Uniwersytet Wrocławski

Wybrane aspekty prawa nowych technologii część 4

red. dr hab. Ewa Galewska

WYBRANE ASPEKTY PRAWA NOWYCH TECHNOLOGII

część 4

PUBLIKACJA STUDENCKIEGO KOŁA NAUKOWEGO „BLOK PRAWA KOMPUTEROWEGO”

WROCŁAW 2018

ISBN 978-83-928515-9-2

Redakcja

dr hab. Ewa Galewska

dr Anna Zalesińska

mgr Anna Materla

mgr Sandra Gali

mgr Adam Majewski

Recenzja

prof. dr hab. Jacek Gołaczyński

Okładka

mgr Wojciech Bijas
mgr Adam Majewski

Wydawca:

Studenckie Koło Naukowe „Blok Prawa Komputerowego”
Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego
ul. Uniwersytecka 22/26
50-145 Wrocław

Producent:
mgr Adam Majewski

Spis treści:

MGR BERENIKA CZERWIŃSKA

E-FAKTURA JAKO PRZYKŁAD DOKUMENTU ELEKTRONICZNEGO W POLSKIM POSTĘPOWANIU CYWILNYM 5

MGR MARIA DYMITRUK

CZY DYNAMICZNE ZMIANY DOBY NOWYCH TECHNOLOGII UZASADNIAJĄ NIEDOOKREŚLONOŚĆ PRZEPISÓW KARNYCH PRAWA AUTORSKIEGO? – UWAGI NA TLE ART. 115 UST. 3 PRAWA AUTORSKIEGO ORAZ WYROKU TRYBUNAŁU KONSTYTUCYJNEGO Z DNIA 17 LUTEGO 2015 R. (K 15/13) 12

MGR ALEKSANDRA GODEK

PROBLEMY I WĄTPLIWOŚCI ZWIĄZANE Z BITCOINAMI W ŚWIETLE PRAKTYKI ORGANÓW PODATKOWYCH..... 19

MGR PAWEŁ JANIEC

RACHUNEK PODSTAWOWY W NOWELIZACJI USTAWY O USŁUGACH PŁATNICZYCH I NIEKTÓRYCH INNYCH USTAW 34

MGR AGATA KOWALSKA

BEZPIECZEŃSTWO DANYCH OSOBOWYCH W CHMURZE 42

MGR ZUZANNA LISOWSKA

MOWA NIENAWIŚCI A WOLNOŚĆ WYRAŻANIA OPINII W INTERNECIE 55

ANNA PANEK

ODPOWIEDZIALNOŚĆ PRAWNA ZA NARUSZENIE OCHRONY DANYCH OSOBOWYCH Z UWZGLĘDNIENIEM ŚRODKÓW PRAWNYCH PRZEWIDZIANYCH W RODO..... 65

MGR ANNA PYKA

MONITORING – PROBLEMATYKA FUNKCJONOWANIA W POLSCE 75

MGR ANNA SOJAT

PROBLEMATYKA WIELOMIEJSCOWOŚCI NARUSZENIA DÓBR OSOBISTYCH – DELIKTY INTERNETOWE..... 87

mgr Berenika Czerwińska

E-faktura jako przykład dokumentu elektronicznego w polskim postępowaniu cywilnym

1. Zagadnienia wprowadzające

W polskim porządku prawnym definicja legalna faktury elektronicznej funkcjonuje od 1 stycznia 2014 r. Zgodnie z art. 2 pkt. 32 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług[1], który został dodany ustawą z dnia 7 grudnia 2012 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw[2] przez fakturę elektroniczną rozumie się fakturę w formie elektronicznej, wystawioną i otrzymaną w dowolnym formacie elektronicznym.

Zmiana u.p.t.u. była podyktowana koniecznością implementowania przepisów unijnych, w tym dyrektywy Parlamentu Europejskiego i Rady 2010/45/UE z dnia 13 lipca 2010 r. zmieniającej dyrektywę Parlamentu Europejskiego i Rady 2006/112/WE w sprawie wspólnego systemu podatku od wartości dodanej w odniesieniu do przepisów dotyczących fakturowania[3]. Dlatego też definicja przyjęta w polskiej ustawie stanowi odzwierciedlenie definicji faktury elektronicznej przyjętej w art. 217 dyrektywy 2006/112/WE w brzmieniu zmienionym dyrektywą 2010/45/UE. Co więcej, zmiana przepisów jest w znacznej mierze odwzorowaniem rozwiązań przyjętych w aktualnie obowiązujących dwóch rozporządzeniach, tj. rozporządzeniu Ministra Finansów z dnia 28 marca 2011 r. w sprawie zwrotu podatku niektórym podatnikom, wystawiania faktur, sposobu ich przechowywania oraz listy towarów i usług, do których nie mają zastosowania zwolnienia od podatku od towarów i usług[4] oraz rozporządzeniu Ministra Finansów z dnia 17 grudnia 2010 r. w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej[5]. Potrzeba zmian dotychczasowych regulacji wynikała przede wszystkim z konieczności transpozycji zmian wprowadzonych dyrektywą 2010/45/UE. Zgodnie z preambułą do wspomnianej dyrektywy fakturowanie elektroniczne może pomóc przedsiębiorcom obniżyć koszty i zwiększyć konkurencyjność. Faktury papierowe i elektroniczne powinny być traktowane równo, a zasada ta powinna mieć zastosowanie również do kompetencji organów podatkowych. Ich uprawnienia kontrolne oraz prawa i obowiązki podatników powinny mieć zastosowanie w równym stopniu, niezależnie od tego, czy podatnik wybierze wystawianie faktur papierowych czy faktur elektronicznych.

[1] t.j. Dz. U. z 2014 r. poz. 312 ze zm., dalej: u.p.t.u.
[2] t.j. Dz. U. z 2013 r. poz. 35 ze zm.
[3] Dz. Urz. UE z dnia 22 lipca 2010 r., seria L, Nr 189.
[4] Dz. U. Nr 68, poz. 360 ze zm.
[5] Dz. U. Nr 249 poz. 1661 ze zm.

Niniejszy artykuł ma na celu wskazanie definicji faktury elektronicznej, ze szczególnym uwzględnieniem kwestii podpisu takiej faktury, sposobów jej akceptacji oraz zapewnienia autentyczności i integralności. Ponadto, przedmiotem opracowania jest omówienie faktury elektronicznej jako środka dowodowego w postępowaniu cywilnym, a w szczególności odrębnym postępowaniu nakazowym.

2. Definicja e- faktury w ustawie o VAT

Przy wystawianiu faktur elektronicznych obowiązują ogólne zasady wystawiania faktur, zawarte przede wszystkim w u.p.t.u., dlatego też faktura elektroniczna powinna zawierać elementy wskazane w art. 106 e wskazanej ustawy tj. m.in.: 1) datę wystawienia; 2) kolejny numer nadany w ramach jednej lub więcej serii, który w sposób jednoznaczny identyfikuje fakturę; 3) imiona i nazwiska lub nazwy podatnika i nabywcy towarów lub usług oraz ich adresy; 4) numer, za pomocą którego podatnik jest zidentyfikowany na potrzeby podatku; 5) numer, za pomocą którego nabywca towarów lub usług jest zidentyfikowany na potrzeby podatku lub podatku od wartości dodanej, pod którym otrzymał on towary lub usługi; 6) datę dokonania lub zakończenia dostawy towarów lub wykonania usługi lub datę otrzymania zapłaty, o ile taka data jest określona i różni się od daty wystawienia faktury; 7) nazwę (rodzaj) towaru lub usługi; 8) miarę i ilość (liczbę) dostarczonych towarów lub zakres wykonanych usług; 9) cenę jednostkową towaru lub usługi bez kwoty podatku (cenę jednostkową netto); 10) kwoty wszelkich opustów lub obniżek cen, w tym w formie rabatu z tytułu wcześniejszej zapłaty, o ile nie zostały one uwzględnione w cenie jednostkowej netto; 11) wartość dostarczonych towarów lub wykonanych usług, objętych transakcją, bez kwoty podatku (wartość sprzedaży netto); 12) stawkę podatku; 13) sumę wartości sprzedaży netto, z podziałem na sprzedaż objętą poszczególnymi stawkami podatku i sprzedaż zwolnioną od podatku; 14) kwotę podatku od sumy wartości sprzedaży netto, z podziałem na kwoty dotyczące poszczególnych stawek podatku; 15) kwotę należności ogółem.

Zgodnie z definicją faktury elektronicznej, aby faktura mogła zostać uznana za fakturę elektroniczną, musi być wystawiona oraz otrzymana w dowolnym formacie elektronicznym. Wybór samego formatu zależy od podatnika.

Zasadniczo faktury wystawia się co najmniej w dwóch egzemplarzach, z których jeden otrzymuje nabywca, a drugi zachowuje w swojej dokumentacji podatnik dokonujący sprzedaży. Natomiast w przypadku faktur przesyłanych w formie elektronicznej podatnik dokonujący sprzedaży lub upoważniona przez niego do wystawiania faktur osoba trzecia przesyła je lub udostępnia nabywcy. W przypadku nabywcy, którym jest podatnik obowiązany wystawić fakturę dokumentującą sprzedaż, a także dostawę towarów i świadczenie usług, dokonywane przez niego na rzecz innego podatnika podatku, podatku od wartości dodanej lub podatku o podobnym charakterze lub na rzecz osoby prawnej niebędącej podatnikiem nabywający towary lub usługi od podatnika może wystawiać w imieniu i na rzecz tego podatnika faktury, nabywca przesyła je lub udostępnia podatnikowi, który upoważnił go do wystawiania faktur, z uwzględnieniem zasad wynikających z procedury zatwierdzania faktur przez podatnika dokonującego sprzedaży. Jeżeli nabywcą jest nabywca towaru lub usługi, który otrzymał fakturę zawierającą pomyłki, może wystawić fakturę nazywaną notą korygującą, przesyła je

lub udostępnia wystawcy faktury. Z kolei faktury dokumentujące dostawę towarów, z tytułu której na dłużniku ciąży obowiązek podatkowy, wystawiają w imieniu i na rzecz dłużnika organy egzekucyjne[6] lub komornicy sądowi wykonujący czynności egzekucyjne[7], przesyła je lub udostępnia nabywcy i dłużnikowi - zachowując je jednocześnie w swojej dokumentacji.

Od 1 maja 2004 r. faktura nie musi być podpisywana co skutkuje tym, że „oryginały" i „kopie" faktur można stworzyć w dowolnej ilości egzemplarzy, w dowolnym czasie i miejscu. Regulacji tej nie stosuje się do faktur przesyłanych w formie elektronicznej, ponieważ w przypadku tych faktur sprzedawca przesyła je, w tym udostępnia, nabywcy, zachowując je jednocześnie w swojej dokumentacji[8]. Podkreślić w tym miejscu należy, iż faktura elektroniczna nie musi być podpisana bezpiecznym podpisem elektronicznym weryfikowany za pomocą ważnego kwalifikowanego certyfikatu[9]. Do 31 grudnia 2010 r. obowiązywały przepisy rozporządzenia Ministra Finansów z dnia 14 lipca 2005 r. w sprawie wystawiania oraz przesyłania faktur w formie elektronicznej, a także przechowywania oraz udostępniania organowi podatkowemu lub organowi kontroli skarbowej tych faktur[10], zgodnie z którymi istniały jedynie dwa formalne warunki przesyłania lub udostępniania faktur elektronicznych, mianowicie, wykorzystanie bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu lub zastosowanie elektronicznej wymiany danych (EDI), zgodnie z umową w sprawie europejskiego modelu wymiany danych elektronicznych. Zmiany w tym obszarze zostały wprowadzone dopiero rozporządzeniem Ministra Finansów z dnia 17 grudnia 2010 r. w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej, i od 1 stycznia 2011 r. ustawodawca wymienia wskazane dwa sposoby jako jedynie przykładowe formy zapewnienia autentyczności, integralności i czytelności faktury. Nie jest to jednak katalog zamknięty. Dzięki takiej regulacji, zdecydowanie zwiększyła się dostępność stosowania faktur elektronicznych.

3. Sposoby akceptacji faktury elektronicznej

Stosowanie faktur elektronicznych wymaga akceptacji odbiorcy faktury. Regulacja ta koresponduje z § 3 rozporządzenia Ministra Finansów z dnia 17 grudnia 2010 r. w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania

[6] tj. organy egzekucyjne określone w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (tj. Dz. U. z 2005 r. Nr 229, poz. 1954, ze zm.).

[7] w rozumieniu ustawy z dnia 17 listopada 1964 r.- Kodeks postępowania cywilnego, (tj. Dz. U. z 2016 r., poz.195 ze zm.).

[8] *B. Kaczmarek- Templin*, Dowód z dokumentu elektronicznego w polskim procesie cywilnym, Warszawa 2012, s. 263.

[9] Zgodnie z ustawą z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450) bezpieczny podpis elektroniczny to podpis elektroniczny, który: jest przyporządkowany wyłącznie do osoby składającej ten podpis; jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń[9] służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego; jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

[10] Dz. U. Nr 133, poz. 1119.

organowi podatkowemu lub organowi kontroli skarbowej. Obecne przepisy odchodzą od obowiązku wyrażania formalnej zgody na otrzymywanie faktur w formie elektronicznej, należy zatem uznać, że ustawodawca pozostawił tę kwestę w gestii umownej stron transakcji[11]. W uzasadnieniu do projektu ustawy z dnia 7 grudnia 2012 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw wskazano przykładowo, że za wystarczającą będzie można uznać zgodę przyszłego odbiorcy faktur wyrażoną ustnie, bądź SMS-em. Za akceptację należy uznać również tzw. akceptację dorozumianą, np. konsument otrzymując fakturę w tej formie, reguluje płatność z niej wynikającą. Wskazano także, że wyraźna wzmianka, iż stosowanie faktur elektronicznych powinno podlegać akceptacji ze strony odbiorcy, znajduje swoje uzasadnienie głównie w technicznych wymogach koniecznych dla odbioru faktury elektronicznej lub w możliwościach odbiorcy w kontekście zapewnienia autentyczności, integralności oraz czytelności, które winny być ustalone, aby otrzymywać faktury elektroniczne, i które nie funkcjonują w zakresie faktur papierowych[12].

W przypadku przesyłania lub udostępniania temu samemu odbiorcy jednocześnie więcej niż jednej faktury elektronicznej dane wspólne dla poszczególnych faktur mogą zostać podane tylko raz, o ile dla każdej faktury są dostępne wszystkie te dane.

4. Autentyczność, integralność i czytelność faktury

W celu dostosowania obowiązujących przepisów do art. 233 dyrektywy 2006/112/WE, w brzmieniu zmienionym przez dyrektywę 2010/45/UE, w nowym art. 106m ust. 1-5 u.p.t.u., określono sposób zapewnienia autentyczności pochodzenia, integralności treści i czytelności faktury. Obecnie to podatnik określa sposób zapewnienia autentyczności pochodzenia, integralności treści i czytelności faktury. Przez autentyczność pochodzenia faktury rozumie się pewność co do tożsamości dokonującego dostawy towarów lub usługodawcy albo wystawcy faktury. Przez integralność treści faktury rozumie się, że nie zmieniono w niej żadnych danych, które powinna ona zawierać. Autentyczność pochodzenia, integralność treści oraz czytelność faktury można zapewnić za pomocą dowolnych kontroli biznesowych, które ustalają wiarygodną ścieżkę audytu między fakturą a dostawą towarów lub świadczeniem usług. Poza wykorzystaniem kontroli biznesowych, autentyczność pochodzenia i integralność treści faktury elektronicznej są zachowane, w szczególności, w przypadku wykorzystania: 1) bezpiecznego podpisu elektronicznego, lub 2) elektronicznej wymiany danych zgodnie z umową w sprawie europejskiego modelu wymiany danych elektronicznych, jeżeli zawarta umowa dotycząca tej wymiany przewiduje stosowanie procedur gwarantujących autentyczność pochodzenia faktury i integralność jej danych.

[11] *J. Zubrzycki*, Leksykon VAT, Wrocław 2013, s. 261.

[12] Druk sejmowy Sejmu VII kadencji, Nr 805, http://orka.sejm.gov.pl/Druki7ka.nsf/0/42A423413920C894C1257A9900529576/%24File/805.pdf, s. 63, [dostęp dnia 30 sierpnia 2016 r.].

5. Faktura elektroniczna w postępowaniu sądowym

Pomimo ustawowego wskazania elementów składowych faktury VAT, nie jest ona dokumentem urzędowym w rozumieniu art. 244 k.p.c.[13]. Zgodnie z tym przepisem dokument urzędowy powinien zostać sporządzony w przepisanej formie przez powołany do tego organ w zakresie jego działania, a w przypadku dokumentu prywatnego wymagane jest złożenie na nim podpisu[14]. Art 244 k.p.c. nie rozstrzyga o znaczeniu dokumentu dla wyniku procesu, reguluje on jedynie formalną moc dowodową dokumentów urzędowych i nakazuje traktować jako udowodnioną daną treść dokumentu[15].

Dokumenty urzędowe korzystają z domniemania autentyczności, które oznacza, że z samego faktu przedłożenia dokumentu należy wywieść wniosek o jego pochodzeniu od osoby lub organu, który na dokumencie figuruje jako jego wystawca[16]. Ponadto dokumenty urzędowe korzystają z domniemania zgodności treści dokumentu z prawdą, które nakazuje uznać za zgodne z prawdą to, co w sposób urzędowy zostało w dokumencie zaświadczone. Dla wyprowadzenia wniosków o zgodności treści dokumentu urzędowego z prawdą wystarczające jest samo przedłożenie dokumentu przez stronę, o ile dokument ten spełnia wymogi stawiane przez ustawę dokumentom urzędowym[17].

W związku z tym, że faktura elektroniczna nie spełnia wymagań ustawowych, aby można ją było ją uznać za dokument urzędowy, stanowi ona dokument prywatny. Zgodnie z art. 245 k.p.c. dokument prywatny w formie pisemnej albo elektronicznej stanowi dowód tego, że osoba, która go podpisała złożyła oświadczenie zawarte w dokumencie. Oznacza to, że z faktu przedłożenia dokumentu prywatnego należy wyprowadzić wniosek o autentyczności pochodzenia zawartego w nim oświadczenia od wystawcy, który go własnoręcznie podpisał[18]. Jak wskazał Sąd Najwyższy dokumenty prywatne nie korzystają z domniemania zgodności z prawdą oświadczeń w nich zawartych, a więc każda osoba mająca w tym interes prawny może stwierdzić i dowodzić, że treść złożonych oświadczeń nie odpowiada stanowi rzeczywistemu[19].

Na gruncie prawa podatkowego z kolei fakturę, również elektroniczną, można zakwalifikować jako dokument publicznoprawny[20]. Na podstawie tego dokumentu organ podatkowy ocenia spełnienie obowiązku podatkowego, nie ma jednak podstaw, by korzystała ona z domniemania prawdziwości[21]. Faktury wystawiane w formie elektronicznej przesyła się i udostępnia w tej formie odbiorcy, co oznacza, że w razie konieczności przedstawienia takiej faktury jako dowodu w sprawie sądowej należy przedłożyć nośnik z utrwalonym na nim dokumentem lub udostępnić ją w postaci elektronicznej[22].

---

[13] *B. Kaczmarek- Templin*, Dowód, s. 263.
[14] *E. Rudkowska- Ząbczyk*, w: Dowody w postępowaniu cywilnym (red. *Ł. Błaszczak, K. Markiewicz, E. Rudkowska- Ząbczyk*), Warszawa 2010, s. 416.
[15] Zob. wyrok SN z dnia 5 września 2008 r., I CSK 117/08, Legalis.
[16] *E. Rudkowska- Ząbczyk,* w: Dowody, s. 414.
[17] *S. Dalka*, Dowód z dokumentów w sądowym postępowaniu cywilnym, Palestra 1974, Nr 8-9 s. 47.
[18] *E. Marszałkowska- Krześ* (red.), Postępowanie cywilne, Warszawa 2011, s. 205.
[19] Zob. wyrok SN z dnia 28 lutego 2007 r., V CSK 441/06, niepubl.
[20] *G. Nauka*, Faktura VAT w obrocie prawnym, PiP 2008, Nr 4, s. 93.
[21] *B. Kaczmarek- Templin*, Dowód, s. 263.
[22] *Ibidem.*

W tym miejscu należy podkreślić możliwość wykorzystania faktury VAT jako szczególnego rodzaju dowodu w postępowaniu nakazowym. Jak stanowi art. 485 k.p.c. w postępowaniu nakazowym sąd wydaje nakaz zapłaty, jeżeli powód dochodzi roszczenia pieniężnego albo świadczenia innych rzeczy zamiennych, a okoliczności uzasadniające dochodzone żądanie są udowodnione dołączonym do pozwu dokumentem urzędowym lub dokumentem prywatnym w postaci zaakceptowanego przez dłużnika rachunku, wezwania dłużnika do zapłaty i pisemnego oświadczenia dłużnika o uznaniu długu, zaakceptowanego przez dłużnika żądania zapłaty, zwróconego przez bank i niezapłaconego z powodu braku środków na rachunku bankowym. Rachunek w powyższym rozumieniu oznacza każdy dokument rozliczeniowy w tym także fakturę, w którym wystawca potwierdza wykonanie umowy, określa wartość świadczenia oraz stronę zobowiązaną do zapłaty i umożliwia dłużnikowi podjęcie czynności mających na celu sprawdzenie, czy świadczenie jest uzasadnione co do zasady i wysokości[23]. Badanie dokumentu rozliczeniowego pod kątem możliwości wydania nakazu zapłaty powinno uwzględniać zarówno ogólną ocenę wiarygodności dokumentu, jak i jego zawartość pod względem treści wymaganej przez przepisy właściwych ustaw, a w szczególności ustawy o rachunkowości oraz u.p.t.u.[24]. Zaakceptowany przez dłużnika rachunek to w istocie faktura, przy czym w tym przypadku akceptacja następuje na ogół poprzez podpisanie jej przez osobę upoważnioną do jej przyjęcia[25]. Możliwe jest także dopuszczenie wydania nakazu w postępowaniu nakazowym na podstawie faktury, która nie została zaakceptowana przez dłużnika po jej wystawieniu, jeśli w zawartej wcześniej umowie dłużnik zgodził się na uiszczanie należności w określonej z góry wysokości, formie i po wystawieniu faktury przez wierzyciela (wypadek akceptacji faktury *ex ante*)[26]. Szczegółowe elementy faktury określa rozporządzenie Ministra Finansów z dnia 17 grudnia 2010 r. w sprawie przesyłania faktur w formie elektronicznej, zasad ich przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej, nie ma natomiast wśród nich podpisu wystawcy ani nabywcy. Wątpliwości wywołuje zagadnienie, czy faktura, która z mocy upoważnienia ustawowego nie musi zawierać żadnych podpisów, może stanowić podstawę wydania nakazu zapłaty. Jeszcze na tle już nieobowiązującego § 20 ust. 1 pkt 13 rozporządzenia Ministra Finansów z dnia 8 grudnia 1994 r. w sprawie wykonania przepisów ustawy o podatku od towarów i usług oraz o podatku akcyzowym[27], który przewidywał możliwość aby faktura zawierała czytelne podpisy osób uprawnionych do jej wystawienia i otrzymania Sąd Najwyższy uznał, iż upoważnienie powoda przez pozwanego do wystawienia faktur VAT bez podpisu może być traktowane jako zaakceptowanie przez dłużnika rachunku uzasadniające wydanie przez sąd nakazu zapłaty[28]. W sytuacji, gdy przepisy przewidują możliwość skutecznego wystawienia dokumentu bez podpisu wystawcy, dokument ten może stanowić podstawę do wydania nakazu zapłaty[29].

