubezpieczeniowej, odmowa zawarcia polisy na życie itp.) do mającej charakter tylko rekomendacji (np. proces rekrutacji czy decyzji w sprawie prawa pobytu w państwie trzecim). W dużej części przeprowadzane analizy nie są ukierunkowane na podejmowanie decyzji jednostkowych, a dotyczących badanych trendów (np. kampanie reklamowe). W każdym przypadku należy pamiętać, że zastosowanie rozwiązań automatycznych (w szczególności algorytmów sztucznej inteligencji) może skutkować wprowadzeniem mechanizmów nieuprawnionej dyskryminacji (określonej niekiedy eufemistycznie w terminologii technicznej jako „klasyfikacja”) czy ograniczaniem swobody podejmowania decyzji.

Podsumowując, Big Data nie prowadzi do pozyskania wiedzy absolutnej – zarówno w aspekcie rozległości, ale i szczegółowości wnioskowania. To technika, która może być – i często jest – pomocna w rozwiązywaniu złożonych problemów, wymagających wieloaspektowych i rozproszonych badań. Z uwagi na swój potencjał może przynieść fenomenalne wyniki (jak w przypadku opisanego we wstępie badania dotyczącego skutków ubocznych leku Vioxx), ale i dramatyczne konsekwencje (jak w przypadku badań ukierunkowanych na przewidywanie prób samobójczych). Big Data jest techniką, która w oparciu o ogrom informacji dostępnych w Internecie pozwala wkrócić w sferę życia prywatnego jednostek w różny sposób i z różną siłą.

7.3.2. Podstawowe źródła danych

Rozpatrując konsekwencje przetwarzania Big Data dla ochrony prywatności, należy ogólnie scharakteryzować najważniejsze źródła danych, stanowiące podstawę przeprowadzanych analiz. Wśród nich znajdują się:

- portale społecznościowe i treści dobrowolnie publikowane przez użytkowników,
- aktywności online, zwłaszcza związane z przeglądaniem stron stron internetowych,
- treści o charakterze niepublicznym,
- informacje udostępniane przez aplikacje zainstalowane na urządzeniach mobilnych,

782 Przykładem takiej nieuprawnionej dyskryminacji byłoby wykorzystane opisanej wcześniej technologii Selectivw w procesie selekcji kandydatów przedstawianych przez biuro zajmujące się pośrednictwem na rynku pracy docelowemu przedsiębiorcy; w zależności od preferencji przedsiębiorcy, z listy osób spełniających kryteria merytoryczne mogliby zostać usunięci rodzice małych dzieci, kobiety starające się o dziecko czy przedstawiciele mniejszości seksualnych itp.
– oficjalne rejestry i publikatory,
– źródła offline,
– powiązane treści i aktywności innych użytkowników.

Pierwsza kategoria – związana z analizą treści publikowanych dobrowolnie przez użytkowników – pozornie nie powinna budzić wątpliwości związanych z ochroną prywatności. Przykładem takiego serwisu może być usługa Twitter, za pośrednictwem której każdego dnia zamieszczanych jest około 500 mln nowych wpisów. Twitter jest modelowym przykładem wartościowego źródła danych dla analiz Big Data: (1) jest narzędziem powszechnym (używany jest na całym świecie), (2) zarówno w celach prywatnych, jak i zawodowych, (3) zawiera aktualne informacje (opinie) publikowane przez użytkowników oraz (4) pozwala prześledzić interakcję pomiędzy użytkownikami a całymi grupami użytkowników (np. społecznościami). Dane z serwisu Twitter są podstawowym źródłem świadczenia usług przez wielu brokerów danych, którzy na podstawie wpisów użytkowników – odpowiednio skatalogowanych (opisanych kategoriami, tzw. metadanymi) – tworzą strumień danych, który następnie jest przesyłany do klientów (dostawców analityki Big Data) lub jest poddawany agregacji z innymi zbiorami danych. Usługi takie świadczy na przykład firma DataSift, która każdego dnia poddaje analizie nie tylko wiadomości z serwisu Twitter, ale i innych portali społecznościowych (jak LinkedIn, Facebook czy Instagram) oraz serwisów online (np. blogów czy komentarzy w popularnych portalach internetowych)783.

Do drugiej kategorii źródeł danych dla Big Data należą aktywności użytkowników w Internecie, związane z codziennym korzystaniem z wyszukiwarki internetowej, przeglądaniem publikowanych treści i interakcją z innymi użytkownikami. Te kategorie informacji zazwyczaj nie mają charakteru publicznego. Sposób interakcji użytkownika z wyszukiwarką określają warunki korzystania z usługi udostępnione przez jej operatora. Podobnie zakres wykorzystania danych gromadzonych w wyniku interakcji użytkownika z dostawcami treści (portale internetowe, sklepy, fora dyskusyjne) powinny być określone w opublikowanej polityce prywatności. Dlatego dla wskazania, czy informacje pozyskane z tych źródeł mogą być gromadzone i agregowane, w analityce Big Data rozstrzygające znaczenie mają warunki, na jakich użytkownik korzysta z określonych usług. Dla przykładu firma Google szczegółowo wskazuje zakres gromadzonych danych – obejmują one zarówno informacje podane przez użytkownika, jak i uzyskane od niego podczas korzystania z usług (w tym wyszukiwane hasła, informacje o lokalizacji, informacje o wykorzystywanych

783 Opis platform Stream oferowanej przez DataSift: http://cli.re/gkZm1j.
urządzeniach czy unikalne numery aplikacji). Firma Google wskazuje także na możliwość agregowania tych informacji784.

Z kolei cel przetwarzania tak połączonego zbioru został określony następująco: „Dane zbierane za pośrednictwem wszystkich naszych usług służą do udostępniania, utrzymywania, ochrony i udoskonalania ich w celu tworzenia nowych usług, a także ochrony firmy Google i jej użytkowników. Wykorzystujemy je również, oferując dostosowane treści – np. w postaci trafniejszych wyników wyszukiwania oraz reklam785. Szeroki zakres możliwej wykorzystania danych oraz użycie ogólnych sformułowań (udoskonalanie istniejących oraz tworzenie nowych usług) powodują, że użytkownik nie dysponuje faktyczną wiedzą ani kontrolą nad dopuszczalnym zakresem przetwarzania. W praktyce więc także informacje niemające charakteru publicznych i gromadzone przez usługodawców internetowych mogą z łatwością być wykorzystane przez nich na potrzeby stosowania analityki Big Data.

Do kolejnej grupy danych wykorzystywanych w profilowaniu Big Data zaliczyć można dane pochodzące z urządzeń mobilnych. W ocenie samych brokerów danych jest to obecnie jedno z bardziej perspektywicznych źródeł informacji o aktywności użytkowników – głównie z uwagi na możliwość gromadzenia różnych danych, niedostępnych w inny sposób. Przykładem mogą być informacje o lokalizacji – pozwalające sprawdzić na przykład, jakie punkty handlowe czy stacje benzynowe odwiedza użytkownik, lub analizować jego preferencje w zakresie różnych innych kategorii decyzji konsumenckich. W szerszym ujęciu dane o lokalizacji pozwalają na odtworzenie schematycznego planu dnia, obrazującego typowe aktywności i formy spędzania czasu. Korzystanie z danych mobilnych ma jeszcze tę jedną zaletę, że o ile użytkownicy coraz częściej są świadomi kontroliowania informacji, które publikują w Internecie (na przykład na serwisach społecznościowych), to nadal często nie rozumieją znaczenia zgód udzielanych poszczególnym aplikacjom które instalują na swoich telefonach i wpływu podejmowanych w ten sposób decyzji na możliwą ingerencję w prywatność.

Nie bez znaczenia dla rynku Big Data są także treści publikowane w oficjalnych rejestrach i publikatorach. Hurtowy dostęp do danych np. członków władz czy organów nadzoru spółek handlowych i to w wielu krajach pozwala również uzupełniać wiedzę na temat jednostek oraz ich wzajemnych relacji i powiązań. Także informacje publikowane w oficjalnych ogłoszeniach (np. licytacje komornicze) mogą w prosty sposób przyczynić się do

785 Ibidem, sekcja: Sposoby wykorzystania zgromadzonych informacji.
stworzenia powiązania w bazie danych pomiędzy profilem opisującym konkretną osobę oraz wskazaną w ogłoszeniu lokalizacją, w której znajduje się licytowany majątek. Dlatego sposób kontroliowania i retencji danych zamieszczonych w rejestrach publicznych także powinien uwzględniać ryzyka związane z wykorzystaniem tych danych w globalnym rynku Big Data.

Do ostatniego z omawianych źródeł informacji dla systemów analizy dużych zbiorów danych należą informacje i powiązania publikowane przez innych użytkowników. Jak wskazano wcześniej, brokerzy danych jak DataSift koncentrują się na budowaniu bazy wiedzy zawierającej nie tylko treści publikowane przez użytkowników, ale także relacje i powiązania, na które treści te wskazują. W efekcie na podstawie informacji wyodrębnionych z wpisów opublikowanych przez innych możliwe jest tworzenie profilu osoby, która w ogóle nie korzysta z mediów społecznościowych. Czasami informacje te są bardzo szczegółowe i dokładne (wraz ze zdjęciem, datą urodzenia, informacjami na temat najbliższej rodziny, miejscem zamieszkania itp.). Przykładem takiego źródła może być serwis MyHeritage, który stanowi internetową platformę oferującą narzędzia do budowy i zarządzania drzewem genealogicznym. Użytkownicy portalu publikują na tworzonych schematach informacje na temat swojej rodziny i dalszych krewnych, często ujawniając wszystkie znane im daty i fakty z życia opisywanych osób. Przykład ten wskazuje, że portale społecznościowe mogą być źródłem szczegółowych informacji także o osobach, które z nich nie korzystają.

Federalna Komisja Handlu rozpoczęła w 2012 roku szczegółowe badanie rynku brokerów danych, w ramach którego przeprowadzono analizę zakresu informacji gromadzonych przez dziewięć reprezentatywnych podmiotów tego rynku działających w Stanach Zjednoczonych. W zaprezentowanym w maju 2014 raporcie podsumowującym badanie FTC zaprezentowała narzędzia i techniki wykorzystywane przez przedsiębiorców do gromadzenia danych, w tym obrazujące źródła danych, oraz procesy związane z oczyszczaniem, korelacją i agregacją danych z różnych strumieni. Raport FTC pozwala zobrazować, jak dalece segment profilowania wkracza w sferę prywatności milionów osób. W tabeli 2 przedstawiono wybrane informacje, jakie są gromadzone przez brokerów danych. Nie jest to lista wyczerpująca, ale daje obraz o szczegółowości pozyskiwanych informacji.

Federalna Komisja Handlu rozpoczęła w 2012 roku szczegółowe badanie rynku brokerów danych, w ramach którego przeprowadzono analizę zakresu informacji gromadzonych przez dziewięć reprezentatywnych podmiotów tego rynku działających w Stanach Zjednoczonych. W zaprezentowanym w maju 2014 raporcie podsumowującym badanie FTC zaprezentowała narzędzia i techniki wykorzystywane przez przedsiębiorców do gromadzenia danych, w tym obrazujące źródła danych, oraz procesy związane z oczyszczaniem, korelacją i agregacją danych z różnych strumieni. Raport FTC pozwala zobrazować, jak dalece segment profilowania wkracza w sferę prywatności milionów osób. W tabeli 2 przedstawiono wybrane informacje, jakie są gromadzone przez brokerów danych. Nie jest to lista wyczerpująca, ale daje obraz o szczegółowości pozyskiwanych informacji.

Wskazuje także, jak duża część informacji nie jest pozyskiwana bezpośrednio od podmiotów danych, ale od innych brokerów oraz z rejestrów publicznych.

---

786 Badaniem objęto przedsiębiorstwa: Axiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf i Recorded Future.
Tabela 2. Przykładowa lista informacji gromadzonych przez brokerów danych\(^{788}\)

<table>
<thead>
<tr>
<th><strong>Dane identyfikujące</strong></th>
<th><strong>Rejestry publiczne</strong></th>
<th><strong>Media społecznościowe</strong></th>
<th><strong>Informacje na temat miejsca zamieszkania i sąsiedztwa</strong></th>
<th><strong>Informacje o środkach transportu</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>– imię i nazwisko</td>
<td>– informacja o ogłoszonych</td>
<td>– posiadane łącza internetowe,</td>
<td>– dokładny adres,</td>
<td>– szczegółowe dane o posiadanych</td>
</tr>
<tr>
<td>– wcześniej używane nazwiska</td>
<td>– postępowaniach upadłościowych,</td>
<td>– dostawca usług internetowych,</td>
<td>– data budowy,</td>
<td>środках transportu,</td>
</tr>
<tr>
<td>– adres wraz z historią wcześniejszych adresów,</td>
<td>– informacja o postawionych zarzutach karnych i skazaniach,</td>
<td>– posiadany system operacyjny,</td>
<td>– podstawa posiadania,</td>
<td></td>
</tr>
<tr>
<td>– dane kontaktowe (numery telefonów, adresy e-mail)</td>
<td>– informacje o posiadanych uprawnieniach.</td>
<td>– rodzaj publikowanych treści,</td>
<td>– wartość rynkowa nieruchomości,</td>
<td></td>
</tr>
<tr>
<td><strong>Wrażliwe dane identyfikujące</strong></td>
<td><strong>Media społecznościowe</strong></td>
<td>– publikowane zdjęcia,</td>
<td>– cena zakupu,</td>
<td></td>
</tr>
<tr>
<td>– numer ubezpieczenia społecznego,</td>
<td>– wykorzystywane urządzenia mobilne,</td>
<td>– wysokość czynszu najmu,</td>
<td>– wysokość nieruchomości,</td>
<td></td>
</tr>
<tr>
<td>– numer prawa jazdy,</td>
<td>– informacje udostępnione w serwisach:</td>
<td>– udzielony kredyt i oprocentowanie,</td>
<td>– wielkość nieruchomości,</td>
<td></td>
</tr>
<tr>
<td>– data urodzenia,</td>
<td>– Digg, Facebook, Flickr, Flixster,</td>
<td>– wielkość nieruchomości, w tym liczba</td>
<td>– informacje dodatkowe - posiadanie garażu, basenu, kominka,</td>
<td></td>
</tr>
<tr>
<td>– daty urodzenia członków rodziny (także dzieci).</td>
<td>– Friendster, hi5, Hotmail, LinkedIn, Live Journal, MySpace, Twitter, Amazon, Bebo, CafeMom, DailyMotion, Match, myYearbook.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dane demograficzne</strong></td>
<td><strong>Informacje ogólne</strong></td>
<td><strong>Informacje ogólne:</strong></td>
<td>– informacja na temat sąsiedztwa (demograficzna, związana z przestępczością itp.).</td>
<td></td>
</tr>
<tr>
<td>– wiek, data, wzrost,</td>
<td>– udział w wydarzeniach sportowych,</td>
<td>– szczególne dane o posiadanych,</td>
<td>– czas pobytu,</td>
<td></td>
</tr>
<tr>
<td>– waga,</td>
<td>– udział w akcjach charytatywnych,</td>
<td></td>
<td>– informacja na temat sąsiedztwa</td>
<td></td>
</tr>
<tr>
<td>– rasa i pochodzenie etniczne,</td>
<td>– hazard – kasyna,</td>
<td></td>
<td>(demograficzna, związana z przestępczością itp.).</td>
<td></td>
</tr>
<tr>
<td>– kraj pochodzenia,</td>
<td>– hazard – loterie stanowe,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– religia,</td>
<td>– informacja o p预案rowanych czasopismach,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– używane języki,</td>
<td>– posiadane zwierzęta,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– status małżeński,</td>
<td><strong>Informacje o środkach transportu</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– posiadanie rodziców w podeszłym wieku,</td>
<td>– szczegółowe dane o posiadanych,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– posiadane dzieci,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– wykształcenie,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– zawód wraz z miejscem zatrudnienia,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>poszczególnych członków rodziny i informacją o pracy zdalnej,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– relacje rodzinne,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– liczba osób w gospodarstwie domowym,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– dodatkowe informacje: samotny rodzie,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– weteran.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

– preferowane gatunki muzyki i filmów,
– oglądane kanały telewizyjne.

Dane finansowe:
– parametry posiadanych kart płatniczych,
– informacja o posiadanych kartach kredytowych, z wyszczególnieniem kart złotych lub platynowych,
– zdolność kredytowa,
– posiadane kredyty hipoteczne,
– posiadane akcje i obligacje,
– posiadanie kredytów gotówkowych w instytucjach finansowych lub pożyczkowych,
– zakupy ratalne,
– liczba posiadanych nieruchomości w celach inwestycyjnych,
– oczekiwany roczny dochód,
– informacja o polisach na życie,
– łączna wartość majątku,
– informacje o zwrotach podatków.

Informacje o stanie zdrowia:
– zdiagnozowane alergie,
– informacja o paleniu papierosów
– kupowanie leków online lub na odległość,
– posiadane ubezpieczenia medyczne
– używane szkła korekcyjne lub soczewki kontaktowe,
– historia zakupów związanych ze stanem zdrowia z podziałem na poszczególne rodzaje schorzeń.

– preferowane marki,
– informacje o ubezpieczeniu,
– data i cena nabycia,
– bieżąca wartość.

Podróże i turystyka:
– czytane książki lub magazyny podróżnicze,
– data ostatniego wyjazdu,
– preferowana linia lotnicza,
– preferowany cel podróży,
– preferowany rodzaj wyjazdów wakacyjnych.

Dane dotyczące zakupów:
– kwota wydawana na konsumpcję,
– wykorzystywane formy płatności,
– preferowane kanały zakupów,
– szczegółowe informacje o zakupach online o wartości większej niż 500 USD oraz offline o wartości większej niż 1000 USD,
– najczęściej kupowane dobra konsumpcyjne,
– wydatki na żywność,
– wydatki na rozrywkę,
– ostatnia data zakupu online/offline.
7.3.3. Ponowna identyfikacja podmiotów danych

Obowiązek stosowania przepisów o ochronie danych powszechnie wiązany jest z przetwarzaniem danych osobowych. Zatem podmiot, który nie przetwarza zbiorów spełniających definicję uznania ich za dane osobowe, nie musi stosować wskazanych przepisów, ponieważ tego typu czynności przetwarzania nie są objęte zakresem materialnym ich stosowania. Techniką pozwalającą na konwersję zbioru danych osobowych do postaci niepozwalającej na identyfikację podmiotów danych jest anonimizacja. Polega ona na usunięciu ze zbioru źródłowego danych pozwalających na jednoznaczną identyfikację (np. nazwiska, identyfikatory PESEL) oraz przetworzeniu pozostałych danych (np. poprzez agregację, uogólnienie informacji) w sposób, który uniemożliwi przeprowadzenie ponownej identyfikacji. Anonimizacja jest więc techniką pozwalającą na dalsze przetwarzanie, sprzedaż i wykorzystanie komercyjne zbioru danych bez konieczności stosowania reżimu wymagań prawnych mających na celu ochronę danych osobowych (np. wymagania związane z międzynarodowym transferem, zapewnieniem praw podmiotu danych). Jest także naturalną formą przedstawiania danych na potrzeby badań statystycznych czy naukowych. Tę zaletę anonimizacji najpełniej przedstawiło w dyrektywie 95/46: „zasady ochrony danych nie mają zastosowania do danych, którym nadano anonimowy charakter w takim i sposób, że podmiot danych nie będzie mógł być zidentyfikowany”.

Wprowadzenie technik Big Data pozwoliło jednak na wykazanie, że większość stosowanych technik anonimizacji jest nieskuteczna, bowiem nawet przetworzone dane mogą być z powodzeniem wykorzystane do jednoznacznjej identyfikacji osób. Pierwsze badania w tym zakresie przedstawiła L. Sweeney w połowie lat dziewięćdziesiątych, prezentując, w jaki sposób zestawienie trzech informacji (kod pocztowy, data urodzenia i płeć) wystarczy do jednoznacnej identyfikacji 87% mieszkańców Stanów Zjednoczonych. W kolejnych ważnych badaniach, opublikowanych w 2006 roku, ukazano, jak można przeprowadzić ponowną identyfikację osób na podstawie opublikowanej i zanonimizowanej bazy 100.000 ocen filmów dokonanych przez 500.000 użytkowników serwisu Netflix. Z kolei w opublikowanym w styczniu 2015 roku badaniu przedstawiono wyniki związane z badaniem

Por. np. definicje wprowadzone w różnych aktach prawnych dotyczących obszaru ochrony danych osobowych, wskazujące na objęcie zakresem materialnym czynności przetwarzania danych o zidentyfikowanych lub możliwych do zidentyfikowania osób: dyrektywa 95/46 – art. 3 ust. 1, rozporządzenie 2016/679 – art. 2 ust. 1, polska ustawa o ochronie danych osobowych - art. 2, amerykańska ustawa HIPPA (zob. przypis 813).

Por. rozważania na temat anonimizacji i pseudonimizacji przedstawione w rozdziale 4.3, s. 133.

Zob. motyw 23 dyrektywy 95/46.

próbki 1,1 mln zanonimizowanych transakcji dokonanych kartami płatniczymi wskazujące na możliwość identyfikacji ok. 90% osób, które transakcje tych dokonały.\footnote{Y. de Montjoye, L. Radaelli, V. Singh, A. Pentland, \textit{Unique in the shopping mall: On the reidentifiability of credit card metadata}, Science 2015, t. 347, z. 6221, s. 536-539.} We wszystkich badaniach zastosowano podobną technikę, polegającą na wstępnej analizie dużego zbioru danych (badanie Netflix – 100 mln rekordów, badanie transakcji płatniczych – 1,1 mln płatności) i agregacji rekordów względem wyodrębnionych z danych (lub wprowadzonych) identyfikatorów. Mając wystarczająco dużą próbkę danych, istnieje statystycznie bardzo niewielkie prawdopodobieństwo, że utworzone w ten sposób profile nie będą unikalne, a więc będą odzwierciedlały zachowanie więcej niż jednej osoby. Dla przykładu: im więcej razy dana osoba występuje w próbie danych źródłowych (np. w odniesieniu do bazy Netflix – obejrzała i oceniła więcej filmów), tym jej zachowanie jest bardziej unikalne i niepowtarzalne wśród innych użytkowników. Mając tak przygotowane dane, wystarczy dokonać korelacji z inną bazą danych, aby uzyskać możliwość jednoznacznej identyfikacji użytkowników w danych źródłowych. Tą dodatkową bazą mogą być np. informacje z serwisów społecznościowych, forum dyskusyjnych lub bezpośrednia rozmowa z daną osobą.


Firmy profesjonalnie zajmujące się analizami Big Data bazują na wielu dużych i wzajemnie powiązanych zbiorach danych, w szczególności pochodzących z mediów społecznościowych. Technikę tę wykorzystali A. Narayanan i V. Shamatikov w badaniu...
polegającym na korelacjii danych z serwisów Twitter i Flickr. Każda z tych usług ma wiele milionów zarejestrowanych użytkowników. Zestawiając obie bazy i szukając trendów (w tym wypadku – powiązań pomiędzy znajomymi), byli w stanie z powodzeniem określić tożsamość osób posługujących się anonimowymi kontami w serwisie Twitter. W oparciu o swoje badania stwierdzili, że zapewnienie pełnej anonimizacji powoduje, że dane są nieprzydatne w dalszych analizach. Z drugiej strony, dane przydatne nigdy nie będą w pełni anonimowe.

Uwzględniając wyniki z powyższych badań, P. Ohm stwierdził, że „anonimizacja nie powinna być dłużej uznawana za technikę gwarantującą zachowanie prywatności”. Nie wszyscy zgadzają się z takim poglądem, zauważając, że podstawową przyczyną stojącą u źródła możliwości ponownej identyfikacji podmiotów danych jest nieprawidłowo przeprowadzony proces anonimizacji, który nie został poprzedzony wcześniejszą analizą ryzyka i oceną możliwości poddania zanonimizowanego zbioru dalszym operacjom przetwarzania.

7.3.4. Aspekty etyczne Big Data

Normy etyczne i prawne często wzajemnie się uzupełniają, stanowiąc łącznie podstawę dla funkcjonowania akceptowanych standardów społecznych. Każdy przypadek, w którym prawo pomija naganne zachowania etyczne, wymaga refleksji i analizy nie tylko w zakresie zasadności zmiany przepisów, ale również przyczyn, które sprawiły, że luka taka powstała. Często jako przyczynę można wskazać brak wystarczającej elastyczności norm prawnych połączony z dynamicznym rozwojem techniki. Także analityka Big Data należy do technologii, w przypadku której etyka na całym świecie sygnalizują brak lub istnienie niewystarczających norm prawnych regulujących zakres jej dopuszczalnego wykorzystania.

Przywołując zawarte w rozdziale 1 rozważania na temat znaczenia zapewnienia prywatności dla prawidłowego rozwoju osobowości oraz łącząc tę obserwację z powszechnym korzystaniem z cyberprzestrzeni, oczywiste wydaje się przeniesienie i zastosowanie do informacji przetwarzanych elektronicznie mechanizmów znanych w prawie

P. Ohm, Broken Promises of Privacy: Responding to The Surprising Failure of Anonymization, UCLA Law Review 2010, t. 57, s. 1743.

O. Tene, Privacy..., op. cit., s. 4.

P. Ohm, Broken Promises of Privacy..., op. cit., s. 1743.


Zob. np.: N. Richards, J. King, Big Data Ethics, Wake Forest Law Review 2014, t. 49, s. 393-432.

Zob. rozdział 1.1, s. 18.
od lat, a związanych ze ścisłym kontrolowaniem zarówno sposobów, jak i celów badań mających za przedmiot zachowania ludzi. Tworzenie rozbudowanych profili ma na celu wierne oddanie preferencji i zachowań konkretnych osób. Zrównanie cyfrowego opisu osoby z innymi towarami, które są przedmiotem obrotu, może mieć poważne konsekwencje także dla osób, których dane są przetwarzane. Należy pamiętać, że wnioski z Big Data budowane są na podstawie profili użytkowników, ale mogą mieć zastosowanie bezpośrednio do nich w przestrzeni fizycznej. K. Davis podsumował tę zależność, wskazując, że „potencjalna krzywda wyrządzona jako niezamierzona konsekwencja stosowania Big Data może szybko przeważać nad korzyściami, jakie innowacja ta dostarcza”801.

Kontrola obrotu i wykorzystywania profili nie może kończyć się z momentem przekazania informacji przez użytkownika do firm zajmujących się świadczeniem usług profilowania. Nawet zakładając konieczność wyrażenia świadomej zgody przez użytkownika802, należy wskazać, że rolą rozsądnego prawodawcy jest ustanowienie takich norm publiczнопrawnych, które uniemożliwią prowadzenie analiz Big Data o wątpliwych etycznie czy moralnie podstawach. Podsumowując powyższe obawy, N. Richards i J. King wskazali, że „jeżeli nie uda nam się zrównoważyć wartości na których nam zależy, takich jak prywatność, poufność, przejrzystość, zachowanie tożsamości czy wolność decydowania z rosnącymi potrzebami i zastosowaniami Big Data, ryzykujemy że społeczeństwo porzuci te wartości na rzecz innowacyjności i praktyczności”803.

Rynek brokerów danych powinien być zatem regulowany, tak samo jak regulowany jest rynek przedsiębiorców ubezpieczeniowych, banków czy instytucji świadczących usługi medyczne.

7.4. Analiza prawna

7.4.1. Najważniejsze ryzyka związane z Big Data

Podsumowując dotychczasowe rozważania: Big Data jako sposób gromadzenia i przetwarzania dużych zbiorów danych bezpośrednio wiąże się z poważnymi ryzykami dla prywatności osób, który dane są przetwarzane. Ryzyka te związane są z uwypukleniem słabości w fundamentalnych koncepcjach stanowiących fundament istniejących norm

801 K. Davis, D. Patterson, Ethics of Big Data: Balancing Risk and Innovation, O'Reilly Media 2012; cyt. za: N. Richards, J. King, Big Data Ethics, op. cit., s. 414.
802 Zob. definicję zgody w ogólnym rozporządzeniu o ochronie danych (art. 4 pkt 11).
803 N. Richards, J. King, Big Data Ethics, op. cit., s. 395.
prawnych związanych z przetwarzaniem danych osobowych. Do najważniejszych zagrożeń i obszarów wymagających pogłębionej analizy zaliczyć należy:

- odniesienie definicji terminu „dane osobowe” do analityki Big Data, jak i zasadności wyróżniania oddzielnego reżimu związanego z przetwarzaniem danych szczególnie wrażliwych;
- konsekwencje efektu przyrostowego zbiorów danych, w szczególności możliwości identyfikacji podmiotów danych w zbiorach wcześniej zanominizowanych;
- rozróżnienie pomiędzy faktami a przypuszczeniami w zakresie procesu budowania wiedzy także w obszarze konsekwencji dla decyzji podejmowanych automatycznie
- prawa podmiotu danych w odniesieniu do wiedzy powstałej w efekcie działania algorytmów Big Data, w szczególności możliwość żądania usunięcia danych oraz kontrolowania obiegu informacji.

7.4.2. **Dane ujawniające a Big Data**

Począwszy od pierwszych aktów prawnych związanych z rynkiem przetwarzania danych osobowych, kluczowym terminem wyznaczającym zakres materiałny stosowania nowych przepisów była definicja danych osobowych. W regulacjach wprowadzanych w latach siedemdziesiątych i osiemdziesiątych dwudziestego wieku dominującym poglądem było wskazywanie, że danymi osobowymi są informacje, które opisują osobę o ustalonej tożsamości lub pozwalają na jej identyfikację. W późniejszych przepisach i rekomentacjach przyjęto założenie, że możliwość identyfikacji osoby musi być oceniana przez pryzmat podmiotu przetwarzającego, a więc jego możliwości technicznych i organizacyjnych, które może zaangażować w proces określenia tożsamości podmiotów danych. W tym miejscu warto przypomnieć orzeczenie TSUE w sprawie *Breyer*, w którym sędzia uznał, że ta sama informacja (w badanej sprawie – adres IP użytkownika) może być uznana za dane osobowe, jeżeli jest przetwarzana przez podmiot publiczny mający zdolność (uprawnienia) do przeprowadzenia na jej podstawie identyfikacji użytkownika. W opisywanym przypadku podmiotem tym był niemiecka agencja bezpieczeństwa wewnętrznego. Wyrok TSUE potwierdził powszechnie akceptowany pogląd, że ocena, czy

---

804 Zob. analizę wczesnych rozwiązań prawnych w obszarze danych osobowych przedstawioną w rozdziale 3, s. 98.
805 Wyrok TSUE z 19.10.2016 w sprawie *Breyer*, sygn. C-582/14; zob. też rozdział 2.4.3, s. 77.
dany zbiór informacji zawiera dane osobowe, musi być dokonana w kontekście podmiotu przetwarzającego.


W podobny sposób działające wyłącznie w oparciu o zbiory informacji ogólnych (niezawierające danych szczególnie chronionych) algorytmy Big Data mogą wydobyć wiedzę o wrażliwych aspektach życia jednostek (np. informacje o stanie zdrowia, pochodzeniu rasowym, orientacji seksualnej). Także w tym wypadku powstaje problem związany ze sposobem klasyfikowania zbioru danych zawierającego wyniki działania algorytmów Big Data – w szczególności czy stanowią one oddzielny zbiór, który należy przetwarzać zgodnie z przepisami o ochronie danych? Co z kwestią jakości danych? Należy odróżnić fakty (informacje zweryfikowane, np. podane lub potwierdzone od użytkownika) od przypuszczeń (efekt działania heurystycznych algorytmów Big Data).

Kolejną trudność stanowi zmienne w czasie wyniki działania tej samej analizy. Jak wskazano we wcześniejszych rozważaniach, omawiając problem efektu przyrostowego, charakter i szczegółowość wniosków generowanych przez algorytmy Big Data zmieniają się
w czasie i zależą od jakości i wielkości danych źródłowych. Dane stale przyrastają, w efekcie zwiększając szczegółowość i precyzję wnioskowania.

Powyższy wniosek ma zastosowanie także w odniesieniu do ogólnego rozporządzenia o przetwarzaniu danych. Chociaż KE oraz instytucje UE w trakcie procedowania aktu były świadome zagrożeń związanych z rynkiem Big Data⁸⁰⁶, zdecydowano, aby zakres materialny stosowania nowej regulacji był nadal wyznaczony wyłącznie faktem przetwarzania danych osobowych. Innymi słowy, obowiązkiem stosowania regulacji mogą nie być objęte czynności gromadzenia i przetwarzania nawet dużych zbiorów danych, jeżeli w efekcie ich przetwarzania nie nastąpi identyfikacja podmiotu. Konsekwencją może być powstanie „szarej strefy” brokerów danych, którzy będą tworzyli i sprzedawali bardzo rozbudowane i wieloaspektowe zbiory danych przy czym sama czynność identyfikacji podmiotów będzie realizowana przez nabywcę, który będzie mógł mieć siedzibę w państwie trzecim. Dlatego wydaje się zasadne, aby zakresem stosowania europejskich przepisów o ochronie danych – nawet w ograniczonym stopniu – objęte były także firmy gromadzące i przetwarzające duże, zagregowane zbiory danych, których wielkość przekracza określone progi (ustalone na przykład wielkością unikalnych identyfikatorów) i dotyczące użytkowników Internetu⁸⁰⁷. Chociaż wobec tego typu podmiotów nie można wymagać stosowania obowiązków informacyjnych czy realizacji żądań kierowanych przez podmioty danych (bo przetwarzane przez nich bazy nie zawierają bezpośrednio informacji osobowych pozwalających na wskazanie uprawnionych podmiotów), to rozsądne wydaje się objęcie ich działalności wymaganiami podobnymi do nałożonych na podmioty przetwarzające, w szczególności związanych z zapewnieniem bezpieczeństwa przetwarzania czy minimalnych wymagań w zakresie korzystania z podwykonawców. Propozycja ta nadal jednak nie rozwiązuje istotnej luki związanej z zakresem terytorialnym stosowania prawa UE. Nawet odrzucając wyrażone wcześniej obawy związane z możliwością skutecznego stosowania europejskiego prawa o ochronie danych wobec przedsiębiorców prowadzących działalność w państwach trzecich⁸⁰⁸, pozostaje problem, w jaki sposób określić, którzy z takich przedsiębiorców powinni stosować

---

⁸⁰⁶ Zob. np. opinię EIOD w sprawie wspólnego stosowania prawa podstawowych w erze Big Data („EDPS Opinion on coherent enforcement of fundamental rights in the age of big data”, https://goo.gl/fsWmFL_), zawierającą liczne odwołania do ogólnego rozporządzenia; także opinia WP29 w sprawie rozwoju Big Data na ochronę praw podstawowych (WP 221, https://goo.gl/3ii8Au).

⁸⁰⁷ Przykładem może być definicja wprowadzona w projekcie amerykańskiej federalnej ustawy o rozliczalności i transparentności działania brokerów danych (zob. przypis 825): Termin „broker danych” oznacza każdą komercyjną organizację, która gromadzi, łączy lub utrzymuje informacje osobiste dotyczące osób, nie będących jej klientami lub pracownikami, w celu sprzedawania informacji lub dostarczania innym podmiotom tych informacji.

⁸⁰⁸ Zob. krytyczne uwagi związane ze stosowaniem ogólnego rozporządzenia w odniesieniu do przedsiębiorców zagranicznych zawarte w rozdziale 6.4.4 (s. 278-280).
się do postulowanych wyżej nowych przepisów, skoro z definicji przetwarzają informacje niepozwalające na identyfikację podmiotów danych? Nie wiedząc, jakie dane są przetwarzane, nie sposób uznać spełnienia przesłanki wskazanej w art. 2 ust. 2 rozporządzenia.

Dlatego – jako wniosek de lege ferenda – zasadne wydaje się, aby na potrzeby przetwarzania dużych zbiorów danych opracowana została odrębna regulacja, stanowiąca lex specialis względem ogólnego rozporządzenia i dotycząca wyłącznie podmiotów prowadzących czynności przetwarzania dużych zbiorów danych (na potrzeby własne lub świadczonych usług). Regulacja taka powinna określać minimalne wymagania w zakresie zabezpieczenia zbiorów (bazujące na wybranych środkach określonych w ogólnym rozporządzeniu) oraz powinna wprowadzać własną definicję zakresu materialnego (przetwarzanie dużych zbiorów danych a nie danych osobowych) oraz terytorialnego, innego niż stosowane w ogólnym rozporządzeniu. W istocie zatem przedstawiona propozycja sprowadza się do wprowadzenia przez unijnego prawodawcę regulacji o zakresie podmiotowym i przedmiotowym podobnym, do projektu ustawy o rozliczalności i transparentności działania brokerów danych (Data Broker Accountability and Transparency Act)809 której wprowadzenie jest od lat dyskutowane w Stanach Zjednoczonych.

W chwili obecnej wniosek ten należy traktować jako głos w dyskusji na temat kierunków rozwoju prawodawstwa unijnego. Z dostępnych informacji, publikowanych przez instytucje UE, nie wynika, aby tego typu regulacja była planowana do wprowadzenia w najbliższym czasie.

7.4.3. Praktyczność zasady minimalizacji danych

Jeden z paradygmatów ochrony danych osobowych związany jest z zasadą minimalizacji danych. Zgodnie z nią administrator powinien ograniczyć zakres gromadzonych i przetwarzanych informacji wyłącznie do niezbędnych z punktu widzenia zamierzonych celów przetwarzania. Zasada minimalizacji prowadzi zatem do uniknięcia sytuacji, w której następuje nadmiarowe gromadzenie danych. Ma ona takie samo zastosowanie w odniesieniu do podmiotów prywatnych, jak i publicznych. Co więcej, w przypadku tych drugich naruszenie zasady minimalizacji – a więc gromadzenie danych niezwiązanych z celem przetwarzania – może być uznane jako naruszenie zasady legalizmu, a więc działania w oparciu i w granicach prawa. Są z nią także związane inne podstawowe

809 Zob. przypisy 824 oraz 825.
zasady przetwarzania, takie jak zasada ograniczonego użycia czy proporcjonalności. Zasada minimalizacji jest też jedną z głównych zasad przetwarzania danych osobowych określonych w ogólnym rozporządzeniu (art. 5 ust. 1 pkt c). W efekcie jej stosowanie stanowi jeden z podstawowych obowiązków administratorów i podmiotów przetwarzających dane. Natomiast zgodnie z art. 5 ust. 2 rozporządzenia administrator jest zobowiązany do wykazania przestrzegania tej zasady w podejmowanych czynnościach przetwarzania.

W przypadku Big Data pojawiają się jednak dwa praktyczne problemy: pierwszy związany z interpretacją znaczenia zasady w odniesieniu do procesów przetwarzania na dużych zbiorach danych, a drugi – z celowością jej dalszego stosowania w odniesieniu do Big Data. Przydatność zasady minimalizacji związana jest z ograniczeniem informacji, jakie są zbierane i przetwarzane na temat jednostek do minimum potrzebnego do realizacji celu przetwarzania. W przypadku Big Data, mając do dyspozycji bardzo duże, wieloaspektowe zbiory danych oraz zaawansowane algorytmy heurystyczne, istnieje możliwość, że informacja wcześniej usunięta z baz źródłowych i tak zostanie ponownie odtworzona. W przypadku Big Data trudno zastosować wprost zasadę minimalizacji, bowiem celem tej formy przetwarzania jest gromadzenie dużych – początkowo ocenianych nawet jako nadmiarowe – zbiorów danych w celu szukania nietrywialnych powiązań między danymi, które służą następnie do budowania szczegółowych wniosków. W momencie gromadzenia danych nie wiadomo, jakie wyniki zostaną uzyskane i z perspektywy tych wyników, które dane okazać się nieprzydane i zbędne. Dlatego Big Data jako technika przetwarzania jest w dużej mierze niepodatna na ograniczenia związane z danymi źródłowymi, ponieważ sama idea tej koncepcji przetwarzania polega na wykraczaniu poza dane źródłowe w zakresie prezentowanych wyników. Ujawniając nową wiedzę, Big Data wykracza poza ramy wyznaczone przez zasadę minimalizacji, tym samym powodując, że jej praktyczne znaczenie dla ochrony danych może zostać zakwestionowane.

Powstaje zatem problem, w jaki sposób podmioty stosujące techniki Big Data mają wykazać zachowanie zasady rozliczalności (art. 5 ust. 2), skoro wymóg minimalizacji danych z definicji nie jest możliwy do spełniania przy analizach dużych zbiorów danych? Problem ten jest dyskusyjny w literaturze przedmiotu. I. Rubenstein zauważa, że sama idea przetwarzania dużych zbiorów prowadzi do kolizji z zasadą minimalizacji. Jej zdaniem, zastosowanie zasady minimalizacji zagroziłoby korzyściami ekonomicznym i społecznym.
związany z analityką Big Data, dlatego organy nadzoru powinny liczyć się z tym, że wymaganie to będzie często naruszane\textsuperscript{810}.

Problem ten zauważył także brytyjski organ nadzoru (ICO) w opublikowanych w marcu 2017 roku rekomendacjach w zakresie dostosowania przesiebiorców stosujących przetwarzanie Big Data do wymagań ogólnego rozporządzenia. Podsumowując rozważania związane z rolą i odniesieniem wymogu minimalizacji danych do Big Data, ICO stwierdził, że „przestrzeganie tych wytycznych może być trudniejsze w kontekście Big Data, ale jesteśmy przekonani, że posiadanie dobrze zarządzanych, aktualnych i związanych z przedmiotem badań danych – bez pozyskiwania i przechowywania danych nadmiarowych – przyczyni się do poprawy jakości danych i wsparcia przeprowadzania analiz”\textsuperscript{811}.

7.4.4. Anonimizacja w regulacjach prawnych

Pomimo poważnych wątpliwości co do skuteczności anonimizacji w pozbawieniu danych cechy identyfikowalności podmiotów środek ten jest nadal preferowany przez prawodawców jako podstawowe – obok szyfrowania – narzędzie służące zmniejszeniu ryzyk związanych z przetwarzaniem danych osobowych.

Duża część zbiorów stanowiących przedmiot analizy Big Data – i niezawierających wprost danych osobowych (poddana wcześniej anonimizacji) – zgodnie z definicjami przyjętymi w ogólnym rozporządzeniu powinna być przetwarzana jak dane pseudonimiczne. Prowadzi to do konkluzji, że duża część (jeżeli nie wszystkie) dużych zbiorów danych publicznie dostępnych (np. wpisy z mediów społecznościowych – takich jak Twitter, Facebook, LinkedIn), nawet niezawierających danych pozwalających na bezpośrednią identyfikację, powinna być przetwarzana zgodnie z europejskimi przepisami o ochronie danych – ponieważ spełniają definicję danych pseudonimicznych oraz obejmują informacje na temat mieszkańców UE (spełniona jest zatem przesłanka związana z zakresem terytorialnym stosowania przepisów wskazana w art. 2 ust. 2 rozporządzenia).

Generalizując powyższy wniosek – oraz łącząc definicję danych pseudonimicznych, zakres terytorialny stosowania ogólnego rozporządzenia oraz specyfikę przetwarzania Big Data (możliwość identyfikacji podmiotów) – można dojść do wniosku, że wszystkie operacje przetwarzania mające za przedmiot duże zbiory danych pochodzące z serwisów społecznościowych, realizowane przez każdy podmiot na świecie, niezależnie od miejsca przetwarzania oraz prawa właściwego obowiązującego przetwarzającego, są objęte zakresem

\textsuperscript{810} I. Rubinstein, Big Data: The End of Privacy..., op. cit., s. 78.
\textsuperscript{811} Information Commissioner’s Office, Big data, artificial intelligence..., op. cit., p. 91.
stosowania ogólnego rozporządzenia, a w konsekwencji – prawa UE. Formułując tę myśl w sposób syntetyczny: ogólne rozporządzenie zostało zdefiniowane w taki sposób, że może prowadzić do uznania prawa UE jako właściwego dla wszystkich operacji przetwarzania Big Data na całym świecie.

Naturalnie podejście takie musi spotkać się z uzasadnioną krytyką. Podobnie jak w przypadku wcześniejszych rozważań dotyczących ryzyk związanych z przetwarzaniem danych w chmurze obliczeniowej, tak i w przypadku Big Data proponowane przez prawodawcę unijnego rozwiązanie problemu globalnego przetwarzania danych mieszkańców UE sprowadza się do próby rozszerzenia stosowania prawa Unii na wszystkie lokalizacje, gdzie dane te są przetwarzane.

W Stanach Zjednoczonych zdecydowano się na odmienne regulowanie kwestii anonimizacji danych. W standardach ochrony prywatności informacji medycznych (HIPAA Privacy Rule) wydanych na podstawie przepisów federalnej ustawy o przenośności i rozliczalności ubezpieczeń zdrowotnych (Health Insurance Portability and Accountability Act, HIPAA) wskazano dwie alternatywne możliwości przeprowadzenia anonimizacji.

Pierwszą jest stwierdzenie pozbawienia zbioru danych cech pozwalających na identyfikację podmiotu w oparciu o ekspertyzę przeprowadzoną przez osobę posiadającą odpowiednie kompetencje i doświadczenie. Drugą jest usunięcie ze zbioru określonych w przepisach osiemnastu rodzajów informacji szczegółowych (takich jak dane adresowe, informacje o diagnozie, identyfikatory sprzętu medycznego czy dane biometryczne). W piśmiennictwie wskazuje się, że chociaż jest to rozbudowana lista, to jednak biorąc pod uwagę rosnące możliwości przetwarzania danych, zrównanie anonimizacji z usunięciem określonych przepisem konkretnych kategorii danych jest błędne. Najlepszym empirycznym potwierdzeniem tej obserwacji są przedstawione w rozdziale 7.3.3 wyniki badań przeprowadzonych przez L. Sweeney na anonimizowanych danych dotyczących świadczeń szpitalnych wykonanych w stanie Waszyngton w roku 2011.

Funkcjonujące obecnie w Unii Europejskiej i Stanach Zjednoczonych prawodawstwo związane z ochroną danych osobowych zawiera trudno realizowane (UE) lub nieskuteczne (USA) regulacje związane z możliwościami oraz skutkami przeprowadzenia anonimizacji zbioru danych osobowych. Wady legislacji zostały unaconczone wraz z upowszechnieniem się analiz

---

812 Zob. analiza przedstawiona w rozdziale 6.4.4 (s. 274).
813 Ustawa federalna USA z dn. 21 sierpnia 1996 o przenośności i rozliczalności ubezpieczeń zdrowotnych (Health Insurance Portability and Accountability Act); sygn. 104–191, publikacja 110 Stat. 1936.
815 Ibidem, § 164.514(b).
Big Data, które w oparciu o łatwo dostępne i anonimowe informacje pozwalają przeprowadzić proces identyfikacji podmiotów danych. Obserwacja ta stanowi kolejną przesłankę uzasadniającą opracowanie norm lex specialis, mających za przedmiot regulacji działalność prowadzoną przez brokerów danych. Skoro nie ma technicznej możliwości przeprowadzenia całkowicie nieodwracalnej anonimizacji danych, prawodawcy powinni zadbać, aby działania podmiotów na rynku Big Data były odpowiednio kontrolowane i nadzorowane.

7.4.5. Kontrola przetwarzania i prawa podmiotów danych

Zgodnie z art. 21 ust. 2 rozporządzenia osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby marketingu bezpośredniego, w tym profilowania. Warto zauważyć, że jest to norma szczególna względem przepisu art. 21 ust 1 który także przewiduje możliwość wniesienia sprzeciwu wobec przetwarzania danych opartego na profilowaniu. O ile jednak przepis ten zawiera wyłączenia ograniczające możliwość stosowania prawa sprzeciwu (np. istnienie ważnych i prawnie uzasadnionych podstaw do przetwarzania lub dochodzenia roszczeń), to ust. 2 – dotyczący przetwarzania na cele marketingu bezpośredniego – takich wyłączeń nie zawiera.

Ponadto, zgodnie z art. 22 ust. 1 rozporządzenia osoba, której dane są przetwarzane, ma prawo nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Także w zakresie czynności profilowania pojawia się wątpliwość co do praktyczności i realności stosowania przyjętych rozwiązań prawnych dla rynku Big Data. Pierwsza trudność może dotyczyć kwestii ustalenia, czy dany podmiot prowadzący działalność w państwie trzecim zobowiązany jest do stosowania przepisów ogólnego rozporządzenia. Aby zaszła przesłanka opisana w art. 2 ust. 2 rozporządzenia – a więc konieczność stosowania rozporządzenia na podstawie przepisów o zasięgu terytorialnym – przedsiębiorca musi mieć możliwość ustalenia, czy przetwarza dane użytkowników z terenu UE. O ile w przypadku standardowych usług, gdzie przedsiębiorca zawiera z użytkownikiem umowę na świadczenie usług, udzielenie odpowiedzi na to pytanie jest relatywnie proste, to w przypadku hurtowego przetwarzania dużych zbiorów danych, często pochodzących z publicznie dostępnych źródeł internetowych – nie jest już to zadanie proste. Nawet jeżeli przedsiębiorca w wyniku analizy
Big Data wielu źródeł danych jest w stanie określić szereg cech i atrybutów osoby (wiek, płeć, adres e-mail, preferencje zakupowe, upodobania w zakresie słuchanej muzyki, oglądanych filmów itp.) to może nie być w stanie określić geograficznej lokalizacji danego użytkownika. Co, jeżeli użytkownik korzysta z wielu lokalizacji geograficznych (agregowane dane wskazują na różne miejsca źródłowe powstania informacji) lub wprowadza inną lokalizację geograficzną, niż wynika ze znaczników (metadanych) opisujących przesyłane informacje?

W chwili obecnej – z uwagi na fakt, że przepisy rozporządzenia nie są jeszcze stosowane – nie sposób określić, jaka będzie praktyka zarówno europejskich organów nadzorów, jak i organów sądowych (w szczególności – TSUE) w przedmiocie rozstrzygnięcia zakresu stosowania przepisów UE przez zagranicznych brokerów danych.

Na praktyczne problemy w możliwości realizacji praw podmiotów danych zwróciła także uwagę Federalna Komisja Handlu (Federal Trade Commission, FTC), która zgodnie z amerykańskim prawodawstwem jest właściwa do nadzorowania większości podmiotów przetwarzających dane osobowe w celach komercyjnych. We wnioskach z opublikowanej w maju 2014 roku analizy rynku brokerów danych w USA zaleca wdrożenie ścisłszego modelu nadzoru oraz uruchomienie centralnego portalu, który służyłyby prezentowaniu zainteresowanym osobom zakresu informacji na ich temat przetwarzanych w celach marketingowych.

Chociaż postulat ten nie został dotychczas zrealizowany, warto zauważyć, że jeden z większych uczestników rynku – firma Acxiom – uruchomiła własny portal pozwalający na weryfikację zakresu przetwarzanych danych oraz dający ograniczoną możliwość do usunięcia niektórych informacji z bazy przedsiębiorcy. Uwagę zwraca możliwość skorzystania z usługi wyłącznie przez rezydentów Stanów Zjednoczonych (wymaganie podania na etapie zakładania konta numeru ubezpieczenia społecznego oraz adresu zamieszkania na terenie USA). Ponadto, zgodnie z zapisami warunków świadczenia usługi i udostępnionej polityki prywatności, informacje podane przez użytkownika na etapie zakładania konta (a więc także unikalny numer ubezpieczenia społecznego oraz adres korespondencyjny), mogą być

---


817 Federal Trade Commission, Data Brokers…, op. cit., s. 50-51.


wykorzystane przez Acxiom do marketingu własnych produktów. Należy uznać tego typu praktykę za naganną – celem uruchomienia portalu jest zwiększenie przejrzystości działań administratora w obszarze gromadzenia i przetwarzania danych milionów użytkowników Internetu. Stworzenie zatem z procedury rejestracyjnej, warunkującej dostęp do danych zgromadzonych przez Acxiom, następnego mechanizmu gromadzenia danych w celach marketingowych trzeba ocenić jednoznacznie negatywnie.

7.5. Podsumowanie i wnioski

Zaprezentowane powyżej rozważania mogą wskazywać na nieuniknioną porażkę prób skutecznego zapewnienia ochrony prywatności w erze przetwarzania dużych zbiorów danych. Byłyby to jednak wniosek przesadny i nieprawdziwy. Jak obrazowo wskazali N. Richards i J. King, „nawet w czasach masowej inwigilacji i Big Data, prywatność nie jest martwa ani umierająca”821. Krytyczne uwagi dotyczące prawnych mechanizmów ochrony prywatności związane są z nieadekwatywnymi paradygmatami, które nie uległy zmianie od czasu opracowania w latach siedemdziesiątych dwudziestego wieku pierwszych standardów ochrony prywatności w odniesieniu do danych przetwarzanych elektronicznie.

W świecie, w którym coraz więcej danych jest gromadzonych i przetwarzanych w Internecie, pochodzące z minionych dziesięcioleci koncepcje związane z minimalizacją danych czy definiowaniem odrębnego reżimu dla przetwarzania danych wrażliwych tracą na aktualności. Nie ma powodów sądzić, że rynek Big Data nie będzie podlegał dalszej ewolucji. Należy oczekiwać szerszego wprowadzenia i udoskonalania algorytmów sztucznej inteligencji oraz budowania coraz szybszych oraz efektywniejszych mechanizmów korelowania dużych zbiorów danych. W rezultacie, w niedalekiej przyszłości może okazać się, że brokerzy danych będą posiadać szczegółową wiedzę o całych społeczeństwach daleko przekraczającą informacje, jakie mogą być gromadzone na poziomie poszczególnych państw czy podmiotów publicznych. Już dzisiaj firmy takie jak Acxiom mają informacje na temat setek milionów osób – a więc ilości większej niż liczba mieszkańców Unii Europejskiej. Jest tylko kwestią czasu, gdy przedsiębiorcy tego typu będą w posiadaniu informacji na temat wszystkich ludzi, których szczegółowość w połączeniu z algorytmami sztucznej inteligencji pozwoli na precyzyjne przewidywanie zachowań tak jednostek jak i całych społeczności.

---

820 Zob. treść polityki prywatności serwisu: https://aboutthedata.com/privacy/.
821 N. Richards, J. King, Big Data Ethics, op. cit., s. 395.
opinii A. Leonarda, „korporacje, które pozyskają technologię pozwalającą na budowanie wiedzy w oparciu o takie dane będą wiedziały o nas więcej, niż my sami”822.