[23] *M. Manowska*, w: Kodeks postępowania cywilnego. Komentarz (red. *M. Manowska*), Warszawa 2013, s. 912.
[24] *Ibidem.*
[25] *K. Flaga- Gieruszyńska*, w: Kodeks postępowania cywilnego. Komentarz (red. A. Zieliński), Warszawa 2014, s. 944, por. wyrok SA w Poznaniu z dnia 13 marca 2007 r., I ACa 1096/06, niepubl.
[26] *S. Cieślak*, Glosa do wyroku SN z 23.2.2006 r., II CSK 131/05, Palestra 2007, Nr 11–12, s. 273.
[27] Dz. U. Nr 133, poz. 688 ze zm.
[28] Zob. wyrok SN z dnia 23 lutego 2006 r., II CSK 131/05, PS 2007, Nr 4, s. 145.
[29] *M. Manowska*, w: Kodeks, s. 912.

W związku z powyższymi uwagami należy stwierdzić, iż prawidłowo wystawiona faktura stanowi podstawę do wydania nakazu zapłaty tylko wtedy, gdy nie budzi wątpliwości[30]. Natomiast należy zauważyć, że zaakceptowanie rachunku przez dłużnika może nastąpić w każdy możliwy sposób, co w przypadku faktur oznacza obowiązek jej podpisania przez osobę upoważnioną do przyjęcia, co jest równoznaczne z akceptacją[31]. Brak podpisu na fakturze uniemożliwia wydanie nakazu zapłaty na podstawie art. 485 § 1 ust. 2 k.p.c. Nie ma poza tym uzasadnienia dla żądania przedłożenia, poza dokumentem rozliczeniowym, pisemnego uznania długu[32]. W sytuacji natomiast, gdy brakuje pisemnego oświadczenia dłużnika o uznaniu długu, obok faktury czy rachunku koniecznie trzeba przedstawić dokument potwierdzający dochodzenie roszczenia (umowa, z której wynika obowiązek zapłaty)[33].

W art. 485 k.p.c. nie wskazano żadnych wymogów co do formy dokumentu zatem bez względu na postać, każda faktura może być dowodem w postępowaniu nakazowym, w tym również faktura elektroniczna[34].

Doręczenie dłużnikowi faktury jest wezwaniem go do spełnienia świadczenia pieniężnego wówczas, gdy zawarto w nim stosowną wzmiankę co do sposobu i czasu zapłaty[35]. Jeżeli w taki sposób napisana faktura zostanie przyjęta przez dłużnika (np. poprzez jej podpisanie przez osobę uprawnioną tj. czynność równoznaczną z niewłaściwym uznaniem długu) to może ona stanowić podstawę do wydania nakazu zapłaty na podstawie art. 485 § 1 ust. 1 pkt 3[36]. Jeżeli faktura nie zawiera wzmianki o sposobie i terminie płatności to w przypadku jej przyjęcia przez dłużnika będzie ona stanowić podstawę do wydania nakazu zapłaty na podstawie art. 485 § 1 ust. 1 pkt 2[37].

6. Podsumowanie

Należy uznać, iż dokument elektroniczny stanowi metodę skutecznego i trwałego przechowywania treści oświadczenia w widzialnej postaci znaków językowych[38]. Wszelkie zmiany wprowadzane przez ustawodawcę na rzecz ułatwienia w stosowaniu faktur elektronicznych, w szczególności rezygnacja z obowiązku wykorzystania bezpiecznego podpisu elektronicznego lub obowiązku elektronicznej wymiany danych (EDI) do zapewnienia autentyczności i integralności, należy ocenić bardzo pozytywnie. Zdecydowanie zwiększyło to dostępność i ułatwiło przedsiębiorcom wystawianie e-faktur. Wprowadzenie do przepisów prawa regulacji związanych z dokumentem elektronicznym jest najlepszym przykładem na to, że prawo dostosowuje się i zmienia do potrzeb zakreślanych przez nowoczesne technologie.

---

[30] *B. Kaczmarek- Templin*, Dowód, s. 263
[31] *M. Manowska,* w: Kodeks, s. 912.
[32] *B. Kaczmarek- Templin*, Dowód, s. 263
[33] *M. Manowska,* Dokumenty, s. 38.
[34] *B. Kaczmarek- Templin*, Dowód, s. 266.
[35] Zob. uchwała SN z dnia 19 maja 1992 r., III CZP 56/92, OSNCP 1002, Nr 12, poz. 219.
[36] Zob. wyrok SN z dnia 23 października 2001 r., I CKN 323/99, OSNC 2002, Nr 7-8, poz. 94.
[37] *R. Flejszar*, w: Kodeks postępowania cywilnego. Tom I. Komentarz do art. 1-729 (red. *A. Góra-Błaszczykowska*), Warszawa 2013, s. 1201.
[38] *B. Kaczmarek- Templin*, Dowód, s. 294.

mgr Maria Dymitruk

Czy dynamiczne zmiany doby nowych technologii uzasadniają niedookreśloność przepisów karnych prawa autorskiego? – uwagi na tle art. 115 ust. 3 Prawa autorskiego oraz wyroku Trybunału Konstytucyjnego z dnia 17 lutego 2015 r. (K 15/13)

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[39] przewiduje dwa reżimy odpowiedzialności za naruszenie wspomnianych praw: odpowiedzialność cywilnoprawną i odpowiedzialność karną. W rozdziale 14 Prawa autorskiego zatytułowanym „Odpowiedzialność karna" ustawodawca zdecydował się na spenalizowanie czynów, stanowiących najbardziej rażące naruszenia praw autorskich lub praw pokrewnych. Wszystkie wskazane w art. 115 – art. 119 Prawa autorskiego czyny są przestępstwami powszechnymi, a więc takimi, które mogą być popełnione przez każdą osobę zdolną do ponoszenia odpowiedzialności karnej[40]. Art. 115 ust. 3 Prawa autorskiego wskazujący, że „*Kto w celu osiągnięcia korzyści majątkowej w inny sposób niż określony w ust. 1 lub 2 narusza cudze prawa autorskie lub prawa pokrewne określone w art. 16, art. 17, art. 18, art. 19 ust. 1, art. 19[1], art. 86, art. 94 ust. 4 lub art. 97, albo nie wykonuje obowiązków określonych w art. 19[3] ust. 2 lub art. 20 ust. 1-4, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku*", penalizuje naruszenie autorskich praw osobistych i majątkowych, prawa do artystycznych wykonań, prawa do fonogramów i wideogramów oraz prawa do nadań programów w jakikolwiek inny sposób niż poprzez: przywłaszczenie sobie autorstwa, wprowadzenie w błąd co do autorstwa, rozpowszechnianie bez podania nazwiska lub publiczne zniekształcenie[41]. Przedmiotem ochrony są więc tutaj zarówno prawa osobiste, jak i prawa majątkowe[42].

Przestępstwo z art. 115 ust. 3 Prawa autorskiego ma charakter bezskutkowy (formalny), a chwilą jego popełnienia jest moment ukończenia samego czynu zabronionego. Bez znaczenia pozostają ewentualne dalsze konsekwencje zachowania danej osoby[43]. Czyn sprawcy może być zarówno działaniem, jak i zaniechaniem zachowania, do którego sprawca był zobowiązany, a jego penalizacja uzależniona jest od umyślności[44]. Przepis art. 115 ust. 3 Prawa autorskiego posługuje się bowiem sformułowaniem „*kto w celu osiągnięcia korzyści majątkowej (...) narusza"*. Zastosowanie przez ustawodawcę zwrotu „*w celu*" oznacza, że omawiane

[39] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2016 r. poz. 666 ze zm.), zwana dalej „Prawem autorskim".
[40] J. Raglewski, *Odpowiedzialność karna* [w:] D. Flisak (red.), *Prawo autorskie i prawa pokrewne. Komentarz LEX*, Warszawa 2015, s. 1410.
[41] J. Sieńczyło-Chlabicz (red.), *Prawo własności intelektualnej,* Warszawa 2015, s. 253.
[42] K. Święcka, J. S. Święcki, *Prawo autorskie i prawa pokrewne. Komentarz. Wybór międzynarodowych aktów prawnych*, Warszawa 2004, s. 182.
[43] Z. Ćwiąkalski [w:] J. Barta, R. Markiewicz (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, Warszawa 2011, s. 724.
[44] J. Sieńczyło-Chlabicz (red.), dz. cyt., s. 253.

przestępstwo ma charakter kierunkowy i może być popełnione jedynie z zamiarem bezpośrednim[45]. „Korzyść majątkową" należy tu rozumieć w zgodzie z brzmieniem art. 115 § 4 Kodeksu karnego[46] jako „*korzyść zarówno dla siebie, jak i dla kogo innego*". Osobą trzecią, która odniosłaby ewentualną korzyść majątkową, może być osoba zupełnie niezwiązana ze sprawcą czynu[47]. Chodzi tutaj o każdego rodzaju korzyść majątkową, a więc o jakiekolwiek dobro w najszerszym tego słowa znaczeniu, obejmujące zarówno zwiększenie aktywów majątkowych, jak i zmniejszenie pasywów (przysporzenie majątkowe, uniknięcie lub ograniczenie straty etc.)[48]. Korzyść ta nie musi mieć substratu materialnego[49]. Przyświecający sprawcy cel, jakim jest osiągnięcie korzyści majątkowej, odróżnia zaś konstrukcję omawianego przestępstwa od czynów wskazanych w art. 115 ust. 1 (przywłaszczenie autorstwa, wprowadzenie w błąd co do autorstwa) oraz art. 115 ust. 2 Prawa autorskiego (rozpowszechnianie bez podana nazwiska lub pseudonimu twórcy), które mogą być dokonane dla osiągnięcia jakiejkolwiek korzyści (nie tylko majątkowej, ale także osobistej)[50]. Zauważyć należy jednak, że poniesienie odpowiedzialności karnej na podstawie art. 115 ust. 3 Prawa autorskiego nie jest uzależnione od tego, czy sprawca faktycznie korzyść majątkową uzyskał. Wystarczy jedynie, że taki był jego pierwotny cel, a nieistotne, czy zamierzenie to sprawca osiągnął[51].

Najistotniejszy – z punktu widzenia oceny przepisu art. 115 ust. 3 Prawa autorskiego – pozostaje jednak sposób określenia czynności sprawczej („naruszenie w inny sposób"). Ustawodawca nie zdecydował się na precyzyjne określenie czynu, którego dokonanie skutkuje pociągnięciem do odpowiedzialności karnej, poprzestając na dość lakonicznym sformułowaniu „inne naruszenie". Tak ujęty sposób popełnienia czynu zabronionego wywołał uzasadnioną krytykę wśród przedstawicieli literatury przedmiotu. Niedookreślenie czynu zabronionego powoduje bowiem, że art. 115 ust. 3 Prawa autorskiego penalizuje różne zachowania sprawcy, niewskazane wprost przez ustawodawcę. Przekłada się to bezpośrednio na znaczące trudności w prawidłowej kwalifikacji prawnej zachowania sprawcy i budzi uzasadnione wątpliwości co do konstytucyjności przepisu art. 115 ust. 3 Prawa autorskiego. W literaturze przedmiotu wskazuje się, że zwrot „*w inny sposób niż określony (...) narusza…*" oznacza taki dobór znamion czynu zabronionego, który stoi w sprzeczności z podstawową zasadą prawa karnego *nullum crimen sine lege,* znajdującą swoje odzwierciedlenie w art. 1 k.k. W efekcie nie zostaje spełniona funkcja gwarancyjna prawa karnego[52]. Wśród przedstawicieli literatury przedmiotu podnosi się, że przepis art. 115 ust. 3 Prawa autorskiego zawiera otwarty katalog znamion czynu zabronionego, co uniemożliwia jednoznaczne rozstrzygnięcie, jakie zachowania podlegają

[45] J. Raglewski, dz. cyt., s. 1427; M. Bojarski (red.), *System Prawa Karnego. Tom 11. Szczególne dziedziny prawa karnego. Prawo karne wojskowe, skarbowe i pozakodeksowe,* Warszawa 2014, s. 1082.
[46] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 2016 r. poz. 1137), zwana dalej „k.k.".
[47] J. Raglewski, dz. cyt., s. 1428.
[48] K. Święcka, J. S. Święcki, dz. cyt., s. 182.
[49] J. Raglewski, dz. cyt., s. 1428.
[50] Z. Ćwiąkalski [w:] J. Barta, R. Markiewicz (red.), *Prawo autorskie…*, s. 735.
[51] J. Raglewski, dz. cyt., s. 1428.
[52] Z. Ćwiąkalski [w:] J. Barta, R. Markiewicz (red.), *Ustawa o prawie autorskim i prawach pokrewnych, Warszawa 2001,* s. 682; M. Mozgawa, J. Radoniewicz, *Przepisy karne w prawie autorskim. Zagadnienia teorii i praktyki,* Prokuratura i prawo 1997, nr 7 – 8, s. 13.

wskazanej w przepisie karze[53]. Oznacza to, że w omawianym przypadku nie zostaje spełniona jedna z podstawowych funkcji prawa karnego, jaką jest motywowanie adresatów norm prawa karnego do zachowań z nimi zgodnych.

Podobne wątpliwości co do konstytucyjności omawianego przepisu powziął Rzecznik Praw Obywatelskich, decydując się na wystąpienie z wnioskiem[54] do Trybunału Konstytucyjnego o stwierdzenie niezgodności art. 115 ust. 3 Prawa autorskiego z art. 42 ust. 1 Konstytucji[55], stanowiącym, że: „*odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia*", a tym samym wyrażającym zasadę określoności czynów zabronionych pod groźbą kary. Rzecznik we wskazanym wniosku do Trybunału Konstytucyjnego wskazał, że ustawodawca, wprowadzając określoną w art. 115 ust. 3 Prawa autorskiego odpowiedzialność karną, nie zachował wystarczającej precyzji, co w efekcie spowodowało, że „*każde bliżej niesprecyzowane i podjęte w celu osiągnięcia korzyści majątkowej działanie (...) rodzi odpowiedzialność karną*[56]". Powołując się na dotychczasowe orzecznictwo Trybunału Konstytucyjnego, Rzecznik Praw Obywatelskich wskazał, że „*zasada określoności czynu zabronionego pod groźbą kary, (...) nakazuje ustawodawcy takie wskazanie czynu zabronionego (jego znamion), aby zarówno dla adresata normy prawnokarnej, jak i organów stosujących prawo i dokonujących «odkodowania» treści regulacji w drodze wykładni normy prawa karnego nie budziło wątpliwości to, czy określone zachowanie in concreto wypełnia te znamiona*[57]". Rzecznik Praw Obywatelskich wskazał także, że niedoprecyzowanie elementów normy prawa karnego pozwala na dowolność w jej stosowaniu przez organy władzy publicznej oraz penalizowanie zachowań, które nie zostały wprost wskazane jako zabronione, co w efekcie powoduje „zawłaszczanie" pewnych sfer życia obywateli. Poprzez swój wniosek Rzecznik Praw Obywatelskich postawił Trybunałowi Konstytucyjnemu problematyczne pytania: Czy do pogodzenia z zasadami demokratycznego państwa prawnego jest istnienie norm prawnych, które nie rodzą po stronie jednostki pewności co do tego, czy jej zachowania są zgodne z prawem czy nie? Czy dopuszczalne jest istnienie takich przepisów karnych, których treść nie pozwala obywatelowi na jednoznaczne zrekonstruowanie prawnokarnych konsekwencji swojego zachowania?

Wątpliwości Rzecznika Praw Obywatelskich co do konstytucyjności przepisu art. 115 ust. 3 Prawa autorskiego podzielił także Prokurator Generalny[58], wskazując w swoim stanowisku w niniejszej sprawie, że „*ustawodawca nie może wymagać od obywatela uświadomienia sobie zakresu zakazu karnego i przestrzegania go, jeżeli sam nie jest w stanie*

[53] Ćwiąkalski [w:] J. Barta, R. Markiewicz (red.), *Prawo autorskie…*, s. 735; E. Ferenc-Szydełko (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz,* Warszawa 2016, s. 1031; P. Kardas, T. Sroka, W. Wróbel (red.), *Państwo prawa i prawo karne. Księga jubileuszowa Profesora Andrzeja Zolla, t. II,* Lex 2012, Wybrane zagadnienia przedawnienia karalności przestępstw przewidzianych w ustawie o prawie autorskim i prawach pokrewnych, punkt II.

[54] Wniosek Rzecznika Praw Obywatelskich z dnia 11 kwietnia 2013 r. nr RPO-729135-II-13/ST, zwany dalej „Wnioskiem Rzecznika".

[55] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.), zwana dalej „Konstytucją".

[56] Wniosek Rzecznika, s. 3 – 4.

[57] Tamże, s. 5.

[58] Stanowisko Prokuratora Generalnego z dnia 22 sierpnia 2013 r. nr PG VIII TK 38/13.

określić wyraźnie jego granic[59]". Odmienny pogląd wyraził zaś Sejm Rzeczypospolitej Polskiej[60]. Zdaniem Marszałka Sejmu art. 115 ust. 3 Prawa autorskiego pozostaje w zgodnie z zasadą wyrażoną w art. 42 ust. 1 Konstytucji. W stanowisku Sejmu wyrażono opinię, zgodnie z którą zawężenie zakresu penalizacji czynu określonego w przepisie art. 115 ust. 3 Prawa autorskiego poprzez takie określenie znamion jego strony podmiotowej, które ogranicza możność ukarania tylko do tych sprawców, który działali w zamiarze kierunkowym (*dolus coloratus*), tj. w celu osiągnięcia korzyści majątkowej, uzasadnia konstytucyjność omawianego przepisu. Stwierdzono ponadto, że z zasady określoności przepisów prawa karnego nie można wywodzić obowiązku tworzenia przez ustawodawcę kazuistycznych regulacji karnoprawnych[61], a syntetyczne ujmowanie przepisów prawa karnego, będące właściwe dla współczesnego sposobu typizacji przestępstw, wymaga ograniczenia rozmiaru dyspozycji przepisów karnych.

Postępowanie przez Trybunałem Konstytucyjnym wszczęte na wniosek Rzecznika Praw Obywatelskich zakończyło się wydaniem dnia 17 lutego 2015 r. wyroku, w którym Trybunał orzekł o zgodności przepisu art. 115 ust. 3 Prawa autorskiego z Konstytucją[62]. Trybunał nie podzielił więc wątpliwości Rzecznika Praw Obywatelskich ani Prokuratora Generalnego co do konstytucyjności brzmienia omawianego przepisu. W uzasadnieniu wyroku Trybunał podkreślił, że przepis art. 115 ust. 3 Prawa autorskiego, zawierający określenie „*w inny sposób niż (...)*", stanowi jedynie dopełnienie przepisów art. 115 ust. 1 i ust. 2, w których ustawodawca wskazał najbardziej typowe naruszenia podlegające penalizacji. Trybunał, powołując się na swoje dotychczasowe orzecznictwo, wskazał, że wynikająca z art. 42 ust. 1 Konstytucji zasada określoności ustawy karnej nie wyklucza posługiwania się przez ustawodawcę zwrotami niedookreślonymi lub ocennymi (o ile możliwe jest ustalenie ich desygnatów), jak również podkreślił, że standard określoności przepisów prawnych nie wymaga jasności czy komunikatywności wyrażenia zakazu lub nakazu prawnego w stopniu absolutnym[63]. Zastosowanie przez ustawodawcę w przepisie art. 115 ust. 3 Prawa autorskiego pojęć niedookreślonych Trybunał uzasadnił zarówno istnieniem marginesu swobody regulacyjnej państwa, jak również charakterem regulacji prawnoautorskiej, „*stosowanej w warunkach dynamicznych zmian doby nowych technologii*".