Jedną z przyczyn umożliwiających gromadzenie tak szczegółowych informacji przez brokerów danych jest niewystarczająca świadomość użytkowników w zakresie konsekwencji udostępniania treści w Internecie. Jakkolwiek według dostępnych badań osoby fizyczne coraz częściej wskazują, że aspekty związane z ochroną prywatności są elementami branymi pod uwagę przy wyborze i korzystaniu z poszczególnych e-usług, to jednak w przypadku Big Data problemem nie jest udostępnianie wrażliwych informacji na swój temat, tylko stałe publikowane nawet mało istotnych informacji opisujących decyzje, zachowania i preferencje związane z życiem codziennym. Chociaż coraz więcej uwagi jest poświęcane prowadzeniu kampanii społecznych823 uświadamiających zagrożenia związane z ujawnieniem szczegółów z życia prywatnego, to jednak ich celem nie jest sklonienie użytkowników do całkowitego zaprzestania z korzystania z Internetu. Dlatego budowanie świadomości użytkowników w zakresie bezpiecznego korzystania z e-usług jest potrzebne, ale nie jest w stanie znacząco wpłynąć na ryzyko związane z Big Data lub ograniczyć je.

Wydaje się zatem, że nastąpił moment, w którym prawodawcy powinni rozważyć konsekwencje realizacji opisanego powyżej scenariusza dla powodzenia koncepcji budowy społeczeństwa opartego na informacji. Wydaje się niezasadne, aby wprowadzane przepisy o ochronie danych nakładały rozbudowane obowiązki na właścicieli niewielkich sklepów internetowych, jednocześnie pomijając zagrożenia związane z przetwarzaniem publicznie dostępnych baz danych zawierających miliardy wpisów użytkowników Internetu. W niektórych państwach podjęto próbę wprowadzenia prawnej regulacji funkcjonowania brokerów danych. Przykładem mogą być Stany Zjednoczone i przedłożone projekty ustawy o rozliczalności i transparentności działania brokerów danych (Data Broker Accountability and Transparency Act). Kolejne projekty, przedkładane w 2014824 i 2015825 roku, nie zostały zatwierdzone.

---

822 Cytat za: N. Richards, J. King, Three Paradoxes of Big Data, op. cit., s. 44.
823 Zob. komunikat jednostki policji w niemieckim mieście Hagen, będący elementem kampanii uświadamiającej rodzicom konsekwencje ich działań dla ochrony prywatności własnych dzieci: https://www.facebook.com/Polizei.NRW.HA/posts/474114729427503:0.
8.1. Wprowadzenie

W ostatnich dwudziestu latach coraz dynamiczniej rozwija się forma inwigilacji, związana z hurtowym i nieukierunkowanym gromadzeniem danych. Jej upowszechnienie jest możliwe dzięki nowym możliwościom przetwarzania bardzo dużych zbiorów danych oraz łatwością dostępu do wielu elektronicznych źródeł informacji o setkach milionów użytkowników Internetu. Analizy Big Data w ten sam sposób mogą być wykorzystywane do korelowania danych całego społeczeństwa w poszukiwaniu wzorców epidemiologicznych, jak i typowaniu osób podejrzewanych o prowadzenie działań ekstremistycznych. Co więcej, mając do dyspozycji praktycznie nieskończone możliwości agregowania danych z różnych źródeł, w tym także dostępnych tylko dla uprawnionych organów, realna pojawia się możliwość zbudowania „cyfrowego Panoptykonu”, przestrzeni, w której wolność, a co za tym idzie prywatność jest tymczasowym złudzeniem, utrzymywanym tak długo i w takim zakresie, w jakim jest to potrzebne władzy. Ujawnione przez E. Snowdenu informacje na temat prowadzenia rozbudowanych programów wywiadowczych przez amerykańską Agencję Bezpieczeństwa Narodowego (National Security Agency, NSA) oraz brytyjską Centralę Łączności Rządowej (Government Communications Headquarters, GCHQ) stały się przyczyną do dyskusji w zakresie granic inwigilacji obywateli oraz skuteczności i przydatności istniejących norm prawnych dla ochrony uzasadnionego interesu jednostek. Z drugiej strony, każda się jednak zastanowić nad konsekwencjami dowolnego wkraczania w sferę prywatności dla trwałości norm stanowiących fundament społeczeństwa demokratycznego – takich jak wolność, równość, swoboda wypowiedzi czy prawo do informacji. Zeznanając przed specjalną komisją Parlamentu Europejskiego i odnosząc się do szerokich uprawnień w dostępie do informacji i zagrożeń wynikających z tego faktu dla ochrony norm demokratycznych, E. Snowden stwierdził: „nie wstając ze swojego fotela, mógłbym czytać prywatne wiadomości każdego z członków tej komisji, jak również dowolnego innego obywatela”.

Przed rozpoczęciem lektury niniejszego rozdziału zalecane jest zapoznanie się z treścią rozdziałów 6 i 7, jako że wiele koncepcji poruszanych w niniejszym rozdziale wprost nawiązuje do rozważań przedstawionych wcześniej.

inwigilacyjnych, należy uwzględnić, czy przekazanie tak rozbudowanych uprawnień i wiedzy na temat prywatnych spraw wszystkich obywateli służbom specjalnym jest faktycznie działaniem sprzyjającym rozwojowi i utrzymaniu standardów państwa demokratycznego.

Powiązanie obszaru tajnej inwigilacji elektronicznej z działalnością wywiadowczą państw skutkuje trudnością w dotarciu o obiektywnych informacjach, pozwalających na analizę zakresu prowadzonych programów oraz ich wpływu na przestrzeń praw i wolności osobistych. Jest to zrozumiałe biorąc pod uwagę niejawną związkę z pracą służb specjalnych, której zachowanie nierządko warunkuje skuteczność podejmowanych działań. Dlatego dla oceny skuteczności prawnych ograniczeń działań inwigilacyjnych państw wartościowe są informacje ujawniane przez tzw. sygnalistów (ang. whistleblower), a także archiwalne dokumenty odtajnione przez poszczególne służby specjalne. Bogatym źródłem wiedzy są także raporty przygotowywane przez niezależne оргany państwowe, np. komisje parlamentarne czy ombudsmanów.

Zwolennicy stosowania masowych programów inwigilacji wskazują na rosnące zagrożenia terrorystyczne oraz związane z przypadkami pojawiania się różnych form ekstremizmu. W takim rozumieniu inwigilacja jest traktowana jako środek konieczny do zapewnienia bezpieczeństwa publicznego, a w konsekwencji jako stanowiący uzasadniony przypadek zastosowania ograniczenia (limitacji) prawnych mechanizmów ochrony prywatności. Przywołując wcześniejsze rozważania związane z charakterem i ograniczeniami związanymi z Big Data, zwłaszcza dotyczących analityki predykcyjnej, należy rozważyć, czy faktycznie rejestrowanie wszystkich informacji w odniesieniu do nieznanej grupy osób i wnioskowanie na tej podstawie z wykorzystaniem nietransparentnych i heurystycznych algorytmów można uznać za środek konieczny dla zapewnienia bezpieczeństwa publicznego.

W szczerszym ujęciu – czy ustanowienie takiego modelu inwigilacji nie zagraża samej idei demokracji, a więc nie prowadzi do naruszenia zasad, dla ochrony których środki te są wprowadzane? J. Rzucidło i J. Węgrzyn wśród zagrożeń związanych z aktywnością w cyberprzestrzeni wymieniają cyberinwigilację, którą definiują jako wykorzystanie cyberprzestrzeni w celu kontroli społecznej. Jednocześnie wiążą tego typu działania z kategorią cyberprzestępstw. Podejście takie nie może być w pełni zaakceptowane, prowadzi

829 Zob. rozdział 7.3.1 (s. 296).
830 J. Rzucidło, J. Węgrzyn, Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni, Przegląd Prawa Konstytucyjnego 2015, nr 5, s. 145.
bowiem do uproszczenia wiążącego techniki inwigilacyjne wyłącznie z aktywnością zabronioną (penalizowaną), podczas gdy większość działań tego typu realizowanych jest w przestrzeni nie objętej regulacjami prawnymi (tym bardziej prawnokarnymi).

Programy masowej inwigilacji są prowadzone w oparciu o odmienną podstawę prawną niż inwigilacja indywidualna. Zazwyczaj są to regulacje związane z funkcjonowaniem rynku telekomunikacyjnego, czy uprawnieniami służb specjalnych. Nie znajdują zatem zastosowania przepisy procedury karnej. Dlatego oddzielnego rozważania wymaga zasadność stosowania restrykcyjnych norm postępowania w zakresie realizacji inwigilacji indywidualnej w sytuacji, gdy stosowania takich samych środków – ale w odniesieniu do nieoznaczonej grupy osób (w skrajnym przypadku – całego społeczeństwa) może być realizowane z pominięciem zabezpieczeń proceduralnych wynikających z procedury karnej.

Tradycyjny podział negatywnych oddziaływań na sferę prywatności na zagrożenia wertykalne i horyzontalne traci coraz bardziej na aktualności. Jego wprowadzenie było związane z podkreślaniem znaczenia szczególnej ochrony przed zagrożeniami płynącymi ze strony władzy publicznej. Spory związane z ochroną prywatności w relacjach horyzontalnych nierzadko pozostawiano regulacjom prywatnoprawnym831. Globalizacja rynku przetwarzania danych oraz pojawienie się nowych form gromadzenia i przetwarzania informacji spowodowało, że obecnie niektóre korporacje dysponują większymi zbiorami danych o obywatelach niż podmioty sektora publicznego832. Pojawia się zatem wątpliwość, czy pogląd, zgodnie z którym głównym zagrożeniem dla prywatności są działania władzy publicznej, jest nadal aktualny. Jeżeli tak – to w jaki sposób odnieść problem kolizji przepisów sankcionujących krajowe programy inwigilacji do ponadnarodowych norm związanych z obszarem prywatności. Przedstawiając problem inaczej – czy i w jaki sposób jednostka może chronić się przed nieuprawnioną inwigilacją ze strony organów państwa trzeciego, realizowanej z wykorzystaniem danych zgromadzonych przez przedsiębiorców zagranicznych. Jeżeli uznać, że wprowadzenie skutecznych środków ochrony przed takimi zagrożeniami nie jest możliwe, to czy w ogólne regulowanie zakresu dopuszczalnej ingerencji w stosunkach wertykalnych jest uzasadnione?

Pytania te mają fundamentalne znaczenie dla przyszłości nie tylko prawnych regulacji funkcjonowania cyberprzestrzeni, ale też – a może przede wszystkim – sukcesu ponadnarodowego projektu budowy społeczeństwa opartego na informacji. Problem został

831 Rozwiązanie takie było stosowane także w Polsce przed przyjęciem Konstytucji z 1997 – zob. rozdział 2.5.1 (s. 85).
832 Zobacz przykład firmy Acxiom omówiony w rozdziale 7.1 (s. 291).
zauważony przez Parlament Europejski, który w wydanej rezolucji wskazał na „programy nadzoru jako kolejny krok w kierunku stworzenia w pełni prewencyjnego państwa, w którym zmianie ulegnie utrwalony w państwach demokratycznych paradygmat prawa karnego, zgodnie z którym jakakolwiek inwazja w prawa podstawowe podejrzanych wymaga zatwierdzenia przez sędziego lub prokuratora na podstawie racjonalnego podejrzenia, natomiast promowane będzie połączenie egzekwowania prawa i działań wywiadowczych o zatartych i osłabionych zabezpieczeniach prawnych, często niezgodne z kontrolą i równowagą demokratyczną oraz prawami podstawowymi, szczególnie w kwestii domniemania niewinności”833.

8.2. Hipotezy badawcze

Odnosząc zakreślone we wstępie obszary problemowe do głównej tezy niniejszej pracy, zasadne wydaje się wyróżnienie następujących hipotez badawczych, które zbadane zostaną w niniejszym rozdziale:

1. Programy hurtowej i nieograniczonej inwigilacji nie spełniają kryterium konieczności w demokratycznym społeczeństwie, dlatego ich realizacja prowadzi do nieuprawnionej inwazji organów publicznych w sferę prywatności obywateli.

2. Z uwagi na globalny charakter Internetu mechanizmy bazujące na terytorialności w sposób ograniczony zapewniają skuteczną ochronę praw jednostek przed naruszeniami ze strony władzy publicznej w cyberprzestrzeni.

3. Wprowadzenie odmiennych zabezpieczeń proceduralno-prawnych w zakresie możliwości stosowania środków inwigilacji indywidualnej oraz nieukierunkowanej prowadzi do zróżnicowania stopni ochrony tego samego dobra chronionego (sfery życia prywatnego) w zależności od podjętych działań ze strony organów władzy publicznej.

Ponadto konieczne jest wprowadzenie dodatkowych ograniczeń i założeń, które pozwolą na uniknięcie zbyt szerokiego omawiania tematu masowej inwigilacji. Uwzględniając przedmiot badań niniejszej pracy, zasadne wydaje się skoncentrowanie

833 Rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188(INI), sygn. P7_TA(2014)0230, p. 12.
analizy na programach inwigilacji realizowanych z wykorzystaniem dużych zbiorów danych dostępnych w Internecie. W efekcie poza zakresem dalszej analizy znajdują się inne działania, związane z inwigilacją w przestrzeni fizycznej – takie jak wykorzystanie informacji z systemów monitoringu wizyjnego, podśluchu łączności telefonicznej834 czy zyskujące w ostatnich latach na znaczeniu wywiadowcze zastosowania dronów835.

8.3. Opis problemu

8.3.1. Kluczowe pojęcia

Inwigilacja nieukierunkowana zmierza do gromadzenia informacji o grupie osób niemających wspólnego wyróżnika. Dla przykładu gromadzenie informacji na temat osób podróżujących do krajów zagrożonych teroryzmem nie ma charakteru inwigilacji nieukierunkowanej. Jakkolwiek różne osoby oraz w różnym celu mogą podróżować do państw znajdujących się w zainteresowaniu organów państwa, to sam fakt odbycia podróży w badanym okresie może być wystarczający do zakreslenia kręgu osób poddanych technikom inwigilacyjnym. Najważniejszą zatem cechą odróżniającą inwigilację ukierunkowaną od nieukierunkowanej jest możliwość wskazania przed przystąpieniem do czynności operacyjnych, wobec kogo (jakiego kręgu osób) zostanie zastosowana inwigilacja. Ponadto działania służb w przypadku inwigilacji ukierunkowanej uzasadnione są znaną wcześniej okolicznością (zazwyczaj zamiarem lub podejrzeniem popełnienia poważnego przestępstwa), która pozwala ocenić prawidłowość i konieczność stosowanych środków. W przypadku inwigilacji nieukierunkowanej, ponieważ krąg inwigilowanych osób nie jest znany, nie można mówić o uzasadnionych podejrzeniach organów ścigania, a co najwyżej o oczekiwaniach w zakresie uzyskanych wyników. W efekcie ściganie przestępstw staje się zaawansowanym rodzajem badania Big Data z wszelkimi konsekwencjami opisanymi w rozdziale 5 – w szczególności brakiem pewności wyników będących skutkiem ograniczonej jakości danych oraz zastosowaniem algorytmów heurystycznych.

Kolejną cechą charakterystyczną inwigilacji nieukierunkowanej jest gromadzenie dużych ilości danych nadmiarowych. W przypadku kontroli operacyjnej, realizowanej w

834 Szeroko omawianym przykładem globalnego systemu podслушу łączności telefonicznej jest program ECHELON realizowany wspólnie przez wywiady FVEY (zob. przypis 841). Omówienie programu oraz analiza prawna jego legalności z punktu widzenia prawodawstwa amerykańskiego w: L. Sloan, ECHELON and The Legal Restraints on Signals Intelligence: A Need for Reevaluation, Duke Law Journal 2001, t. 50, s. 1467-1510.
835 Por. np. opinia WP29 nr 01/2015 na temat aspektów prywatności i ochrony danych w związku z wykorzystaniem dronów, WP 231, https://goo.gl/mfDZzg.
ramach procedury karnej, działania służb są nadzorowane i kontrolowane przez organy wymiaru sprawiedliwości. Skutkiem jest ograniczenie gromadzonych informacji do zakresu potrzebnego i uzasadnionego celem postępowania. Inwigilacja nieukierunkowana realizowana jest w odmienny sposób – działania inwigilacyjne nie są poprzedzone rozpoznaniem potrzeb informacyjnych, w efekcie decyzje o zakresie wykorzystania danych podejmowane są nie na etapie ich gromadzenia ale na etapie analizy. To kolejne ryzyko związane z prowadzeniem programów nieukierunkowanej inwigilacji – jeżeli podmiot publiczny może bez nadzoru gromadzić duże zbiory nadmiarowych danych to istnieje ryzyko, że kontrola wykorzystania tych danych nie będzie mogła być sprawnie przeprowadzona, a w efekcie znacznie zwiększa się ryzyko związane z nadużyciem władzy.

Drugim pojęciem, często wiązanym z programami masowej inwigilacji, jest hurtowe (ang. bulk) gromadzenie danych. Termin ten wskazuje na techniczny sposób realizacji czynności przechwytywania danych, często przeprowadzanych z wykorzystaniem podслушu kanałów komunikacyjnych. W efekcie podsłuchiwana jest cała łączność realizowana w określony sposób, niezależnie czy obejmuje jednego użytkownika sieci, czy sto milionów i niezależnie od tego, jaka jest lokalizacja samych nadawców i odbiorców wiadomości oraz treść przekazywanych komunikatów. Termin hurtowego przechwytywania wskazuje też na gromadzenie danych surowych, niepoddanych wcześniejszemu przetworzeniu – a więc w dużej mierze nadmiarowych. Także w tym przypadku możliwe jest już na etapie przechwytywania łączności stosowanie filtrów ograniczających zakres gromadzonych informacji. Według dostępnych raportów, możliwości takie stosuje np. GCHQ, prowadząc program TEMPORA w odniesieniu do nasłuchu łączności światłowodowej, którą transmitowany jest ruch internetowy przebiegający przez terytorium Wielkiej Brytanii 836.

Pod pojęciem masowych programów inwigilacji należy zatem rozumieć takie działania władzy publicznej lub podmiotów prywatnych działających w jej imieniu, których celem jest nieukierunkowane i hurtowe gromadzenie informacji na temat nieoznaczonej grupy osób (często całej populacji). Programy tego typu nie mają powszechnie znanych i przejrzystych zasad wykorzystywania danych, nie wiadomo więc, jaki jest cel przetwarzania, komu dane mogą być udostępnione – w szczególności czy i jakie są zasady ich przekazywania do państw trzecich.

W literaturze wskazuje się, że przymiotnik „masowy” – choć nie jest terminem prawniczym – stosuje się jako przeciwieństwo dla inwigilacji ukierunkowanej. Komisja

Wenecka podkreśla, że dobór terminu wskazuje na powiązanie tego typu programów z działaniami realizowanymi w państwach policyjnych, których przedmiotem jest kontrola całego społeczeństwa, a nie faktyczne wykrywanie najpoważniejszych przestępstw czy zapobieganie im.  

Programy masowej inwigilacji mają zatem za przedmiot wprowadzenie nieograniczonej kontroli w zakresie łączności elektronicznej. Dla zrozumienia ich zakresu i wpływu na prawa jednostek konieczne jest jeszcze wyjaśnienie różnicy pomiędzy danymi a metadanymi. Dane odzwierciedlają treść merytoryczną przekazu – w przypadku połączeń głosowych jest nią rozmowa, w przypadku poczty elektronicznej treść wiadomości e-mail, natomiast w przypadku komunikatorów OTT – komunikaty przekazywane między użytkownikami. Z kolei metadata to informacje przekazywane razem z wiadomością merytoryczną, służące ułatwieniu procesu transmisji lub odczytania jej treści, a także rozliczania usług. Klasycznym przykładem metadanych dla połączeń głosowych są informacje bilingowe (numery rozmówców, czas wywołania, długość połączenia), w przypadku poczty elektronicznej są nimi identyfikatory internetowe nadawcy i odbiorcy wiadomości, jak również czas wysłania, informacje na temat lokalizacji nadawcy (adres IP, informacje o wykorzystywanym komputerze itp.). Z obszarem przetwarzania metadanych bezpośrednio związane jest zagadnienie retencji danych. W odniesieniu do programów zakładających nieukierunkowane gromadzenie danych pod pojęciem retencji należy rozumieć nałożenie na operatorów telekomunikacyjnych obowiązku zatrzymania określonych informacji (najczęściej metadanych) związanych z realizowanymi usługami łączności na wskazany okres czasu. Retencja służy zatem wydłużeniu czasu, w jakim metadata są dostępne dla uprawnionych organów i mogą być pobrane na potrzeby wykonywanych analiz czy prowadzonych postępowań. Należy podkreślić, że cechą szczególną retencji jest powszechność obowiązku, co należy rozumieć jako konieczność zatrzymania danych dotyczących wszystkich użytkowników, a nie konkretnej osoby lub grupy osób pozostających w zainteresowaniu służb. Retencja jest zatem de facto techniką prowadzącą do usankcjonowania nieukierunkowanego gromadzenia danych, ale na koszt i ryzyko operatorów telekomunikacyjnych. Podobnie jak w przypadku innych


838 De facto ograniczonymi możliwościami technicznymi związanymi z dostępną pojemnością macierzy dyskowych, mocą obliczeniową oraz przepustowością łączy. W dokumentach E. Snowdena odnaleźć można wiele przykładów wskazujących, że ograniczanie przechwytywania danych przez NSA nie było spowodowane chciwą gromadzeniu tylko przydatnych informacji lub obawami o naruszenie prawa, ale wyłącznie trudnościami technicznymi, które planowano przewyciędźć.

839 Definicja – zob. przypis 534 (s. 189).
form nieukierunkowanego gromadzenia danych (np. w następstwie podsłuchu łączności światłowodowej), tak i w przypadku retencji środków ten nie służy ułatwieniu prowadzenia konkretnych postępowań karних, ponieważ podstawą do zatrzymania danych nie są przepisy prawnokarne, ale administracyjne – związane ze sposobem świadczenia usług łączności elektronicznej. Obowiązek zatrzymania danych może dotyczyć także innych strumieni danych, niezależnych wprost z łącznością elektroniczną. Przykładowo może być zatrzymanie danych dotyczących informacji o pasażerach (PNR), pozwalające na wykorzystywanie tego typu informacji na potrzeby analizy przedłużonych, często kilkuletnich, okres czasu. Dlatego obowiązek retencji danych należy postrzegać w kategoriach środka prowadzącego do gromadzenia danych nadmiarowych, a w efekcie zasadnicze wydają się wątpliwości związane z jego legalnością, zwłaszcza w odniesieniu do poszanowania zasady proporcjonalności jako koniecznego warunku ingerencji w obszar praw i wolności osobistych.

8.3.2. **Główne programy inwigilacyjne i związane z nimi możliwości techniczne**

Prowadzenie operacji wywiadowczych jest naturalnym uprawnieniem państwa, o istotnym wpływie na jego relacje zewnętrzne oraz wewnętrzne. Celem niniejszego punktu ani całego rozdziału nie jest analizowanie prawnych podstaw prowadzenia operacji wywiadowczych, a wpływu konkretnych programów – zakładających hurtowe i nieukierunkowane gromadzenie danych – na prawa obywateli oraz normy ustrojowe państwa.


---

840 W przypadku prawodawstwa polskiego przepisy Prawa telekomunikacyjnego; zob. rozdział 8.4.3 (s. 351).
841 Współpraca w zakresie wywiadu elektronicznego oparta została na umowie z 5 marca 1946 zawartej pomiędzy Wielką Brytanią a Stanami Zjednoczonymi, do której następnie przyleczyły się Australia, Kanada i
masowej inwigilacji, udziela sobie wzajemnej pomocy w zakresie kwestionowanych prawnie czynności przechwytywania danych oraz przekazuje pozyskane przez siebie dane poza granice własnej jurysdykcji celem ich swobodnego przetwarzania bez ograniczeń wynikających z obowiązującego prawa.

Jednym z głównych programów wywiadu elektronicznego, związanym z gromadzeniem masowych ilości informacji, jest PRISM. W ramach tego programu NSA ma stały dostęp do danych zgromadzonych przez wiodących dostawców usług internetowych – w tym Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL oraz Apple.

Co ważne, program ten nie jest realizowany dzięki podsłuchowi łączności tylko poprzez bezpośredni dostęp do danych zgromadzonych na serwerach usługodawców internetowych. Choć ujawnione materiały nie wskazują, czy dostęp ten odbywa się za zgodą i wiedzą dostawców usług, a niektórzy z nich oficjalnie zaprzeczają współpracy z NSA, to w rzeczywistości trudno przyjąć, aby opracowanie i zainstalowanie dedykowanych systemów informatycznych do obsługi żądań dostępu do danych przez służby specjalne mogło odbyć się bez współpracy poszczególnych dostawców usług. Co więcej, biorąc pod uwagę globalną infrastrukturę potrzebną do świadczenia każdej ze wskazanych usług, umożliwienie dostępu NSA jest działaniem skomplikowanym techniczne i wymagającym stałego zaangażowania dużych zasobów ze strony usługodawców.


843 Por. oświadczenie wydane przez L. Page’a, prezesa zarządu oraz D. Drummonda, wiceprezesa ds. prawnych, w którym zaprzaszają, że jakakolwiek agencja rządowa ma bezpośredni dostęp do danych zgromadzonych na serwerach Google oraz że sama firma uczestniczy w programie PRISM. Źródło: https://googleblog.blogspot.com/2013/06/what.html.
odniesieniu do tylko jednego użytkownika – musiałyby zgodnie z prawem USA uzyskać sądowy nakaz przeszukania (search warrant). NSA może bez uzyskania takiego nakazu przetwarzać wszystkie informacje, zgromadzone we wszystkich usługach przez wszystkich użytkowników.

Program RAMPART-A umożliwia NSA pozyskiwanie dowolnych informacji przekazywanych w Internecie na całym świecie844. Według potwierdzonych informacji, w jego ramach współpracowały agencje wywiadowcze z Niemiec i Danii, umożliwiając zamontowanie urządzeń podsłuchowych na łączach światłowodowych i przekazywanie uzyskiwanych danych do dalszego przetwarzania w USA. Co interesujące, warunki programu zakładały, że NSA nie będzie przechwytywała łączności dotyczącej obywateli kraju, w którym dane są pozyskiwane. Program realizowany z partnerem niemieckim (BND845), zidentyfikowany w informacjach medialnych jako mający kryptonim EIKANOL, został zakończony w 2008 roku przez BND z uwagi na obawy związane ze zgodnością podejmowanych działań z prawem, w szczególności z normami konstytucyjnymi związanych z ochroną prywatności obywateli846.

W ujawnionych przez E. Snowdena dokumentach widnieje informacja na temat wspólnych działań realizowanych przez amerykańską NSA z polskim partnerem (ujawniony dokument nie precyzuje, czy była to ABW, AW czy SKW). Operacja pod kryptonimem ORANECRUSH (znana partnerowi polskiemu pod nazwą BUFALLOGREEN) pozwalała NSA na przechwytywanie metadanych (od 3 marca 2009) oraz treści komunikacji (od 25 marca)847. Działanie te były realizowane w ramach programu OAKSTAR (stanowiącego część UPSTREAM) i ukierunkowane na gromadzenie informacji związanych z międzynarodową łącznością przechodzącą przez terytorium Polski. Nie wiadomo, czy działania te zostały zakończone oraz jakie były prawne podstawy współpracy polskich służb z NSA w zakresie hurtowego gromadzenia i przekazywania informacji objętych tajemnicą telekomunikacyjną obcemu wywiadowi, zwłaszcza uwzględniając, że prawo do poszanowania prywatności zagwarantowane w konstytucji podmiotowo obejmuje wszystkie osoby podległe polskiej jurysdykcji, a nie tylko obywateli848. Nie wiadomo, czy i w jaki

845 Federalna Służba Wywiadowcza (Bundesnachrichtendienst).
846 The German operation Eikonal as part of NSA’s RAMPART-A program, https://goo.gl/4NMLPu.
847 Źródło: https://edwardsnowden.com/2014/06/13/orange-crush/.
848 Zob. rozdział 2.5.2 (s. 87).
sposób Agencja Bezpieczeństwa Wewnętrznego kontrolowała i zapewniała, że NSA nie gromadzi informacji na temat mieszkańców Polski.

Chociaż warunki współpracy z partnerami europejskimi zakładały, że NSA nie będzie gromadziła za pomocą zainstalowanych urządzeń danych dotyczących mieszkańców danego kraju, zobowiązanie to nie było rozszerzane na możliwość przechwytywania tego samego ruchu w innych lokalizacjach. W literaturze wskazuje się, że biorąc pod uwagę architekturę Internetu oraz sposób przekazywania (trasowania) pakietów danych, nie ma technicznej możliwości skutecznego odfiltrowania ruchu pochodzącego z określonego kraju w całym strumieniu danych. W efekcie gromadzenie danych lokalnych jest nieuniknione. Fakt ten był jedną z przyczyn zakończenia współpracy BND z NSA.

Oddzielnego omówienia wymaga współpraca z NSA z brytyjską służbą wywiadu elektronicznego – GCHQ. Wielka Brytania, jako państwo członkowskie UE oraz jednocześnie członek wspólnoty Five Eyes, ma szczególne relacje w zakresie współpracy wywiadowczej ze Stanami Zjednoczonymi. Wielka Brytania posiada także własny, rozbudowany program podслушu informacji przekazywanych za pośrednictwem łączy światłowodowych – o nazwie kodowej TEMPORA. Biorąc pod uwagę, że duża część międzycountryalnych łączy światłowodowych przechodzi przez teren Wielkiej Brytanii, TEMPORA pozwala na przechwytywanie łączności krajojowej i międzynarodowej, pochodzącej także z innych państw członkowskich UE. W rezultacie GCHQ każdego dnia przechwytuje i analizuje miliardy komunikatów elektronicznych (połączeń głosowych, wiadomości e-mail, informacji o odwiedzanych stronach internetowych, danych z komunikatorów itp.). Informacje te są współdzielone z innymi agencjami wywiadowczymi, w tym NSA. Co więcej, GCHQ wraz z NSA prowadzi wspólne programy masowej inwigilacji. Przykładem jest program MUSCULAR, ukierunkowany na przechwytywanie danych pochodzących z centrów przetwarzania Google i Yahoo zlokalizowanych w Wielkiej Brytanii. W ten sposób agencja wywiadowcza państwa członkowskiego UE przyczynia się do ujawnienia służbow wywiadowczym państwa trzeciego danych osobowych oraz

---

849 Tym bardziej, że z opublikowanych statystyk wiadomo, że w omawianym okresie (rok 2009) NSA dziennie gromadziło informacje dotyczące ponad 3 mln połączeń telefonicznych z obszaru Polski – nie jest jednak znane źródło pozyskania tych danych, w szczególności czy był nim prowadzony wspólnie z polskimi służbami program ORANGECRUSH.

850 Zob. przypis 846.


informacji prywatnych mieszkańców UE korzystających z usług świadczonych za pośrednictwem centrów danych zlokalizowanych na obszarze Unii i – zgodnie z zawartymi z usługodawcom umowami – podlegających prawu UE853.


Wątpliwą legalność prowadzonych działań inwigilacyjnych dostrzegają też same agencje wywiadowcze. Jak wcześniej wskazano, niejasności prawne stały się przyczyną wycofania się BND ze współpracy z NSA w ramach programu RAMPART-A. Z ujawnionych analiz GCHQ wynika zrozumienie analityków i prawników agencji, że prowadzone działania znacząco wykraczają poza ramy prawne zarówno prawodawstwa krajowego, jak i unijnego855. Także NSA, chociaż działa w najmniej restrykcyjnym reżimie prawnym, musi stosować środki pozwalające jej na zalegalizowanie niektórych pozyskanych informacji. Przykładem może być opisywana w literaturze przedmiotu technika celowego kierowania ruchu internetowego poza granice USA, tak aby mógł być przechwycony poza jurysdykcją stosowania prawa amerykańskiego.

Powyższe rozważania można podsumować w następujących, najważniejszych punktach:

- prowadzone przez Stany Zjednoczone programy masowej inwigilacji obejmują techniki nieukierunkowanego przechwytywania danych pochodzących z różnych źródeł,
- w programach tych uczestniczą partnerzy z UE, umożliwiając instalację infrastruktury potrzebnej do przechwytywania łączności, ale także współpracując w zakresie wzajemnego udostępniania zbiorów danych,
- państwa europejskie prowadzą własne programy, ukierunkowane na gromadzenie hurtowych ilości danych; dane te są wymieniane z partnerami zagranicznymi,

853 Zob. rozważania na temat prawa właściwego w umowach dotyczących usług internetowych świadczonych w modelu chmury obliczeniowej – rozdział 6.4.3 (s. 262).
poza podслушem łączności światłowodowej, informacje pozyskiwane są bezpośrednio z centrów przetwarzania wiodących dostawców usług (także zlokalizowanych na obszarze UE),

w niektórych przypadkach NSA współpracuje bezpośrednio z zagranicznymi operatorami telekomunikacyjnymi, którzy udostępniają Agencji możliwość pobierania danych lub we własnym zakresie – na zlecenie NSA – wstępnie filtrują przechwytywany ruch; z uwagi na brak szczegółowych informacji na temat charakteru tych działań, nie sposób przeprowadzić oceny ich zgodności z przepisami właściwego systemu prawnego.

8.3.3. Środki technicznej ochrony prywatności i anonimowości w Internecie

Omawiając zagrożenia wynikające z prowadzenia rozbudowanych programów inwigilacyjnych przez organy władzy publicznej, należy przedstawić najważniejsze technologie, mające zastosowanie w obszarze ochrony przed przechwyceniem i dalszym przetwarzaniem prywatnej komunikacji. Należą do nich:

- szyfrowanie komunikacji,
- szyfrowanie danych,
- stosowanie technologii VPN.

Celem niniejszej pracy nie jest szczegółowe omawianie technicznych rozwiązań służących ochronie prywatności i anonimowości w Internecie. Jednak aby przeprowadzane rozważania w odpowiedni sposób przedstawiały znaczenie prawnych środków ochrony, konieczne jest wskazane braku możliwości skutecznego ograniczenia programów masowej inwigilacji na drodze rozwiązań wyłącznie technicznych.

Wszystkie wymienione wyżej rozwiązania mogą być nieskuteczne, zwłaszcza w odniesieniu do środków inwigilacyjnych będących w posiadaniu największych agencji wywiadowczych (takich jak NSA czy GCHQ). Służby specjalne wielu krajów (w tym Polski) mają specjalistyczne urządzenia pozwalające na przechwytywanie transmisji szyfrowanych (tzw. deszyfratory SSL). Do niedawna rozwiązania tego typu – z uwagi na ograniczenia techniczne – były wykorzystywane do inwigilacji indywidualnej, a więc w odniesieniu do łączności realizowanej przez konkretną osobę, będącą w zainteresowaniu służb. Jak wielokrotnie wskazano w niniejszej pracy, stosowanie tego typu inwigilacji nie budzi wątpliwości prawnych i od lat jest szczegółowo uregulowane w ramach procedury karnej. Obecnie jednak dostępne są urządzenia pozwalające na masowe rozszyfrowywanie ruchu
internetowego. W ten sposób możliwe jest przechwytywanie łączności wszystkich użytkowników korzystających z szyfrowanej łączności z danego obszaru lub kierowanych do danego serwera docelowego. Chociaż urządzenia tego typu oferowane są do sprzedaży wyłącznie uprawnionym organom, możliwość ich stosowania wydaje się prowadzić do dalszego rozbudowania środków masowego gromadzenia informacji na temat użytkowników Internetu.

Również szyfrowanie danych nie jest rozwiązaniem w pełni zabezpieczającym przed przechwyteniem informacji i ich wykorzystaniem w czynnościach profilowania – także w przypadku korzystania z usług świadczonych w chmurze obliczeniowej. Dzieje się tak, ponieważ usługodawcy sami nie korzystają z mechanizmów szyfrowania danych z uwagi na ograniczenia wydajnościowe (np. dane gromadzone w chmurze Google czy Apple nie są szyfrowane). Dane te są więc podatne na przechwytenie bezpośrednio u dostawców usług (np. w ramach programu PRISM). Ponadto skorzystanie z technik kryptograficznych może nie zabezpieczyć użytkownika przed ujawnieniem informacji, jeżeli oprogramowanie szyfrujące z którego korzysta zostało celowo zmanipulowane (np. poprzez zainstalowanie tzw. backdoora) w sposób umożliwiający uprawnionym organom odczyt treści bez posiadania hasła użytkownika856.

Niezależnie od tego zasadniczym ograniczeniem szyfrowania jest nieadekwatność tej techniki do obszaru ochrony prywatności. Nawet jeżeli zastosowanie szyfrowania wiązałoby się ze 100-% gwarancją ochrony przed nieuprawnionym dostępem, to w ten sposób możliwe jest zabezpieczenie tylko konkretnych, a zazwyczaj wrażliwych danych. Nie można zaszyfrować swoich nawyków, zwyczajów, upodobań, przekonań politycznych, lokalizacji swojego telefonu czy informacji, z kim spędza się czas. Wszystkie te informacje mogą być łatwo ustalone, korelując inne dane, pochodzące z poczty elektronicznej, kalendarzy, wpisów w portalach społecznościowych czy wiadomościach SMS. Zagrożenie związane z rozwojem programów masowej inwigilacji nie polega na braku możliwości zapewnienia skutecznej ochrony konkretnej, wrażliwej informacji, ale na zdobudowaniu systemu stałego nadzorowania i

monitorowania całego społeczeństwa, a w ten sposób wpłynęciu na wolność kształtowania się myśli i poglądów.

Podobnie korzystanie z technik pozwalających na anonimizację obecności w Internecie (ang. Virtual Private Network, VPN) może zwiększyć poczucie prywatności jednostki, ale w odniesieniu do mechanizmów stojących za programami masowej inwigilacji rozwiązania takie mają ograniczoną skuteczność. Przykładem mogą być wprowadzone w lipcu 2017 roku nowe przepisy w Rosji zmierzające do ograniczenia (de facto zakazu) możliwości korzystania z połączeń VPN. Podobnie jak w przypadkach innych ekspansywnych działań państw w zakresie gromadzenia informacji i kontrolowania społeczeństwa, tak i wprowadzenie wskazanych zmian prawnych uzasadnione jest względami bezpieczeństwa publicznego, a w szczególności przeciwdziałaniem przestępczości realizowanej w Internecie. Zamiast więc zwiększać transparentność działań władzy i w ten sposób eliminować konieczność ochrony prywatności poprzez korzystanie z nowoczesnych rozwiązań technicznych władze Rosji zdecydowały się na delegalizację tych rozwiązań – skutkującą dalszym zwiększeniem inwigilacji łączności elektronicznej.

Sposób, w jaki działalność organów państwa może celowo przyczyniać się do zmniejszenia skuteczności rozwiązań technicznych dedykowanych ochronie prywatności, można przeanalizować na przykładzie mającego miejsce w 2016 roku sporu prawnego pomiędzy firmą Apple a Federalnym Biurem Śledczym (Federal Bureau of Investigation, FBI) na tle próby zobowiązania tej pierwszej do opracowania technicznego sposobu ominięcia zabezpieczeń stosowanych w jej produktach. Powstałe zagadnienie prawne można uogólnić do problemu, czy wystąpienie jednostkowej potrzeby procesowej jest wystarczające do opracowania technologii, która pozwala organom państwa na pomijanie

857 Reuters, Putin bans VPNs to stop Russians accessing prohibited websites, https://www.reuters.com/article/us-russia-internet-idUSKBN1AF0QI.

858 Tłem sprawy było dochodzenie prowadzone przez FBI przeciwko osobom podejrzewanym o powiązaniu z wydarzeniami terrorystycznymi, które miały miejsce w San Bernardino w grudniu 2015 roku. Jeden z zatrzymanych posiadał telefon iPhone, którego pamięć wewnętrzna została zaszyfrowana przed nieuprawnionym dostępem. Urządzenie standardowo blokuje możliwość odczytania danych (są one trwale usuwane) po wystąpieniu z górę określonej liczby prób wprowadzenia błędnego hasła. Ponieważ agenci FBI nie znali hasła, a dane zapisane w pamięci telefonu mogły stanowić istotny dowód w sprawie, wystąpili o wydanie nakazu sądowego (ang. court order) zobowiązującego firmę Apple (producenta telefonu) do opracowania specjalnej wersji systemu operacyjnego telefonu, który w formie poprawki dla funkcjonariuszy FBI, który w formie poprawki zostanie wgrany na telefon i spowoduje wyłączenie mechanizmu blokowania telefonu po wprowadzeniu błędnego hasła. W ten sposób agenci zamierzały metodą brute-force uzyskać dostęp do danych telefonu. Przedstawiciele firmy Apple odmówili wykonania nakazu i skorzystali z drogi odwoławczej – argumentując, że nie mają wpływu na to, kto i kiedy użyje opracowanej przez nich poprawki, aby uzyskać dostęp do danych innych użytkowników ich produktu. W szczególności wskazywali, że wykonanie nakazu sądowego spowoduje, że potencjalnie każdy użytkownik iPhone będzie mógł być poddany nieuprawnionej inwigilacji z wykorzystaniem opracowanego oprogramowania.
mechanizmów ochrony prywatności w odniesieniu do każdego użytkownika. Chociaż spór pozostał de facto nierozstrzygnięty, w oczywisty sposób zobrazował brak możliwości ograniczenia zakresu ingerencji władzy w prawo do prywatności wyłącznie poprzez stosowanie komercyjnych rozwiązań technicznych.

Rozważania te prowadzą do wniosku, że prawne środki ochrony prywatności są jedynymi skutecznymi mechanizmami, które mogą przyczynić się do ograniczenia zakresu danych gromadzonych przez państwo, w tym na potrzeby programów masowej inwigilacji. Skorzystanie z innych środków, w tym technicznych, chociaż w jednostkowych przypadkach może zwiększać poczucie prywatności, to nie prowadzi do systemowego rozwiązania problemu braku poszanowania przez społeczeństwo wywiadowczą praw wynikających z aktów prawnomiedzynarodowych i prawodawstwa krajowego poszczególnych państw.

8.4. Analiza prawna

8.4.1. Masowa inwigilacja w orzecznictwie ETPC

Dzięki bogatemu orzecznictwu ETPC możliwe jest nie tylko wskazanie warunków, po spełnieniu jakich programy tajnej inwigilacji mogą zostać uznane za nienaruszające postanowień Konwencji, ale również przeprowadzenie rozważań na temat zgodności z nimi istniejących przepisów krajowych.

Na wstępie należy przypomnieć dwie zasadnicze przesłanki wzmacniające znaczenie orzeczeń ETPC w zakresie omawianej problematyki. Po pierwsze, Konwencja – w przeciwieństwie do prawa UE – nie zawiera przedmiotowego wyłączenia związanego z celami bezpieczeństwa publicznego. Prawo do prywatności może być ograniczone tylko w zakresie wynikającym z art. 8 ust. 2, a więc po spełnieniu kryterium zgodności z prawem oraz konieczności w demokratycznym społeczeństwie. Państwa nie mają zatem możliwości wskazania, że ewentualne spory dotyczące możliwości i zakresu stosowania nieograniczonej inwigilacji podlegają wyłączeniu z zakresu stosowania Konwencji. Natomiast jednostki zyskują narzędzie nie tylko do zaskarżania wybranych elementów związanych z prowadzeniem tego typu programów (jak np. przepisów nakładających na przedsiębiorców

859 Konsekwencje udzielenia twierdzącej odpowiedzi na to pytanie podsumował W. Diffie zauważając, że „komunikacja elektroniczna będzie budulcem jutrzenki społeczeństwa (...) Wprowadzenie uprawnień rządu do tajnego szpiegowania tej łączności stanowi olbrzymi krok w kierunku świata, w którym zapewnienie prywatności będzie dostępne dla bogaty... Cyt. za: D. Brin, The Transparent Society, Nowy Jork 2009, s. 249.
telekomunikacyjnych obowiązki związane z ogólną retencją danych), ale i kwestionowania legalności całych programów inwigilacyjnych prowadzonych przez organy państwowe.

Po drugie, chociaż wyroki ETPC są kierowane do państw, a sam wyrok Trybunału nie jest wystarczający do derogacji niezgodnych przepisów krajowych z porządku prawnego, jak i nie stanowi samodzielnej przesłanki skutkującej wznawieniem postępowania przed sądami krajowymi, to jednak stwierdzenie naruszenia przez państwo norm zagwarantowanych Konwencją jest jednoznaczną i rozstrzygającą oceną bezprawnego działania władzy publicznej.


Fundamentalne znaczenie dla dalszych rozważań mają tezy wyroku w sprawie Klass i in v. Niemcy. Trybunał musiał rozstrzygnąć, czy do uznania naruszenia ze strony państwa konieczne jest wykazanie przez skarżącego, że był on faktycznie objęty kwestionowanymi technikami inwigilacyjnymi. Innymi słowy – czy jednostka może skarżyć przepisy krajowe, pozwalające na stosowanie rozbudowanych środków inwigilacyjnych, nawet jeżeli nie może wykazać, że środki te były wobec niej zastosowane. Doktryna, zgodnie z którą bez wykazania szkody nie można dochodzić swoich praw, stanowi jedną z przyczyn, dla których programy masowej inwigilacji nie mogą być skutecznie kwestionowane przed sądami amerykańskimi. Gdyby ETPC zajął podobne stanowisko, warunkując podjęcie sprawy wstępnym wykazaniem, że wobec jednostki zastosowano techniki inwigilacji, to biorąc pod uwagę brak przejrzystości prowadzonych programów, w praktyce znacząco ograniczałoby to możliwość sądowej ochrony prawa do prywatności. Trybunał zajął jednak odmienne stanowisko – zauważył, że gwarancje wynikające z Konwencji nie mogą być ograniczone samym faktem tajności środków służących do przeprowadzania ingerencji. W tym zakresie Trybunał uznał za niedopuszczalne, „aby zapewnienie możliwości korzystania z prawa gwarantowanego

860 Por. art. 1 Konwencji – Wysokie Układające się Strony zapewniają każdemu człowiekowi, podlegającemu ich jurysdykcji, prawa i wolności określone w rozdziale I niniejszej konwencji.
861 Wyrok ETPC z 6.09.1978 r. w sprawie Klass i in. v. Niemcy, sygn. 5029/71.
przez Konwencję mogło zostać zniesione przez prosty fakt, że osoba pozostaje nieświadoma wystąpienia naruszenia”862.

Ponadto Trybunał wskazał, że samo istnienie możliwości ingerencji stanowi wystarczającą podstawę do uznania, że osoby, które mogą być poddane takim środkom, mają legitymację do kwestionowania tych środków na drodze sądowej863.

Wskazana w sprawie Klass i in. argumentacja znalazła potwierdzenie w kolejnych wyrokach Trybunału864, w ten sposób przyczyniając się do wypracowania  ugruntowanej linii orzecznicy, zgodnie z którą w przypadku prowadzenia tajnych programów inwigilacji jednostki mają prawo kwestionować legalność przepisów, na podstawie których programy takie zostały wprowadzone bez konieczności wykazania, czy faktycznie zostały objęte jakimkolwiek środkami kontrolnymi. Zdaniem Trybunału, samo już istnienie tajnego programu inwigilacyjnego może prowadzić do naruszenia prywatności. Warto przypomnieć, że jest to pogląd zgodny ze stanem wiedzy nauki w zakresie psychologicznych uwarunkowań związanych z potrzebą prywatności – jak wskazano w rozdziale 1.1, oczekiwanie prywatności może być naruszone nie tylko przez dokonywanie nieuprawnionej obserwacji, ale również przez sam fakt możliwości jej przeprowadzenia. Z kolei w sprawie Rotaru v. Rumunia Trybunał uznał, że już samo gromadzenie danych przez ograny władzy publicznej może stanowić nieuprawnioną ingerencję. Bez znaczenia przy tym pozostaje, czy i w jakim zakresie dane te są następnie przetwarzane865.

Należy przypomnieć, że nie każda ingerencja w prawo do prywatności obarczona jest bezprawnością takiego działania. Ingerencja może być uzasadniona, jeżeli spełnia łącznie przesłanki określone w art. 8 ust. 2 Konwencji, a więc kryterium zgodności z prawem oraz konieczności w demokratycznym społeczeństwie. Trybunał w orzecznictwie dotyczącym stosowania przez państwa tajnych programów inwigilacji określił kryteria konieczne do stwierdzenia spełnienia każdej z tych przesłanek.

Według ugruntowanego orzecznictwa ETPC zgodność z prawem programów inwigilacyjnych powinna być zapewniana poprzez łącze spełnienie następujących warunków:

- oparcie ich prowadzenia na odpowiednich przepisach krajowych,
- zgodność z zasadą rządów prawa,

862 Ibidem, §36.
863 Ibidem, §38.
865 Wyrok ETPC z 4.05.2000 w sprawie Rotaru v. Rumunia, sygn. 28341/95, §46.
– zapewnienie przewidywalności przepisów z punktu widzenia jednostki\(^866\).

Pierwszy warunek powinien być spełniony poprzez oparcie realizacji programów w przepisach rangi ustawowej. Jak ponadto wskazał Trybunał, niedopuszczalne jest pozostawienie zbyt dużego luzu decyzyjnego (np. w zakresie warunków zastosowania inwigilacji) uprawnionym organom. Zgodność z zasadą rządów prawa powinna oznaczać w szczególności możliwość kontroli niezależnego organu nad przeprowadzanymi czynnościami inwigilacyjnymi, ale także istnienie skutecznej drogi sądowej dla osób, objętych takimi działaniami. Co więcej, Trybunał podkreślił, że także pozostawienie organom sądowym zbyt dużej uznaniowości w zakresie podejmowanych decyzji prowadzi do naruszenia zasady rządów prawa\(^867\). Ostatni z warunków – związany z przewidywalnością stosowania inwigilacji – polega w szczególności na możliwości określenia przez jednostkę okoliczności, w jakich jej życie prywatne może być monitorowane, oraz zakresu dopuszczalnej inwigilacji.

Trybunał wypracował własny test określający listę minimalnych zabezpieczeń, jakie powinny być uwzględnione w krajowych przepisach wprowadzających programy inwigilacyjne. W ocenie Trybunału przepisy rangi ustawowej muszą określać:

- kategorię przestępstw, z którymi może wiązać się autoryzacja zastosowania środków inwigilacyjnych;
- kategorię osób, które mogą być poddane inwigilacji;
- ograniczenie maksymalnego czasu stosowania środków;
- procedury związane z badaniem, przechowywaniem i wykorzystywaniem zgromadzonych danych;
- środki ostrożności zastosowane w przekazywaniu zgromadzonych danych innym podmiotom;
- przesłanki, po spełnieniu których zebrane dane powinny lub muszą zostać usunięte bądź zniszczone\(^868\).

Trybunał określił też szczegółowe wytyczne w zakresie interpretacji drugiego z kryteriów uzasadniających zastosowanie środków inwigilacyjnych, wskazanych w art. 8 ust. 2 Konwencji, tj. przypadków „koniecznych w demokratycznym społeczeństwie”. Trybunał wskazał, że chociaż władze państwowe dysponują pewnym marginesem uznania w doborze środków prowadzących do zapewnienia uzasadnionego celu, jakim jest ochrona bezpieczeństwa publicznego, to jednak należy pamiętać, że wprowadzenie tajnych

\(^{866}\) Postanowienie ETPC z 29.06.2006 w sprawie Weber i Saravia v. Niemcy, sygn. 54934/00, §84.

\(^{867}\) Postanowienie ETPC w sprawie Weber i Saravia v. Niemcy, op. cit., §94.

\(^{868}\) Ibidem, §95.
programów inwigilacyjnych w przypadku pozbawienia ich odpowiednich zabezpieczeń może doprowadzić do osłabienia lub nawet zniszczenia zasad stojących u podstaw funkcjonowania państwa demokratycznego. Dlatego choć ochrona porządku publicznego jest przesłanką usprawiedliwiającą ingerencję w prawo do prywatności, to nie może być uznana za przesłankę wystarczającą. Istotne jest również zachowanie proporcjonalności podejmowanych działań – wyraźnych nie tylko skalą potencjalnego zagrożenia, ale i konsekwencjami dla praw jednostek. W tym miejscu należy odwołać się do przymiotnika „konieczny“, wskazującego na brak możliwości osiągnięcia zamierzonego celu innymi, mniej inwazyjnymi środkami. Dlatego Trybunał w sprawie Szabo i Vissy po raz pierwszy zastosował termin ścisłej konieczności869 (ang. strict necessity), który powinien mieć zastosowanie w przypadku analizy legalności prowadzonych programów inwigilacyjnych. W ocenie ETPC ścisłą konieczność należy rozumieć nie tylko jako potrzebę zastosowania danego środka w celu ochrony demokratycznych instytucji państwa (rozumienie węższe, stosowane we wcześniejszych orzeczeniach), ale także jako konkretną potrzebę procesową, związaną z pozyskaniem istotnych informacji dotyczących inwigilowanych jednostek, których nie można pozyskać w inny sposób870.

Zestawiając wymagania określone przez Trybunał – zwłaszcza związane ze zgodnością z prawem, koniecznością uwzględnienia minimalnych zabezpieczeń proceduralnych a także spełnienia kryterium proporcjonalności oraz ścisłej konieczności – sposób, zakres i działania podejmowane w ramach obecnie realizowanych programach masowej inwigilacji prowadzą w sposób oczywisty do naruszenia zobowiązań konwencyjnych. W szczególności stosowanie nieukierunkowanego przechwytywania danych nie daje pogodzić się z wymaganiem określenia zamkniętego katalogu przesłanek uzasadniających zastosowanie inwigilacji. Osoby poddane takim środkom nie mają możliwości określenia, czy podejmowane przez nich aktywności wiążą się z ryzykiem objęcia działaniami inwigilacyjnymi. Co więcej, osoby takie nie mają możliwości następnego kwestionowania zasadności i legalności podjętych działań. Dane są gromadzone bez istnienia jakiegokolwiek podejrzenia popełnienia przestępstwa, co prowadzi do wniosku, że każda osoba może zostać poddana inwigilacji.

W konsekwencji powyższych obserwacji Trybunał, badając sprawę zgodności rosyjskich przepisów inwigilacyjnych, orzekł o ich niezgodności z postanowieniami

869 Trybunał w rzeczywistości przeniósł doktrynę wąskiego rozumienia terminu „konieczność” wypracowaną w orzecznictwie TSUE (zob. np. C-473/12, p. 39). W oficjalnej polskiej wersji językowej orzeczeń TSUE termin „strictly necessary” tłumaczyony jest jako „absolutnie konieczny”.

870 Wyrok ETPC z 12.01.2016 r. w sprawie Szabo i Vissy v. Węgry, sygn. 37138/14, §73.
Konwencji. W ocenie Trybunału nałożenie na przedsiębiorstwa telekomunikacyjne obowiązku umożliwienia uprawnionym organom rejestrowania dowolnych transmisji w odniesieniu do każdego użytkownika sieci łączności, przy jednoczesnym braku zastosowania zabezpieczeń prawnych związanych z rejestrowaniem wykonywanych czynności oraz brakiem skutecznej kontroli sądowej – skutkuje ryzykiem nadużycia władzy, a w konsekwencji nie spełnia wymagań określonych w art. 8 ust. 2 EKPC, a więc prowadzi do zastosowania nieuprawnionej ingerencji w prawo do prywatności.