Uzasadnione wątpliwości budzić powinno poparcie Trybunału Konstytucyjnego dla tak szerokiego jak w art. 115 ust. 3 Prawa autorskiego ujęcia odpowiedzialności karnej. W literaturze przedmiotu podnoszono, że przepis ten w sposób nieuzasadniony uprzywilejowuje twórców, artystów wykonawców, producentów fonogramów i wideogramów oraz organizacje radiowe i telewizyjne[64]. Z konstrukcji przepisu wynika, że każde naruszenie ich praw (o ile dokonane będzie w celu osiągnięcia korzyści majątkowej) zrodzi odpowiedzialność karną, a przecież relacje tworzone przez prawo własności intelektualnej mają charakter cywilistyczny. Wydaje się, że przepis art. 115 ust. 3 w sposób zbyt intensywny

[59] Tamże, s. 33.
[60] Stanowisko Sejmu Rzeczypospolitej Polskiej z dnia 30 stycznia 2014 r. nr BAS-WPTK-961/13.
[61] Tamże, s. 15 – 16.
[62] Wyrok Trybunału Konstytucyjnego z dnia 17 lutego 2015 r. (sygn. akt K 15/13), OTK Seria A 2015 nr 2, poz. 16.
[63] Zob. wyrok Trybunału Konstytucyjnego z dnia 28 stycznia 2003 r. (sygn. akt K 2/02), OTK ZU nr 1/A/2003, poz. 4.
[64] Z. Ćwiąkalski [w:] J. Barta, R. Markiewicz (red.), *Ustawa…*, s. 684.

wkracza w stosunki cywilnoprawne, wyręczając uprawnionego w dochodzeniu jego roszczeń[65]. Wprowadzenie odpowiedzialności karnej za konkretne naruszenie prawa powinno stanowić *ultima ratio* (środek ostateczny) w staraniach o ochronę danego dobra prawnego. Trudno uznać, że taki przypadek zachodzi w omawianej sytuacji. Bardziej racjonalne wydaje się ukształtowanie ochrony prawnokarnej jako ochrony uzupełniającej w stosunku do tej gwarantowanej przez normy prawa cywilnego, a dodatkowo znajdującej zastosowanie np. tylko w przypadkach charakteryzujących się znacznym stopniem społecznej szkodliwości[66]. Wśród przedstawicieli literatury przedmiotu wyrażane jest również stanowisko, że penalizacja czynów określonych w przepisie art. 115 ust. 3 Prawa autorskiego jest zbędna, ponieważ ochrona praw majątkowych gwarantowana pozostałymi przepisami rozdziału 14 Prawa autorskiego jest ukształtowana na dostatecznym poziomie[67].

Pamiętać należy, że przestępstwo stypizowane w art. 115 ust. 3 Prawa autorskiego ścigane jest obecnie z oskarżenia publicznego z urzędu[68]. Z punktu widzenia podmiotu, którego prawa zostały naruszone, o wiele bardziej atrakcyjnym środkiem ochrony będzie złożenie zawiadomienia o podejrzeniu popełnienia przestępstwa, a następnie zgłoszenie wniosku o nałożenie na sprawcę obowiązku naprawienia szkody, o którym mowa w art. 46 Kodeksu karnego, niż dochodzenie swoich praw na drodze powództwa cywilnego (związanego – co oczywiste – z koniecznością poniesienia kosztów sądowych). Ogół tych argumentów, częściowo zauważonych przez Trybunał, został w uzasadnieniu wyroku odparty jedynie lakonicznym stwierdzeniem, że „*w granicach swobody ustawodawcy, która oczywiście limitowana jest przepisami Konstytucji, mieści się wybór instrumentów prawa karnego jako właściwych dla dochodzenia roszczeń z tytułu naruszenia praw autorskich lub praw pokrewnych*". Trudno uznać takie wytłumaczenie Trybunału za kompleksowe i wszechstronne rozważenie argumentów od lat podnoszonych w literaturze przedmiotu. Warto również podkreślić, że nie ma racji Trybunał Konstytucyjny, twierdząc w uzasadnieniu wyroku, że „*Dobrem chronionym przez art. 115 ust. 3 ustawy o prawie autorskim i prawach pokrewnych jest »ojcostwo« utworu i artystycznego wykonania*". Przepis wskazanego artykułu chroni bowiem zarówno autorskie prawa osobiste (w tym prawo do „ojcostwa" utworu), jak również autorskie prawa majątkowe.

Po lekturze uzasadnienia wyroku można odnieść wrażenie, że Trybunał zasadniczo widzi i rozumie problem zaakcentowany zarówno przez Rzecznika Praw Obywatelskich, jak i Prokuratora Generalnego – wątpliwość co do konstytucyjności posługiwania się przez ustawodawcę w przepisach kreujących odpowiedzialność karną zwrotami niedookreślonymi. Jednakże, jak wskazuje się w uzasadnieniu orzeczenia, „*sięgnięcie przez ustawodawcę do pojęć niedookreślonych wynika z charakteru regulacji prawnoautorskiej, stosowanej w warunkach*

[65] Dla zobrazowania intensywności ochrony praw w art. 115 ust. 3 Prawa autorskiego można wyobrazić sobie sytuację, w której ustawodawca podjąłby próbę stworzenia analogicznej do art. 115 ust. 3 Prawa autorskiego normy, która penalizowałaby dokonane w celu osiągnięcia korzyści majątkowej naruszenia praw na gruncie Kodeksu cywilnego (własności, innych praw rzeczowych, dóbr osobistych etc.). Wydaje się, że taka próba aktywności legislacyjnej spotkałaby się ze znaczącą dezaprobatą środowiska prawniczego (zwrócili na to uwagę R. Markiewicz, S. Sołtysiński, *Konstytucyjne aspekty praw autorskich (uwagi na marginesie dwóch orzeczeń Trybunału Konstytucyjnego),* Państwo i Prawo 12/2015, s. 8 – 9).

[66] Propozycję taką wysunął J. Raglewski, dz. cyt., s. 1399.

[67] Tamże, s. 1425.

[68] Do dnia 1 września 2005 r. przestępstwo z art. 115 ust. 3 Prawa autorskiego ścigane było z oskarżenia prywatnego (zob. J. Raglewski, dz. cyt., s. 1428).

dynamicznych zmian doby nowych technologii". Powyższa teza wydaje się być najbardziej kontrowersyjna ze wszystkich przedstawionych przez Trybunał Konstytucyjny, a dodatkowo nie została ona w żaden sposób rozwinięta ani jakkolwiek uargumentowana. Czy rozwój nowych technologii faktycznie może uzasadniać niedookreśloność przepisów karnych? Wydaje się, że za takim stanowiskiem stoi następujące rozumowanie: postęp technologiczny stale przekształca otaczającą nas rzeczywistość, w efekcie czego zmianom ulegają również techniczne możliwości korzystania z dzieł chronionych prawami autorskimi (pojawiają się nowe, dotychczasowe podlegają znaczącym przekształceniom). W konsekwencji powyższych przemian ustawodawca staje przed wyzwaniem odpowiedniego zabezpieczenia twórców, a jako że nie jest w stanie przewidzieć wszystkich możliwych rodzajów naruszeń praw autorskich (a w efekcie ich spenalizować), sięga po pojęcia co prawda nieprecyzyjne, ale za to rodzące nadzieję na większą praktyczną skuteczność. Podobne stanowisko w tym zakresie przestawił Sejm Rzeczypospolitej Polskiej, który w cytowanym już stanowisku w sprawie konstytucyjności przepisu art. 115 ust. 3 Prawa autorskiego stwierdził, że niezwykle dynamiczny rozwój techniki powoduje, że regulacje prawne błyskawicznie tracą na aktualności i stają się nieadekwatne do dynamicznie zmieniającej się rzeczywistości. To zaś zmusza ustawodawcę do częstych nowelizacji, niekorespondujących ze stabilnością prawa[69]. Jakie remedium na powyższy problem proponuje Trybunał Konstytucyjny? Przyzwolenie na niedookreśloność przepisów prawa karnego.

Należy stanąć na stanowisku przeciwstawnym do poglądu wyrażonego w komentowanym orzeczeniu Trybunału Konstytucyjnego. Skala zmian technologicznych nie powinna łagodzić dotychczas obowiązującego nakazu zachowania przez ustawodawcę najwyższego stopnia precyzji w określaniu zakresu odpowiedzialności karnej. Trudno znaleźć racjonalne argumenty przemawiające za poglądem, że w obliczu zmian technologicznych obywatel ma ponosić większe ryzyko związane ze skierowaniem do niego prawnego zakazu, którego nawet sam ustawodawca nie potrafi precyzyjnie określić. Z konstytucyjnego postulatu maksymalnej określoności przepisów karnych wynika, że powinny one charakteryzować się dostateczną precyzyjnością, pozwalającą na bezproblemowe odkodowanie przez adresata normy prawnej znamion czynu zabronionego. Nie wydaje się, żeby „*daleko idące niedogodności*" wynikające z dynamicznego rozwoju techniki, a związane z tworzeniem norm w obszarze praw autorskich i praw pokrewnych, o których wspomniano w cytowanym stanowisku Sejmu[70], uzasadniały zwiększenie ryzyka prawnego po stronie obywatela.

Należy również stanąć na stanowisku, że dynamiczne zmiany doby nowych technologii nie uzasadniają nadmiernego ograniczenia sfery wolności korzystania z dóbr intelektualnych. Nie powinny one również skutkować niedostosowaniem przepisów prawa do współczesnych uwarunkowań cywilizacyjnych i potrzeb społeczeństwa informacyjnego. Pewnego rodzaju paradoksem byłaby bowiem sytuacja, w której dzięki postępowi techniki (głównie rozwojowi Internetu) obywatel wyposażony zostaje w nieosiągalne wcześniej możliwości korzystania z przedmiotów ochrony prawa autorskiego, ale w konsekwencji tegoż postępu nie jest w stanie precyzyjnie określić, które z jego internetowych aktywności są prawnie dopuszczalne, a dokonanie których stworzy ryzyko jego odpowiedzialności karnej. Stan taki

[69] Stanowisko Sejmu Rzeczypospolitej Polskiej z dnia 30 stycznia 2014 r., s. 17 – 18.
[70] Tamże.

w nieuzasadniony sposób wpływałby na sferę wolności użytkowników dóbr intelektualnych. Uzasadnione byłoby również stwierdzenie, że nadmierna ochrona własności intelektualnej stanowić może wręcz zagrożenie dla dalszego postępu nauki i techniki.

Niezaprzeczalnym faktem jest, że zmieniająca się rzeczywistość technologiczna (w tym przede wszystkim rozwój Internetu i innych środków porozumiewania się na odległość) stanowi poważne wyzwanie dla ustawodawcy. Wydaje się jednak, że w konsekwencji rozwoju nowych technologii nie powinno się godzić na taką regulację prawnokarną, która powoduje, że adresat norm prawnych nie jest w stanie ocenić, czy jego zachowania mogą zostać zakwalifikowane jako przestępstwo. Możliwa jest wręcz argumentacja, że Trybunał Konstytucyjny w omawianym orzeczeniu potwierdził swoją (i ustawodawcy) bezradność wobec różnorodności stanów faktycznych, które przynosi rzeczywistość wirtualna. Skoro w toczącej się przez Trybunałem Konstytucyjnym dyskusji podniesiono, że rozwój technologiczny powoduje, że regulacje prawne błyskawicznie tracą na aktualności, przez co stają się nieadekwatne do aktualnego etapu rozwoju techniki, to dlaczego nie podjęto próby stawienia czoła temu wyzwaniu. Należałoby bowiem zastanowić się, czy w zakresie obowiązków ustawodawcy w obliczu rozwoju nowych technologii pozostaje kreowanie takich regulacji, które pozostają aktualne niezależnie od postępów techniki, w efekcie zapewniają stałość prawa i pogłębiają zaufanie obywateli do państwa i stanowionego przezeń prawa. Wydaje się, że odpowiedź na powyższe pytanie powinna być twierdząca. Zupełnie niezrozumiałe pozostaje zatem podejście Trybunału do „świata nowych technologii". Zgodnie ze jego stanowiskiem jest to rzeczywistość uzasadniająca rozluźnienie wymogów, które spełniać powinny regulacje prawnokarne. Z powyższego można wyciągnąć wniosek, że Trybunał Konstytucyjny poczytuje rozwój technologiczny jako pewnego rodzaju stan atypowy, uzasadniający nieprecyzyjność regulacji karnej. Wydaje się, że jest to podejście błędne, ponieważ świat nowych technologii to jedyny świat, w jakim przyjdzie ustawodawcy tworzyć regulacje prawne. Nie jest to więc sytuacja nietypowa bądź przejściowa. Ustawodawca (i Trybunał Konstytucyjny) powinien zdawać sobie sprawę, że rzeczywistość technologiczna podlegać będzie stałej ewolucji i stanowić będzie nieodłączny element współczesnego świata, a w efekcie będzie musiała być brana pod uwagę przy prawie każdej aktywności legislacyjnej ustawodawcy (w tym być może przede wszystkim w zakresie aktywności legislacyjnej na polu prawa własności intelektualnej).

mgr Aleksandra Godek

Problemy i wątpliwości związane z Bitcoinami w świetle praktyki organów podatkowych

1. Uwagi wstępne – charakterystyka bitcoinów

Bitcoiny są tematyką nową, ale coraz częściej stanowią przedmiot badań na gruncie wielu dziedzin polskiego prawa. Potwierdza to zarówno różnorodność tematyczna rozważań poczynionych na konferencji zorganizowanej przez Forum Mediów Elektronicznych, którego owocem jest publikacja pokonferencyjna obejmująca niniejsze opracowanie, jak również obecność bitcoinów w wielu aspektach gospodarczej codzienności, jak technika, ekonomia, czy prawo.

Zainteresowanie bitcoinami wynika przede wszystkim z jego charakteru, na który składają się elementy techniczne i ekonomiczne – jest to zapisany na twardym dysku jako plik zbiór cyfr i liter bez wartości, oprócz przyjętej w nieoficjalnej umowie uznającej bitcoiny za pieniądz[71]. Bitcoin to nazwa własna[72]. W literaturze przedmiotu podkreśla się jego zdematerializowany charakter – nie istnieje bowiem żaden fizyczny odpowiednik, surogat bitcoina – jest to pieniądz fiducjarny[73]. Wartość bitcoina jest ustalona w sposób umowny, uwierzytelniony dzięki systemowi informatycznemu zarządzającemu emisją i obrotem tej waluty, zaś jego cena to wynik zderzenia ze sobą podstawowych praw rynku: popytu i podaży[74]. Bitcoina można scharakteryzować wskazując jego techniczne cechy, takie jak: możliwość przesyłania go za pomocą sieci między dowolnymi adresami na świecie, transakcje, mające go za przedmiot mogą być dokonywane w sposób anonimowy i mogą być odbierane niezależnie od tego, czy komputer odbiorcy jest włączony, czas transakcji liczony jest w sekundach, a przeprowadzane transakcje są nieodwracalne[75] i obarczone limitem 21 milionów bitcoinów[76]. Jego techniczny charakter niesie ze sobą wiele potencjalnych zagrożeń – w szczególności należy podkreślić, że wirtualne pieniądze mogą łatwo stać się przedmiotem kradzieży (zarówno on-line – w przypadku ataków na tzw. portfele on-line, jak i poprzez wejście do osobistego komputera i pozyskanie danych z dysku twardego), można ograniczyć dostępność do systemu

[71] G. Rosłan, M. P. Stolarski, *Cyfrowa waluta bitcoin – nowe zagrożenie dla systemu finansowego. Część II,* Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie nr 2(27)2014, s. 275.
[72] K. Zacharzewski, *Bitcoin jako przedmiot stosunków prawa prywatnego,* Monitor Prawniczy nr 21 rok 2014, s. 1132.
[73] D. Homa, *Sekrety bitcoina i innych kryptowalut. Jak zmienić wirtualne pieniądze w realne zyski,* Gliwice 2015, s. 19.
[74] *Ibidem*, s. 19-20.
[75] Nieodwracalność transakcji stanowi poważne zagrożenie dla obrotu bitcoinem w szczególności w sytuacji, gdy druga ze stron umowy jej nie dotrzyma; G. Rosłan, M. P. Stolarski, *Cyfrowa waluta bitcoin...*, s. 284.
[76] D. Homa, *op. cit.*, s. 20-21.

i opóźnić transfer środków, a także śledzić wszystkie transakcje w zakresie sieci, czy też stworzyć dodatkowe elementy, fałszywe części sieci, które będą stanowić etap pośredni danych transakcji (do transakcji można również dołączyć dodatkowe, niedozwolone dane)[77]. Mając na uwadze powyższe należy wskazać, że wszelkie negatywne konsekwencje o charakterze technicznym związane z funkcjonowaniem bitcoinów, mają bezpośrednie znaczenie dla skutków ekonomicznych wywoływanych ich obrotem – na uwypuklenie zasługuje zwłaszcza potencjalne zagrożenie destabilizacji ekonomicznej państwa, wyłączenie interwencjonizmu państwowego na tym obszarze działalności gospodarczej bądź przeciwnie – uznaniem w obliczu prawa bitcoinów za nielegalne[78].

Dotychczasowe rozważania mają znaczenie zwłaszcza z uwagi na to, że na gruncie normatywnym brak jednoznacznej kwalifikacji bitcoinów, ponieważ ustawodawca nie uregulował tej materii poprzez wprowadzenie powszechnie obowiązującej, legalnej definicji. Kwestia ta nie znajduje unormowania zarówno w prawie międzynarodowym, europejskim, jak i krajowym. Europejski Bank Centralny dokonał określenia waluty wirtualnej jako "cyfrową reprezentację wartości, niewyemitowaną przez bank centralny, instytucję kredytową lub instytucję pieniądza elektronicznego, która w pewnych okolicznościach może być użyta jako alternatywa dla pieniędzy", ale nie będącą pieniądzem z prawnego punktu widzenia[79].

Wskazany powyżej krok w kierunku określenia czym jest waluta wirtualna, wykonany przez najważniejszą instytucję z punktu widzenia europejskiej unii gospodarczej i walutowej, nie znajduje odzwierciedlenia w obowiązującym polskim prawie – wobec tego, wirtualne środki umożliwiające dokonywanie rozliczeń na podobieństwo pieniędzy nie są zdefiniowanym, prawnie uregulowanym, powszechnie używanym i akceptowanym środkiem płatniczym. Zgodnie z art. 2 ust. 1 pkt 6 ustawy Prawo dewizowe[80] krajowymi środkami płatniczymi są waluta polska oraz papiery wartościowe i inne dokumenty, pełniące funkcję środka płatniczego, wystawione w walucie polskiej. W punkcie 7 omawianego artykułu, ustawodawca wskazał, że walutą polską są znaki pieniężne (banknoty i monety) będące w kraju prawnym środkiem płatniczym, a także wycofane z obiegu, lecz podlegające wymianie, zaś z punktu 10 wynika, że walutami obcymi są znaki pieniężne (banknoty i monety) będące poza krajem prawnym środkiem płatniczym, a także wycofane z obiegu, lecz podlegające wymianie. Bitcoiny jako rodzaj waluty wirtualnej, nie mieszczą się w zakresie żadnej z podanych powyżej definicji. W tym zakresie, nie spełniają również wymogów stawianych przez ustawę o usługach płatniczych[81], która w art. 2 pkt 29 stanowi, że transakcją płatniczą jest zainicjowana przez płatnika lub odbiorcę wpłata, wypłata lub transfer środków pieniężnych, zaś na gruncie z art. 2 pkt 27 jako system płatności jest rozumiany system transferu środków pieniężnych oparty na formalnych i znormalizowanych zgodnie z przepisami ustawy o ostateczności rozrachunku[82]. Nie istnieje centralny organ, który nadzorowałby emitowanie

[77] G. Rosłan, M. P. Stolarski, *Cyfrowa waluta bitcoin...,* s. 276-279.
[78] *Ibidem,* s. 285-286.
[79] Europejski Bank Centralny, *Virtual Currency Schemes - a further analysis,* luty 2015 r., s. 25 za Pismo Podsekretarza Stanu z dnia 28 maja 2015 r., *Regulacje dotyczące wirtualnej waluty Bitcoin,* Ministerstwo Finansów, nr LEX 263724.
[80] Ustawa z dnia 27 lipca 2002 r. - Prawo dewizowe (Dz. U. z 2012 r. poz. 826 z późn. zm.).
[81] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2014 r. poz. 873 z późn. zm.).
[82] Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami (Dz. U. z 2013 r. poz. 246 z późn. zm.).

bitcoinów oraz ich funkcjonowanie w obrocie[83]. Ponadto, bitcoiny jako wirtualna waluta nie spełniają wymogów uznania ich za powszechny środek płatniczy, nie podlegają obowiązującym regulacjom prawnym i z tego względu stanowią swoisty synonim luki w prawie, która nie jest wypełniona pomimo ich funkcjonowania w obrocie jako przedmiotu stosunków prawa prywatnego i jako skutek tych stosunków – będąc przedmiotem stosunków prawa publicznego.

Na gruncie prawa prywatnego, można wyróżnić szereg aspektów, w jakich bitcoin może znaleźć zastosowanie. W pierwszej kolejności warto wskazać na stanowisko wyrażone w doktrynie o tym, że dla prawa cywilnego bitcoin w swojej konstrukcji może stanowić środek symbolizujący prawo podmiotowe, a także stanowi miernik wartości inny niż pieniądz, zgodnie z art. 358^1 § 2 kodeksu cywilnego[84]. Mając na uwadze powyższe należy wskazać, że w rozumieniu art. 44 kc nie jest rzeczą, ale stanowi pewnego rodzaju mienie – jest zbywalny i stanowi prawo majątkowe[85]. W stosunkach obligacyjnych stanowi określoną wierzytelność[86]. W tym zakresie, bitcoin może mieć zastosowanie w stosunkach cywilnoprawnych jako przykładowo możliwość wskazania wartości odsetek w bitcoinach jako innego niż pieniądz miernika wartości, czy jako formę kary umownej, odstępnego oraz zadatku, czy też dokonać potrącenia wierzytelności wyrażonych za pomocą bitcoina[87].

Wskazane sytuacje powstające na gruncie prawa prywatnego stanowią przyczynę wystąpienia zdarzeń prawnopodatkowych. Najbardziej problematyczna kwestią w tym zakresie wydaje się niesprecyzowany i niejednoznaczny charakter prawny bitcoinów – skutki podatkowe należy bowiem poddawać analizie z punktu widzenia jedynie przepisów ogólnych[88]. W tym miejscu warto w szczególności podkreślić, że opodatkowanie bitcoinów jako rodzaju wirtualnej waluty, która nie jest prawnie uregulowana, jest świadectwem na uznanie ich legalności[89] - jest to zatem niejako wyjście przed działania samego ustawodawcy, wyprzedzenie ich; praktyka stwarza w ten sposób pewien schemat postępowania z bitcoinami, który nie ma oparcia w powszechnie obowiązujących przepisach. Dlatego, coraz częściej pojawiające się skutki podatkowe dotyczące bitcoinów budzą wiele wątpliwości wśród podatników. Znajduje to odzwierciedlenie w zwiększeniu się ilości wydawanych przez Ministra Finansów interpretacji indywidualnych prawa podatkowego. W systemie informacji podatkowej prowadzonego on-line przez Ministerstwo Finansów można odnaleźć 23 wydane indywidualne interpretacje podatkowe dotyczące bitcoinów[90]. W 2013 r. zostały wydane jedynie 2 interpretacje dotyczące skutków prawnopodatkowych obrotu bitcoinami na gruncie podatku od towarów i usług. W 2014 r. interpretacji zostało wydanych 21, a przedstawiane przez podatników wątpliwości dotyczyły nie tylko podatku od towarów i usług, ale również podatku dochodowego od osób fizycznych oraz podatku dochodowego od osób prawnych.

---

[83] G. Rosłan, M. P. Stolarski, *Cyfrowa waluta bitcoin...,* s. 282.
[84] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.); K. Zacharzewski, *op. cit.,* s. 1133.
[85] K. Zacharzewski, *op. cit.,* s. 1133.
[86] *Ibidem,* s. 1134.
[87] *Ibidem,* s. 1137-1139.
[88] J. Prokurat, *Podatkowe aspekty obrotu wirtualnymi walutami,* pkt 3., Przegląd Podatkowy 2015/3/24-37, LEX nr 248854.
[89] J. Prokurat, *op. cit.,* pkt 3.
[90] dostępne on-line na podstronie portalu: http://www.finanse.mf.gov.pl/web/wp/pp; dostęp na dzień 3 lipca 2015r.

Celem niniejszego opracowania jest przedstawienie, w jaki sposób kreuje się stanowisko organów podatkowych wobec obrotu bitcoinami i jego skutkami podatkowymi poprzez przedstawienie wybranych zagadnień wyjaśnianych w wydawanych przez Ministra Finansów interpretacjach indywidualnych prawa podatkowego oraz dokonanie analizy problemów i wątpliwości podatkowych, z jakimi na tym etapie funkcjonowania bitcoina w polskiej rzeczywistości prawnej borykają się podatnicy.

2. Obrót bitcoinami a powstanie obowiązku podatkowego w podatku od towarów i usług w świetle indywidualnych interpretacji prawa podatkowego

Podatek od towarów i usług[91] jest rodzajem podatku obrotowego, którego osią konstrukcyjną jest opodatkowanie obrotu[92]. Podatek ten ma charakter wielofazowy[93]. Podmiot tego podatku nie jest w rzeczywistości obciążany nim ekonomicznie – jego istota polega bowiem na neutralności cenowej dla przedsiębiorców w poszczególnych fazach obrotu i faktycznym obciążeniu ostatecznego konsumenta w momencie wyłączeniu towaru z obrotu (podatek konsumpcyjny)[94]. Podatek od towarów i usług, jako powszechny podatek konsumpcyjny, dotyczy w równej mierze wszystkich dóbr dostępnych na rynku, dlatego nie wpływa na konkurencję rynkową i pozostaje neutralny dla międzynarodowej wymiany towarów[95]. W tym zakresie niezbędne wydaje się uwypuklenie profesjonalnego charakteru tego podatku – zgodnie z art. 15 omawianej ustawy, jego podatnikami są osoby prawne, jednostki organizacyjne niemające osobowości prawnej oraz osoby fizyczne wykonujące samodzielnie działalność gospodarczą bez względu na cel lub rezultat tej działalności. Opodatkowanie tym podatkiem dotyczy odpłatnej dostawy towaru lub odpłatnego świadczenia usług, przy czym nie jest istotne czy przedmiot podatku mieścił się w warunkach i formach określonych prawem[96]. Podstawą opodatkowania jest cena netto, a obok niej wyodrębnia się podatek od towarów i usług obliczony według jednej ze stawek – 22% (obecnie podwyższona do 23%), 0% (dla eksportu towarów oraz dla wewnątrzwspólnotowej dostawy towarów), 5% i 7% (obecnie podwyższona do 8%)[97].

W zakresie wydawanych indywidualnych interpretacji prawa podatkowego dotyczących wpływu obrotu bitcoinami na podatek od towarów i usług, w pierwszej kolejności należy wskazać na wątpliwości podatników związane z tym, czy czynności polegające na przekazaniu bitcoinów nabytych za pośrednictwem specjalistycznego portalu internetowego podlegają opodatkowaniu podatkiem od towarów i usług. W interpretacji indywidualnej prawa podatkowego wydanej przez Dyrektora Izby Skarbowej w Poznaniu, z dnia 8 stycznia 2014 r.,

[91] Wprowadzony ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. Dz.U. 2004 nr 54 poz. 535 z późn. zm.).
[92] R. Mastalski, *Prawo podatkowe,* s. 505.
[93] R. Mastalski, *Podatek od towarów i usług [w:] Prawo finansowe 2. wydanie poszerzone i uaktualnione red. nauk. R. Mastalski, E. Fojcik-Mastalska,* Warszawa 2013, s. 318.
[94] R. Mastalski, *Prawo...*, s. 521.
[95] *Ibidem*, s. 521.
[96] R. Mastalski, *Podatek od towarów...*, s. 321-322.
[97] *Ibidem,* s. 324-325.

sygn. ILPP1/443-912/13-2/AW, organ wskazał, że usługą (świadczeniem) jest każde zachowanie (działanie bądź zaniechanie). Jednakże oceniając charakter świadczenia jako usługi należy pamiętać, że usługą jest tylko takie świadczenie, w przypadku którego istnieje bezpośredni konsument, odbiorca świadczenia odnoszący z niego korzyść, musi istnieć bezpośredni związek przyczynowy pomiędzy świadczoną usługą a otrzymanym świadczeniem wzajemnym – wynagrodzenie powinno być konsekwencją wykonanego odpłatnego świadczenia. Organ podkreślił, że w przypadku przekazania osobom trzecim bitconów występuje prowizja za dokonywany obrót, co wypełnia przesłankę odpłatności. Dlatego, obrót bitcoinami powinien podlegać zasadniczej, podstawowej stawce podatku od towarów i usług, w obecnie ustalonej wysokości 23%.

W ramach pobocznych rozważań warto przytoczyć pogląd Dyrektora Izby Skarbowej w Katowicach wyrażony w indywidualnej interpretacji prawa podatkowego z dnia 14 listopada 2013 r., sygn. IBPP2/443-762/13/Icz, zgodnie z którym, jeżeli działalność usługowa podatnika występującego z wnioskiem o wydanie interpretacji, polegająca na obrocie bitcoinami została sklasyfikowana przez Urząd Statystyczny w Łodzi w grupowaniu PKWiU 66.19.99.0, czyli jako pozostałe usługi wspomagające usługi finansowe, z wyłączeniem ubezpieczeń i funduszów emerytalnych, to podatnik jest zwolniony z obowiązku prowadzenia ewidencji przy zastosowaniu kasy rejestrującej. Organ wskazał, że zgodnie z § 2 rozporządzenia Ministra Finansów w sprawie zwolnień z obowiązku prowadzenia ewidencji przy zastosowaniu kas rejestrujących[98] z obowiązku ewidencjonowania w danym roku podatkowym, nie później jednak niż do dnia 31 grudnia 2014r., zwalnia się czynności wymienione w załączniku do rozporządzenia. We wspomnianym załączniku, pod pozycją 23, wymienione zostały usługi finansowe i ubezpieczeniowe (PKWiU 64-66) - zwolnienie nie zostało ograniczone do czynności wykonywanych wyłącznie przez takie instytucje finansowe jak banki, jest to bowiem zwolnienie o charakterze przedmiotowym (uzależnione od przedmiotu prowadzonej działalności, a nie od podmiotu, który ją prowadzi). Zatem, w tej konkretnie wskazanej sytuacji podatnika i dokonaniu takiej klasyfikacji przez Urząd Statystyczny, każda transakcja wraz z wielkością należnej prowizji będzie dokumentowana przez system informatyczny, z którego w sposób jednoznaczny będzie wynikało z jakiej transakcji wynika konkretna prowizja, będzie także ewidencjonował na kontach użytkowników zawarte transakcje oraz zapłacone prowizje uwidocznione w raportach, będących podstawą wyliczenia dochodu i dlatego nie jest konieczne prowadzenie rejestracji transakcji za pomocą kasy fiskalnej.

Wątpliwości podatników dotyczyły również sprzedaży bitcoinów przez podatnika na rzecz podmiotów prowadzących i nieprowadzących działalność gospodarczą na terenie Unii Europejskiej i poza jej granicami, w tym prawidłowego ustalenia miejsca opodatkowania usług. Dyrektor Izby Skarbowej w Warszawie, w interpretacji indywidualnej prawa podatkowego z dnia 31 grudnia 2014 r., sygn. IPPP3/443-1020/14-2/KT uznał za prawidłowe stanowisko podatnika, który wskazał, że w takiej sytuacji podejmowane przez niego czynności nie będą podlegały opodatkowaniu podatkiem od towarów i usług na terytorium kraju. Organ w szczególności zwrócił uwagę na zakres przedmiotowy ustawy o podatku od towarów i usług oraz wprowadzonego przez nią rozumienia świadczenia usług. Nadto, analiza przepisów

[98] Rozporządzenie Ministra Finansów z dnia 29 listopada 2012 r. w sprawie zwolnień z obowiązku prowadzenia ewidencji przy zastosowaniu kas rejestrujących (Dz. U. z 2012 r. poz. 1382).

dokonana przez organ doprowadziła go do konkluzji, że bitcoina nie można traktować tak samo, jak inne prawne środki płatnicze i nie jest, w prawnym sensie, powszechnie stosowany w rozliczeniach międzynarodowych – nie jest używany przez instytucje publiczne i nie funkcjonuje jako instrument rynku pieniężnego. Zatem, sytuacja dokonywania sprzedaży na rzecz podmiotów działających na terenie Unii Europejskiej lub poza nią, musi zostać poddana rozważaniom z punktu widzenia zasad ustalania miejsca świadczenia. W omawianej interpretacji organ zwrócił uwagę na to, że miejsce opodatkowania usługi należy ustalić na podstawie przepisów dotyczących miejsca świadczenia usług. Miejsce świadczenia usługi jest jednocześnie miejscem jej opodatkowania. Usługa sprzedaży bitcoinów to, jak już zostało wskazane wcześniej, ma charakter usług elektronicznych, świadczonych za pomocą sieci internetowej, których miejsce świadczenia zależy od podmiotu, na rzecz którego usługa jest wykonywana. Co do zasady, miejscem świadczenia usług w przypadku świadczenia usług na rzecz podatnika jest miejsce, w którym podatnik będący usługobiorcą posiada siedzibę działalności gospodarczej, a w przypadku, gdy usługi są świadczone dla stałego miejsca prowadzenia działalności gospodarczej podatnika, które znajduje się w innym miejscu niż jego siedziba działalności gospodarczej, miejscem świadczenia tych usług jest to stałe miejsce prowadzenia działalności gospodarczej. Przepisy ustawy o podatku od towarów i usług uzależniają określenie miejsca świadczenia usługi od statusu podmiotu, na rzecz którego usługa jest świadczona - a w przypadku, gdy odbiorcą usługi jest podmiot niebędący podatnikiem od miejsca, w którym znajduje się jego siedziba lub miejsce zamieszkania. W sytuacji, gdy usługa świadczona jest na rzecz podatnika - miejsce świadczenia tej usługi określa się na podstawie zasady ogólnej. W przypadku, gdy usługa jest świadczona na rzecz podmiotu niebędącego podatnikiem, posiadającego siedzibę, stałe lub zwykłe miejsce zamieszkania poza terytorium kraju - miejsce świadczenia usługi ustala się w oparciu o art. 28c omawianej ustawy. Jeśli natomiast odbiorcą usługi jest podmiot niebędący podatnikiem, posiadający siedzibę, stałe lub zwykłe miejsce zamieszkania poza terytorium Unii Europejskiej, to w odniesieniu do pewnych kategorii usług miejsce świadczenia ustala się na podstawie zasady szczególnej określonej w art. 28l omawianej ustawy – w przypadku usług elektronicznych na podstawie pkt 10 wskazanego artykułu. Podobne rozważania zostały poczynione przez Dyrektora Izby Skarbowej w Warszawie w wydanej przez niego indywidualnej interpretacji prawa podatkowego z dnia 24 czerwca 2014 r., sygn. IPPP2/443-243/14-4/BH.

Kolejnym, ważkim problemem przedstawionym przez podatników, było pytanie o możliwość zastosowania zwolnienia z opodatkowania podatkiem od towarów i usług obrotu bitcoinami. Dyrektor Izby Skarbowej w Poznaniu, w interpretacji indywidualnej prawa podatkowego z dnia 21 października 2014 r., sygn. ILPP1/443-626/14-2/HW stanął na stanowisku, że działalność gospodarcza założona w celu sprzedaży bitcoinów może korzystać jedynie ze zwolnienia od podatku VAT, gdy wartość sprzedaży nie przekroczy kwoty określonej w art. 113 ust. 1 ustawy o podatku od towarów i usług (150.000 zł), w proporcji do okresu prowadzonej działalności przy założeniu, że podatnik nie wykona innych czynności, które ze zwolnienia korzystać nie mogą (określonych w omawianej ustawie). Na powyższe nie ma wpływu zawieszenie działalności gospodarczej spowodowane czasowym zaprzestaniem dokonywania sprzedaży w danym okresie czasu wakacyjnym - nie wpływa to na zmniejszenie kwoty limitu uprawniającej do korzystania ze zwolnienia w podatku od towarów i usług. Uzasadniając swoje stanowisko, organ szczególną uwagę zwrócił na art. 43 ust. 1 pkt 7 ustawy

o podatku od towarów i usług, który stanowi, że zwalnia się od podatku transakcje, łącznie z pośrednictwem, dotyczące walut, banknotów i monet używanych jako prawny środek płatniczy, z wyłączeniem banknotów i monet będących przedmiotami kolekcjonerskimi, za które uważa się monety ze złota, srebra lub innego metalu oraz banknoty, które nie są zwykle używane jako prawny środek płatniczy, lub które mają wartość numizmatyczną, a także na pkt 40 omawianego artykułu, który stanowi, że zwalnia się od podatku usługi w zakresie depozytów środków pieniężnych, prowadzenia rachunków pieniężnych, wszelkiego rodzaju transakcji płatniczych, przekazów i transferów pieniężnych, długów, czeków i weksli oraz usługi pośrednictwa w świadczeniu tych usług. Jak wskazał organ w omawianej interpretacji, Trybunał Sprawiedliwości Unii Europejskiej wielokrotnie podkreślał, że zakres zwolnień przewidzianych w Dyrektywie VAT nie może być interpretowany w sposób rozszerzający - czynności zwolnione z opodatkowania stanowią autonomiczne pojęcia prawa wspólnotowego, a ich ujednolicona interpretacja ma służyć unikaniu rozbieżności w stosowaniu systemu podatku VAT w poszczególnych państwach członkowskich, zaś zgodnie z utrwalonym orzecznictwem, pojęcia używane do opisania zwolnień wymienionych w art. 13 szóstej dyrektywy powinny być interpretowane w sposób ścisły, ponieważ stanowią one odstępstwa od ogólnej zasady, zgodnie z którą podatkiem VAT objęta jest każda dostawa towarów i każda usługa świadczona odpłatnie przez podatnika (por. wyrok TSUE z dnia 19 listopada 2009 r. C-461/08 w sprawie Don Bosco Onroerend Goed BV). W tym zakresie, jak zauważył organ, zgodnie z art. 31 ustawy o Narodowym Banku Polskim, znakami pieniężnymi Rzeczypospolitej Polskiej są banknoty i monety opiewające na złote i grosze, zaś jak wynika z art. 32 wskazanej ustawy, znaki pieniężne emitowane przez NBP są prawnymi środkami płatniczymi na obszarze Rzeczypospolitej Polskiej. Organ odniósł się również do ustawy o usługach płatniczych, aby ustalić, czy jej przepisy w rozpatrywanym zakresie są tożsame z pojęciem świadczenia usług na gruncie ustawy o podatku od towarów i usług oraz ustawy Prawo bankowe[99] i wprowadzonym w niej katalogiem czynności bankowych. Na bazie tych ustaleń organ wskazał, że bitcoin pełni funkcje elektronicznej waluty, ale nie posiada uregulowania w przepisach prawa, nie ma centralnego organu, ani jakiejkolwiek instytucji sprawującej nad nią nadzór i przez to nie może być traktowany na równi z prawnym środkiem płatniczym, bowiem nie funkcjonuje on jako instrument rynku pieniężnego w rozumieniu odrębnych przepisów. Nie jest zatem walutą uznawaną jako prawny środek płatniczy. Dlatego, obrotu bitcoinami nie można uznać za usługi w rozumieniu wyżej wskazanych ustaw i w tym zakresie będzie to czynność podlegająca opodatkowaniu podatkiem od towarów i usług. Jednakże, podatnik może skorzystać ze zwolnienia od podatku na podstawie i według zasad określonych przepisami art. 113 ust. 1-12 ustawy, pod pewnymi warunkami: wartość sprzedaży nie przekroczyła łącznie w poprzednim roku podatkowym kwoty 150.000 zł (ustawa wskazuje, czego nie zalicza się w ramach ustalania wartości sprzedaży do tej kwoty). Zatem, skorzystanie ze zwolnienia przez Wnioskodawcę będzie możliwe do czasu, gdy wartość sprzedaży nie przekroczy wskazanej kwoty, w proporcji do okresu prowadzonej działalności przy założeniu, że podatnik nie wykona innych czynności, które ze zwolnienia korzystać nie mogą. W kwestii wpływu zawieszenia działalności gospodarczej przez podatnika na możliwość skorzystania przez niego ze zwolnienia z opodatkowania podatkiem od towarów i usług organ wskazał, że

[99] Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2012 r. poz. 1376, z późn. zm.).

zgodnie przepisami ustawy o swobodzie działalności gospodarczej[100] przedsiębiorca niezatrudniający pracowników może zawiesić wykonywanie działalności gospodarczej na okres od 30 dni do 24 miesięcy. Zawieszenie działalności gospodarczej nie stanowi zaprzestania wykonywania działalności gospodarczej przez podatnika – podatnik w takiej sytuacji nadal pozostaje podatnikiem podatku od towarów i usług z tym, że w okresie zawieszenia wykonywania działalności przedsiębiorca nie prowadzi aktywnej działalności. Zgłoszenie zawieszenia działalności gospodarczej nie oznacza zatem ustania bytu przedsiębiorcy, a jedynie przerwę w wykonywaniu działalności gospodarczej. Wznowienie zawieszonej działalności gospodarczej nie będzie zatem rozpoczęciem działalności, lecz jej kontynuacją. Dlatego, prawo do zwolnienia od podatku od towarów i usług, dotyczy podatnika w pełnej wysokości, niezależnie od zawieszenia działalności gospodarczej w kolejnych latach w trakcie roku podatkowego a następnie jej ponownego wznowienia.