Z kolei w sprawie Szabo i Vissy v. Węgry Trybunał zauważył, że szerokie uprawnienia władzy wykonawczej – w szczególności związane z prawem do autoryzowania operacji inwigilacyjnych – nie mogą zastąpić kontroli ze strony niezależnego organu, a w przypadku braku takiej kontroli prowadzą do naruszenia zobowiązań konwencyjnych. Ponadto, korzystając z kryterium ścisłej konieczności, Trybunał uznał, że przepisy pozwalające na zastosowanie technik inwigilacyjnych w przypadkach, gdy środki takie nie są konieczne z uwagi na specyfikę prowadzonego postępowania, także nie mogą zostać uznane za spełniające wynikającą z art. 8 ust. 2 EKPC przesłankę „konieczności w państwie demokratycznym”.

Nieuukierunkowane gromadzenie danych, realizowane np. poprzez nałożenie ogólnego obowiązku retencji danych, prowadzi do naruszenia zobowiązań wynikających z EKPC. Wniosek taki wprost wynika z orzeczenia w sprawie Kennedy v. Wielka Brytania, gdzie Trybunał uznał brak możliwości nieograniczonego gromadzenia danych za jedną z przesłanek świadczących o zgodności badanych przepisów z Konwencją.

Należy jednak przypomnieć, że biorąc pod uwagę różne źródła danych, na jakich bazują rozbudowane programy masowej inwigilacji, zakwestionowanie legalności korzystania z obowiązku retencji danych nie skutkuje brakiem możliwości dalszego prowadzenia tego typu programów. W dotychczasowych orzeczeniach ETPC nie wypowiadał się wprost w sprawie możliwości prowadzenia przez państwa działań wywiadowczych związanych z prowadzeniem nieograniczonej inwigilacji. W orzeczeniach analizowana była głównie kwestia przepisów rozszerzających kompetencje organów ścigania w zbyt szeroki sposób, pozbawiony wystarczających zabezpieczeń ze strony niezależnych organów. Sprawą otwartą pozostaje jednak ocena Trybunału możliwości prowadzenia działań inwigilacyjnych...

---

871 Wyrok ETPC z 4.12.2015 r. w sprawie Zacharow v. Rosja, sygn. 7143/06.
872 Zob. przypis 870.
874 Wyrok ETPC z 18.05.2010 r. w sprawie Kennedy v. Wielka Brytania, sygn. 26839/05, §160.
podejmowanych wobec mieszkańców innych państw, nieraz także stron Konwencji. Dla przykładu programy realizowane przez GCHQ prowadzą do naruszenia prywatności nie tylko mieszkańców Wielkiej Brytanii, ale i (a może – głównie) mieszkańców innych państw UE. Dopiero w przyszłych orzeczeniach Trybunał wypowie się, na ile tego typu działania są legalne, a jeżeli prowadzą do naruszenia zobowiązań konwencyjnych, to kwestią dalszej analizy będzie określenie możliwych do podjęcia środków prawnych.

W chwili obecnej na rozpoznanie oczekuje kilka spraw złożonych przez organizacje pozarządowe kwestionujące wprost legalność prowadzonych programów inwigilacyjnych nastawionych na masowe przetwarzanie komunikacji elektronicznej. Przykładem może być sprawa Big Brother Watch i in. v. Wielka Brytania, w której wnioskujący wnoszą między innymi o uznanie przepisów krajowych, na podstawie których realizowany jest program inwigilacyjny TEMPORA, za naruszające art. 8 Konwencji.

8.4.2. Masowa inwigilacja w orzecznictwie TSUE

Kontynuując rozważania związane z prawnymi podstawami prowadzenia programów inwigilacji w regionie państw europejskich, szczególnego omówienia wymaga prawodawstwo UE oraz związany z nim dorobek orzeczniczy TSUE.

Na wstępie należy odpowiedzieć na trzy pytania, które pozwolą określić, na ile prawo unijne może stanowić praktyczny środek regulowania zakresu prowadzenia programów masowej inwigilacji:

875 Na tym tle warto przytoczyć argumentację zawartą w Raporcie Wysokiego Komisarza NZ ds. Praw Człowieka pt. „Prawo do prywatności w erze cyfrowej” (The right to privacy in the digital age). W raporcie wskazuje się, że zakres stosowania MPPOP – a zatem i obowiązki państw-stron traktatu – nie wyznaczone są wyłącznie granicami terytorialnymi jurysdykcji, ale skutkami podejmowanych działań dla jednostek. Wynika z tego wniosek, że miejsce przebywania jednostki (w szczególności fakt, czy znajduje się ona na terytorium określonego państwa-strony) nie przesądza o możliwości objęcia jej prawami i gwarancjami wynikającymi z traktatu (p. 32 raportu). Co więcej, zgodnie z wytycznymi Komitetu Praw Człowieka nieakceptowalna jest sytuacja, w której państwa-strony mogłyby podejmować poza obszarem swojej jurysdykcji działania naruszające prawa jednostki, które nie byłyby dopuszczalne uwzględniając ich własny system prawny (p. 33 raportu). Wnioski dotyczące zakresu stosowania MPPOP są interesujące także przy rozważaniach dotyczących EKPC z uwagi na zbliżony zakres art. 2 ust. 1 MPPOP („każe z państw-stron niniejszego Paktu zobowiązuje się przestrzegać i zapewnić wszystkim osobom, które znajdują się na jego terytorium i podlegają jego jurysdykcji...”) do art. 1 EKPC („strony zapewniają każdemu człowiekowi, podlegającemu ich jurysdykcji...”). Treść raportu: http://undocs.org/A/HRC/27/37.


878 Zob. rozdział 8.3.2 (s. 330).
w jaki sposób należy interpretować wyłączenie obszaru bezpieczeństwa narodowego wynikające z art. 4 ust. 2 TUE w odniesieniu do programów zakładających nieukierunkowane i hurtowe gromadzenie danych?

czy i w jakim zakresie przepisy wprowadzające programy masowej inwigilacji mogą być oceniane pod kątem zgodności z prawem UE?

z jakich narzędzi ochrony prawnej mogą skorzystać obywatele UE, zamierzający zakwestionować programy masowej inwigilacji prowadzone przez inne państwa członkowskie?

Odpowiadając na pierwsze pytanie, należy przypomnieć, że zgodnie z ugruntowanym orzecznictwem TSUE żadne ograniczenia praw i wolności nie mogą być traktowane w sposób rozszerzający. Ponadto uprawnienie państwa członkowskiego do skorzystania z odstępstwa przewidzanego w traktatach nie stoi na przeszkodzie sądowej kontroli działań podjętych w ramach tego odstępstwa879, zwłaszcza że działanie takie może być niezbędne, aby znaczenie nadawane poszczególnym terminom nie było jednostronnie ustalane przez poszczególne państwa członkowskie bez kontroli instytucji UE880.

Z porównania art. 4 ust. 2 TUE oraz art. 52 ust. 1 KPP nie wynika, aby wszelkie działania podejmowane przez Państwo jako uzasadnione względnym bezpieczeństwa narodowego korzystały z wyłączenia z prawa UE. Przyjęcie takiego stanowiska mogłoby bowiem w praktyce doprowadzić do erozji praw przewidzianych w traktatach oraz niejednakowego traktowania tych samych zobowiązań wnikających z prawa UE przez różne państwa członkowskie. Prawdą jest natomiast, że działania (1) podejmowane przez organy państwa oraz (2) wyłącznie związane z celami bezpieczeństwa narodowego, korzystają z wyłączenia przedmiotowego z zakresu stosowania prawa UE. Nawet jednak w takim wypadku ocenę, czy wyłączenie to ma zastosowanie, może i powinien dokonać TSUE jako jedyny organ uprawniony do interpretacji postanowień traktatowych881. Brak precyzyjnej definicji „bezpieczeństwa narodowego” jest także wskazywany w literaturze przedmiotu jako jedno z ryzyk, które mogą prowadzić do nudażywania tej podstawy prawnej dla wprowadzania przepisów krajowych niezgodnych z prawem UE (w szczególności postanowieniami KPP)882.

879 Wyrok TSUE z 4.12.1974 r. w sprawie van Duyn, sygn. 41/74.
880 Wyrok TSUE z 14.10.2004 r. w sprawie Omega Spielhallen- und Automatenaufstellungs, sygn. C-36/02.
881 Art. 267 TFUE; por. także wyrok TSUE z dn. 22.10.1987 w sprawie Foto-Frost, C-314/85, p. 15.
882 Grupa Robocza Art. 29, Working Document on surveillance of electronic communications for intelligence and national security purposes, WP 228, s. 24.
W istniejącym orzecznictwie Trybunału odnaleźć można wskazówki, w jaki sposób interpretować należy wyłączenie wskazane w art. 4 ust. 2. W pierwszej kolejności należy podkreślić, że zastosowanie jakiegokolwiek wyłączenia motywowanego porządkiem czy bezpieczeństwem publicznym może być uzasadnione tylko w przypadku istnienia rzeczywistego i dostatecznie poważnego zagrożenia podstawowego interesu społecznego⁸⁸³. Ponadto zakres wyłączenia musi być interpretowany wąsko i obejmować tylko takie działalności, które zostały wyraźnie wymienione lub które mogą być zaliczone do tego samego rodzaju⁸⁸⁴. Jak wskazał TSUE, bezpieczeństwo narodowe, obronność czy bezpieczeństwo publiczne, a więc dziedziny wskazane w art. 4 ust. 2 TUE, są właściwe działaniom państw i władzom państwowym, natomiast obce działalności osób prywatnych⁸⁸⁵. Zatem do zastosowania wyłączenia wynikającego ze wskazanej normy traktatowej, konieczne jest spełnienie zarówno kryterium przedmiotowego (wskazane obszary aktywności), jak i podmiotowego (działania podejmowane przez organy władzy publicznej).

Prawo UE nie ma zastosowania do działań własnych podejmowanych przez organy państwowe – takie jak związane z pozyskiwaniem danych w wyniku podsłuchu łączności elektronicznej. W efekcie – na podstawie art. 35 ust. 5 TUE w brzmieniu obowiązującym przed traktatem lizbońskim – TSUE nie był właściwy w sprawie oceny zgodności z prawem lub proporcjonalności działań policji bądź innych organów ścigania jednego z państw członkowskich ani wykonywania przez państwa członkowskie obowiązków dotyczących utrzymania porządku publicznego i ochrony bezpieczeństwa wewnętrznego. Obecnie, wraz z likwidacją podziału na trzy filary funkcjonowania UE, wyłączenie stosowania prawa UE w obszarze działalności organów państwowych w zakresie prowadzonych działań inwigilacyjnych może być uzasadniane przesłankami wskazanymi w omówionym wcześniej art. 4 ust. 2 TUE.

Prawo UE znajduje jednak praktyczne zastosowanie w zakresie zobowiązań nakładanych przez normy prawa krajowego na przedsiębiorców, także związanych z ogólnym obowiązkiem retencji danych. Kwestia interpretacji obowiązku retencji danych, jego zakresu oraz zgodności z prawe UE jest od wielu lat jest przedmiotem badań Trybunału – zarówno w sprawach dotyczących wprost zagadnienia retencji jako elementu prawa UE (sprawa DRI⁸⁸⁶), jak i spraw dotyczących transatlantyckiego przepływu danych (sprawa Schrems⁸⁸⁷) czy

---

⁸⁸⁴ Wyrok TSUE z 6.11.2003 w sprawie Lindqvist, sygn. C-101/01, pkt 43–44.
⁸⁸⁵ Wyrok TSUE z 29.01.2008 w sprawie Promusicae, sygn. C-275/06, pkt 51.
⁸⁸⁶ Omówienie wyroku w sprawie DRI: rozdział 2.4.3, s. 75.
⁸⁸⁷ Omówienie wyroku w sprawie Schrems: rozdział 2.4.3, s. 77.
międzynarodowej współpracy w zakresie wymiany danych PNR (opinia w projektu umowy sprawie UE – Kanada888). W każdym przypadku Trybunał podkreślał znaczenie proporcjonalności jako niezbędnej przesłanki do uznania za uzasadnioną ingerencję w prawo do prywatności. Wniosek ten wywodził wprost z art. 52 ust. 1 KPP oraz norm prawa wtórnego – w szczególności art. 15 ust. 1 dyrektywy 2002/58. Normy te pozwalały na określenie następujących kryteriów, jakie musi spełniać środek wkraczający na sferę prywatności, aby można go było uznać za nienaruszający prawa UE:

1) spełnienie zasady proporcjonalności,

2) spełnienie zasady konieczności (KPP), określonej w dyrektywie 2002/58 jako „niezbędność”,

3) rzeczywista realizacja celu interesu ogólnego uznawanego przez Unię lub potrzeby ochrony praw i wolności innych osób.

Zaznaczyć należy przy tym, że o ile warunki stosowania ograniczeń wskazane w KPP dotyczą wszelkich środków wprowadzanych w prawie krajowym, to warunki określone i wprowadzane na mocy art. 15 ust. 1 dyrektywy 2002/58 są ograniczone do środków służących „zapewnieniu bezpieczeństwa narodowego (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej”.

Nie budzi wątpliwości, że wykrywanie najpoważniejszym przestępstw i zapobieganie im jest celem ogólnym uznawanym przez Unię. Jak wskazał TSUE w sprawie Inuit, „ochrona bezpieczeństwa narodowego i porządku publicznego (...) rzeczywiste realizuje uznawany przez Unię cel interesu ogólnego”889. W efekcie także podejmowanie działań, służących realizacji tego celu, należy uznać za spełniające ostatnią ze wskazanych przesłanek. Tym niemniej podkreślić należy, że użyteczność określonych środków nie przesądza o konieczności ich zastosowania. W szczególności działanie może prowadzić do osiągnięcia celu, ale jednocześnie nie spełniać kryterium „konieczności”. W tym miejscu przywołać należy wcześniejsze rozważania na temat zakresu pojęcia ścisłej konieczności, ustanowione przez ETPC w swojej linii orzecniczej związanej z oceną legalności programów tajnej inwigilacji. Działanie, które nie jest konieczne, a więc prowadzące do efektu, który można uzyskać innymi, mniej inwazyjnymi środkami, nie może być uznanne za proporcjonalne. Wniosek ten potwierdził TSUE, wskazując, że „zgodnie z utrwalonym

888 Zob. rozdział 4.6.2 (s. 197).
orzecznictwem ochrona prawa podstawowego do prywatności wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia trzymały się w granicach tego, co absolutnie konieczne"890. Rozpatrując okoliczności stosowania ogólnego obowiązku retencji danych, wprowadzonego do prawodawstwa Unii przez dyrektywę 2006/24, TSUE wskazał, że środek tego nie można uznać za spełniającego kryterium konieczności – skoro prowadzi do gromadzenia danych nie mających żadnego związku z celem przetwarzania (ochroną przed najpoważniejszą przestępczością)891.

Omawiając przyczyny niezgodności ogólnego obowiązku retencji, Trybunał przywołał okoliczności i argumenty opisujące de facto każdy program nieukierunkowanego gromadzenia danych: „[Ogólna retencja danych] nie wymaga istnienia żadnego związku między danymi, które mają być zatrzymywane, a zagrożeniem dla bezpieczeństwa publicznego; w szczególności dyrektywa nie ogranicza się do zatrzymywania danych związanych albo z określonym czasem, określonym obszarem geograficznym lub określonym kręgiem osób mogących, w taki czy inny sposób, mieć związek z poważnym przestępstwem, albo osobami, których zatrzymane dane z innych powodów mogłyby przyczynić się do zapobiegania poważnym przestępstwom oraz ich wykrywania lub ścigania”892.

Wyrok w sprawie DRI zawiera jeszcze jeden, bardzo istotny wniosek, mający z kolei zastosowanie do transgranicznego przekazywania danych pozyskiwanych w wyniku stosowania programów inwigilacyjnych przez państwo – konieczność zatrzymywania danych na obszarze Unii, tak aby w pełni zagwarantowane było poszanowania wymogów ochrony bezpieczeństwa wynikających z prawa UE oraz możliwość przeprowadzenia kontroli przez niezależny organ893 w zakresie, w jakim wynika to z art. 8 ust. 2 KPP894. W ten sposób Trybunał odniósł się do kwestii współpracy ponadnarodowej w obszarze budowania wspólnych programów inwigilacyjnych przesądzając, że działania takie – o ile będą w ogóle mogły uznanne za zgodne z prawem UE (a więc spełniające przesłanki konieczności i proporcjonalności, co z koleiimplikuje ich ukierunkowany charakter) – muszą dodatkowo być realizowane w sposób zapewniający stosowanie prawa Unii.

Wszelkie wątpliwości związane z możliwością funkcjonowania w państwach członkowskich UE prawnego obowiązku retencji danych zostały rozstrzygnięte w wyroku wydanym w sprawie Tele2, w którym Trybunał wprost odniósł się do zakresu dopuszczalnych

890 Wyrok TSUE z 7.11.2013 w sprawie IPI, sygn. C-473/12, p. 39.
891 Wyrok TSUE w sprawie Digital Rights Ireland, op. cit., p. 58.
892 Ibidem, p. 59.
893 Dalsze rozważania o roli niezależnego organu nadzoru w unijnych przepisach o ochronie danych przedstawiono w rozdziale 4.5.4 (s. 173).
894 Wyrok TSUE w sprawie Digital Rights Ireland, op. cit., p. 68.
przepisów krajowych stwierdzając, że art. 52 ust. 1 (wymóg proporcjonalności i konieczności) stoi na przeszkodzie uregulowaniu krajowemu przewidującemu do celów zwalczania przestępczości uogólnione i nieróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej.

Z kolei w opinii 1/15 dotyczącej zgodności z prawem UE projektu umowy międzynarodowej pomiędzy UE a Kanadą dotyczącej przekazywania danych PNR Trybunał podjął temat zakresu przetwarzania danych gromadzonych przez organy władzy publicznej do podejmowania automatycznych decyzji w oparciu o nieprzejrzyste algorytmy. Na tym tle TSUE podkreślił znaczenie stosowania weryfikowalnych modelli przetwarzania danych, jak i bazowania na informacjach aktualnych i wiarygodnych, tak aby zminimalizować ryzyko błędu w ocenie zagrożeń.

Jakkolwiek tłem powyższych rozważań było przetwarzanie danych PNR, to wnioskowanie przedstawione przez Trybunał można odnieść do każdego przetwarzania informacji przez podmioty publiczne, których celem jest ocena jednostki lub budowanie wiedzy na jej temat z wykorzystaniem korelowania informacji z wielu baz danych. W rzeczywistości zatem wskazane obserwacje mają bezpośrednie zastosowanie do każdego programu tajnej inwigilacji.

Co więcej, wydając opinię w sprawie projektowanej umowy dotyczącej przekazywania danych PNR do Kanady, Trybunał odniósł się pośrednio także do innego aspektu funkcjonowania programów masowej inwigilacji obywateli, jakim jest nieprzejrzystość procedury dalszego przetwarzania i udostępniania danych, wskazując, że "uregulowanie Unii nie może ograniczać się do stawiania wymogu, by dostęp do rzeczonych danych odpowiadał jednemu z celów tego uregulowania, lecz powinno również określać materialne i formalne przesłanki regulujące takie wykorzystywanie."

Pamiętając o normie wynikającej z art. 53 ust. 3 KPP – a więc de facto związaniu TSUE zakresem orzeczeń wydanych przez ETPC w odniesieniu do warunków i granic stosowania prawa do ochrony prywatności (art. 7 KPP) – powyższy wniosek jest zgodny z prezentowanym w linii orzecznikiej ETPC, zwłaszcza w zakresie uwzględnienia w prawie ustanawiającym ramy dla prowadzonych programów inwigilacyjnych zabezpieczeń proceduralnych zapobiegających nadużyciu władzy. Przypominając także wcześniejsze

895 Wyrok TSUE w sprawie Tele2 Sverige AB, op. cit., p. 112.
896 Zob. przypis 587.
897 Ibidem, p. 192.
rozważania przedstawione w rozdziale 2.4.4, warto wskazać, że Trybunał zauważył, że europejska konwencja do czasu przystąpienia do niej Unii nie stanowi aktu prawnego formalnie obowiązującego w porządku prawnym Unii. Wynika z tego, że art. 53 ust. 3 KPP nie ogranicza swobody wyrokowania TSUE, a jedynie służy zapewnieniu spójności orzecznictwa obu trybunałów – inny bowiem wniosek mógłby mieć „negatywny wpływ na autonomię prawa Unii i Trybunału Sprawiedliwości Unii Europejskiej”.

Podsumowując, w ocenie Trybunału stosowanie środków polegających na nieukierunkowanym i nieograniczonym gromadzeniu danych stanowi nieproporcjonalną ingerencję w prawa podstawowe, a w efekcie jest niezgodne z prawem UE. Wniosek ten dotyczy każdego działania, także wynikającego z prawa krajowego, którego skutkiem jest zatrzymywanie wszystkich danych – nawet jeżeli jego zakresem objęte są tylko metadane. Co więcej, Trybunał zdefiniował ramy, w jakich powinny funkcjonować programy inwigilacji, aby nie prowadziły do naruszenia prawa UE. Co oczywiste, są one zgodne z omówionymi wcześniej uwagami ETPC, jednak w niektórych obszarach zawierają bardziej precyzyjne wytyczne.

Podkreślania wymaga, że przytoczone wyżej orzecznictwo TSUE – z uwagi na zakres stosowania prawa UE – ma zastosowanie wyłącznie do zakazu stosowania technik nieukierunkowanego gromadzenia danych w zakresie nieobjętym zastosowaniem wyłączenia z art. 4 ust. 2 TUE, a więc nierealizowanym bezpośrednio przez organy władzy publicznej. Wyroki te z jednej strony prowadzą zatem do zakazu hurtowego gromadzenia danych przez operatorów telekomunikacyjnych, jednocześnie jednak nie stanowią wystarczającego środka prawnego uniemożliwiającego gromadzenie danych bezpośrednio przez służby specjalne.

Z drugiej strony, TSUE ma kognicję w zakresie oceny działań instytucji UE dotyczących współpracy międzynarodowej, także w zakresie wymiany danych. W efekcie Trybunał może analizować zgodność z prawem mechanizmów komercyjnego transferu danych i przy tej okazji oceniać, czy zastosowano wystarczające zabezpieczenia powodujące, że państwo trzecie, do którego następuje ekspor danych nie może wykorzystać przekazywanych informacji w tajnych programach inwigilacyjnych. Również kontrola sprawowana przez TSUE nad umowami międzynarodowymi zawieranymi przez UE, jak w przypadku projektowanej umowy z Kanadą, pozwala na niedopuszczenie do obrotu prawnego regulacji naruszającej prawa podstawowe mieszkańców UE. W efekcie, chociaż kognicja Trybunału w sprawach dotyczących programów inwigilacji jest ograniczona, to jednak nadal

899 Wyrok TSUE w sprawie Staatssecretaris van Veiligheid en Justitie, op. cit., p. 47.
instytucja ta ma silne narzędzia oddziaływania na państwa członkowskie w zakresie przestrzegania praw podstawowych w zakresie wynikającym z regulacji unijnych.

Przenosząc te rozważania na opisane wcześniej programy inwigilacyjne, nadal nie jest jasne, w jakim zakresie orzecznictwo TSUE przesądza o zakazie współpracy przedsiębiorców telekomunikacyjnych z uprawnionymi organami w zakresie umożliwienia tym drugim realizacji programów masowej inwigilacji. Pamiętając, że TSUE nie jest właściwy do orzekania o ważności prawa krajowego, problem ten powinien być rozstrzygnięty przez właściwe sądy krajowe oraz ustanowione krajowe organy nadzoru danych osobowych. W szczególności w systemie europejskim rolą organów nadzoru jest podejmowanie działań zapewniających przestrzeganie prawa zarówno przez przedsiębiorstwa komercyjne (w tym wypadku – operatorów telekomunikacyjnych), jak i przez podmioty sektora publicznego. Akceptowanie stanu, w którym niejawnąność pracy służb specjalnych będzie wystarczającym uzasadnieniem do braku możliwości sądowego kwestionowania legalności podejmowanych działań, prowadzi do podważeniaasad, na których ustanowiona została Unia i które stanowią fundament funkcjonowania państw demokratycznych.

8.4.3. Przepisy krajowe i ich zgodność z normami międzynarodowymi

Omówienie regulacji prawnych dotyczących programów tajnej inwigilacji zakładających nieukierunkowane i hurtowe gromadzenie danych należy podsumować, przedstawiając analizę krajowego prawodawstwa. Szczególnie interesujące może być porównanie standardów oceny legalności działań inwigilacyjnych państw wypracowanych przez EKPC i TSUE w odniesieniu do prawa stanowionego w Polsce.

W pierwszej kolejności należy omówić regulacje związane z ogólnym obowiązkiem retencji danych. Zgodnie z art. 180a ustawy – Prawo telekomunikacyjne (dalej: pr. tel.) operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt zatrzymywać i przechowywać dane potrzebne do ustalenia stron komunikacji, daty i czasu połączenia oraz lokalizacji urządzenia końcowego, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia. Przepis ten stanowi, że po zakończeniu okresu przechowywania dane powinny być niszczone, za wyjątkiem tych, które zostały zabezpieczone, zgodnie z

---

900 Ustawa z 16 lipca 2004 roku – Prawo telekomunikacyjne (Dz.U. Nr 171, poz. 1800 ze zm.).
przepisami odrębnymi. Wskazany przepis został wprowadzony do krajowego porządku prawnego jako implementacja dyrektywy retencyjnej (dyrektywa 2006/24)901.

Jak wcześniej wskazano, TSUE w wyroku DRI stwierdził nieważność dyrektywy retencyjnej. Jednocześnie wskazał, że wprowadzenie środka związanego z gromadzeniem danych opisujących korzystanie z usług łączności elektronicznej przez wszystkich abonentów, bez zastosowania żadnego wyróżnika pozwalającego uzasadnić zbierane dane prowadzonymi postępowaniami lub realnymi zagrożeniami dla bezpieczeństwa publicznego, prowadzi do nieproporcjonalnej ingerencji, a w konsekwencji do naruszenia praw wynikających z KPP. Zgodnie z dominującym w doktrynie poglądem stwierdzenie nieważności dyrektywy wydane w trybie prejudycjalnym nie prowadzi do wycofania kwestionowanych przepisów z porządku prawnego892. Trybunał nie ma też kompetencji do stwierdzania nieważności przepisów krajowych. W efekcie wydanie orzeczenia w sprawie DRI nie skutkowało automatycznym wycofaniem z obiegu prawnego przepisów krajowych implementujących ogólne obowiązek retencji danych.

Orzeczenie TSUE stanowiło jednak oczywistą wykładnię prawa UE, na podstawie której właściwe sądy krajowe mogły orzec o niezgodności przepisów wprowadzających ogólne obowiązek retencji danych czego skutkiem byłoby wycofanie kwestionowanych regulacji z obiegu prawnego. Procedura taka została zastosowana w wielu państwach członkowskich UE jeszcze przed wydaniem orzeczenia w sprawie DRI i doprowadziła do uznania przepisów krajowych za niezgodnych z ustawą zasadniczą903. W innych państwach przepisy wprowadzające ogólne obowiązek retencji zostały wycofane z obiegu prawnego już po wyroku TSUE w sprawie DRI. Natomiast w przypadku Szwecji i Wielkiej Brytanii na skutek pytań prejudycjalnych sprawa zgodności krajowych przepisów z prawem UE została skierowana do rozstrzygnięcia przez TSUE. Jak wcześniej wskazano, w sprawie Tele2 Trybunał przesądził, że art. 7 i 8 w zw. z art. 52 ust. 1 stoi na przeszkodzie uregulowaniu krajowego wprowadzającemu ogólne obowiązek retencji danych904. O ile zatem wyrok DRI...
odnosił się do ważności norm prawa UE, to już wyrok w sprawie Tele2 wprost odwołuje się do możliwości istnienia krajowych przepisów takich, jak określone w art. 180a pr. tel.