Niezwykle istotne, z punktu widzenia możliwości zastosowania bitcoinów, jest rozpatrywana w interpretacji indywidualnej Dyrektora Izby Skarbowej w Warszawie z dnia 24 czerwca 2014 r., sygn. IPPP2/443-334/14-2/BH, możliwość umarzania zobowiązań przy pomocy alternatywnego środka płatniczego jakim jest Bitcoin i podleganie tej czynności opodatkowaniu podatkiem od towarów i usług. Organ wskazał, że umorzenie długu kontrahentom i uregulowanie zobowiązań za pomocą bitcoinów nie powoduje powstania konsekwencji podatkowych na gruncie podatku od towarów i usług, ponieważ nie jest dostawą towarów ani świadczeniem usług i w tym zakresie nie mieści się w katalogu czynności podlegających opodatkowaniu tym podatkiem. Uzasadniając swoje stanowisko, organ w szczególności zwrócił uwagę na fakt, że bitcoiny to rodzaj waluty, niebędącej prawnym środkiem płatniczym, której funkcjonowanie opiera się na umowie zawartej pomiędzy użytkownikami akceptującymi taką formę płatności. Nie mają mocy umarzania zobowiązań nadanej przez prawodawcę, chyba że płatności dokonywane są na rzecz podmiotów, które akceptują taką formę płatności. Zatem, w sytuacji, gdy zarówno wierzyciel, jak i dłużnik na mocy porozumienia zamierzają rozliczyć powstałe zobowiązania z tytułu dokonanych dostaw towarów, bądź świadczenia usług przy pomocy bitcoinów, powinno dojść do skutecznego umorzenia zobowiązania. Zaznaczyć należy, że ustawa o podatku od towarów i usług nie definiuje również pojęcia „uregulowania" należności wynikającej z faktury dokumentującej dostawę towarów lub świadczenie usług na terytorium kraju. Organ podkreślił, że przez pojęcie „należność uregulowana" należy rozumieć zaspokojenie wierzyciela powodujące wygaśnięcie jego roszczeń wobec dłużnika – strony powinny zatem mieć możliwość ukształtowania uregulowania wierzytelności w jakiejkolwiek formie, poprzez zaspokojenie całości lub części roszczeń wynikających z wierzytelności, wskutek uiszczenia należności przez dłużnika bądź osobę trzecią na rzecz wierzyciela. Jak wskazał organ, wierzytelność jest prawem majątkowym, które może być przedmiotem obrotu gospodarczego. Instytucja potrącenia, odnowienia, zwolnienia z długu została uregulowana w przepisach art. 498-508 kodeksu cywilnego. Zgodnie z art. 506 § 1 kodeksu cywilnego, jeżeli w celu umorzenia zobowiązania dłużnik zobowiązuje się za zgodą wierzyciela spełnić inne świadczenie albo nawet to samo świadczenie, lecz z innej podstawy prawnej, zobowiązanie dotychczasowe wygasa

[100] Art. 14a ust. 1 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2013 r., poz. 672 z późn. zm.)

(odnowienie), jak zaś stanowi art. 508 § 1 omawianej ustawy, zobowiązanie wygasa, gdy wierzyciel zwalnia dłużnika z długu, a dłużnik zwolnienie przyjmuje. Dla skutecznego umorzenia zobowiązania (lub jego części) koniecznym jest zatem zaistnienie dwóch elementów: zwolnienie z długu przez wierzyciela oraz przyjęcie zwolnienia przez dłużnika - zwolnienie z długu jest dwustronną czynnością prawną (umową). Zatem, jak argumentował organ, w przypadku umorzenia długu nie dochodzi do zaspokojenia roszczeń wierzyciela z tytułu istniejącego stosunku cywilnoprawnego łączącego strony transakcji - poprzez uiszczenie należności w jakiejkolwiek części, jednakże należność zostanie uregulowana, a powstałe zobowiązania wygasną, gdyż dług zostanie uregulowany przy pomocy wirtualnej waluty jaką jest bitcoin i z chwilą umorzenia przestanie istnieć. Dlatego, zwolnienia dłużnika z długu przez wierzyciela w okolicznościach przedstawionych we wniosku nie należy utożsamiać z czynnościami podlegającymi opodatkowaniu podatkiem VAT. Podobnej analizy dokonał Dyrektor Izby Skarbowej w Poznaniu, w interpretacji indywidualnej z dnia 8 stycznia 2014 r., sygn. ILPP1/443-910/13-2/Awa.

Mając na względzie poczynione powyżej rozważania należy stwierdzić, że sprzedaż bitcoinów, dokonywanie obrotu bitcoinami, dla celów podatkowych na gruncie podatku od towarów i usług, jest zatem usługą. Zakwalifikowana została jako świadczenie usług elektronicznych i w tym zakresie podlega opodatkowaniu 23% stawką podatku od towarów i usług. Potwierdzają to interpretacje indywidualne – przykładowo, interpretacja Dyrektora Izby Skarbowej w Katowicach z dnia 21 czerwca 2013 r., sygn. IBPP2/443-258/13/Icz, czy interpretacja Dyrektora Izby Skarbowej w Łodzi z dnia 7 kwietnia 2014 r., sygn. IPTPP2/443-52/14-6/IR, zaś samo wydobywanie bitcoinów nie rodzi definitywnego i wymiernego przysporzenia, a zatem nie powoduje powstania zobowiązania podatkowego[101].

3. Skutki obrotu bitcoinami dla podatku dochodowego od osób fizycznych w świetle indywidualnych interpretacji prawa podatkowego

Istotą podatku dochodowego od osób fizycznych jest opodatkowanie osiąganego przez osoby fizyczne dochodu – nadwyżki przychodów nad kosztami poniesionymi w celu ich uzyskania[102]. W tym sensie, opodatkowaniu podlega przyrost majątku powstający w wyniku obrotu gospodarczego jako efekt pracy bądź posiadania określonego kapitału[103]. Ma charakter osobowy[104], powszechny podmiotowo i przedmiotowo[105]. Konstrukcja podatku dochodowego od osób fizycznych oparta jest o wyróżnienie, w formie otwartego katalogu, źródeł przychodów

[101] D. Homa, *op. cit.,* s. 137. Samodzielne wydobywanie bitcoinów nie wiąże się z przyczynowo związaną z nim odpłatnością i w tym zakresie nie wypełnia wymogów stawianych usługom w rozumieniu ustawy o podatku od towarów i usług, a ponadto nie stanowi również nieodpłatnego świadczenia usług w rozumieniu omawianej ustawy; por. J. Prokurat, *op. cit.,* pkt 4.2., LEX nr .....

[102] A. Mariański, *Komentarz do ustawy o podatku dochodowym od osób fizycznych pod red. W. Nykiela, A. Mariańskiego,* Gdańsk 2014, s. 45.

[103] R. Mastalski, *Prawo...,* Warszawa 2014, s. 380.

[104] *Ibidem*, s. 393.

[105] A. Huchla, *Podatek dochodowy od osób fizycznych [w:] Prawo finansowe 2. wydanie poszerzone i uaktualnione red. nauk. R. Mastalski, E. Fojcik-Mastalska,* Warszawa 2013, s. 287.

podlegających opodatkowaniu – podstawą opodatkowania jest bowiem globalna kwota dochodu powstała z łącznie ujętych przychodów, po dokonaniu odliczeń przewidzianych przez ustawę[106]. Warto podkreślić, że podatek dochodowy od osob fizycznych może przybrać również formę ryczałtu podatkowego w postaci ryczałtu od dochodów ewidencjonowanych, karty podatkowej, podatku tonażowego oraz ryczałtu od dochodów osób duchownych. Są to wyjątki od opodatkowania podatkiem dochodowym od osób fizycznych na zasadach ogólnych, które opierają się o progresywne stawki w taryfie szczeblowej – 18% i 32%[107].

W zakresie wydawanych indywidualnych interpretacji prawa podatkowego dotyczących wpływu obrotu bitcoinami na podatek dochodowy od osób fizycznych, należy w pierwszej kolejności wskazać na podnoszone przez podatników wątpliwości czy dochód ze zbycia bitcoinów powinien podlegać opodatkowaniu podatkiem od osób fizycznych. W dalszej kolejności, czy dokonywane transakcje mające za przedmiot bitcoiny należą do kategorii pozarolniczej działalności gospodarczej czy są to transakcje mające za przedmiot kapitały pieniężne i prawa majątkowe (w tym odpłatne zbycie praw majątkowych), a także czy dochód ze zbycia bitcoinów należy uznać za należący do kategorii przychodów od środków pieniężnych podlegających opodatkowaniu stawką podatku w wysokości 19%. Odpowiedzi na powyższe pytania udzielił Dyrektor Izby Skarbowej w Warszawie w interpretacji indywidualnej z dnia 26 czerwca 2014 r., sygn. IPPB1/415-276/14-4/EC, stwierdzając, że przychód ze sprzedaży waluty Bitcoin stanowić będzie przychód z praw majątkowych - zgodnie z art. 18 ustawy o podatku dochodowym od osób fizycznych. Uzyskany dochód należy opodatkować na zasadach ogólnych, tj. wg skali podatkowej i wykazać w zeznaniu rocznym, w terminie do dnia 30 kwietnia następnego roku i w tym samym terminie wpłacić należny podatek. W kwestii kwalifikacji transakcji organ wskazał, że prawa majątkowe na gruncie ustawy o podatku dochodowym od osób fizycznych należy rozumieć jako prawa podmiotowe, mogące występować w trzech postaciach: roszczenia, uprawnienia kształtujące i zarzuty. Odwołując się do doktryny prawa podatkowego, Dyrektor Izby Skarbowej w Warszawie wskazał, że definiowanie praw majątkowych powinno obejmować wykładnię systemową i odnosić się do ustaleń poczynionych na gruncie prawa cywilnego[108]. Prawa majątkowe to rodzaj praw podmiotowych związanych z ekonomicznym interesem uprawnionego: mogą być przedmiotem obrotu i posiadają określoną wartość majątkową. Dalej, organ odwołując się do przepisów ustawy o Narodowym Banku Polskim[109] oraz ustawy o elektronicznych instrumentach płatniczych[110] dokonał analizy obowiązujących przepisów wskazując, co jest powszechnie uznanym środkiem płatniczym i znakami pieniężnymi. Poczynione rozważania doprowadziły organ do konkluzji, że na gruncie polskiego prawa bitcoiny nie mogą być traktowane tak, jak prawne środki płatnicze, bo nie są instrumentem rynku pieniężnego. Zatem, dla celów podatkowych, przychód z tytułu sprzedaży bitcoinów powinien zostać zakwalifikowany jako przychód z praw majątkowych. Organ wskazał ponadto, że przepisy nie stawiają podatnikowi szczególnych wymogów dokumentowania kosztów uzyskania

[106] *Ibidem*, s. 291.
[107] Zob. szerzej, R. Mastalski, *Prawo...*, s. 478.
[108] Zob. A. Gomułowicz, J. Małecki, *Ustawa o podatku dochodowym od osób fizycznych. Komentarz*, Warszawa 2002 s. 93, 153-154.
[109] Ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz. U. z 2005 r., Nr 1, poz. 2 z późn. zm.).
[110] Ustawa z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. z 2012 r., poz. 1232 z późn. zm.).

przychodów z praw majątkowych – zgodnie z ogólnie przyjętą regułą w ustawie o podatku dochodowym od osób fizycznych, za koszty uzyskania przychodów należy uznać wydatki poniesione w celu osiągnięcia przychodów lub zachowania albo zabezpieczenia źródła przychodów, z wyjątkiem wydatków wyłączonych przez ustawę, których nie można uznać za koszty. Zatem, jak wskazał organ podatkowy, jeżeli specyfika transakcji (dokonywanych w ramach „wymiany giełdowej") uniemożliwia pozyskanie dokumentów indywidualizujących strony umowy, a podatnik posiada dokumenty potwierdzające zakup bitcoinów, to mogą one stanowić podstawę do zaliczenia wydatków na nabycie bitcoinów do kosztów uzyskania przychodów. Dalsza część omawianej interpretacji dotyczyła możliwości rozliczenia bitcoinów - czy nabywanie i zbywanie bitcoinów należy rozliczyć tak, że pierwsze zakupione bitcoiny należy uznać za sprzedane jako pierwsze – a zatem, czy przy rozliczaniu bitcoinów należy zastosować księgową metodę FIFO (first in first out – pierwsze przyszło, pierwsze wyszło). Zastosowanie metody FIFO umożliwiłoby, aby wydatek poniesiony na nabycie pierwszych bitcoinów stanowił koszt uzyskania przychodu uzyskanego z bitcoinów zbytych jako pierwsze. Jak wskazał Dyrektor Izby Skarbowej w Warszawie, podatnik może zastosować metodę FIFO, jeżeli dokumentacja transakcji obrotu bitcoinami nie pozwala na ich identyfikację. W tym zakresie warto wskazać, że stanowisko organów podatkowych w zakresie zastosowania tej metody jest zbieżne do prezentowanego przy okazji rozpatrywania innych problemów podatników, również związanych z ograniczoną możliwością identyfikacji poszczególnych składników dokonywanej transakcji. Przykładowo można wskazać problem sprzedaży udziałów, rozważany w indywidualnej interpretacji prawa podatkowego Dyrektora Izby Skarbowej w Poznaniu z dnia 14 października 2014 r., sygn. ILPB3/423-339/14-2/PR, w której organ potwierdził prawidłowość stanowiska podatnika, który wykazywał, że w przypadku, gdy zbywający nie jest w stanie zindywidualizować elementów składających się na zbywany przedmiot w danej transakcji, to podatnik może wtedy oprzeć się na założeniu, na jakim bazuje metoda FIFO.

Warto również wskazać, że opodatkowanie obrotu bitcoinami podatkiem dochodowym jest uzależnione również od tego, w jakim charakterze tego obrotu się dokonuje. Jeżeli jest to działalność profesjonalna, przychód powinien być rozliczony w ramach prowadzonej przez podatnika działalności gospodarczej – w tym zakresie, podatek powinien być płacony w taki sposób, w jaki podatnik jest opodatkowany, a zatem z zastosowaniem skali podatkowej, skali liniowej w wysokości 19% lub określonego ryczałtu[111].

W tym zakresie warto zwrócić uwagę na pytanie zadawane przez podatników w ramach wniosku o wydanie interpretacji indywidualnej prawa podatkowego – czy wobec faktu prowadzenia przez podatnika jednoosobowej działalności gospodarczej w celu prowadzenia handlu bitcoinami (kupnie oraz sprzedaży bitcoinów na giełdach internetowych lub bezpośrednio) i sklasyfikowaniu działalności przez symbol PKWiU 47.00.89.0 - więc sprzedaż detaliczna towarów niekonsumpcyjnych, nieżywnościowych, gdzie indziej niesklasyfikowanych, może rozliczać się w ramach ryczałtu od przychodów ewidencjonowanych w stawce 3%? Jak wskazał Dyrektor Izby Skarbowej w Poznaniu, w interpretacji indywidualnej z dnia 30 października 2014 r., sygn. ILPB1/415-746/14-4/AA, ustawa o zryczałtowanym podatku dochodowym od niektórych przychodów osiąganych przez

[111] D. Homa, *op. cit.*, s. 137.

osoby fizyczne[112] reguluje opodatkowanie zryczałtowanym podatkiem dochodowym niektórych przychodów (dochodów) osiąganych przez osoby fizyczne prowadzące pozarolniczą działalność gospodarczą, którą należy rozumieć zgodnie z przepisami ustawy o podatku dochodowym od osób fizycznych, czyli jako działalność zarobkową: wytwórczą, budowlaną, handlową, usługową, polegającą na poszukiwaniu, rozpoznawaniu i wydobywaniu kopalin ze złóż, polegającą na wykorzystywaniu rzeczy oraz wartości niematerialnych i prawnych; prowadzoną we własnym imieniu bez względu na jej rezultat, w sposób zorganizowany i ciągły; również, gdy działalność ta jest prowadzona w formie spółki cywilnej osób fizycznych lub spółki jawnej osób fizycznych[113]. Uzyskiwane przychody będą mogły podlegać zryczałtowanemu podatkowi, jeżeli nie mogą zostać zaliczone do innych źródeł, zgodnie z art. 10 ust. 1 pkt 1, 2 i 4-9 ustawy o PIT. Zatem, zdaniem organu wyrażonym w omawianej interpretacji indywidualnej, jeżeli podatnik świadczy usługi polegające na sprzedaży detalicznej towarów niekonsumpcyjnych, nieżywnościowych, gdzie indziej niesklasyfikowanych, to przychody z tego tytułu jako przychody z działalności usługowej w zakresie handlu, podlegają opodatkowaniu 3% stawką ryczałtu.

Mając na względzie powyższe warto wskazać, że podatnicy pytali również, czy pomimo przekroczenia przez prowadzoną spółkę cywilną prowadzącą obrót bitcoinami w danym roku kwoty obrotu w wysokości 150.000 EUR, zachowają prawo do opodatkowania przychodów w formie ryczałtu do końca tego roku bez względu na wysokość faktycznie osiągniętego w tym roku obrotu. Dyrektor Izby Skarbowej w Łodzi w interpretacji indywidualnej z dnia 18 lipca 2014 r., sygn. IPTPB1/415-220/14-8/KSU uznał za prawidłowe stanowisko podatnika, który wskazał, że ustawa o zryczałtowanym podatku dochodowym zawiera limity, których nie należy przekroczyć w roku poprzedzającym rok podatkowy, aby nadal można było korzystać z opodatkowania zryczałtowanym podatkiem dochodowym w kolejnym roku. A zatem, pomimo przekroczenia w danym roku kwoty obrotu w wysokości 150.000 EUR, prawo do opodatkowania przychodów w formie ryczałtu zachowane zostanie do końca tego roku, a w kolejnym roku dochody będą podlegały opodatkowaniu na zasadach ogólnych. Na podobnym stanowisku stanęli: Dyrektor Izby Skarbowej w Bydgoszczy w interpretacji indywidualnej wydanej w dniu 15 października 2013 r., sygn. ITPB1/415-804/13/IG, czy przez ten sam organ w interpretacji indywidualnej z dnia 11 października 2013 r., sygn. ITPB1/415-809/13/IG. Zatem, prowadzenie działalności mającej za przedmiot obrót bitcoinami, nie jest obwarowane szczególnymi zasadami na gruncie podatku dochodowego od osób fizycznych, duże znaczenie ma po prostu sposób opodatkowania podatnika, prowadzenie bądź nie przez niego działalności, kwalifikacja rodzaju prowadzonej przez niego działalności. Zasadniczo, do obrotu bitcoinem, mają zastosowanie wszelkie zasady ogólne, jak w przypadku innych uzyskiwanych przez podatników przychodów.

Podobne wątpliwości podatników oraz zbieżne poglądy organów podatkowych na przedstawione powyżej problemy zostały przedstawione m.in. w interpretacji indywidualnej Dyrektora Izby Skarbowej w Łodzi z dnia 18 lipca 2014 r., sygn. IPTPB1/415-221/14-10/KSU

[112] Ustawa z dnia 20 listopada 1998 r. o zryczałtowanym podatku dochodowym od niektórych przychodów osiąganych przez osoby fizyczne (Dz. U. Nr 144, poz. 930, z późn. zm.).
[113] Art. 5a pkt 6 ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz. U. 2015 poz. 766 z późn. zm.)

oraz interpretacjach wydanych przez ten sam organ z dnia 18 lipca 2014 r. o sygn. IPTPB1/415-220/14-7/KSU oraz o sygn. IPTPB1/415-220/14-6/KSU.

Konieczne jest również podkreślenie, że nieco inaczej należy rozpatrywać obrót bitcoinami w porównaniu do samego ich pozyskania – wykopywania bitcoinów lub innego ich nabycia w sposób pierwotny. Takie zdarzenia nie stanowią bowiem, na gruncie podatków dochodowych, definitywnego przysporzenia – nie powstaje wymierny przychód, nie można zatem rozpoznać związanych kosztów uzyskania przychodów[114].

4. Obrót bitcoinami a skutki w podatku dochodowym od osób prawnych w świetle indywidualnych interpretacji prawa podatkowego

Podatek dochodowy od osób prawnych jest podatkiem obciążającym dochód – dodatni efekt prowadzonej przez podatnika działalności[115]. Za dochód należy rozumieć nadwyżkę przychodów nad kosztami ich uzyskania[116]. Zakres przedmiotowy omawianego podatku ma charakter bardziej jednorodny w porównaniu do podatku dochodowego od osób fizycznych – obejmuje bowiem działalność gospodarczą *sensu largo*[117]. Co istotne i odróżniające od podatku dochodowego od osób fizycznych, dochód uzyskiwany przez podatników podatku od osób prawnych jest opodatkowany bez względu na to, z jakiego źródła pochodzi – podatnik ma zatem możliwość potrącenia straty z całego dochodu, jak również z całego dochodu może pokrywać straty w następnych latach[118]. Zakres podmiotowy tego podatku obejmuje osoby prawne, spółki kapitałowe w organizacji oraz jednostki organizacyjne niemające osobowości prawnej, z wyjątkiem spółek niemających osobowości prawnej: spółki cywilnej, spółki jawnej, spółki partnerskiej, spółki komandytowej. Spółka komandytowo-akcyjna, pomimo tego, że jest spółką osobową, jest podatnikiem podatku dochodowego od osób prawnych[119]. Katalog przysporzeń, które mogą być przychodem ma charakter otwarty i prezentuje ich zróżnicowane formy, przykładowo wartości pieniężne czy nieodpłatne świadczenia. Również otwarty katalog przewidział ustawodawca wskazując wymogi stawiane wydatkom, które mogą być uznane za koszty uzyskania przychodów, z zastrzeżeniem jednak kazuistycznie i szczegółowo wskazanych w zamkniętym katalogu wydatków, które za takie koszty nie mogą być uznane. Również odmiennie w stosunku do podatku dochodowego od osob fizycznych kształtuje się stawka podatku dochodowego od osób prawnych – jest to stawka proporcjonalna, liniowa w wysokości 19%. Ma ona zastosowanie do całości podstawy opodatkowania[120].

---

[114] Należy bowiem zauważyć, że *de facto* pierwotne nabycie bitcoinów nie powoduje powstania podstawy opodatkowania i nie jest możliwe inne zakwalifikowanie tego zdarzenia, jak choćby poprzez zaliczenie go do kategorii darowizn czy znalezienia lub zawłaszczenia rzeczy; zob. szerzej J. Prokurat, *op. cit.*, pkt 4.1.

[115] P. Borszowski, A. Huchla, *Podatek dochodowy od osób prawnych [w:] Prawo finansowe 2. wydanie poszerzone i uaktualnione red. nauk. R. Mastalski, E. Fojcik-Mastalska, Warszawa 2013,* s. 294.

[116] *Ibidem*, s. 295.

[117] R. Mastalski, *Prawo...*, s. 424.

[118] *Ibidem*, s. 425.

[119] Od 1 stycznia 2014 r. zgodnie z art. 25 ust. 1 ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych (tekst jedn.: Dz. U. z 2014 r. 851 z późn. zm.)

[120] P. Borszowski, A. Huchla, *op. cit.*, s. 303.

W zakresie obrotu bitcoinami i jego wpływu na powstanie konsekwencji podatkowych w podatku dochodowym od osób prawnych została wydana tylko jedna interpretacja indywidualna prawa podatkowego z dnia 10 lipca 2014 r. przez Dyrektora Izby Skarbowej w Warszawie, sygn. IPPB5/423-397/14-4/MW. Dotyczyła ona wątpliwości podatnika związanych z rozliczaniem kosztów uzyskania przychodu – podatnik zamierzał nabyć bitcoiny, aby przeprowadzić transakcje barterowe ze swoimi kontrahentami, którzy wyrażą zgodę na ten sposób regulowania wzajemnych zobowiązań. Pytanie podatnika dotyczyło tego, w jaki sposób na gruncie ustawy o podatku dochodowym od osób prawnych rozliczać w czasie koszty związane z transakcjami barterowymi – czy stanowią one koszty bezpośrednio związane z przychodami, czy też inne niż bezpośrednio związane z przychodami. W obszernym uzasadnieniu organ wskazał, że w związku z pytaniem wystosowanym przez podatnika należy przede wszystkim zauważyć, że kosztem związanym z transakcją barterową, jest koszt pozyskania bitcoinów. Pierwszym sposobem nabycia Bitcoinów jest ich zakup, zaś drugim sposobem jest ich „wykopanie". Regulacje dotyczące umowy barterowej zawierają przepisy kodeksu cywilnego, który w art. 603 stanowi, że każda ze stron zobowiązuje się przenieść na drugą stronę własność rzeczy w zamian za zobowiązanie się do przeniesienia własności innej rzeczy. Barter jest zatem traktowany jak jeden z rodzajów umowy zamiany, choć jest pojęciem szerszym niż zamiana, której przedmiotem mogą być tylko rzeczy - jest transakcją o charakterze bezgotówkowym, a w jej wyniku dochodzi do wymiany dóbr o tej samej wartości, zaś jej celem jest niedokonywanie dodatkowych rozliczeń pieniężnych pomiędzy kontrahentami. Jak podkreślił organ, barter nie wymaga ponoszenia żadnych kosztów związanych z dokonywaniem zapłaty, a zamieniane dobra muszą równoważyć się wartościowo. Z perspektywy podatku dochodowego od osób prawnych, przy barterze przedmiotem opodatkowania tym podatkiem jest uzyskany przez podatnika dochód - transfer bitcoinów przez podatnika w zamian za usługi biura rachunkowego oraz sprzęt komputerowy, czyli występowanie podatnika jednocześnie w charakterze dostawcy, jak i nabywcy, rodzi konieczność rozpoznania przez strony umowy barterowej odpowiednio przychodu jak i związanego z nim kosztu jego uzyskania. W przypadku umowy barterowej przychodem jest wartość należnych świadczeń wzajemnych określona w umowie, ale wartość tę powinno się jednak określać według cen rynkowych stosowanych w obrocie rzeczami lub prawami tego samego rodzaju i gatunku, z uwzględnieniem w szczególności ich stanu i stopnia zużycia oraz czasu i miejsca uzyskania. Kosztami uzyskania przychodów są zaś wszelkie racjonalnie i gospodarczo uzasadnione wydatki związane z działalnością gospodarczą, których celem jest osiągnięcie, zabezpieczenie lub zachowanie źródła przychodów. Ustawodawca wyróżnia koszty podatkowe bezpośrednio związane z przychodami, których poniesienie przekłada się wprost na uzyskanie konkretnych przychodów oraz inne niż bezpośrednio związane z przychodami, których nie można w taki sposób przypisać do określonych przychodów, ale są racjonalnie uzasadnione jako prowadzące do ich osiągnięcia (tzw. koszty pośrednie). Kwalifikacja danego wydatku jako kosztu pośredniego lub bezpośredniego ma natomiast wpływ na moment jego potrącalności ustalany według przepisu art. 15 ust. 4-4e ustawy o podatku dochodowym od osób prawnych: koszty bezpośrednie są potrącalne w tym roku podatkowym, w którym osiągnięte zostały odpowiadające im przychody, z zastrzeżeniem ust. 4b i 4c, a koszty pośrednie są potrącalne w dacie ich poniesienia. Zatem, mając na uwadze powyższe, organ wskazał, że wydatki na nabycie specjalistycznego sprzętu komputerowego

powinny być rozliczane jako koszty uzyskania przychodu poprzez odpisy z tytułu zużycia środków trwałych oraz wartości niematerialnych i prawnych (odpisy amortyzacyjne) z uwagi na to, że dotyczą środka trwałego.
W dalszej kolejności organ stwierdził, że koszty energii elektrycznej to koszty ogólnozakładowe, związane z ogólnym funkcjonowaniem prowadzonej przez podatnika działalności gospodarczej, których nie da się wprost przypisać do osiąganych przychodów stanowią zatem koszt pośrednio związany z przychodami. Wydatki poniesione na nabycie bitcoinów, należy zaś uznać za bezpośrednio powiązania z przychodem.

Przytoczone powyżej stanowisko organu podatkowego i zaprezentowany zakres wątpliwości podatnika wyraźnie wskazują na to, że obrót bitcoinami w pełni może się mieścić w ogólnych regułach rozpatrywania kosztów uzyskania przychodu w podatku dochodowego od osób prawnych i pomimo braku normatywnego uregulowania jego prawnego charakteru, nie budzi większych wątpliwości na gruncie omawianego podatku, w przeciwieństwie do prezentowanych wcześniej problemów związanych z funkcjonowaniem podatku dochodowego od osób fizycznych.

5. Uwagi końcowe

Mając na uwadze poczynioną powyżej analizę wydanych interpretacji indywidulnych prawa podatkowego należy w szczególności podkreślić sygnalizowany wcześniej problem zaistnienia skutków prawnopodatkowych dokonywania transakcji, które nie mają oparcia w przepisach prawa – nie tyle z uwagi na same mechanizmy przeprowadzanych kontaktów gospodarczych, bo te wynikają z ugruntowanych instytucji prawnych (przykładowo, zawieranie umowy sprzedaży, zamiany, umorzenia długu), ale z perspektywy przedmiotu dokonywanych transakcji – bitcoinów. W ten sposób dochodzi do legalizacji środka, który nie został prawnie scharakteryzowany i nie jest ujęty w żadne normy prawne.

Z tego punktu widzenia należy uznać, że przy braku narzędzi prawnych organy podatkowe rzetelnie wypełniają stojące przed nimi zadania stosując znane im dotychczas instrumenty i oceniając zjawiska związane z bitcoinami przez pryzmat innych podobnych mechanizmów i na podstawie ogólnych reguł i zasad prawa podatkowego.

Warto jednakże zauważyć, że już teraz, przy dość ubogim katalogu sytuacji, w których pojawiają się wątpliwości z bitcoinami, można zauważyć pewne zagubienie organów (chociażby w zakresie posługiwania się odpowiednią nomenklaturą – organy z jednej strony bitcoiny nazywają walutą wirtualną, z drugiej zaś elektronicznymi certyfikatami). Dlatego, wydaje się niezbędne jak najszybsze wprowadzenie jakiejkolwiek regulacji prawnej dotyczącej bitcoinów z uwagi na duży dynamizm ich funkcjonowania w obrocie gospodarczym i prognozowany jego rozwój. Zapewni to nie tylko zabezpieczenie interesów samych użytkowników bitcoinów, ale i również zagwarantuje stabilizację ekonomiczną państwa w tym zakresie.

mgr Paweł Janiec

Rachunek podstawowy w nowelizacji ustawy o usługach płatniczych i niektórych innych ustaw

1. Wstęp

W dobie powszechnej i szybko postępującej informatyzacji społeczeństwa można dostrzec trend przenoszenia czynności do tej pory spotykanych w świecie realnym do Internetu. Ruch ten jest zrozumiały zważywszy na łatwy dostęp do sieci i znaczną oszczędność czasu w przy wykonaniu konkretnych czynności. Sztandarowym przykładem tego kierunku zmian jest handel w Internecie, gdzie co roku odnotowuje się wzrost wartości sprzedanych dóbr za pomocą tego kanału dystrybucji[121]. W kontekście e-handlu omawiany trend występuje również po stronie sprzedawców. Co roku zauważalny staje się przyrost sklepów oferujących towary za pośrednictwem zdematerializowanego kanału dystrybucji, w tym roku zanotowano progres ilości podmiotów partycypujących w rynku rzędu 7%[122].

Nie tylko handel otwiera się na nowe możliwości. Kolejnym polem, gdzie widać znaczącą zmianę w sposobie dotychczasowego funkcjonowania społeczeństw jest sposób płacenia comiesięcznych zobowiązań. Z łatwością można zaobserwować wzrost zapotrzebowania na usługi płatnicze w tej dziedzinie. Według badań Polskiego Radia z 2015 roku już 66% dorosłych Polaków płaci większość swoich miesięcznych zobowiązań za pośrednictwem konta internetowego[123]. Te dwa przykłady dobrze ilustrują zapotrzebowanie społeczne na tanie konta bankowe oraz potrzebę coraz szerszego rozpowszechniania usług płatnościowych dostępnych przez łącze. Zmiany te wynikają ze swoistych przemian o randze historycznej, które powodują, że obecne społeczeństwo można nazwać mianem społeczeństwa informacyjnego[124]. Przemiany te determinują pewne zachowania i wymuszają na nas dostosowanie się do nich. Niestety w związku z tym pojawiają się również zjawiska negatywne.

Biorąc pod uwagę zaistniały stan rzeczy oraz zwiększający się w życiu codziennym udział czynności dokonywanych przez Internet, niezwykle ważne jest, aby przeciwdziałać tzw. wykluczeniu elektronicznemu. Nic nie wskazuje póki co, aby cały handel przeniósł się do sieci lub, aby płacenie rachunków było możliwe jedynie za pośrednictwem konta internetowego. Jednak część społeczeństwa, niekorzystająca z Internetu jako kanału komunikacji, może w najbliższym czasie być stopniowo wykluczana z życia publicznego lub może mieć problemy z załatwieniem podstawowych spraw. Za przykład może posłużyć fakt, że już teraz organy

[121] Źródło: http://www.biznes.newseria.pl/news/sklepy_internetowe,p118997350 [dostęp: 9.09.2016].
[122] *Ibidem.*
[123] Źródło: http://www.polskieradio.pl/42/273/Artykul/1546970,Jak-Polacy-oplacaja-rachunki [dostęp: 9.09.2016].
[124] M. Kęsy, Społeczeństwo *Informacyjne w rozwoju cywilizacyjnym ludzkości*, Źródło: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.desklight-602668b9-47cb-4273-a5b3-31aa20a6634f/c/Kesy_M1.pdf [dostęp: 9.09.2016].

podatkowe zachęcają do dostarczania zeznań podatkowych drogą elektroniczną[125], co jest o wiele wygodniejsze niż osobiste stawiennictwo i składanie dokumentu w formie papierowej oraz pozwala zaoszczędzić tak cenny dziś czas.
To właśnie chęć przeciwdziałania wykluczeniu bankowemu oraz pośrednio internetowemu, przyświecała prawodawcy europejskiemu przy wprowadzeniu w życie dyrektywy Parlamentu Europejskiego i Rady 2014/92/UE z dnia 23 lipca 2014 r. w sprawie porównywalności opłat związanych z rachunkami płatniczymi, przenoszenia rachunku płatniczego oraz dostępu do podstawowego rachunku płatniczego[126] zwanej dalej Dyrektywą lub Dyrektywą 2014/92/UE. Jednak z uwagi ograniczonego zakresu tematycznego niniejszego tekstu, wspomniana Dyrektywa zostanie poddana analizie jedynie w zakresie przepisów nakładających na banki obowiązek otwierania i prowadzenia podstawowych rachunków płatniczych. Rozważony zostanie cel wprowadzenia tych regulacji, szczególnie w kontekście obecnie dostępnych ofert banków funkcjonujących na polskim rynku. Dla zobrazowania powyższej problematyki posłużono się jako metodą badawczą, analizą tekstów prawnych oraz materiałów źródłowych, dokonano również w przedmiotowym zakresie porównania wymogów postawionych w Dyrektywie z przepisami zawartymi w Ustawie o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw[127] zwaną dalej Ustawą Zmieniającą. Podstawę pozyskanych informacji rynkowych stanowią badania własne.

2. Analiza przepisów unijnych oraz krajowych

2.1. Przepisy unijne

Dyrektywa 2014/92/UE wprowadzając przepisy o rachunku podstawowym w zamyśle prawodawcy miała za zadanie usprawnić i rozwinąć bankowość detaliczną,[128] ułatwić konsumentom wchodzenie na nowy rynek w obrębie wspólnoty (szczególnie w kontekście realizacji zasady swobody przepływu osób)[129], zbudować szeroko pojęty system przeciwdziałania dyskryminacji[130], upowszechnić dostęp do konta bankowego[131] – w tym do zestawu podstawowych usług płatniczych nie tylko przez Internet[132] oraz ujednolicić przepisy dotyczące tej materii na terytorium całej Unii Europejskiej[133]. Oczywiście jest to jedynie część zadań przewidzianych przez procedowane przepisy i w związku z zakresem materii tekstu, zostały one wybrane w kontekście instytucji rachunku podstawowego.

[125] http://www.e-deklaracje.gov.pl/web/bip/ministerstwo-finansow/wiadomosci/aktualnosci/ministerstwo-finansow2/-/asset_publisher/M1vU/content/wyslij-pit-przez-internet! [dostęp: 9.09.2016].
[126] dyrektywy Parlamentu Europejskiego i Rady 2014/92/UE z dnia 23 lipca 2014 r. w sprawie porównywalności opłat związanych z rachunkami płatniczymi, przenoszenia rachunku płatniczego oraz dostępu do podstawowego rachunku płatniczego (Dz. Urz. UE; Seria L 257/214).
[127] Ustawa z dnia 30.11.2016 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz.U. 2016 poz. 1997.)
[128] Zob.: art. 3 preambuły Dyrektywy 2014/92/UE.
[129] Zob.: art. 6 preambuły, *Op. cit*.
[130] Zob.: art. 35 preambuły, *Op. cit*.
[131] Zob.: art. 38 preambuły, *Op. cit*.
[132] Zob.: art. 44 preambuły, *Op. cit*.
[133] Zob.: art. 15, *Op. cit.*

Dyrektywa 2014/92/UE w art. 1 ust 2. nakłada na Państwa Członkowskie obowiązek zagwarantowania konsumentowi prawa do otwarcia i korzystania z podstawowych rachunków płatniczych w Unii[134]. Szczegóły tego obowiązku można odnaleźć w rozdziale IV Dyrektywy zatytułowanym „Dostęp do rachunków płatniczych". Prawodawca podaje tu szereg wymogów, które mają zostać spełnione. Jako pierwsze pojawia się zasada powszechnej dostępności do niniejszej usługi.[135] Zasada ta ma w przytaczanym przepisie kilka płaszczyzn. Wyróżnić tu można zobowiązanie do prowadzenia rachunku podstawowego przez instytucję kredytową[136]. Poprzez upowszechnienie obowiązku świadczenia usług przez wszystkie instytucje kredytowe prawodawca uchyla się przed zakłóceniem konkurencyjności. Podmiotem, do którego ma być kierowana oferta rachunku podstawowego ma być natomiast każdy konsument legalnie znajdujący się na terytorium danego kraju, niezależnie od jego miejsca zamieszkania[137]. Kolejną płaszczyzną jest wymiar dostępności usługi, która w założeniu prowadzona będzie również za pośrednictwem standardowych narzędzi, nie tylko tych związanych z internetową obsługą rachunku[138]. Ta gwarancja nakierowana jest na osoby wykluczone cyfrowo, aby w związku ze swoją sytuacją i tak mogły korzystać z wprowadzanych przepisów i przezwyciężały swoje wykluczenie bankowe, które według prawodawcy unijnego często idzie w parze z wykluczeniem cyfrowym.

W tym miejscu warto zwrócić uwagę na definicję instytucji finansowej, o ile w słowniczku Dyrektywy pozycja ta znalazła swoje miejsce, o tyle przepis tam zawarty jest norma odsyłającą[139]. Kieruje on do rozporządzenia Parlamentu i Rady w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/20122013/36/UE[140] gdzie w art. 4 ust. 1 pkt. 1 znajduje się właściwa definicja instytucji kredytowej. W ten sposób zakres zastosowania omawianych przepisów jest zdefiniowany poza Dyrektywą, dzięki temu nie mnoży się niepotrzebnych bytów, a wykładnia przepisów oparta jest o jednolitą definicję oraz powstałe do tej pory orzecznictwo.

Państwa członkowskie w przepisach wykonawczych zobowiązane są zawrzeć gwarancję świadczenia przez dostarczyciela takich usług jak: otwarcie, prowadzenie i zamknięcie rachunku[141]; wpłacanie środków[142]; wypłacanie środków w kasie lub bankomacie[143]; dokonywanie transakcji: poleceń zapłaty, płatności kartą, poleceń przelewu (w tym i zlecań stałych zlecanych w terminalach i kasie oraz przez Internet).[144] Zakres tych usług musi się pokrywać z usługami już dostępnymi w danej instytucji dla innych rachunków niż rachunek podstawowy. Natomiast ustawodawca krajowy dodatkowo uznaniowo może nałożyć na

[134] Ibidem.
[135] Zob.: art. 16 ust. 1, *Op. cit.*
[136] Zob.: art. 2 ust. 8, *Op. cit.*
[137] Zob.: art. 16 ust. 2, *Op. cit.*
[138] Zob.: art. 16 ust. 1, *Op. cit.*
[139] Zob.: art. 2 ust. 8, *Op. cit.*
[140] rozporządzenia Parlamentu i Rady w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/20122013/36/UE (Dz. Urz. UE; Seria L 176/1; 2 czerwca 2013).
[141] Zob.: art. 17 ust. 1. pkt. a, Dyrektywy 2014/92/UE.
[142] Zob.: art. 17 ust. 1. pkt. b, *Op. cit*.
[143] Zob.: art. 17 ust. 1. pkt. c, *Op. cit.*
[144] Zob.: art. 17 ust. 1. pkt. d, *Op. cit*.

dostawce usług obowiązek świadczenia usługi uznanej powszechnie w obrębie danego kraju za podstawową[145]. W praktyce polskiej taki obowiązek może dotyczyć polecenia zapłaty podatku dochodowego na konto właściwego Urzędu Skarbowego – funkcja ta jest dostępna u niemal wszystkich podmiotów świadczących usługi płatnicze w Polsce[146]. Innym przykładem jest możliwość złożenia wniosku o dofinansowanie z programu powszechnie zwanego „500+", również dostępnego z poziomu konta[147]. Niestety w Ustawie Zmieniającej taki wymóg się nie pojawił. Postawienie tego wymogu, mogło by pomóc przyczynić się wprowadzanej instytucji rachunku podstawowego do przeciwdziałania wykluczeniu bankowemu i cyfrowemu - zgodnie z założeniami Dyrektywy 2014/92/UE.

Wymienione powyżej usługi poza poleceniami zapłaty oraz poleceniami przelewów powinny być darmowe. Jedyne dopuszczalne opłaty nie mogą się wiązać z liczbą dokonanych operacji, powinny być rozsądnej wysokości i nie mogą być wyższe niż stosowane do tej pory dla innych podobnych instrumentów i usług w ich ramach[148].

2.2. Regulacja krajowa

Polski ustawodawca, na którym ciąży obowiązek implementacji powyższych przepisów do krajowego systemu prawnego, postanowił dokonać tego w drodze nowelizacji Ustawy o usługach płatniczych[149]. Nowelizacja, między innymi, art. 1 ust. 17) dodaje w oddziale III Ustawy o usługach płatniczych rozdziały 7. i 8. Jednak z uwagi na zakres tematyczny tekstu, analizie poddane zostaną rozwiązania z rozdziału 7, jako że to one dotyczą dostępu do podstawowego rachunku płatniczego.

Do określenia zakresu podmiotów zobowiązanych do wprowadzenia do swojej oferty rachunku podstawowego ustawodawca posłużył się w Ustawie Zmieniającej już istniejącą definicją. Niestety, odmiennie niż w przypadku regulacji na poziomie ogólnoeuropejskim, w polskim systemie prawnym definicja ta jest rozproszona. W pierwszej kolejności należy zwrócić uwagę na art. 4 ust. 2 pkt 1-3 oraz pkt 9 Ustawy o usługach płatniczych, znajdziemy tam katalog dostawców usług płatniczych, którzy zgodnie z procedowanymi przepisami będą zobowiązani do prowadzenia rachunków podstawowych. Podmiot wymieniony w pkt 1 to bank krajowy rozumiany zgodnie z art. 4 ust. 1 pkt 1 Ustawy Prawo bankowe,[150] pkt 2 poszerza katalog podmiotów poprzez kolejne odesłanie do Ustawy Prawo bankowe, tym razem do art. 4 ust. 1 pkt 20 o oddziały banku zagranicznego działające na terytorium RP. Pkt 3 zalicza do zobowiązanych również instytucje kredytowe i oddziały instytucji kredytowej działające na terytorium RP. Tu odnaleźć można kolejne dwa przepisy odsyłające do art. 4 ust. 1 pkt 17 i art. 4 ust. 1 pkt 18 Ustawy Prawo bankowe precyzyjnie wskazujące te instytucje. Ostatni pkt 9 zalicza do grona zobowiązanych Spółdzielcze Kasy Oszczędnościowo-Kredytowe i Krajową Spółdzielczą Kasę Oszczędnościowo-Kredytową w rozumieniu ustawy z dnia 5 listopada 2009

[145] Zob.: art. 17 ust. 2, *Op. cit.*
[146] Zob.: Tabela 1.
[147] Ibidem.
[148] Zob.: art. 17 ust. 5, art. 17 ust. 6, art. 18, Dyrektywy 2014/92/UE.
[149] Ustawa z dnia 19.08.2011 r. o usługach płatniczych (Dz. U. z 2014 r. poz. 873 z późn. zm.).
[150] Ustawa z dnia 29.08.1997 r. Prawo bankowe (Dz.U. 1997 Nr 140 poz. 939).

r. o spółdzielczych kasach oszczędnościowo-kredytowych[151] dalej SKOK. Warto zaznaczyć, że obowiązek prowadzenia rachunku podstawowego przez SKOKi będzie dotyczył jedynie członków danej kasy oszczędnościowo-kredytowej. Tak więc niedaleko szukając odnajdujemy w polskim ustawodawstwie kilka przepisów odsyłających, które powodują, że kompletną definicją należy dekodować z trzech rozmaitych ustaw.