Wyroki Trybunału, także wydane w trybie prejudycjalnym, mają nie tylko skutek inter partes ale i erga omnes. Oznacza to, że poza rozstrzygnięciem problemu prawnego w sporze, który stał się przyczyną skierowania wniosku do TSUE, stanowią ponadto powszechnie obowiązującą interpretację prawa UE. Przy czym orzeczenia TSUE – zgodnie z zasadą lojalnej współpracy (art. 4 ust. 3 TUE) – wiążą wszystkie instytucje państw członkowskich, a więc nie tylko władzę sądowniczą, ale też wykonawczą i prawodawczą. W takim rozumieniu stanowienie prawa, które w sposób oczywisty naruszy normy UE, prowadzi do deliktu (naruszenia zobowiązań traktatowych) ze strony państwa członkowskiego. Co więcej, nawet jeżeli przepisy tego rodzaju zostałyby uchwalone, to jako niezgodne z prawem wyższego rzędu, nie powinny być stosowane przez sądy krajowe w sprawach przed nimi zjawiskiem. Środkiem, który sąd krajowy powinien zastosować w przypadku pojawienia się wątpliwości, czy istniejące orzeczenia TSUE stanowią wystarczającą podstawę do rozstrzygnięcia określonego problemu prawnego, jest zadanie pytania prejudycjalnego. Rozważania te prowadzą do konkluzji, że brak skierowania przez sąd krajowy wniosku w trybie prejudycjalnym oraz wydanie prawomocnego orzeczenia niezgodnego z wcześniejszymi wyrokami TSUE także skutkuje powstaniem deliktu ze strony państwa członkowskiego (por. art. 267 zd. 3 TFUE).

Przenosząc te rozważania na grunt ogólnego obowiązku retencji danych nadal funkcjonującego na gruncie ustawy – Prawo telekomunikacyjne, stwierdzić należy, że z uwagi na orzeczenia w sprawach DRI oraz Tele2 przepisy te powinny zostać niezwłocznie uchylone. Co więcej, nawet w przypadku braku działań prawodawcy lub sądu konstytucyjnego, przepisy art. 180a i n. powinny być pomijane w rozstrzygnięciach dokonywanych przez sądy powszechne jako niezgodne z prawem UE. W efekcie dalsze funkcjonowanie omawianej regulacji w obiegu prawnym przyczynia się do naruszenia zasady pewności prawa. 905

Problem ten został rozpoznany przez Rzecznika Praw Obywatelskich, który w piśmie z 1 lutego 2017 skierowanym do Minister Cyfryzacji zadał pytanie o planowane działania związane z dostosowaniem prawa krajowego do standardów wyznaczonych w przywołanych wyrokach Trybunału oraz o zajęcie stanowiska w sprawie zgodności przepisów pr. tel. oraz

905 Na problem związany z nie zapewnianiem przez prawo polskie standardu sformułowanego w wyroku TSUE wydanego w sprawie Tele2 zwraca także uwagę A. Lach w: Obowiązek retencji danych telekomunikacyjnych i udostępniania tych danych organom ścigania, Monitor Prawniczy 2017, nr 11, s. 614.
aktów wykonawczych przyjętych w celu implementacji dyrektywy reencyjnej, z przepisami KPP po wyroku TSUE w sprawie Tele2.

Odrębnym zagadnieniem jest kwestia kompetencji uprawnionych organów w gromadzeniu i dalszym przetwarzaniu danych. W ostatnich latach krajowy prawodawca wprowadził dwie ważne regulacje, dotyczące omawianego obszaru:

- ustawę o zmianie ustawy o Policji oraz niektórych innych ustaw (zwana dalej „ustawą inwigilacyjną“)
- ustawę o działaniach antyterrorystycznych (zwaną dalej „ustawą antyterrorystyczną“).

Jak zauważyła D. Nadazdin, szefowa Amnesty International Polska: „obie ustawy razem zezwalają na praktycznie nieograniczony dostęp władz państwowych do informacji z życia prywatnego nie tylko cudzoziemców, ale i polskich obywateli”. W pracy poświęconej ochronie prywatności w cyberprzestrzeni konieczne jest przeanalizowanie i odniesienie się do regulacji wprowadzanych w każdym ze wskazanych aktów.

Ustawa inwigilacyjna została wprowadzona w związku ze stwierdzeniem przez TK w wyroku K 23/11 niezgodności z konstytucją ówczesnych przepisów oraz bliskim upływem terminu utraty przez nie mocy. Z punktu widzenia możliwości prowadzenia tajnych programów inwigilacji, w szczególności zakładających nieukierunkowane gromadzenie danych, istotną zmianą wprowadzoną ustawą była zmiana przepisów kompetencyjnych regulujących dostęp do danych o użytkownikach określonych w poszczególnych ustawach sektorowych (określających zasady funkcjonowania poszczególnych służb – Policji, ABW, AW, ŻW i innych). I tak zgodnie z nowym brzmieniem art. 20c ustawy o Policji służba ta może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

1) art. 180c i art. 180d pr. tel. („dane telekomunikacyjne”),
2) art. 82 ust. 1 pkt 1 ustawy - Prawo pocztowe („dane pocztowe”),
3) art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną („dane internetowe”).

906 Ustawa z 15.01.2016 o zmianie ustawy o Policji oraz innych ustaw (Dz.U. z 2016 r. poz. 147).
907 Ustawa z 10.06.2016 o działaniach antyterrorystycznych (Dz.U. z 2016 r. poz. 904 ze zm.).
910 Ustawa z 6.04.1990 o Policji (Dz.U. z 1990 Nr 30, poz. 179 ze zm.).
911 Ustawa z 23.11.2012 – Prawo pocztowe (Dz.U. z 2012 r. poz. 1529 ze zm.).
Pozyskane w ten sposób dane mogą być przetwarzane bez wiedzy i zgody osoby, której dotyczą. Uwagę zwraca rozszerzenie – względem wcześniej obowiązujących przepisów – zakresu udostępnianych informacji. Nowością są w szczególności dane internetowe, które na mocy przywołanego artykułu ustawy o świadczeniu usług drogą elektroniczną obejmują szeroki zestaw danych i informacji związanych z wykorzystaniem usług przez abonenta. W szczególności zgodnie z art 18 ust. 4 dane te mogą obejmować informacje wykorzystywane na potrzeby profilowania użytkowników i to także po zakończeniu umowy z usługodawcą (por. art. 19 ust. 2 pkt 2). Co więcej, art. 18 ust. 5 stanowi, że dane gromadzone i przetwarzane przez usługodawcę w związku ze świadczeniem usług drogą elektroniczną mogą także obejmować szczegółowe informacje o zakresie korzystania z usług, w tym oznaczenia identyfikujące abonenta, strony komunikacji oraz czasie i zakresie korzystania z usług. Pamiętając, że informacje te dotyczą łączności elektronicznej (np. korzystania z Internetu), powstaje pytanie, w jaki sposób usługobiorca, gromadząc szeroki zakres danych, wynikający z art. 18 ust. 1-5, ma jednocześnie zapewnić, że informacje przekazywane uprawnionym organom (np. Policji – na podstawie art. 20c ust. 1 pkt 3) będą zawierały wyłącznie „dane niestanowiące treść przekazu”. Prawodawca nie doprecyzował tego zagadnienia, a ma ono kluczowe znaczenie dla ochrony prywatności użytkowników. O ile bowiem np. treść wiadomości e-mail stanowi merytoryczną treść przekazu, to już nie jest oczywiste, co powinno być traktowane jako taka treść w przypadku korzystania ze stron internetowych – czy nazwa odwiedzanych stron, treści wprowadzane do wyszukiwarki internetowej, czy dane pobierane z Internetu. Pamiętając, że zgodnie z art. 20c ustawy o Policji organ może przetwarzać dane bez wiedzy i zgody osoby zainteresowanej, brak wiedzy o dopuszczalnym zakresie stosowania działań inwigilacyjnych państwa w sposób oczywisty prowadzi do kolizji ze standardem „przewidywalności” prawa wyznaczonym przez ETPC913. Sytuacja, w której wprowadzane są przepisy ustawowe nieprecyzuje zakres udostępnianych służbom informacji, może prowadzić do stworzenia po stronie użytkowników (potencjalnie – całego społeczeństwa) przesądzenia, że każde działanie może być monitorowane i oceniane, co z kolei było wskazane przez TSUE jako jedna z przyczyn stwierdzenia niezgodności dyrektywy retencyjnej z prawem UE914.

Dodatkowe obawy budzą przesłanki zastosowania technik wynikających z art. 20c ustawy o Policji. Pierwotne brzmienie przepisu, wskazujące na przypadki „zapobiegania lub

---

913 Zob. rozważania na ten temat w rozdziale 8.4.1 (s. 338).
914 Wyrok TSUE w sprawie Digital Rights Ireland, op. cit., p. 37.
wykrywania przestępstw”, zostały rozszerzone o sytuacje związane z „ratowaniem życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych”. Brak wymagania, aby działania inwigilacyjne były związane z określonymi osobami lub kręgiem osób, a także konkretnymi, weryfikowalnymi podejrzeniami związanymi z poważnymi przypadkami naruszenia prawa prowadzi do dalszego rozszerzenia kręgu osób, które mogą być poddane inwigilacji. W rzeczywistości Policja nie jest ograniczona żadnymi przesłankami i może zastosować mechanizmy wynikające z art. 20c względem każdej osoby i w szerokim zakresie (dane telekomunikacyjne, pocztowe, internetowe). Co więcej, ustawodawca, wprowadzając nowe regulacje, nie zadbał nawet o spójność z innymi przepisami – zgodnie z art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną usługodawca udostępnia dane uprawnionym organom państwa na potrzeby prowadzonych przez nie postępowań. Wymogu prowadzonych postępowań nie wprowadzono do art. 20c ustawy o Policji.

Jednocześnie ze zmianą (wzmocnieniem) uprawnień służb w dostępie i gromadzeniu danych dotyczących łączności elektronicznej ustawodawca przewidział możliwość pobierania tych danych w sposób elektroniczny za pośrednictwem dedykowanych systemów informatycznych. W ten sposób dane określone w art. 20c mogą być pozyskiwane bez angażowania pracowników przedsiębiorcy zobowiązanego do ich udostępniania, co w szczególności oznacza, że także bez potrzeby przedstawiania dodatkowych upoważnień czy zezwoleń. W ten sposób zniesione zostało też proceduralne zabezpieczenie związane z koniecznością wydania zgody na zastosowanie środków wynikających z art. 20c. Możliwość pobierania informacji zdalnie za pośrednictwem sieci telekomunikacyjnej jest kolejnym czynnikiem zwiększającym ryzyko nadejścia władzy. Dodatkowo połączenie informatyczne pomiędzy systemem gromadzącym informacje (administrowanym przez zobowiązanej przedsiębiorcę) oraz systemem, w którym informacje te są następnie przewarzane (administrowanym przez upoważniony organ), powoduje, że istnieje techniczna możliwość pobierania dużej ilości danych (teoretycznie – wszystkich dostępnych), a w efekcie zbudowania w oparciu o mechanizm wynikających z art. 20c ustawy o Policji (oraz analogiczne przepisy określone w pozostałych ustawach regulujących działanie innych służb) programu masowej inwigilacji. Co więcej, z uwagi na brak jakichkolwiek zabezpieczeń proceduralnych wynikających z przepisów ustawowych, dalsze przekazywanie tych danych (do innych organów, ale i np. podmiotów zagranicznych) nie wymaga zgody niezależnego

915 Tak: A. Lach, Obowiązek retencji danych..., op. cit., Monitor Prawniczy 2017, nr 11, s. 615.
organu sądowego. Teoretycznie zatem przepisy ustawy inwigilacyjnej zbudowały nie tylko ramy do prowadzenia programów masowej inwigilacji, ale również umożliwiają przekazywanie gromadzonych danych obwym służbom specjalnym. W tym kontekście niezrozumiałe brzmi przepis art. 20c ust. 6, zgodnie z którym dane niemające znaczenia dla postępowania karnego podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu. Ustawodawca nie określił ani czasu, w jakim powinno nastąpić ustalenie, czy dane mają znaczenie procesowe, ani środków ich „protokolarnego” zniszczenia (co nie jest zadaniem oczywistym – zwłaszcza w przypadku danych pozyskanych w sposób elektroniczny). Nie jest także jasne, dlaczego przesłanka przydatności dla postępowania karnego nie jest oceniana przed pobraniem informacji, co znacząco ogranicza ryzyko nadużycia władzy oraz zwiększyłoby skuteczność następnej kontroli sądowej.

Ustawą inwigilacyjną nadano podobne uprawnienia również innym organom ścigania, do których należą: Agencja Bezpieczeństwa Wewnętrznego\(^916\), Straż Graniczna\(^917\), Centralne Biuro Antykorupcyjne\(^918\), Służba Celna\(^919\), Służba Kontrwywiadu Wojskowego\(^920\), Żandarmeria Wojskowa\(^921\) i wywiad skarbowy\(^922\). Przypominając wcześniejszą analizę programów masowej inwigilacji, w szczególności podejrzenia związane z prowadzeniem wspólnych programów przez polskie i amerykańskie służby specjalne (nazwa kodowa ORANGECRUSH\(^923\)), nowe uprawnienia dają szerokie możliwości nieukierunkowanego gromadzenia danych przez siedem różnych uprawnionych podmiotów. Powstaje oczywiste pytanie o zasadność aż takiego rozbudowania aparatu kontroli i monitorowania obywateli, np. o faktyczną potrzebę (prowadzącą do spełniania przesłanki konieczności i proporcjonalności) nadania szerokich uprawnień dla Służby Celnej czy Straży Granicznej związanych z gromadzeniem danych telekomunikacyjnych czy internetowych względem wszystkich obywateli\(^924\). W dalszej kolejności konieczne jest wyjaśnienie, w jaki sposób prawodawca

\(^{916}\) Zob. art. 28 ustawy z 24.05.2002 o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2016 r. poz. 1897 ze zm.).

\(^{917}\) Zob. art. 10b ustawy z 12.10.1990 o Straży Granicznej (Dz.U. z 2014 r. poz. 1402 ze zm.).

\(^{918}\) Zob. art. 18 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2016 r. poz. 1310 ze zm.).

\(^{919}\) Zob. art. 75d ustawy z 27.08.2009 o Służbie Celnej (Dz.U. z 2016 r. poz. 1799 ze zm.).

\(^{920}\) Zob. art. 32 ustawy z 9.06.2006 o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2016 r. poz. 1318 ze zm.).

\(^{921}\) Zob. art. 30 ustawy z 24.08.2001 o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. z 2016 r. poz. 96).

\(^{922}\) Zob. art. 36bb ustawy z 28.09.1991 o kontroli skarbowej (Dz.U. z 2015 r. poz. 553 ze zm.).

\(^{923}\) Zob. rozdział 8.3.2 (s. 330).

\(^{924}\) Zgodnie z informacjami otrzymanymi od Straży Granicznej przez Fundację Panoptikon do początku lutego 2017 (a więc przez pierwszy rok obwiązywania przepisów znowelizowanych ustawą inwigilacyjną) Straż Graniczna zawarła pięć porozumień z przedsiębiorstwami telekomunikacyjnymi, na podstawie których może za pośrednictwem łączy informatycznych pobierać dane bezpośrednio z systemów operatora.
zapewnił możliwość skutecznej kontroli tak rozbudowanych kompetencji, będących w posiadaniu szerokiego kręgu podmiotów uprawnionych.

Zgodnie z art. 20ca ust. 1 ustawy o Policji (oraz analogicznymi przepisami w ustawach regulujących funkcjonowanie pozostałych służb) kontrolę nad uzyskiwaniem danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby podmiotu, któremu udostępniono te dane. Jest to jednak kontrola następca, przeprowadzana w okresach półrocznych (art. 20ca ust. 2) i na podstawie zbiorczych statystyk przekazanych przez uprawniony podmiot. Powstaje zasadnicze pytanie, w jaki sposób sąd może obiektywnie ocenić legalność działań organu – zwłaszcza w odniesieniu do spełnienia przesłanek uzasadniających skorzystanie z uprawnień inwigilacyjnych – bazując wyłącznie na jego oświadczeniach i przekazywanych statystykach. W tym zakresie prawodawca przewidział, że sąd może (ale nie musi) zapoznać się z materiałami uzasadniającymi udostępnienie danych telekomunikacyjnych, pocztowych lub internetowych (art. 20ca ust. 3). Z uwagi na co do zasady tajny charakter stosowanej kontroli oraz brak poinformowania (nawet następczego) podmiotu danych o fakcie jej przeprowadzenia osoby poddane inwigilacji nie mają żadnych prawnych środków dochodzenia zadośćuczynienia za naruszenie swoich praw. Co więcej, ocena działania organów na podstawie statystyk przez nich przedstawianych nie prowadzi do ograniczenia ryzyka nadużycia władzy. Z informacji zgromadzonych w raporcie Fundacji Panoptykon, dotyczącego omówienia skutków wprowadzenia ustawy inwigilacyjnej, wskazano, że sądy okręgowe swoje uprawnienia kontrolne realizują wyłącznie na podstawie przedstawionych informacji zbiorczych i bez analizy materiałów dotyczących indywidualnych spraw.925

Powyższe niejasności stały się przyczyną skierowania przez Rzecznika Praw Obywatelskich 18 lutego 2016 roku wniosku o stwierdzenie niezgodności z Konstytucją znowelizowanych w następstwie wejścia w życie ustawy inwigilacyjnej przepisów ustawy o Policji i innych ustaw stanowiących podstawę funkcjonowania służb926. W szczególności RPO wniósł o zbadanie zgodności art. 20c ust. 1 (uprawnienie dostępu do danych), art. 20c ust. 3 (zawieranie porozumień ze zobowiązanymi przedsiębiorcami w zakresie przekazywania danych) oraz art. 20ca (kontrola sądowa) ustawy o Policji oraz odpowiedników wskazanych przepisów w pozostałych ustawach stanowiących podstawę funkcjonowania pozostałych

---

925 Fundacja Panoptykon, Rok z ustawą inwigilacyjną, https://goo.gl/MaB7ZR, s. 6.
służb z wzorcem kontroli, jakim jest art. 2, 30, 47, 49, 51 ust. 2 w zw. z art. 31 ust. 3 Konstytucji, art. 8 EKPC oraz art. 7 i 8 w zw. z art. 52 ust. 1 KPP. W rozbudowanej analizie Rzecznik podkreślił, że wprowadzane zmiany co do zasady prowadzą do zwiększenia uprawnień służb, nie wiążąc jednak możliwości ich zastosowania z prowadzonymi postępowaniami karnymi927.

Dalsze zwiększenie kompetencji służb specjalnych, w szczególności ABW, związane jest z wejściem w życie ustawy o działaniach antyterrorystycznych. W szczególności zgodnie z art. 11 pkt 1 ustawy Szef ABW może nieodpłatne uzyskać dostęp do danych i informacji zgromadzonych w rejestrach publicznych i ewidencjach prowadzonych przez wszystkie inne uprawnione organy i służby, a także pochodzące z enumeratywnie wymienionych podmiotów sektora publicznego – wśród których znajdują się Zakład Ubezpieczeń Społecznych oraz Kasa Rolniczego Ubezpieczenia Społecznego. W efekcie ABW może uzyskać dostęp do szczegółowych danych o osobach ubezpieczonych, wraz z informacjami o ich stanie zdrowia, a więc danych wrażliwych w rozumieniu przepisów o ochronie danych osobowych. W ustawie oraz w przedstawionym uzasadnieniu projektu928 brakuje wskazania przyczyny uwzględnienia w katalogu podmiotów zobowiązanych do udostępniania danych ZUS i KRUS. Nie przewidziano także żadnych ograniczeń w zakresie udzielanych informacji ani nie powiązano wystąpienia z wnioskiem o udzielenie informacji z koniecznością istnienia rzeczywistej potrzeby wynikającej z prowadzonych postępowan w karnym. Ustawodawca nie przewidział też, aby realizacja nowych uprawnień ABW ograniczona była zasadą konieczności czy proporcjonalności.

Dodatkowe wątpliwości pod kątem zgodności ze standardami wyznaczanymi orzecznictwem ETPC i TSUE budzi regulacja wprowadzona art. 9 ust. 1, zgodnie z którą Szef ABW może – bez zgody sądu i prokuratury – zarządzić wobec osoby niebędącej obywatelem Rzeczpospolitej Polskiej na okres nie dłuższy niż 3 miesiące niejawne prowadzenie czynności polegających między innymi na uzyskiwaniu i utrwalaniu treści rozmów, obrazu i dźwięku, korespondencji oraz danych zawartych na informatycznych nośnikach danych. Przesłanką do zastosowania kontroli jest rozpoznanie, zapobieganie lub zwalczanie przestępstw o charakterze terrorystycznym. Biorąc pod uwagę szeroki zakres uprawnień, ingerujących w każdą sferę życia prywatnego, brak (także następczej) kontroli sądowej oraz ogólne przesłanki stosowania (w szczególności brak wymagania prowadzenia konkretnego

927 Ibidem, s. 8-9.
928 Rządowy projekt ustawy o działaniach antyterrorystycznych oraz o zmianie niektórych innych ustaw, druk sejmowy 516.
postępowania karnego – nawet na etapie in rem) prowadzi do naruszenia standardów wypracowanych w orzecznictwie ETPC. Ograniczenie zakresu stosowania uprawnienia wynikającego z art. 9 do osób niemających polskiego obywatelstwa prawdopodobnie motywowane było potrzebą uniknięcia kolizji z normami wynikającymi z konsytucji, jednak, co oczywiste, także obywatele RP są objęci zakresem stosowania wprowadzonego środka, jeżeli komunikują się z obcokrajowcym poddany inwigilacji. Trybunał Konstytucyjny w wyroku K 23/11 wskazał, że „mając na uwadze przede wszystkim art. 30 i art. 37 ust. 1 Konstytucji, trzeba przyjmować – jako założenie wyjściowe – jednakowy standard ingerencji w konstytucyjne wolności oraz prawa, bez względu na to, czy ich podmiot ma obywatelstwo polskie. Każdy znajdujący się pod władzą Rzeczypospolitej, tj. podlegający polskiemu prawu – niezależnie od statusu obywatelskiego – może zatem zasadnie oczekiwać ochrony przed nieuzasadnioną ingerencją w przysługujące mu wolności i prawa”.

Treść tego orzeczenia była znana projektodawcom ustawy antyterrorystycznej, o czym najlepiej świadczy fakt przywołania wybranych tez wyroku w uzasadnieniu złożonego projektu929. Co więcej, projektodawcy przywołali art. 31 ust. 1 Konstytucji, podkreślając, że ograniczenia w zakresie praw przewidzianych w ustawie zasadniczej mogą być ustanawiane wyłącznie 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. Zupełnie niezrozumiałe jest zatem, dlaczego będąc świadomym norm konstytucyjnych (zasady konieczności – i wynikającej z niej – zasady proporcjonalności) oraz orzeczenia TK w sprawie K 23/11, zaproponowali wprowadzenie mechanizmów inwigilacji budzących zastrzeżenia nie tylko w zakresie zgodności z ustawą zasadniczą, ale i aktami prawnomiędzynarodowymi, którymi Polska jest związana.

Już na etapie prac legislacyjnych organizacje pozarządowe zgłaszały uwagi krytyczne do przedstawionego projektu ustawy antyterrorystycznej930. Po jej zatwierdzeniu i wejściu w życie Rzecznik Praw Obywatelskich skierował do Trybunału Konstytucyjnego wniosek o zbadanie wskazanych przepisów ustawy pod kątem zgodności z ustawą zasadniczą i aktami prawnomiędzynarodowymi931. W obszernym uzasadnieniu, datowanym na 11 lipca 2016, Rzecznik wskazał na konieczność oceny między innymi art. 9 ust. w ustawy (możliwość inwigilacji obcokrajowców bez kontroli sądowej) w zakresie, w jakim „przewidziana w nim możliwość stosowania niejawnych czynności operacyjno-rozpoznawczych stanowi zbyt

929 Ibidem, s. 11.
daleko idącą i nieuzasadnioną ingerencję w prawa i wolności jednostki, a także w zakresie, w jakim różnicuje sytuację prawną osób, które nie są obywatelami Rzeczypospolitej Polskiej i obywateli RP oraz w zakresie, w jakim nie ustanawia mechanizmu kontroli stosowania przewidzianych w nim czynności”932. Ponadto podkreślił bardzo szeroki dostęp do rejestrów publicznych wynikający z art. 11 ustawy, obejmujący „w zasadzie wszystkie podmioty publiczne na szczeblu centralnym, które prowadzą jakiekolwiek rejestry oraz ewidencje”933.

Tak szeroki zakres przedmiotowy połączony z zastosowaniem ogólnych warunków uzasadniających dostęp do danych oraz brakiem odniesienia do zasady konieczności czy proporcjonalności uzasadnił złożenie przez RPO wniosku o zbadanie przepisów ustawy z Konstytucją934.

Istniejące krajowe przepisy wprowadzające ogólny obowiązek retencji danych oraz określające uprawnienia oraz sposób działania służb specjalnych w zakresie realizowanych tajnych programów inwigilacyjnych, budzą poważne wątpliwości w zakresie zgodności z prawem UE i europejską konwencją. O ile kwestia niezgodności pr. tel. z KPP w zakresie wynikającym z orzeczeń TSUE w sprawie DRI oraz Tele2 jest wydaje się oczywista, a dalsze funkcjonowanie przepisów prowadzi do naruszenia zasady pewności prawa, o tyle niezgodność uprawnień wprowadzonych na mocy ustawy inwigilacyjnej i antyterrorystycznej powinna być oceniona na drodze skarg do sądu konstytucyjnego oraz ETPC.

Niezależnie, jako wniosek de lege ferenda, zasadne wydaje się przebudowanie całego krajowego prawodawstwa związanego z gromadzeniem i przetwarzaniem danych przez uprawnione organy tak, aby funkcjonujące normy bezpośrednio ograniczały stosowanie uprawnień do przypadków koniecznych w demokratycznym społeczeństwie, przy jednoczesnym poszanowaniu zasad proporcjonalności. Wniosek ten wydaje się w szczególności aktualny, biorąc pod uwagę zbliżający się termin implementationi dyrektywy 2016/680935, w ramach której wymagane będzie zweryfikowanie i gruntowne zmodyfikowanie istniejących przepisów regulujących funkcjonowanie poszczególnych służb specjalnych.