Po przebrnięciu przez konstrukcje definicji warto zwrócić uwagę na uprawnienia jakie przysługują danym podmiotą z tytułu zakładania dla klienta rachunku podstawowego. Z uwagi na swoista funkcję socjalną, jaką ma zapewnić rachunek podstawowy ustawodawca krajowy zdecydował się przyznać usługodawcy fakultatywne uprawnienie do zażądania informacji o rachunkach konsumenta, poprzez centralną informację o rachunkach, o której mowa w Ustawie prawo bankowe, w celu sprawdzenia czy posiada on rachunek płatniczy u innego podmiotu świadczącego usługi na terytorium RP. Uprawnienie to nie zostało obwarowane np.: koniecznością przedstawienia wniosku, złożonego przez konsumenta w celu uprawdopodobnienia podjęcia przez niego czynności związanych z założeniem rachunku podstawowego. Choć sama konstrukcja jest zasadna i ma zabezpieczyć usługodawców przed powielaniem rachunków, gwarantując możliwość sprawdzenia nieuczciwych konsumentów. To jeżeli wymóg kontroli wniosków o sprawdzenie w ewidencji rachunków nie powstanie, luka ta może posłużyć nadużyciom. Dobrym rozwiązaniem jest z kolei istotne ograniczenie usługodawców, które silnie chroni konsumenta. Chodzi o zakaz uzależniania otwarcia rachunku podstawowego od zawarcia dodatkowej umowy o usługi[152]. W praktyce − wszelkie funkcjonujące obecnie na rynku ograniczenia odnośnie zawarcia umowy[153] nie mogą się w żaden sposób odnosić do rachunku podstawowego. Niezgodne z tą regulacją będzie uzależnienie wysokości opłat za rachunek np.: od kwoty miesięcznego wpływu czy dokonanego obrotu. W kontekście poruszanych norm ograniczających możliwość nakładania przez dostawcę dodatkowych zobowiązań na posiadaczy rachunku podstawowego należy również zaznaczyć, że SKOK zarówno jak pozostałe instytucje nie mogą uzależnić założenia rachunku podstawowego dla klienta od dodatkowych przesłanek, np.: zawarcie umowy konta oszczędnościowego. Jednak SKOKi z uwagi na swój charakter, zostały obarczone obowiązkiem świadczenia rachunku podstawowego w ograniczonym zakresie. Zgodnie z Ustawą Zmieniającą mogą one zakładać rachunki podstawowe jedynie swoim członkom[154]. Z tego wynika, że jeżeli SKOK będzie wymagał, od konsumenta, by ten przelewał comiesięczne wynagrodzenia na swój rachunek lub był posiadaczem rachunku oszczędnościowego, aby móc być członkiem SKOK - to możliwe jest, w taki pośredni sposób, uzależnienie otwarcia rachunku podstawowego od spełnienia dodatkowych przesłanek. Ograniczając tak zakres podmiotów zobowiązanych.

3. Podsumowanie i wnioski

[151] Ustawa z dnia 5.11.2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz.U. 2012 poz. 855).
[152] Zob.: art. 59ic ust. 2, ustawy o spółdzielczych kasach oszczędnościowo-kredytowych.
[153] Zob.: tabela 1.
[154] Zob.: art. 59ia ust. 1. zdanie ostatnie, ustawy o spółdzielczych kasach oszczędnościowo-kredytowych.

Biorąc pod uwagę dostępne na rynku oferty poszczególnych instytucji finansowych, samo prowadzenie rachunku, jak również jego otwarcie, nie generuje zazwyczaj żadnych opłat[155]. Zupełnie inaczej jest z kartami wydawanymi do konta, gdzie trend wskazuje na konieczność umieszczania opłat za otrzymanie i prowadzenie karty − bezpłatnych po spełnieniu dodatkowych warunków[156]. Jednak wprowadzone przepisy w żaden sposób nie wpływają na zmianę tego segmentu świadczonych usług. Poza zakresem wskazanych możliwości, czyli swobodnej decyzji usługobiorcy czy chce posiadać kartę czy nie, brak jest regulacji dotyczącej kosztów wiążących się z jej posiadaniem. Jeżeli chodzi o ilość dostępnych przelewów z pozycji konta, przy łączu internetowym prawie wszystkie podmioty oferują nieograniczoną darmową liczbę zleceń w miesiącu. Wyjątek stanowi bank BZ WBK, gdzie ograniczenie stanowi liczba dostępnych miesięcznie darmowych sms-kodów. Chodź w banku tym obecnie obowiązuje promocja dla wszystkich klientów znosząca czasowo opłatę za sms-kod. W tym zakresie więc, wprowadzane przepisy nie znajdą szerszego zastosowania, wręcz przeciwnie. Wprowadzone rozwiązanie zakłada jedynie 5 darmowych transakcji miesięcznie a pozostałe mogą być płatne. Ich koszt wyznacza średni koszt takiej usługi świadczonej przez danego dostarczyciela przez ostanie 12 miesięcy. Rozwiązanie to pozwala usługodawcą na wprowadzenie opłat, lecz gdy przelewy w ciągu minionych 12 miesięcy były darmowe, muszą takie pozostać również dla rachunku podstawowego. Zobowiązanie do zapewnienia 5 darmowych zleceń przelewów odniesie się do bardzo wąskiego grona dostarczycieli usług. Wydaje się, że lepszym rozwiązaniem jest pozostawienie tej kwestii konsumentom oraz prawom rynku. Z uwagi na bardzo podobne warunki ofert, na podstawie których dostępne są w tej chwili rachunki bankowe, wszelkie powyższe rozwiązania mogłyby zostać w dalszym ciągu poza regulacją prawną. W obecnym stanie wystarczająco reguluje to mechanizm prawa popytu i podaży. Tym bardziej, że oferowane rozwiązania w kontekście danych prezentowanych w tabeli są mniej atrakcyjne niż obecne usługi oferowane przez dostarczycieli.

Jak może się wydać, ustawodawca dokonał również pewnego przeoczenia, które powoduje, że rachunek podstawowy, może się okazać jeszcze mniej funkcjonalny niż dostępna już teraz, standardowa oferta usługodawców. Jeżeli ustawodawca zdecydowałby się na skorzystanie z fakultatywnego uprawnienia do rozszerzenia katalogu usług dostępnych obligatoryjnie, o te, uważane w praktyce danego kraju za standardowe, wprowadzone przepisy mogły by się okazać bardziej odpowiadające na potrzeby społeczeństwa. Szczególnie biorąc pod uwagę jako jeden z argumentów podniesionych w preambule Dyrektywy, zwalczanie wykluczenia internetowego i bankowego. Cel ten byłby z pewnością pełniej realizowany. Obecnie prawie wszystkie podmioty ułatwiają złożenie wniosku o dofinansowanie z programu „500+" poprzez swoje konta standardowe. Taka sama sytuacja występuje względem możliwości płacenia zobowiązań podatkowych. Każda platforma bankowa na poziomie dostępu przez Internet umożliwia te usługi. Ustawodawca jednak nie wskazał w przepisach, że dostęp do tych dwóch elementów jest wymagany poprzez rachunek podstawowy. Z tego powodu dostawcy mogą nie zawrzeć ich w swojej ofercie obowiązkowej. Spowodować to może, że rachunki te będą mniej korzystne niż dotychczas dostępne konta standardowe. Wprowadzanie dodatkowych usług z punktu widzenia konsumentów zagranicznych, którzy

[155] Zob.: Tabela 1.
[156] Ibidem.

potrzebują rachunek na chwilę lub dla rozliczeń związanych np. z tymczasowym zatrudnieniem, jest obojętne. Dla konsumenta krajowego może oznaczać, że przy zakładaniu rachunku podstawowego zostanie skuszony przez instytucję do jej standardowej oferty rachunku, powiązanej z wieloma dodatkowymi możliwościami. Pod tym względem można przyznać, że poprzez minimalizację oferty, konkurencyjność w zakresie ofert rachunków standardowych zostanie poza wpływem regulacji. Niestety też zwalczanie wykluczenia okaże się mniej efektywne.

Najistotniejsze zmiany zostaną wprowadzone w zakresie obsługi klientów w siedzibie banku. Do teraz dostępne oferty w większości obciążają konsumenta wysokimi opłatami przy dokonywaniu czynności przy okienku w banku. Zlecania przelewów, generuje koszty od 5 zł do nawet 9 zł za jednorazowe zlecenie. Ustawa Zmieniająca zobowiązuje podmioty do zapewnienia obsługi okienkowej – jeżeli jest ona dostępna u danego dostarczyciela w ilości co najmniej 5 darmowych operacji w miesiącu. W tym wypadku na pierwszy plan wyłania się przeciwdziałanie wykluczeniu bankowemu. Ludzie, którzy nigdy nie korzystali z usług instytucji bankowych, właśnie z powodu wysokich opłat w okienku, a nie potrafią posługiwać się Internetem, mogą być potencjalnymi beneficjentami tej regulacji. Jedynie pozostaje dotrzeć do nich z ofertą.

Biorąc pod uwagę wszelkie zalety i wady regulacji, należy zadać pytanie czy rzeczywiście do regulacji tej materii potrzebna była interwencja Unii Europejskiej. Odpowiedź zapewne pojawi się wraz z pierwszymi statystykami dotyczącymi ilości otwartych rachunków podstawowych.

Tabela 1 Zestawienie ofert wybranych instytucji

Instytucja	Nazwa konta	Suma opłat za otwarcie konta, prowadzenie w złotych	Ilość darmowych przelewów przez Internet	Warunki do spełnienia, aby konto było darmowe	Koszt w złotych obsługi w okienku: wpłata/wypłata	Koszt w złotych przelewu dokonanego w okienku	Dostępność wniosku o 500+[1]	Możliwość przelewu na poczet podatku
Millenium	Konto 360	15	bez ograniczeń	1000 zł miesięcznego wpływu zewnętrznego oraz przynajmniej jedna płatność kartą	0/0	5	TAK	TAK
ING bank Śląski	Konto Direct	0	bez ograniczeń	brak	9/9[2]	9	TAK	TAK
BZW BK	Konto Godne Polecenia	0	5 w miesiącu[3]	brak	zwolnione z opłat do 30 kwietnia 2017/5	8	TAK	TAK
T–mobile usługi bankowe	Konto Freemium	0	bez ograniczeń	brak	brak takiej możliwości	brak takiej możliwości	TAK	TAK

[1] Niedostępne np.: w banku Crédit Agricole.
[2] Możliwość wpłaty i wypłaty za darmo dowolną ilość razy za pomocą bankomatów i wpłatomatów na terenie całego kraju. Karta nie generuje kosztów przy dokonaniu płatności na kwotę 300 zł, inaczej 7 zł.
[3] Dokładnie oferta przewiduje 5 darmowych sms kodów potrzebnych do zatwierdzenia zlecenia.

mgr Agata Kowalska

Bezpieczeństwo danych osobowych w chmurze

1. Chmura obliczeniowa

Udzielenie odpowiedzi na pytanie czym jest chmura obliczeniowa (*ang. cloud computing)* nie jest dla przeciętnego użytkownika sieci zadaniem łatwym. I o ile intuicyjnie prawdopodobnie umielibyśmy podać kilka przykładów wykorzystania chmury, o tyle wytłumaczenie jej działania to coś, co niewątpliwie sprawi wspomniane trudności. Choć z pozoru może się wydawać, że wiedza o chmurze obliczeniowej jest dla nieprofesjonalisty zbędna, okazuje się, że chmura obliczeniowa, eksplorując coraz szersze obszary gospodarki, staje się nieodłącznym elementem codziennego życia, a i jej dalsza ingerencja jest nieunikniona. I aby móc właściwie wykorzystywać jej, zdaje się nieograniczony potencjał, trzeba mieć świadomość jej działania, pojawiających się zagrożeń, i w konsekwencji umieć zapewnić sobie właściwy poziom bezpieczeństwa.

Rozwój chmury obliczeniowej to, zdaje się, naturalna konsekwencja upowszechnienia korzystania z Internetu oraz oferowanych przez niego usług, oraz intensywnych zmian w technologiach na przełomie ostatnich dziesięcioleci, Obecnie już przeważająca większość narzędzi, programów i aplikacji opiera się na rozwiązaniach dostarczanych przez chmurę. Jednak sformułowanie precyzyjnej definicji chmury utrudnia fakt różnorodności wykorzystywanych modeli dostarczania usług w chmurze, oraz ich eksploatacji[157], dlatego też spotkać można wiele prób ustalenia czym jest chmura.

Zgodnie z definicją dostępną na Wikipedii, chmura jest opisywana jako "model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez usługodawcę (wewnętrzny dział lub zewnętrzna organizacja). Funkcjonalność jest tu rozumiana jako usługa (dająca wartość dodaną użytkownikowi) oferowana przez dane oprogramowanie (oraz konieczną infrastrukturę)"[158]. J. Byrski, A. Wachowska wskazują, że usługi *cloud computing* "charakteryzuje się jako usługi świadczone przez zewnętrznych dostawców (przedsiębiorców), którzy udostępniają oprogramowanie, infrastrukturę i wszelkie zasoby IT przez Internet, poza siedzibą odbiorcy[159]. Zgodnie zaś z definicją przyjętą przez Narodowy Instytut Standardów i Technologii w Stanach Zjednoczonych, *Cloud Computing* jest modelem umożliwiającym wielokrotny, wygodny dostęp za pośrednictwem sieci do wspólnych zasobów obliczeniowych (tj. sieć, serwery, pamięć masowa, aplikacje i usługi), które mogą być szybko zapewnione

[157] E.Molenda, *Prawne aspekty Cloud Computingu*, Kraków 2012, s 11. dostęp: [20.12.2015r.]
[158] Wikipedia, Chmura Obliczeniowa, https://pl.wikipedia.org/wiki/Chmura_obliczeniowa. dostęp: [27.12.2015r.]
[159] J.Byrski, A.Wachowska, *Cloud computing* w działalności instytucji płatniczej, Monitor Prawa Bankowego 2012, nr 9, s. 59.

i uwolnione przy minimalnym zarządzaniu lub ingerencji dostawcy. Model ten charakteryzuje się pięcioma, podstawowymi cechami oraz składają się na niego trzy modele dostarczania i cztery eksploatacji[160].

Wspomniane w definicji cechy charakterystyczne chmury obliczeniowej to samoobsługa na żądanie, nieograniczony dostęp do sieci, pula zasobów - tzw. wielodzierżawa[161], szybka elastyczność, oraz mierzalności usługi[162]. Wymieniona powyżej samoobsługa na żądanie oznacza, że użytkownik może samodzielnie i w sposób automatyczny otrzymać zasoby chmury konieczne do przetwarzania danych np. może rozpocząć korzystanie z aplikacji[163]. Elastyczność oznacza dynamiczne skalowanie zasobów chmury, tak aby mogły być dostarczone na każde zgłoszenie klienta i związku z tym być dla niego niewyczerpane - uzupełniane na każde żądanie[164]. Mierzalność oznacza stałe monitorowanie wykorzystywania zasobów przez dostawców w chmurze. To umożliwia dostawcy optymalizowanie ich pracy a klientowi dostarcza przejrzystą informację o kosztach usługi.[165]. Z kolei, pula zasobów jest zbiorem wszystkich zasobów posiadanych przez dostawcę[166], możliwym dzięki wirtualizacji, którą R. Marchini definiuje jako technologię, która umożliwia użytkownikowi uruchomienie oprogramowania na wirtualnym serwerze[167]. Oznacza to, że aby móc korzystać z danego programu użytkownik nie musi mieć go zainstalowanego na własnym komputerze, ale może korzystać z takiego programu online z każdego komputera na całym świecie, dzięki udostępnieniu go przez dostawcę.

Modelami *Cloud Computing są Saas* (*Software as a Service*), który zapewnia użytkownikom pełne środowisko oprogramowania[168] oraz PaaS (*Platform as a Service*). i IaaS (*Infrastructure as a Service*) będące w głównej mierze usługami dla programistów - umożliwiającymi tworzenie aplikacji. Dodatkowo wyróżniamy również różne typy chmur, a mianowicie chmurę prywatną, którą zarządza organizacja korzystająca na własny użytek, a idea współ-dzierżawności nie jest w tym przypadku przewidziana. Kolejnym typem chmury, najbardziej popularnym jest chmura publiczna, którą tworzy jeden dostawca i oferuje do używania szerokiej publiczności, jako przykład wystarczy podać Dysk Google. I ostatnim rodzajem jest chmura hybrydowa, łącząca w sobie elementy obu wcześniej scharakteryzowanych chmur.

W obecnym społeczeństwie trudno nie zgodzić się, że informacja stała się kluczowym dobrem. Jak podkreśla A. Suchorzewska, stanowi ona zarówno wartościowy towar, jak i narzędzie produkcji, gdzie kolejne sektory gospodarki są obsługiwane przez systemy informatyczne.

---

[160] P. Mell, T. Grance, *The NIST definition of Cloud Computing*, US. Department of Commerce, wrzesień 2011 r., dostęp: [27.12.2015 r.]

[161] J.Muszyński, Bezpieczeństwo w chmurze, http://www.computerworld.pl/news/376996_2/Bezpieczenstwo.w.chmurze.html dostep: [28.12.2015r.]

[162] P. Mell, T. Grance, *The NIST definition of Cloud Computing*, US. Department of Commerce, wrzesień 2011 r., dostęp: [27.12.2015 r.]

[163] Cloud'owe ryzyka biznesowe, http://it-manager.pl/ryzyka-biznesowe-w-przedsiewzieciach-cloud-computing-rekomendacje-dla-cio-i-cfo/, dostęp: [27.01.2016 r.]

[164] *Ibidem*

[165] *Ibidem*

[166] *Ibidem*

[167] R.Marchini, *A practical…, opt.cit.,* s.5.

[168] *Chmury obliczeniowe. Ekspertyza,* PE 475.104 2012 r.http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf, dostęp: [15.01.2016 r.]

Nawet dobrobyt państw oraz bezpieczeństwo obywateli zależy od informacji przechowywanych i przekazywanych przez nowoczesne rozwiązania technologii[169]. W konsekwencji nie mniej istotnym jest również jej bezpieczeństwo. W tym miejscu należy przyznać, że przełomowe rozwiązania oferowane przez chmurę, wpływające na szybkość przetwarzania, możliwość jednoczesnego wykonywania wielu operacji, oraz zdolność do gromadzenia dużej ilości danych, mają również drugą, ciemniejszą stronę medalu. Krytycy zarzucają *Cloud Computing* znaczne ryzyko dla bezpieczeństwa oraz ochrony danych przechowywanych w chmurze[170]. Z charakteru *Cloud Computing* wynika wszakże, że pula zasobów chmury, tj. zgromadzonych danych, znajduje się w zewnętrznej pamięci masowej, co wpływa na ograniczenie możliwości ich kontrolowania. Dodatkowo, dzięki wirtualizacji istnieje możliwość jednoczesnego korzystania przez wielu użytkowników, co w konsekwencji zwiększa ryzyko ich udostępnienia i przejęcia przez innych współużytkowników lub grupę hakerów[171]. Sytuację pogarsza przechowywane danych w chmurze w jawnej postaci[172]. I chociaż pojawiają się obserwatorzy, którzy podkreślają, że przechowywanie i udostępnianie danych w chmurze obliczeniowej bywa bezpieczniejsze niż korzystanie z wewnętrznego centrum danych[173], gdyż awaria komputera nie wpłynie na ich utratę lub zniszczenie, to nie ulega wątpliwości, że istotną, z punktu widzenia potencjalnego użytkownika chmury obliczeniowej, kwestią jest zachowanie przez usługodawcę standardów bezpieczeństwa danych osobowych przechowywanych w chmurze. I chociaż często czynnikiem determinującym wybór dostawcy, będzie potrzeba minimalizowania kosztów, analiza polityki bezpieczeństwa usługodawcy winna być głównym obowiązkiem usługobiorcy[174].

2. Ochrona danych na gruncie ustawy o ochronie danych osobowych

W związku z tym, to zagwarantowanie prawidłowej ochrony danych osobowych staje się kluczowym zagadnieniem prawnym *Cloud Computing*. Pojawiającymi się w tym zakresie problemami, wymagającym rozstrzygnięcia, jest kwestia faktycznego miejsca przechowywania danych. Dynamiczna skalowalność zasobów chmury w wielu centrach jednocześnie utrudnia jego sprecyzowanie, a w konsekwencji również, ewentualne pociągniecie usługodawcy do odpowiedzialności za utratę tych danych. Ponadto znaczące są istniejące komplikacje w zdefiniowaniu pojęć takich jak administrator danych, czy podmiot przetwarzający dane, w związku z czym nie jest wystarczająco jasne na kim ciążą określone obowiązki. Grupa robocza

[169] A.Suchorzewska., *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*. Oficyna 2010 s. 1.
[170] E. Molenda., *Prawne aspekty…, opt.cit.,* s.25.
[171] E.Molenda- Kropielnicka, *Cloud computing - zagadnienia prawne,* ZNUJ 2013/1 s.117.
[172]J.Muszyński, Bezpieczeństwo w chmurze, http://www.computerworld.pl/news/376996_2/Bezpieczenstwo.w.chmurze.html dostęp: [28.12.2015r.]
[173] L.Determann, *Data Privacy in the Cloud: Dozen Myths and Facts*, The Computer&Internet Lawyer, tom 28, nr 11, listopad 2011 r.
[174] R.Marchini, *A practical… , opt.cit,* s.18.

w opinii 5/2012[175] wskazuje w związku z tym również kwestię braku kontroli klienta nad danymi przekazywanymi dostawcy usług w chmurze. Nie mniej istotny jest wreszcie transfer danych do podmiotów trzecich.