8.5. Podsumowanie i wnioski

932 Ibidem, s. 2.
933 Ibidem, s. 59.
934 Ibidem, s. 69.
935 Szczegółowe omówienie dyrektywy 2016/680 w rozdziale 4.5.6 (s. 189).
„Nie chodziło o to, czy obserwowaliśmy ludzi czy nie, chodziło o to, że obserwowaliśmy ich w takim stopniu, że nie rozumieliśmy pozyskiwanych informacji. Problem polega na tym, że gdy przechwytujesz wszystkie dane, gdy obserwujesz wszystkich, nie rozumiesz nic”936.


skonstruowany w taki sposób, aby stworzyć pozory obserwacji wszystkich i w ten sposób wpływać na zachowanie osadzonych, niezależnie od tego, czy obserwacja faktycznie następowała. W wersji skrajnej Panoptikon nie wymagał strażników, ich rolę przejmowali więźniowie, dostosowując się poprzez daleko posuniętą samokontrolę do wyznaczonych przez nadzorców zasad i reguł funkcjonowania w społeczności. Dla stwierdzenia, że prywatność została naruszona, nie jest zatem istotne to, czy ktoś „obserwuje”, ale to, że obserwować może i ta okoliczność w sposób stały wpływa na wolność jednostki, zmuszając ją do określonego zachowania.

Problem programów masowej inwigilacji doskonale wpisuje się w powyższą koncepcję. W istocie bowiem ich celem nie jest zapobieganie przestępstwom, a kontrola, która może być wykorzystana w różnym zakresie i z różnym skutkiem, w zależności od motywacji decydentów. Systemy ochrony praw człowieka zostały stworzone właśnie w celu zapobiegania takim ryzykom – podejmowania arbitralnych decyzji przez nieznanych decydentów w oparciu o dane, których wiarygodność jest nieweryfikowalna, oraz algorytmy, których sposób działania jest nieznany, przy niewystarczającej kontroli sądowej oraz w sposób nieodzwierciedlający wartości społeczeństwa demokratycznego.

Przez wiele lat sądowa kontrola działań inwigilacyjnych władz publicznej – zwłaszcza realizowana w systemie europejskiej konwencji – prowadziła do wypracowania minimalnego zestawu zabezpieczeń, jakie powinny zostać uwzględnione w prawie krajowym w celu odpowiedniej ochrony jednostki przez nieuprawnioną ingerencję. Rozwiązania te stały się obecnie w wielu państwach częścią procedury karnej i stanową podstawą dla realizacji czynności operacyjnych przez uprawnione organy. Jednocześnie jednak poza kontrolą pozostały działania organów państwowych prowadzących działania w obszarze rozpoznania elektronicznego.

W następstwie zwiększonej w ostatnich latach uwagi opinii publicznej na problemy masowej inwigilacji problematyka ta coraz częściej staje się elementem debaty publicznej. Także instytucje UE przedstawiają własne analizy i rekomendacje związane z regulacją tego zagadnienia. Niedawne orzeczenia ETPC (zwłaszcza w sprawie Zakharov v. Rosja i Szabo i

938 Tak ideę Panoptikonu przedstawiał M. Foucault: „To główny efekt Panoptikonu: wzbudzić w uwielbionym świadome i trwale przeswietlenie o widzialności, które daje gwarancję automatycznego funkcjonowania władzy. Spowodować, by nadzór był nieprzerwanie skuteczny, nawet jeśli będzie nieciągły w działaniu; by doskonałość władzy czyniła zdobnym jego stałe sprawowanie; by ten architektoniczny aparat stał się mechanizmem do tworzenia i podtrzymywania zależności od władzy niezależnie od tego, kto ja sprawuje; słowem, by więźniowie podlegali władzy, której sami są nosicielami. Toteż bezustanne obserwowanie więzienia przez nadzorcę to jednocześnie za dużo i za mało: za mało, bo chodzi tylko o to, by wiedział on, że jest nadzorowany; za dużo, bo faktycznie robić tego nie ma potrzeby”. Cytat za: M. Foucault, Nadzorować i karać, Fundacja Aletheia 1998, s. 196.
Przedstawiona analiza zobrazowała, że rozwiązanie problemu masowej inwigilacji wymyka się jednak tradycyjnym normom prawa, których cechą charakterystyczną jest ich terytorialność. Omówione przykłady współpracy służb specjalnych różnych państw, podległych odmiennym jurysdykcjom, funkcjonujących w państwach należących do różnych kręgów kulturowych i systemów ochrony praw człowieka, pokazują, że kwestia prowadzenia nieukierunkowanych programów inwigilacyjnych powinna być rozwiązana poprzez zakazanie prowadzenia tego typu działań w aktach o zasięgu międzynarodowym. Sytuacja, w której służby specjalne celowo wykorzystują swoje możliwości techniczne, aby doprowadzić do przekierowania interesującego je ruchu poza granice własnej jurysdykcji, tak aby dane te mogły być przechwycone i poddane analizie przez współpracujące służby innego kraju, pokazuje, że tylko rozwiązanie ponadnarodowe może okazać się skuteczne. N. Richards postuluje, aby przyszłe normy prawne regulujące prowadzenie programów inwigilacyjnych opręć na czterech najważniejszych zasadach:

- zakazie prowadzenia tajnych programów inwigilacyjnych, czyli takich, których samo nawet istnienie jest znane opinii publicznej;
- braku legalności prowadzenia masowych programów inwigilacyjnych, pozwalających władzy na rejestrowanie całości informacji przesyłanych w Internecie;
- możliwości dochodzenia zadośćuczynienia za doznaną krzywą w przypadku przez osoby niesłusznie objęte działaniami inwigilacyjnymi;
- odrzuceniem w prawodawstwie podziału na techniki inwigilacji i monitorowania aktywności w zależności od pomiotu, który je stosuje – a więc bez rozróżniania na podmioty prywatne i publiczne939.

Propozycje N. Richards, będące efektem analizy amerykańskiego systemu prawnego, mogą znaleźć zastosowanie także w szukaniu wspólnej płaszczyzny dla ponadnarodowego porozumienia w zakresie dopuszczalnego zakresu działań państw w odniesieniu do monitorowania aktywności dużych grup osób (społeczeństw) z wykorzystaniem nowoczesnych środków przetwarzania danych.

Odrębnym zagadnieniem jest odpowiedzialność krajowego prawodawcy w stanowieniu nowych norm prawa odzwierciedlających standardy wyznaczone w ponadnarodowych systemach ochrony praw człowieka. W przypadku Polski niezrozumiały jest nie tylko brak wycofania z obiegu prawnego przepisów wprost niezgodnych z orzeczeniami TSUE, ale także wprowadzanie nowych regulacji zbliżających krajowe ustawodawstwo do przepisów obowiązujących w państwach nie w pełni demokratycznych (por. np. wnioski ze sprawy Zakharov v. Rosja oraz rozwiązania wprowadzone w ustawie inwigilacyjnej). Polska jako kraj, w którym normy demokratyczne stanowią podstawę ustrojową od stosunkowo niedługiego czasu, powinna szczególną uwagę przykładać do unikania wprowadzania rozwiązań, które mogą skutkować osłabieniem zasady rządów prawa. Jest to rola nie tylko prawodawcy i egzekutywy, ale także judykatury, a szerzej – całego społeczeństwa. Jednym z ważniejszych narzędzi do osiągnięcia tego celu jest wprowadzenie skutecznych środków ograniczających uprawnienia służb oraz wzmacniających nadzór nad nimi.
Wnioski końcowe

Podstawowa teza niniejszej rozprawy, określona w jej wstępie, brzmiała, że istniejące regulacje prawne nie zapewniają skutecznej ochrony przed zagrożeniami dla prywatności wynikającymi z nowoczesnych technik przetwarzania danych. Przestrzeń badawcza wyznaczona tą tezą została przeanalizowana wieloaspektowo – zarówno z perspektywy prawa krajowego, norm prawa międzynarodowego, ale również mając za punkt wyjścia różne nowoczesne techniki przetwarzania informacji wraz z ich implikacjami dla ochrony prywatności, a także oceną zdolności regulowania tych technik przez istniejące prawodawstwo. Podstawowym ograniczeniem istniejących norm prawnych jest ich terytorialność, skutkująca brakiem możliwości całościowego uregulowania zjawisk mających miejsce w cyberprzestrzeni. Jest to wada immamentnie związana i z prawem krajowym, i z istniejącymi normami prawa międzynarodowego. Dlatego w ramach podsumowania pracy interesujące może być podjęcie próby zakreślenia warunków, jakie powinny być spełnione, aby normy prawne oraz wprowadzający je traktat międzynarodowy mogły mieć potencjał do skutecznego rozwiązania problemu ochrony prywatności w cyberprzestrzeni.

Funkcjonujące systemy ochrony praw człowieka doprowadziły do ugruntowania mechanizmów ochrony prywatności w prawodawstwie wielu państw. Nie okazały się jednak środkiem wystarczającym, aby zapewnić ochronę tych samych praw w przestrzeni wirtualnej. Można wskazać dwie najważniejsze przyczyny takiego stanu rzeczy – pierwsza to brak powszechności istniejących norm prawnomiędzynarodowych, druga to brak wystarczających środków kontrolnych, stanowiących skuteczną przeszkodę w naruszaniu przepisów traktatowych. Oba powyższe problemy zostaną syntetycznie przedstawione w kolejnych akapitach.

Jak wykazano w rozdziale 1, stanowione prawo, którego zasięg oddziaływania wyznaczony jest granicami terytorialnymi, nie może być skuteczne w regulowaniu zjawisk mających miejsce w przestrzeni niefizycznej, jaką jest cyberprzestrzeń. W sposób oczywisty cyberprzestrzeń wykracza swoim zasięgiem poza każdy system ochrony praw – niezależnie czy jest wprowadzany przepisami krajowymi (normy konstytucyjne), traktatami regionalnymi (np. EKPC lub KPP) czy ponadregionalnymi (MPPOP). Tylko w przypadku, gdyby wszystkie państwa na świecie przystąpiły do określonego traktatu, normy prawne przez niego wprowadzane miałyby pełne zastosowanie do wszystkich zdarzeń mających miejsce w cyberprzestrzeni. To założenie nierealne, dlatego zostanie pominięte w dalszych rozważaniach. Dość powiedzieć, że pomimo siedemdziesięcia lat rozwoju systemów ochrony

Brak uniwersalności nie jest jednak jedynym problemem stojącym na przeszkodzie, aby systemy ochrony praw człowieka mogły stanowić skuteczny prawnym mechanizm ochrony prywatności w cyberprzestrzeni. Również ważne – jeżeli nie ważniejsze – zagadnienie stanowi ich wyraźnie ochronny charakter, pozbawiony praktycznie mechanizmów regulacyjnych. Jak wskazano we wcześniejszych rozważaniach, przepisy o ochronie danych tym różnicą się od ogólnych norm dotyczących ochrony prywatności, że oparte są na reżimie publicznoprawnym – wprowadzają zatem funkcje regulacyjne i kontrolne, mające na celu podniesienie standardów przetwarzania informacji a nie tylko reagowanie na występujące naruszenia. Celem przepisów jest zatem wprowadzenie podobnych zasad przetwarzania informacji na regulowanym obszarze. W ten sam sposób zostały opracowanie unijne przepisy o ochronie danych, czego efektem jest stworzenie jednolitego rynku wewnętrznego w obszarze przetwarzania informacji. Brak regulacji publicznoprawnych (przez co należy rozumieć obowiązek powołania niezależnego nadzoru, ale także organów współpracy międzynarodowej władznych do definiowania wspólnych standardów) skutkuje realnym brakiem mechanizmu, za pomocą którego mogą być wprowadzone te same zasady związane z ochroną danych w różnych państwach. Konsekwencją jest ograniczona przydatność międzynarodowych systemów ochrony praw człowieka w ograniczaniu naruszeń horyzontalnych.

Bazując na wnioskach szczegółowych z przeprowadzonej analizy w odniesieniu do systemów ochrony praw człowieka (rozdział 2), ram prawnej ochrony danych osobowych (rozdział 3 i 5), ale także uwzględniając wnioski i doświadczenia ze stosowania prawa UE (rozdział 4), można wskazać następujące warunki brzegowe, które powinny zostać uwzględnione przy projektowaniu przyszłych rozwiązań legislacyjnych mających na celu skuteczną ochronę prywatności w cyberprzestrzeni:

1) Podstawę formalną powinna stanowić umowa międzynarodowa, o charakterze prawnie wiążącym.
2) Przedmiotem umowy powinno być ustanowienie organizacji międzynarodowej właściwej do definiowania wymagań i nadzorowania ich przestrzegania w zakresie przetwarzania danych w cyberprzestrzeni.
3) Sposobem realizacji tego celu powinno być nadanie organizacji kompetencji potrzebnych do stanowienia własnych standardów postępowania i norm prawnych w odniesieniu do cyberprzestrzeni, o charakterze regulacyjnym, a nie stricte ochronnym.
4) Prawo stanowione przez organizację powinno mieć charakter bezpośrednio skuteczny w systemach prawnych państw-stron konwencji.
5) W ramach traktatu powinien zostać powołany organ posiadający kompetencje opracowywania wytycznych i rekomendacji – na wzór WP29 (element samoregulacji rynku).
6) Traktat powinien powoływać lub wskazywać organ sądowy, przy czym poddanie się procedurze rozstrzygania sporów nie powinno zależeć od opcjonalnego uznania przez stronę, a wydane wyroki powinny mieć skutek erga omnes.

Najważniejszą propozycją bez trudu odnaleźć można zapożyczenia z istniejących umów międzynarodowych – w szczególności z traktatów ustanawiających UE, Konwencji 108, ale również EKPC oraz MPPOP. Przedstawiona propozycja wymaga szerszego omówienia.

W pierwszej kolejności należy uzasadnić postulat powołania organizacji międzynarodowej. Cyberprzestrzeń nie ma charakteru stałego zarówno w kategorii nieprecyzyjnych granic geograficznych, jak i zmienności w czasie zastosowań, a co za tym idzie – potrzebnych obszarów regulacji. Opracowanie stałych, zapisanych w traktacie zasad przetwarzania i ochrony danych, bez uwzględnienia możliwości późniejszej ich interpretacji albo uszczegółowienia, może skutkować szybką dezaktualizacją. Z drugiej strony, poprzestanie na ogólnych normach, niepodatnych na zmiany w stosowanych technologiiach przetwarzania, nie pozwoli na stworzenie jednolitej przestrzeni ochrony danych. Przedstawiając projekt Konwencji 108, wskazano, że „co do zasady nie powinno stanowić różnicy dla użytkowników oraz podmiotów danych, czy realizowane operacje przetwarzania mają miejsce w jednym czy wielu krajach. Stosowane powinny być te same podstawowe
zasady, a osoby, których dane są przetwarzane, powinny posiadać te same środki ochrony swoich praw i interesów.”

Powodem nieosiągnięcia powyższego postulatu była właśnie niewystarczająca szczegółowość przepisów połączona z wymaganiem ich transpozycji do krajowych porządków prawnych. Doprowadziło to do powstania znaczących różnic legislacyjnych w poszczególnych państwach, będących efektem różnego rozumienia tych samych przepisów konwencji. Brak organu, który byłby władny do wydania rekomendacji czy interpretacji w zakresie stosowania konwencji połączony z brakiem możliwości realizacji innych funkcji regulacyjnych, skutkował niewielką przydatnością Konwencji 108 do budowy bezpiecznej, ponadnarodowej przestrzeni ochrony danych.

W przedstawionej propozycji proponuje się, aby państwa członkowskie przeniosły na powołaną organizację międzynarodową część swoich uprawnień związanych z możliwością regulowania zdarzeń realizowanych w cyberprzestrzeni mających miejsce na obszarze podległym ich jurysdykcji. Organizacja miałaby zatem kompetencję do wykonywania tego zadania w imieniu państw – co oczywiście jest zapożyczeniem z koncepcji kompetencji wyłącznych przypisanych Unii w traktatach ustanawiających UE. Biorąc pod uwagę przekazanie części własnych kompetencji organizacji międzynarodowej, państwa członkowskie dążyłyby do zapewnienia zrównoważenia interesów różnych stron poprzez odpowiednie określenie sposobu powoływania organów poszczególnych instytucji organizacji oraz zasad podejmowania decyzji, jednak kwestię tę na tym etapie omawiania koncepcji można pominać jako zbyt szczegółową.

Ponieważ powołana organizacja miałaby kompetencje do stanowienia wiążących aktów w zakresie regulowania funkcjonowania cyberprzestrzeni (de facto Internetu), przepisy przez nią wprowadzane doprowadziłyby do unifikacji zasad ochrony i przetwarzania informacji we wszystkich państwach-stronach, które przystąpiłyby do traktatu.

W tym momencie należy odnieść się do dwóch, na pozór oczywistych, problemów związanych z przedstawioną koncepcją. Po pierwsze, w jaki sposób odnieść funkcjonowanie postulowanej organizacji do braku możliwości zapewnienia uniwersalności stanowionych przez nią norm; mówiąc inaczej – skoro we wcześniejszych rozważaniach wskazywano, że brak powszechności jest wadą systemów ochrony praw człowieka, to proponowany traktat zapewne także nie byłby uniwersalny, a zatem zasięg regulacji wprowadzanych na jego mocy nie obejmowałby całej cyberprzestrzeni (brak zasięgu globalnego). Istnieje jeszcze drugi

---

problem, związany z trudnością w wypracowaniu wspólnych zasad ochrony w gronie państw wysokorozwiniętych, zwłaszcza biorąc pod uwagę różnice występujące obecnie na tle prawodawstwa UE i Stanów Zjednoczonych w zakresie ochrony prywatności.

W zakresie pierwszego z problemów: Internet bez granic to idea, jednak idea nieprawdziwa. To utopia - i jak każda utopia, wprowadzając uogólnienia, prowadzi do fałszu. Internet zawsze miał granice, co więcej – zawsze istniały w nim mechanizmy regulacyjne. Nie jest zatem prawdą, że Internet jest zjawiskiem zawieszonym w przestrzeni niezależności, gdzie nic i nikt nie jest w stanie wpływać na jego kształt. Już dzisiaj kraje niedemokratyczne skutecznie separują swoje fragmenty cyberprzestrzeni od sieci globalnej, tworząc rodzaj „krajowego Internetu”. Doskonalem przykładem są Chiny – mające ponad 700 mln użytkowników Internetu\(^4\), z których większość korzysta głównie z krajowych zasobów i usług online. Komunikacja z siecią globalną jest kontrolowana i nadzorowana przez państwo. Podobne rozwiązania zaczyna wprowadzać Rosja, coraz dalej ingerując w sposób funkcjonowania sieci łączności elektronicznej. Państwa niedemokratyczne, zwłaszcza niektóre państwa arabskie, mają własne mechanizmy nadzoru usług udostępnionych użytkownikom Internetu, co wynika głównie z obawy, że swobodna wymiana treści będzie stanowiła zagrożenie dla przyjętych norm ustrojowych. Internet ma więc granice, tyle że w chwili obecnej są one budowane przez państwa niedemokratyczne, a celem ich wprowadzania jest ograniczanie praw własnych obywateli.

Nie jest także prawdą, że Internet jest siecią niepodlegającą regulacji. Wręcz przeciwnie: od lat główne funkcje regulacyjne dotyczące najważniejszych funkcji sieci, bez których nie może ona działać prawidłowo (takie jak adresacja IPv4 i IPv6 oraz schemat nazewnictwa DNS), są realizowane przez ICANN (Internet Corporation for Assigned Names and Numbers) – organizację pozarządową zarejestrowaną w Stanach Zjednoczonych i podlegającą prawu stanu Kalifornia. ICANN została utworzona w 1998 roku, a posiadane kompetencje zostały jej przekazane przez władze USA. Jednocześnie jest to organizacja niepodlegająca żadnemu innemu prawodawstwu niż Stanów Zjednoczonych, a do 2016 roku formalnie podlegała nadzorowi ze strony Departamentu Handlu USA\(^5\). Od strony technicznej prawidłowe działanie Internetu w dużej mierze zależy od poprawnego

\(^4\) Tech In Asia, China now has 731 million internet users, 95% access from their phones, https://www.techinasia.com/china-731-million-internet-users-end-2016.

funkcjonowania trzynastu tzw. głównych serwerów DNS\textsuperscript{945}. Pierwotnie wszystkie one były zlokalizowane w Stanach Zjednoczonych, państwach Europy Zachodniej oraz Japonii. Także dzisiaj większość serwerów jest kontrolowanych przez podmioty podlegające prawu Stanów Zjednoczonych, przy czym władze publiczne USA jako jedyne na świecie bezpośrednio nadzorują trzy serwery (w tym dwa – armia amerykańska)\textsuperscript{946}. Nie jest więc prawdą, że Internet, nawet dzisiaj, nie podlega określonym formom regulacji i nadzoru.

Dlatego w opinii autora budowa społeczeństwa opartego na wiedzy i informacji wymaga odrzucenia koncepcji „\textit{Internetu bez granic}”. Internet bez granic to też Internet bez regulacji, co z kolei prowadzi do nadużyć. Jeżeli Internet ma stanowić ważne, w niektórych obszarach podstawowe, medium komunikacji, ale także budowy relacji międzyludzkich, a w szerszym kontekście – tworzenia e-społeczeństwa, to konieczne jest wzmocnienie zaufania i wiarygodności z nim związanej. Prawo stanowione w zgodzie z zasadami państwa demokratycznego służy ochronie wartości ustrojowych, w tym poszanowania praw podstawowych. Brak możliwości skutecznej ochrony praw podstawowych, takich jak prawo do prywatności, czyni z koncepcji Internetu bez granic pusty slogan o ograniczonej przydatności w zakresie budowy społeczeństwa informacyjnego. Prawodawstwo krajowe nie ma potencjału potrzebnego, aby problem ten rozwiązać. Realizacja zaproponowanej koncepcji, a więc powołanie nowej organizacji międzynarodowej i przekazanie jej niezbędnych kompetencji regulacyjnych przez państwa-strony traktatu, doprowadziłaby do powstania bezpiecznej przestrzeni przetwarzania w ramach obecnie istniejącej sieci Internet, z którą można by wiązać większe gwarancje w zakresie bezpieczeństwa i wiarygodności prowadzonych procesów przetwarzania. Zatem powszechność nie jest warunkiem skuteczności przedstawionej koncepcji. Ponieważ mechanizmy wprowadzone traktatem miałyby głównie funkcje regulacyjne, przystępujące państwa mogłyby uprościć (zlikwidować) procedury międzynarodowego transferu danych, skoordynować działanie krajowych organów nadzoru, ale przede wszystkim zapewnić możliwość korzystania z tych samych swobód i obowiązków przez rozproszone geograficznie podmioty. Złożone problemy

\begin{footnotesize}
945 Należy zauważyć, że obecnie używanie terminu „\textit{serwer}” w odniesieniu do powszechnej usługi świadczonej w Internecie może być mylące. Jak wyjaśniono w rozdziale 6, w rozproszonym modelu przetwarzania danych ta sama funkcjonalność może być realizowana przez wiele geograficznie rozlokowanych urządzeń (technologia znana pod pojęciem \textit{anycast}). W efekcie pomimo faktu, że faktycznie istnieje tylko 13 usług głównych zarządzania przestrzenią DNS, to każda z nich może być realizowana za pomocą wielu serwerów fizycznych. Nie zmienia to jednak faktu, że każdą z tych usług zarządza jedna, wyznaczona organizacja. Bliższe wprowadzenie w tematykę głównych serwerów DNS: Netnod, \textit{What are root name servers}\textsuperscript{946}, https://www.netnod.se/i-root/what-are-root-name-servers.

946 Aktualna lista podmiotów zarządzających głównymi serwerami DNS: http://www.iana.org/domains/root/servers
\end{footnotesize}
prawne mogłyby zostać rozwiązane w stosunkowo prosty sposób – np. dostawcy świadczący usługi w chmurze mogliby zostać zobowiązani, aby wszystkie centra przetwarzania danych były lokalizowane na terytorium państw uczestniczących w systemie, a transfer dużych zbiorów danych do państw trzecich mógłby zostać objęty odpowiedniemu nadzorowi.

Poważniejszą trudnością zdaje się wypracowanie w gronie państw potencjalnie zainteresowanych udziałem w takim porozumieniu wspólnie akceptowalnych standardów ochrony danych osobowych. Problem ten jest doskonale zauważalny w przypadku prawodawstwa UE i USA. W przypadku Unii ograniczeniem może być wskazanie w art. 6 ust. 3 TUE europejskiej konwencji w katalogu zasad ogólnych prawa, ale także nadanie orzeczeniom ETPC dotyczącym ochrony prywatności de facto rangi wiążącej w systemie prawa UE (art. 52 ust. 3 KPP w zw. z art. 6 ust. 1 TUE). W efekcie przyjęte rozwiązanie traktatowe może stać na przeszkodzie przystąpieniu UE do jakiejkolwiek umowy międzynarodowej, której wykonanie będzie wymagało przekazywania danych osobowych z Unii, jeżeli postanowienia tej umowy nie będą przewidywały de facto nałożenia standardów ochrony wyznaczonych przez EKPC na pozostałe strony traktatu, co wydaje się rozwiązaniem niewykonальным. Problem ten doprowadził już do stwierdzenia nieważności decyzji KE 2000/520, stanowiącej podstawę prowadzenia programu Bezpieczna przystań (transfer z UE do USA danych osobowych w ramach współpracy gospodarczej), a w lipcu 2017 stał się jedną z przyczyn stwierdzenia przez TSUE braku możliwości zawarcia umowy UE – Kanada w zakresie wymiany danych PNR. Wydaje się zatem, że Unia, przyjmując konstrukcję przewidzianą w art. 52 ust. 3 KPP w zw. z art. 6 ust. 1 TUE, wprowadziła standardy ochrony skutkujące znacznym utrudnieniem współpracy międzynarodowej w dziedzinie przetwarzania danych osobowych.

Z drugiej strony, w prawodawstwie Stanów Zjednoczonych – największego globalnego dostawcy usług przetwarzania danych – ochrona prywatności nie jest wprost zdefiniowana w przepisach rangi konstytucyjnej. Ochrona danych osobowych jest traktowana wybiórczo i sektorowo, przy czym nie wprowadzono nawet nadzorującego przestrzegania standardów urzędu ombudsmana.

Zarówno UE, jak i USA nie przystąpiły dotychczas do Konwencji 108, chociaż z różnych powodów. W przypadku UE początkową trudność stanowiła treść samej konwencji oraz niewystarczające umocowanie traktatowe instytucji UE. W konsekwencji w 1999 roku

947 Szczegółowe omówienie problematyki transatlantyckich programów wymiany danych znajduje się w rozdziale 4.5.3.2 (s. 164), a umów międzynarodowych zawieranych przez UE w obszarze wymiany danych PNR w rozdziale 4.6.2 (s. 197).

Dlatego wydaje się, że wypracowanie wspólnych ram prawnych postulowanej umowy międzynarodowej może wymagać podjęcia niezbędnych prac dostosowawczych na poziomie prawa wewnętrznego. Uwaga ta może mieć szczególne znaczenie w odniesieniu do Stanów Zjednoczonych, gdzie niezmiennie żywa jest dyskusja w zakresie koniecznych zmian dotyczących prawnej ochrony prywatności.


W efekcie realizacji propozycji G. Greenleafa model ochrony prywatności opierałby się co do zasady na systemie wynikających z Paktu rozszerzonym o przepisy Konwencji 108. Wśród zauważalnych wad takiego rozwiązania można wymienić wprowadzenie dwóch odrębnych reżimów ochrony, innych dla państw europejskich (dla których podstawą byłaby EKPC) oraz pozaeuropejskich (opierających się na MPPOP). Ponadto oparcie modelu ochrony w odniesieniu do państw pozaeuropejskich na Pakcie doprowadziłoby do powielenia wszelkich ograniczeń tego traktatu (w szczególności – związanych z szeroko stosowanymi zastrzeżeniami i interpretacjami zgłoszonymi w procesie ratyfikacyjnym). Dlatego nie można uznać, że realizacja propozycji G. Greenleafa stanowiłaby skuteczną odpowiedź na problem

948 Rada Europy, Amendments approved by the Committee of Ministers, Strasbourg, 15.06. 1999, https://rm.coe.int/168008c2b8.
951 Szczegółowe omówienie propozycji G. Greenleafa przedstawiono w rozdziale 3.7.
związany z właściwą ochroną prywatności w cyberprzestrzeni w skali globalnej. Już sam fakt, że 47 państw funkcjonujących w systemie europejskiej konwencji związanych byłoby siłęniejszymi mechanizmami ochrony prywatności niż kraje niebędące stroną tego traktatu, doprowadziłoby do powstania znaczących różnic w poziomie ochrony realizowanym przez prawodawstwo różnych krajów. Propozycja ta w żaden sposób nie przyczyniłaby się także do realizacji funkcji regulacyjnej, ponieważ Pakt oraz Konwencja 108 pozbawione są organów umocowanych do wydawania prawnie wiążących rekomendacji związanych z interpretacją traktatów.

Również uczestnicy Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności wskazali na MPPOP jako traktat stanowiący podstawę do budowy ponadnarodowych ram ochrony danych. Podczas 35. Konferencji przyjęto Rezolucję na rzecz zapewnienia ochronie danych i prywatności stałego miejsca w prawie międzynarodowym, w której podkreślono konieczność wprowadzenia prawnie wiążącego międzynarodowego porozumienia w sprawie ochrony danych952. Uczestnicy Konferencji wskazali, że postulat ten powinien zostać zrealizowany poprzez nadanie Międzynarodowym Standardom Ochrony Prywatności953 rangi prawnie wiążącej poprzez ich uwzględnienie w treści nowego, trzeciego protokołu fakultatywnego do MPPOP. Jest to zatem alternatywna względem wysuniętej przez G. Greenleafa propozycji opierającej się na Pakcie. Zatem i w tym wypadku aktualne pozostają uwagi krytyczne przedstawione wcześniej na tle rozważań związanych z możliwością oparcia na Pakcie skutecznego modelu ochron prywatności w cyberprzestrzeni.

Ochrona prywatności to jedno, ale nie jedyne, z praw, które wymaga ochrony w odniesieniu do nowych zagrożeń związanych z upowszechnianiem Internetu. Omówione powyżej alternatywne propozycje, związane z budową modelu regulacyjnego na bazie systemów ochrony praw człowieka, mają jeszcze jedno istotne ograniczenie – praktyczną trudność w zapewnieniu aktualności wprowadzanych zasad w odniesieniu do nowych pojawiających się modeli przetwarzania danych. Zarówno propozycja powiązania MPPOP z Konwencją 108, jak i rozszerzenia MPPOP o MSOP pozbawione są mechanizmu dostosowania przepisów do zmieniającego się rynku przetwarzania informacji. Problem taki nie występująłby w koncepcji zawarcia nowego traktatu, na podstawie którego powołana zostałaby organizacja międzynarodowa, wyposażona w kompetencje potrzebne do wprowadzania prawnie wiążących regulacji dotyczących cyberprzestrzeni. Co oczywiste,
postulowana umowa mogłaby także określać szerszy cel działania organizacji niż tylko ochrona prywatności. Dlatego postulowana propozycja zawarcia nowej umowy międzynarodowej powinna być postrzegana nie tylko jako prowadząca do wzmocnienia mechanizmów ochrony danych i prywatności w cyberprzestrzeni, ale w szerszym ujęciu – podejmująca problem ochrony praw podstawowych w Internecie.

Kwestia wprowadzenia prawnomiędzynarodowych regulacji dotyczących Internetu nie jest tematem nowym954. W literaturze przedmiotu najczęściej jednak omawiana jest z perspektywy ustanowienia mechanizmów nadzorczych i regulacyjnych dotyczących technicznych aspektów cyberprzestrzeni. J. Kulesza, uzasadniając potrzebę opracowania Ramowej Konwencji Internetu, wskazuje, że „konieczne jest wypracowanie szerokiego międzynarodowego konsensusu i poddanie kluczowych zasobów sieci władzy organizacji cieszącej się międzynarodowym zaufaniem”955. Inaczej – jak przewiduje – „dojść może do rozpadu sieci globalnej na mniejsze fragmenty – krajowe, zamknięte, niezależne od siebie i podlegające lokalnym regulacjom prawnym”956. Propozycja omawiana przez J. Kuleszę wpisuje się w dorobek funkcjonującego przy ONZ Forum Zarządzania Internetem i prowadzi de facto instytucjonalizacji Internetu, ale ograniczonej do technicznego zarządzania siecią. Nie jest to zatem koncepcja nie dająca się pogodzić z przedstawionym w niniejszej pracy. Obie propozycje funkcjonują jednak na innych płaszczyznach – projekt dyskutowany przez J. Kuleszę dotyczy wspólnego, ponadnarodowego zarządzania utrzymaniem i rozwojem technologii wspierającej działanie Internetu, podczas gdy propozycja przedstawiona w niniejszej pracy dotyczy utworzenia bezpiecznej przestrzeni przetwarzania, nadzorowanej i regulowanej przez ustanowiony do tego organ. Pomimo licznych głosów wspierających potrzebę

Podsumowując najważniejsze wnioski przedstawione w rozprawie, należy też odnieść się do płaszczyzny prawa polskiego. Pomimo silnych gwarancji związanych z ochroną prywatności, wynikających z przepisów konstytucyjnych, i ratyfikowanych norm prawnomiędzynarodowych, w pracy przedstawiono liczne uwagi krytyczne związane głównie z wprowadzaniem środków ustawodawczych skutkujących prawnie wątpliwa ingerencją w obszar praw podstawowych. Należy przywołać tu w szczególności rozważania związane z wprowadzoną w 2016 roku ustawą inwigilacyjną oraz antyterrorystyczną (por. rozdział 8.4.3).

955 J. Kulesza, Projekt Ramowej Konwencji Internetu, Państwo i Prawo 2009, nr 10, s. 17.
956 Ibidem, s. 10.
Na podkreślenie zasługuje także konieczność podjęcia pilnych prac legislacyjnych związanym z wycofaniem z krajowego porządku prawnego przepisów w sposób oczywisty niezgodnych z prawem UE oraz ustaloną linią orzeczniczą TSUE. W efekcie, wskutek bierności władzy wykonawczej, ochrona praw obywateli będzie musiała być coraz częściej opierana na stosowanych bezpośrednio przepisach prawnomеждуnarodowych i/lub międzynarodowych organach sądowych. Stąd też, także z perspektywy krajowej, realizacja propozycji wypracowania nowego traktatu zapewniającego ochronę prywatności w cyberprzestrzeni jest wnioskiem, który poprzez pozbawienie krajowej władzy możliwości wydawania arbitralnych decyzji przyczyni się do wzmacnienia przestrzeni ochrony praw podstawowych w Polsce, a nasze prawodawstwo oddali od modelu obowiązującego w państwach niedemokratycznych.

Przedstawiona koncepcja może wydawać się trudna w realizacji – zwłaszcza uwzględniając aspekty geopolityczne. Być może nie zostanie ona nigdy zastosowana w praktyce. Warto jednak pamiętać, że przywołana we wstępie idea Panoptykonu J. Benthama znalazła praktyczne zastosowanie dopiero wiele lat po jej sformułowaniu i to w obszarze z gruntu odmiennym od pierwotnie zakładanego (kontrola społeczeństwa w miejsce nadzoru nad więźniami). Niewykluczone zatem, że koncepcja budowy uniwersalnego traktatu mającego za cel wprowadzenie skutecznych środków ochrony praw podstawowych w cyberprzestrzeni zostanie podjęta dopiero w bardziej odległej przyszłości – co nie powinno zmieniać faktu, że jest to propozycja interesująca i wart dalszych analiz.

957 Ministerstwo Cyfryzacji w informacji udzielonej 31.08.2017 roku autorowi pracy wskazało, że aktualne pozostaje stanowisko wyrażone we wcześniejszym piśmie do RPO, w którym stwierdzono brak potrzeby nowelizacji obowiązujących przepisów w zakresie obowiązku retencji danych. Ministerstwo jednocześnie wskazało, że ew. podjęcie zmiany dotyczącej trybu dostępu do gromadzonych danych przez upoważnione organy jest decyzją Ministra Spraw Wewnętrznych i Administracji (pismo Ministerstwa Cyfryzacji z dn. 31 sierpnia 2017, sygn. BM-WOP.0123.130.2017, zb. własne autora).

Bibliografia

A.1. Akty prawne

A.1.1. Międzynarodowe


A.1.2. Unijne/wspólnotowe


[A-16] Traktat ustanawiający Konstytucję dla Europy z dnia 29.10.2004 (Dz.Urz. UE z 2004 nr C 310) [akt nieobowiązujący]


Dyrekcja 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7.03.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (CELEX: 32002L0021, Dz. Urz. UE z 2002 Nr L 108, s. 33).

Dyrekcja 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. Urz. UE Nr L 201, str. 37).

Dyrekcja 2009/140 Parlamentu Europejskiego i Rady z dnia 25.11.2009 r. zmieniająca dyrektywy 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, 2002/19/WE w sprawie dostępu do sieci i usług łączności elektronicznej oraz wzajemnych połączeń oraz 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (CELEX: 32009L0140, Dz. Urz. UE z 2009 Nr L 337, s. 37).

Rozporządzenie 593/2008 Parlamentu Europejskiego i Rady (WE) z dnia 17.06.2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Dz. Urz. UE z 2008 Nr L 177, s. 6).

Rozporządzenie 1215/2012 Parlamentu Europejskiego i Rady (UE) z dnia 12.12.2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (CELEX: 32012R1215, Dz. Urz. UE z 2012 Nr L 351, s. 1).

Rozporządzenie 2016/679 Parlamentu Europejskiego i Rady (UE) z 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE L 119 z 4.5.2016).

Rozporządzenie 2016/680 Parlamentu Europejskiego i Rady (UE) z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (CELEX: 32016L0680, Dz. Urz. UE z 2016 Nr L 119 s. 89).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27.04.2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (CELEX: 32016L0681, Dz. Urz. UE z 2016 Nr L 119 s. 132).

Decyzja Komisji (UE) 2000/520 z 26.07.2000 przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz. Urz. WE z 2000 nr L 215) – „Bezpieczna przystań”.

Decyzja Komisji (UE) 2016/1250 z 12.07.2016 przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA (CELEX: 32016D1250, Dz. Urz. UE z 2016 Nr L 207 s. 1) – „Tarcza prywatności”.

A.1.3. Krajowe

Konstytucja Rzeczypospolitej Polskiej z dnia 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.).

Ustawa z 23.04.1964 – Kodeks cywilny (Dz.U. z 2017 r. poz. 459 ze zm.).
A.1. Państwa trzecie

A.1.1. Państwa trzecie

A.1.2. Orzecznictwo

A.2. Orzecznictwo

A.2.1. KPC

Dostęp online do opinii KPC: http://juris.ohchr.org/.

A.2.2. ETPC

Dostęp online do orzeczeń ETPC: https://hudoc.echr.coe.int/eng.


Wyrok ETPC z 27.08.1997 w sprawie M. S. v. Szwecja, sygn. 20837/92.

Wyrok ETPC z 24.02.1998 w sprawie Botta v. Włochy, sygn. 21439/93.

Wyrok ETPC z 4.05.2000 w sprawie Rotaru v. Rumunia, sygn. 28341/95.

Wyrok ETPC z 17.07.2003 w sprawie Perry v. Wielka Brytania, sygn. 63737/00.

Wyrok ETPC z 30.06.2005 w sprawie Bosphorus, sygn. 45036/98.

Wyrok ETPC z 6.06.2006 w sprawie Segerstedt-Wiberg i in. v. Szwecja, sygn. 62332/00.

Wyrok ETPC z 29.06.2006 w sprawie Weber i Saravia v. Niemcy, sygn. 54934/00.

Wyrok ETPC z 3.04.2007 w sprawie Copland v. Wielka Brytania, sygn. 62617/00.


Wyrok ETPC z 30.07.2009 w sprawie VgT v. Szwajcaria, sygn. 32772/02.

Wyrok ETPC z 18.05.2010 r. w sprawie Kennedy v. Wielka Brytania, sygn. 26839/05.

Wyrok ETPC z 2.09.2010 w sprawie Uzun v. Niemcy, sygn. 35623/05.

Wyrok ETPC z 7.02.2012 w sprawie von Hannover v. Niemcy, sygn. 40660/08 i 60641/08.


Wyrok ETPC z 4.12.2015 r. w sprawie Zacharov v. Rosja, sygn. 7143/06.

Wyrok ETPC z 12.01.2016 r. w sprawie Szabo i Vissy v. Węgry, sygn. 37138/14.

Ponadto służby prasowe Trybunału publikują własne zestawienie najważniejszych wyroków dotyczących ochrony prywatności w związku ze stosowaniem technik masowej inwigilacji:


A.2.3. TSUE

Dostęp online do orzeczeń TSUE: https://curia.europa.eu/.

– odnoszące się do obszaru ochrony prywatności

Wyrok TSUE z 6.11.2003 w sprawie Lindqvist, sygn. C-101/01.

Wyrok TSUE z 7.11.2013 w sprawie IPI, sygn. C-473/12.

Wyrok TSUE z 8.04.2014 w sprawie Digital Rights Ireland Ltd, sygn. C-293/12 i C-594/12.

Wyrok TSUE z 13.05.2014 w sprawie Google Spain SL, sygn. C-131/12.

Wyrok TSUE z 1.10.2015 w sprawie Weltimmo, sygn. C-230/14.


– odnoszące się do roli praw podstawowych w systemie prawa UE

Wyrok TS (TSUE) z 4.02.1959 w sprawie Stork, sygn. 1/58.

Wyrok TS (TSUE) z 15.07.1960 w sprawie Geitling, sygn. 36/58, 37/58, 38/59 i 40/59.

Wyrok TS (TSUE) z 12.11.1969 w sprawie Stauder, sygn. 29/69.
Wyrok TSUE z 17.12.1970 w sprawie Internationale Handelsgesellschaft, sygn. 11/70.

Wyrok TS (TSUE) z 14.05.1974 w sprawie Nold, sygn. 4/73

– pozostałe (w tym podział kompetencji instytucji UE, rola niezależnego nadzoru, znaczenia wyroków TSUE, zasady prymatu, pomocnictwo i bezpośrednie skutki prawa UE itp.)

Wyrok TSUE z 4.12.1974 w sprawie van Duyn, sygn. 41/74.


A.2.4. Sądów zagranicznych

– Republika Federalna Niemiec

Wyrok Federalnego Trybunału Konstytucyjnego z 29.05.1974, sygn. BVerfGE 37, 271 (Solange I).

Wyrok Federalnego Trybunału Konstytucyjnego z 15.12.1983, sygn. BVerfGE 65, s. 1 (ochrona danych osobowych jako gwarancja konstytucyjna).

Wyrok Federalnego Trybunału Konstytucyjnego z 22.10.1986, sygn. BVerfGE 73, 339 (Solange II).

– Stany Zjednoczone

Wyrok Sądu Najwyższego USA z 7.06.1965 w sprawie Griswold v. Connecticut, 381 U.S. 479 (1965).


Wyrok Sądu Najwyższego USA z 20.06.1979, sprawa Smith v. Maryland, sygn. 442 U.S. 735 (1979).


A.2.5. Krajowe

– Trybunał Konstytucyjny


Wyrok TK z 30.06.2006, sygn. P 10/06, OTK-A 2006, nr 9, poz. 128 (ochrona prywatności a wolność słowa).

Wyrok TK z 23.06.2009, sygn. K 54/07, OTK-A 2009, nr 6, poz. 86 (ochrona prywatności jako związana z godnością człowieka).


Sąd Najwyższy


Wyrok SN z 24.06.2014, sygn. I CSK 532/13, OSNC 2015, nr 5, poz. 61 (ochrona danych osobowych jako element prawa do prywatności).

Uchwała SN z 26.06.2014, sygn. I KZP 14/14, OSNKW 2014, nr 8, poz. 59 (wyrok trybunału międzynarodowego jako przesłanka do wznowienia postępowania karnego).

Wyrok SN z 12.01.2016, sygn. IV KK 196/15, Legalis 1406408 (ocena istotności naruszenia prawa do prywatności).

Wyrok SN z 4.05.2016, sygn. IV CSK 270/15, OSNC 2017, nr 1, poz. 12 (KPP jako podstawa orzekania).

Sądownictwo administracyjne


Wyrok NSA z 22.11.2016, sygn. I OSK 3374/15, Legalis 1554775 (prawo do informacji a ochrona prywatności)


A.3. Strategie, dokumenty soft-law, opinie i rekomendacje
A.3.1. Dokumenty ONZ i KPC


A.3.2. OECD


A.3.3. Rada Europy


Zbiór dokumentów Rady Europy dotyczących ochrony prywatności, w tym opinie i rekomendacje Komitetu Doradczego Konwencji nr 108 publikowane są na stronie internetowej:

A.3.4. Instytucje UE

[A-139] Rezolucja Parlamentu Europejskiego z 21.02.1975 w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych (Dz.U. WE z 1975 Nr C 60, s. 48).

[A-140] Rezolucja Parlamentu Europejskiego z 8.05.1979 w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych (Dz.U. WE z 1979 Nr C 140, s. 34).


A.3.5. Opinie i rekomendacje Grupy Roboczej Art. 29


[A-158] Opinia 01/2014 w sprawie stosowania pojęć konieczności i proporcjonalności oraz ochrony danych w sektorze egzekwowania prawa, WP 211.

[A-159] Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, WP 217.

[A-160] Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, WP 221.


Pełna lista opinii i innych dokumentów wypracowanych przez WP29 dostępna na stronie internetowej:

A.3.6. Inne dokumenty prawnie niewiążące, w tym dokumenty innych organizacji międzynarodowych i zagranicznych organów nadzoru


A.3.7. Dokumenty krajowe


A.4. Komentarze


A.5. Monografie

A.6. Artykuły i rozdziały w monografiach

− ochrona praw człowieka – zagadnienia ogólne


[A-237] Symonides J., Powszechna Deklaracja Praw Człowieka (po 60 latach od jej przyjęcia), Państwo i Prawo 2008, nr 12, s. 3-16.


− cyberprzestrzeń


[A-244] Dobrzeniecki K., Normatywna i pozanormatywna regulacja Internetu – modele konkurencyjne czy komplementarne, [w:] Wykładnia prawa i inne problemy filozofii prawa pod. red. L. Morawskiego, Toruń 2005, s. 261-278.


— zakres i celowość prawnej ochrony prywatności


Kopff A., *Koncepcja praw do intymności i do prywatności życia osobistego*, Studia Cywilistyczne 1972, t. 20, s. 3-44.


Kubiński K., *Ochrona życia prywatnego człowieka*, Ruch Prawniczy, Ekonomiczny i Socjologiczny 1993, nr 1, s. 61-72.


– prywatność w cyberprzestrzeni, zagadnienia ogólne


Safjan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, Państwo i Prawo 2002, nr 6, s. 3-12.

Siwicki M., *Ochrona osób fizycznych w związku z przetwarzaniem i swobodnym przepływem danych osobowych*, Państwo i Prawo 2016, nr 3, s. 68-86.


– prywatność z perspektywy europejskiej nauki prawa

Brzeziński P., *Stanowisko wybranych sądów konstytucyjnych państw członkowskich UE/WE w sprawie zgodności regulacji implementujących dyrektywę 2006/24/WE z prawami podstawowymi*, Ius Novum 2017, nr 1, s. 77-81.

Buttarelli G., *The EU GDPR as a clarion call for a new global digital gold standard*, International Data Privacy Law 2016, t. 6, s. 77-78.


Rokita K., *Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych*, Europejski Przegląd Sądowy 2016, nr 7, s. 4-12.


– *ryzka dla prywatności w związku z nowymi technikami przetwarzania danych*


Konarski X., *Przetwarzanie danych osobowych w chmurze obliczeniowej*, Monitor Prawniczy 2013, nr 8 dodatek, s. 39-44.


Leja P., *Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych*, Prawo Mediów Elektronicznych 2017, nr 3, s. 10-17.


Streszczenie i słowa kluczowe

Przedmiotem pracy jest próba oceny, czy istniejące lub planowane rozwiązania prawne stanowią skuteczny środek ochrony prywatności przed zagrożeniami związanymi z nowymi technikami przetwarzania informacji. W ostatnich latach problem niedopasowania norm prawnych do regulacji zdarzeń mających miejsce w cyberprzestrzeni coraz częściej jest wskazywany jako jedna z barier dalszej ewolucji w kierunku społeczeństwa opartego na wiedzy. Nowoczesne techniki przetwarzania, takie jak przetwarzanie w chmurze (cloud computing), analityka dużych zbiorów danych (Big Data) czy Internet Rzeczy (Internet of Things) łączą się z nowymi możliwościami, ale również nieznanymi dotąd zagrożeniami – w tym dla obszaru praw podstawowych.

Przystępując do analizy powyższego problemu, szczególną uwagę zwrócono na omówienie regulacji ponadnarodowych, zarówno związanych z systemami ochrony praw człowieka, jak i aktami dotyczącymi ochrony danych osobowych. Systemy ochrony praw człowieka od przeszło pięćdziesięciu lat stanowią prawnie wiążący międzynarodowy mechanizm ochrony praw podstawowych, w tym także prawa do prywatności. W pracy omówiono i przeanalizowano treść prawa oraz zakres ochrony przewidzianej między innymi postanowieniami Międzynarodowego Paktu Praw Obywatelskich i Politycznych oraz Europejskiej Karty Praw Człowieka.

Szczegółowej analizie poddano także system prawa UE, w tym reformowany obecnie europejski model ochrony danych oparty przepisy rozporządzenia 2016/679. Na przykładzie prawa unijnego poszukiwano odpowiedzi na pytanie, czy transnarodowe prawo UE ma potencjał prowadzący do standardyzacji w zakresie ochrony prywatności, a w efekcie do stworzenia bezpiecznej przestrzeni przetwarzania danych, wykraczającej poza granice państw członkowskich UE.

W pracy rozważono także, czy i w jakim zakresie krajowy prawodawca może poprzez przepisy lokalne uzupełnić luki lub braki związane z funkcjonowaniem regulacji ponadnarodowych. W szerszym ujęciu – czy w ogóle kwestia ochrony prywatności w cyberprzestrzeni może być zapewniona poprzez normy, których zakres stosowania wyznaczany jest granicami poszczególnych państw?

Celem przedstawionych rozważań było zbadanie niedoskonałości obowiązujących norm prawnych – krajowych, unijnych i międzynarodowych. Jednocześnie na podstawie wyników cząstkowych możliwe stało się sformułowanie wniosków de lege ferenda odnośnie warunków brzegowych, jakie powinny być uwzględniane w przyszłych działaniach.
legislacyjnych, aby stanowione prawo w odpowiedni sposób rozwiązywało zidentyfikowane problemy.

Rozprawę podzielono na osiem rozdziałów, zgrupowanych w dwóch częściach. W rozdziale pierwszym omówiono kluczowe terminy, takie jak *prywatność*, związane z nią *prawo do prywatności*, a także *cyberprzestrzeń*, oraz wzajemna relacja pomiędzy ochroną danych osobowych a ochroną prywatności. W rozdziale drugim przedstawiono analizę i omówienie najważniejszych systemów ochrony praw człowieka. Rozdział trzeci poświęcono przedstawieniu najważniejszych aktów prawnomiedzinadrowych, w większości o charakterze niewiążącym, wprowadzających wytyczne dotyczące ochrony danych osobowych. W kolejnym, czwartym rozdziale przedstawiono akty prawne oraz obszary regulacji związane z prawem UE. W rozdziale piątym omówiono płaszczyznę przepisów krajowych oraz roli krajowego prawodawcy w obszarze ochrony prywatności w cyberprzestrzeni. W kolejnych trzech rozdziałach omówiono wybrane zagadnienia dotyczące najważniejszych, zdaniem autora, problemów związanych z ochroną prywatności w cyberprzestrzeni: w rozdziale szóstym - model chmury obliczeniowej, w rozdziale siódmym – analizy dużych zbiorów danych (*Big Data*), a w rozdziale ósmym – obecne możliwości władzy publicznej związane z prowadzeniem masowych programów inwigilacji.

Rozprawę kończy podsumowanie, w którym zebrano wnioski cząstkowe i na ich podstawie określono, czy i w jaki sposób normy prawnomiedzinadrowe powinny tworzyć ramy ochronne i regulacyjne w zakresie prawa do prywatności w cyberprzestrzeni.

**Słowa kluczowe:** prawo do prywatności, ochrona danych osobowych, cyberprzestrzeń, prawo międzynarodowe, transgraniczne przetwarzanie danych, rozporządzenie 2016/679, przetwarzanie w chmurze, Big Data, masowa inwigilacja.
Summary and key words

The subject of the thesis is an attempt to assess whether existing or planned laws are an effective means of protecting privacy against threats related to new information processing technologies. In recent years, the problem of the maladjustment of legal norms to the regulation of events taking place in cyberspace has been more and more often indicated as one of the barriers to further evolution towards a knowledge-based society. Modern processing techniques, such as cloud computing, big data analytics and the Internet of Things entail not only new possibilities, but also as yet unknown threats, including those to the fundamental rights.

In the analysis of the above problem, particular attention was paid to the discussion of supranational regulations related to both human rights systems and data protection laws. For over fifty years human rights systems have constituted a legally binding international mechanism for the protection of the fundamental rights, including the right to privacy. The work discusses and analyses the content of this right and the scope of protection stipulated, inter alia, by the provisions of the International Covenant on Civil and Political Rights and the European Convention on Human Rights.

The EU law system was also analyzed in detail, including the reformed European data protection model based on the provisions of Regulation 2016/679. The example of EU law was used to seek an answer to the question of whether transnational EU law has the potential to standardize privacy protection, and thus to create a secure data processing space that goes beyond the borders of the EU Member States.

It was also considered whether and to what extent the national legislature may, through local regulations, fill gaps or deficiencies related to the functioning of supranational regulations. In a broader perspective, is it possible to ensure the protection of privacy in cyberspace through norms whose scope of application is determined by the borders of particular states?

The main goal of the presented considerations was to examine the imperfections of the applicable legal norms at the national, EU and international levels. At the same time, based on partial results, it became possible to formulate de lege ferenda conclusions regarding the key factors that should be taken into account in the future legislation, so that the law enacted can solve the identified problems in an appropriate manner.

The dissertation is divided into eight chapters, grouped in two parts. The first chapter discusses key terms such as privacy, the related right to privacy, as well as cyberspace and the
relationship between data protection and privacy. The second chapter presents an analysis and discussion of the most important human rights systems which function in the Polish legal system. The third chapter is devoted to the presentation of the most important instruments of international law, mostly non-binding ones, which introduce guidelines in the personal data protection area. The next, fourth chapter presents the most important laws and areas of regulation related to EU law. The fifth chapter discusses national regulations and the role of the national legislature in the area of privacy protection in cyberspace. The next three chapters refer to selected issues in respect of the most important, in the author's opinion, problems related to the protection of privacy in cyberspace: the sixth chapter pertains to processing in the cloud computing model; the seventh chapter contains an analysis of processing of large data sets (Big Data); in the eighth chapter the possibilities of public authorities related to mass surveillance programs are discussed.

The dissertation ends with a summary in which partial conclusions were collected. On the basis of those conclusions it was determined whether and how international legal norms should be used to create a protective and regulatory framework in the field of the right to privacy in cyberspace.

Key words: right to privacy, data protection, cyberspace, international law, transborder data flows, Resolution 2016/679, cloud computing, Big Data, mass surveillance.