Aby móc lepiej zrozumieć czego dotyczą pojawiające się wątpliwości w związku z przetwarzaniem danych w chmurze, niezbędne wydaje się sięgnięcie do aktów prawnych regulujących kwestie przetwarzania danych. Najnowszym aktem prawnym dotyczącym tej materii jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych i uchylenia dyrektywy 95/46/WE. Rozporządzenie to będzie bezpośrednio stosowane jednak dopiero od dnia 25 maja 2018 r. dlatego dalsze rozważania oparte będą na wciąż jeszcze obowiązujących aktach prawnych dotyczących ochrony danych osobowych w państwach Unii Europejskiej tj. dyrektywie 95/46/WE Parlamentu Europejskiego i Komisji z dnia 24 października 1995r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[176], oraz będących implementacją dyrektywy regulacjami krajowymi, w przypadku Polski ustawą z 29 sierpnia 1995 r. o ochronie danych osobowych[177]. Kilka kwestii zostanie omówionych w oparciu o zasady ochrony danych osobowych zawarte w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[178] znajdującej zastosowanie do usług *Cloud Computing* będących w istocie usługami świadczonymi drogą elektroniczną. Wspomniane regulacje mają chronić osobę fizyczną, których dane osobowe są lub mogą być przetwarzane przez różne podmioty i instytucje.

W art 6 pkt 1 u.o.d.o ustawodawca wskazuje, że dane osobowe są rozumiane jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zaś w w art 6 pkt 2 u.o.d.o definiuje, że osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka ze specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Jednocześnie w pkt 3 powołanego artykułu 6 ustawodawca zastrzega, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeśli wymagałoby to nadmiernych kosztów, czasu i działań.

Należy zauważyć, że powyższa definicja obejmuje swoim zakresem nie tylko dane niezbędne do zidentyfikowania określonej osoby jak np, imię i nazwisko. Użycie zwrotu "wszelkie informacje" ma podkreślić, że informacje mogą dotyczyć każdego aspektu życia danej osoby, jej życia prywatnego i zawodowego, stosunków rzeczowych[179]. Co istotne, aby informacja mogła być uznana za dane osobowe nie musi być prawdziwa ani sprawdzona, oraz

---

[175] Opinia 5/2012 Grupy Roboczej art. 29 w sprawie przetwarzania danych w chmurze, http://www.giodo.gov.pl/457/id_art/4760/j/pl/ tłumaczenie nieoficjalne dostęp: [13.01.2016 r.]

[176] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. WE L 281 z 23.11.1995r., s. 31, dalej dyrektywa.

[177] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2002r. Nr 101, poz. 926 ze zm., (dalej u.o.d.o.)

[178] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. Nr. 144 poz 1204 ze zm. (dalej u.o.ś.u.d.e.)

[179] J.Barta, P.Fajgielski, R.Markiewicz, *Ochrona danych osobowych*, LEX 2015 nr 478998.

może być utrwalona w jakiejkolwiek postaci, na przykład w formie dokumentu elektronicznego, jeśli spełnione są dodatkowo inne kryteria z definicji danych osobowych. Za dane osobowe można uznać również adres email danej osoby, jeśli tylko uda się na jego podstawie zidentyfikować daną osobę bez inwestowania zbyt wiele czasu, działań oraz kosztów, dobrym przykładem może być imie..nazwisko@email.com. Pod podobnymi warunkami za dane osobowe uznaje się adres IP komputera, z którego przez dłuższy czas korzysta dana osoba[180].

Ustawa o ochronie danych osobowych jak i dyrektywa definiują również pojęcie danych wrażliwych. W art 27 u.o.d.o wskazano, że zabrania się przetwarzania danych ujawniających pochodzenie etniczne lub rasowe, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Wprowadzony zakaz jest realizacją normy konstytucyjnej określonej w art 51 oraz w art 47. ale jednocześnie ingerencją w prawa i wolności konstytucyjne, dlatego jego implementacja nastąpiła po właściwym wyważeniu norm i spełnia przesłankę proporcjonalności określoną w art 31 Konstytucji[181]. Ustawodawca wyodrębnił pojęcie danych wrażliwych ze względu na odmienności w ukształtowaniu przesłanek uchylających wspomniany zakaz, od zakazu określonego w art 23 u.o.d.o dotyczącego przetwarzania wszystkich danych osobowych. Artykuł ten wskazuje materialne przesłanki przetwarzania danych osobowych, które odnoszą się do wszystkich form przetwarzania danych zarówno dla własnych potrzeb administratora jak i "na zewnątrz"[182], stanowiąc, że przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy osoba której dotyczą wyrazi na to zgodę, chyba, że chodzi o usunięcie dotyczących jej danych, jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą jest jej stroną, jest niezbędne do zadań realizowanych dla dobra publicznego, jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Każda z tych przesłanek mam charakter "autonomiczny i niezależny"[183].

Zbiór danych jest kolejnym pojęciem używanym przez ustawodawcę. Zgodnie z definicją ustawową, zawartą w art 7 pkt 1 u.o.d.o jest to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Wynika z tego, że o zbiorze danych można mówić wtedy, gdy jest to zestaw, czyli „całość złożona z odpowiednio dobranych elementów[184]. W konsekwencji zbiór danych można określić jako zespół informacji łącznie posiadający trzy cechy - dane w nim zebrane spełniają definicję

[180] Opinia 4/2007 w sprawie definicji danych osobowych, http://www.giodo.gov.pl/462/id_art/2375/j/pl, dostęp: [20.01.2016 r.]
[181] A.Drozd, *Zakres zakazu przetwarzania danych osobowych*, Państwo i Prawo 2003/2 s. 40.
[182] J.Barta, P.Fajgielski, R,Markiewicz, *Ochrona danych osobowych*, LEX, 2015 nr 478998.
[183] *Ibidem*
[184] M.Szymczak, *Słownik języka polskiego. Tom III*, Warszawa 1981, s.1003.

danych osobowych, dane mają określoną strukturę, oraz dostęp do nich jest możliwy po spełnieniu odpowiednich kryteriów[185]. Podobną definicję zawiera dyrektywa, która wskazuje, że zbiór danych oznacza „każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, scentralizowanych, zdecentralizowanych lub rozproszonych funkcjonalnie lub geograficznie". Co niezwykle istotne to fakt, że w zależności od przeznaczenie przetwarzanie zbioru danych poddane jest odrębnemu reżimowi prawnemu[186].

Art 40 u.o.d.o enumeratywnie wskazuje przesłanki wyłączeń od obowiązku rejestracji zbioru danych osobowych nałożonego na administratora tych danych. Użyte w przepisie "przetwarzanie" zostało zdefiniowane w art 7 pkt 2 u.o.d.o i oznacza jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Na tej podstawie należy zauważyć, że w zakres pojęcia przetwarzanie danych wchodzi również ich przeglądanie[187], oraz użyte w art. 7 pkt 2 u.o.d.o. "przekazywanie"[188] co pozwala na stwierdzenie, że podobnie jak w przypadku danych osobowych, również do przetwarzania ustawodawca przyjął szeroką definicję pojęcia.

Zarówno u.o.d.o jak i dyrektywa określają zasady z zachowaniem których może nastąpić wskazane przetwarzanie. I tak, art 26 u.o.d.o wskazuje na obowiązek zachowania szczególnej staranności w celu ochrony interesów osób, których dane dotyczą nałożony na administratora danych. Są to: obowiązek zapewnienia, aby przetwarzanie danych następowało zgodnie z prawem, aby ich zbieranie następowało dla oznaczonych, zgodnych z prawem celów a dane nie były poddawane dalszemu przetwarzaniu, niezgodnego z tymi celami, dane były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, oraz żeby były przechowywanie w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celów przetwarzania.

Analizując podany przepis należy zauważyć, że nadrzędnym obowiązkiem administratora danych jest dołożenie szczególnej staranności, w celu ochrony interesów osób, których dane dotyczą. Chociaż ustawa nie precyzuje, o jakich interesach mowa, dotyczą one niewątpliwie poszanowania prywatności, intymności, wizerunku własnej osoby[189]. R. Markiewicz i J. Barta zauważają ponadto, że sformułowanie "szczególnej" oznacza, że staranność w ochronie tych interesów musi być większa od "zwykłej", "przeciętnej", a nawet "należytej"[190]. Odnosząc się zaś do kwestii zbierania danych dla oznaczonych, zgodnych z prawem celów nie sposób nie wywnioskować, że zatajenie celu pozyskiwania tych danych lub ogólnikowego informowania będzie naruszeniem tego przepisu, który wymaga, aby cel zbierania danych został określony w możliwie najbardziej precyzyjny sposób, zakomunikowany najpóźniej w momencie, w którym zbierane są dane osobowe.

Scharakteryzowany obowiązek ciąży na administratorze danych osobowych i w związku z tym nie sposób nie odnieść się w tym miejscu do ustawowej i dyrektywalnej definicji

---

[185] J.Barta, R.Markiewicz, *Ochrona.. , opt.cit.,* s.323.

[186] M. Polok, *Bezpieczeństwo danych osobowych*, wyd. C. H. Beck 2008r.

[187] A.Kocon, *Każdy kto przetwarza dane musi je zabezpieczyć,* http://www.lex.pl/czytaj/-/artykul/kazdy-kto-przetwarza-dane-osobowe-musi-je-zabezpieczyc dostęp: [7.01.2016 r.]

[188] B.Fischer, D.Karwala, *Transfer danych osobowych do państw trzecich*, Państwo i Prawo, 2007/1 s.100.

[189] J.Barta, P.Fajgielski, R,Markiewicz, *Ochrona ..., opt.cit.*

[190] *Ibidem*

tego pojęcia. Co istotne jednak, w analizie nie można zapomnie również o podmiocie przetwarzającym dane osobowe. Administrator danych, zgodnie z art 4 pkt 4 u.o.d.o jest to organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych. Definicja zawarta w dyrektywie, dotycząca ang. *file controller, czyli* właśnie administratora danych stanowi zaś, że administrator to osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych.

Konstytutywnymi elementami wskazanej definicji są: decydowanie o celach przetwarzania danych osobowych oraz decydowanie o środkach przetwarzania danych, które łącznie oznaczają sprawowanie władztwa nad danym. Samodzielność w decydowaniu o tych celu przetwarzania oraz narzędziach używanych do jego realizacji jest więc niezbędnym elementem do możliwości uznania danego podmiotu za administratora danych osobowych[191]. To co należy w tym miejscu zauważyć, to fakt, że bycie administratorem danych nie zawsze oznacza ich faktyczne posiadanie, a to jest podstawowym kryterium odróżniającym administratora danych od podmiotu przetwarzającego dane, który sprawuje faktyczną kontrolę nad przetwarzanymi danymi[192]. Podobne wnioski wywiódł SN, i w postanowieniu z dnia 11 grudnia 2001 r., za administratora uznał jedynie ten podmiot, który decyduje o celach i środkach przetwarzania danych, natomiast administrującym jest taki podmiot, który "zarządza, zawiaduje zbiorem danych lub danymi"[193].

Instytucja powierzenia przetwarzania danych osobowych została określona w art 31. u.o.d.o, który przewiduje, że administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Przepis ten nakłada dodatkowo na podmiot przetwarzający, w dyrektywie określony jako ang. *processor*, obowiązek przetwarzania danych wyłącznie w zakresie w i w celu przewidzianym w umowie, oraz podjęcie środków zabezpieczających zbiór danych. Zgodnie z art 36 u.o.d.o. są to min. zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, zabezpieczenie przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem lub zniszczeniem. Powierzenie przetwarzania nie oznacza jednocześnie, co zostało już wskazane utraty przez administratora danych władztwa. Podmiot przetwarzający uprawniony jest do wykonywania jedynie zleconych mu czynności[194], i w konsekwencji nie ciążą na nim, wspomniane już, obowiązki nałożone przez ustawę na administratora danych. W związku z tym, administrator, powierzając przetwarzanie danych innemu podmiotowi, powinien w umowie zagwarantować sobie utrzymanie przez procesora przez cały okres jej trwania właściwego poziomu bezpieczeństwa.

Ustawa o ochronie danych osobowych nie zabrania możliwości dalszego powierzenia przetwarzania danych przez procesora, co w konsekwencji oznacza, że jeśli administrator danych chce takiej sytuacji uniknąć, bądź też chce posiadać wiedzę o dalszych podmiotach

[191] P.Litwiński, *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Oficyna 2009, s.101.
[192] A.L.Bygrave, *Data Protection Law, Approaching its Rationale, Logic and Limits*, Kluwer Law International 2002, s.21.
[193] Wyrok Sądu Najwyższego (dalej SN) z 11.12.2001 r.(II KKN 438/00) LEX, nr 45466.
[194] T.Wypych, M.Wielisiej, *Instytucja powierzenia przetwarzania danych osobowych*, http://www.temidium.pl/artykul/instytucja_powierzenia_przetwarzania_danych_osobowych-2172.html#_ftn2 dostęp: [7.01.2016 r.]

zaangażowanych w przetwarzanie danych to jedyną możliwością jest zawarcie tego w treści umowy zawartej z podmiotem przetwarzającym[195]. Nie mniej istotna jest również kwestia odpowiedzialności za zapewnienie bezpieczeństwa przetwarzanym danym. Art 31 ust 4 u.o.d.o wskazuje, że odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową. Jednocześnie ust 3 art 31 u.o.d.o stanowi, że podmiot przetwarzający dane ponosi w pewnym zakresie odpowiedzialność jak administrator danych[196]. Można w tym miejscu wyprowadzić wniosek, że powierzenie danych do przetwarzania innemu podmiotowi nie powoduje jednoczesnego przeniesienia pełnej odpowiedzialności za przestrzeganie obowiązujących przepisów, a jednocześnie, że mimo odpowiedzialności administratora danych, odpowiedzialność podmiotu przetwarzającego nie jest całkowicie wyłączona, a i oparta jest na tych samych przepisach prawa materialnego oraz proceduralnego[197]. Z powyższego wynika, że ustalenie czy określony podmiot jest administratorem danych czy też podmiotem przetwarzającym dane ma "doniosłe konsekwencje prawne"[198].

3. Ochrona danych w ustawie o świadczeniu usług drogą elektroniczną

Omawiając problematykę chmury obliczeniowej należy również pamiętać, że umowami *Cloud Computing* są umowy o świadczenie usług drogą elektroniczną regulowane ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[199] oraz dyrektywą 2003/31/WE[200]. Przepisy wspomnianych aktów prawnych znajdują zastosowanie do przetwarzania danych osobowych w zakresie odrębności zawartych w nich uregulowań do u.o.d.o oraz dyrektywy.

Art 16 ust. 2 u.o.ś.u.d.e. wskazuje, że ochronie podlegają dane osobowe w zakresie ich przetwarzania niezależnie od tego, czy jest ono dokonywane w zbiorach danych. Ponieważ u.o.ś.u.d.e. nie definiuje tego pojęcia, należy je interpretować zgodnie z definicją przyjętą w u.o.d.o. W przypadku przetwarzania danych za pomocą systemu informatycznego istnieje domniemanie faktyczne, które stanowi, że skoro dane pozostają w systemie, to oznacza to, że dane te przetwarzane są w zbiorze danych[201].

Ochrona obejmuje dane usługobiorców, którymi są, zgodnie z definicją zawartą w u.o.ś.u.d.e., osoby fizyczne, osoby prawne albo jednostki organizacyjne nieposiadającą

---

[195] *Ibidem*
[196] P.Litwiński, *Ochrona danych… , opt.cit.,* s. 111.
[197] *Ibidem*
[198] E.Molenda-Kropielnicka, *Cloud Computing ..., opt.cit.,* s.121.
[199] U.o.ś.u.d.e.
[200] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz. Urz. WE L 178 z 17.07.200 r., s.1 (dalej dyrektywa o handlu elektronicznym.)
[201] J.Gołaczyński (red.), K.Kowalik-Bańczyk, A.Majchrowska, M.Świerczyński, *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz.* Oficyna 2009 s.72.

osobowości prawnej, które korzystają z usług świadczonych drogą elektroniczną. Jednak ze względu na brak definicji danych osobowych w u.o.ś.u.d.o. zastosowanie znajdują przepisy u.o.d.o i w związku z tym przepisy u.o.ś.u.d.e. stosuje się wyłącznie dla usługobiorców będących osobami fizycznymi[202].

Pod pojęciem usługodawcy rozumie się zaś dwa rodzaje podmiotów, i tak są to: 1) podmioty udostępniające usługi (treści) własne lub osób trzecich (ang. *content providers*) oraz 2) podmioty pośredniczące w dostępie do takich usług (ang. *intermediary service providers*), jednak w odniesieniu do u.o.od.o i rozdziału IV u.o.ś.u.d.e., który określa zasady ochrony danych osobowych w związku ze świadczeniem usług drogą elektroniczną kluczowym podziałem jest rozróżnienie usługodawców, którzy są administratorami danych osobowych oraz usługodawców będących podmiotami przetwarzającymi dane na zlecenie administratora danych w rozumieniu u.o.d.o[203], ze względu na fakt ponoszenia przez nich odrębnej odpowiedzialności za przetwarzanie danych osobowych.

Art 17 u.o.ś.u.d.e. wskazuje przesłanki jego dopuszczalności stanowiąc, że przetwarzanie musi odbywać się w celu i zakresie określonym w u.o.ś.d.e. Wspomnianymi celami są nawiązanie, ukształtowanie treści, zmiany lub rozwiązania stosunku prawnego, jak również potrzeba rozliczenia usługi lub dochodzenie roszczeń z tytułu płatności za korzystanie z usługi, cele reklamowe, lub do badań rynku oraz zachowań i preferencji usługobiorców, wyjaśnienia okoliczności niedozwolonego korzystania z usługi, w uwzględnieniem warunków przewidzianych w tym przepisie. Należy zauważyć, że jest to dodatkowe zawężenie podstawowej zasady ochrony danych osobowych określonej w u.o.d.o., czyli zasady celowości, oraz że możliwość przetwarzania danych w celach innych niż wskazane, nie jest przewidziana również w przypadku zgody usługobiorcy[204].

Ustawa wskazuje ponadto przykładowe dane, jakie mogą być przetwarzane przez usługodawcę. Obwarowane jest to zgodnością celu usługodawcy z ustawowo określonymi celami, a pozyskanie konkretnej informacji, których katalog określony w ustawie nie jest zamknięty, musi być niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia[205]. Nie sposób nie wspomnieć w tym miejscu o danych, których wykorzystanie przez usługodawcę łączy nierozerwalnie i jest wymagane do realizacji określonej usługi. Art. 22 u.o.ś.u.d.e. uprawnia usługodawcę do odmówienia świadczenia usługi w przypadku braku zgody usługobiorcy, co prowadzi do wniosku, że warunkiem wykorzystywania tych danych jest jej udzielenie. Określony w tym przepisie wymóg uzyskania zgody znajduje swoje odzwierciedlenie w art 7 pkt 5 u.o.d.o i mimo że bezpośrednio nie odwołuje on do oświadczenia woli, jak w przypadku u.o.d.o, to interpretuje się, że w rzeczywistości tym właśnie jest[206].

Ostatni przykład danych, które mogą być przetwarzane przez usługodawcę określony jest w art 18 ust. 5 u.o.ś.u.d.e. i dotyczy tzw. danych eksploatacyjnych, pozyskiwanych w sposób automatyczny przez system teleinformatyczny, co do których nie ma konieczności spełniania powyższych warunków - tj. uzyskania zgody usługobiorcy bądź zgodności z celami

[202] E.Molenda-Kropielnicka, *Cloud Computing ..., opt.cit.,* s.122.
[203] J.Gołaczyński (red.), K.Kowalik-Bańczyk, A.Majchrowska, M.Świerczyński, *Ustawa… , opt.cit.,* s.72.
[204] *Ibidem*
[205] A.Frań-Adamek, *Komentarz do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.02.144.1204),* LEX.el., 2002 nr 8206.
[206] X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną,* Difin 2004 s. 89.

określonymi w u.o.ś.u.d.e. Ustawodawca formułuje katalog tego typu danych, wskazując, że są to oznaczenia identyfikujące usługobiorcę, oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną, oraz informacje o skorzystaniu z usług świadczonych drogą elektroniczną. Należy również zauważyć, że uzyskanie przez ustawodawcę tych podstawowych danych nie będzie konieczne, jeśli usługobiorca zdecyduje się na anonimowe bądź przy użyciu pseudonimu skorzystanie z odpłatnej usługi.

Dopuszczalność takiego rozwiązania zależy od możliwości technicznej, co w przypadku usług odpłatnych może okazać się niełatwe[207]. Ustawa wskazuje również liczne obowiązki nałożone na usługodawcę celem zapewnienia usługobiorcy ochrony koniecznej dla zachowania prywatności przy korzystaniu z usługi[208]. Usługodawca jest zobowiązany do zapewnienia usługobiorcy dostępu do aktualnej informacji o udostępnianych środkach technicznych zapobiegających pozyskiwaniu i modyfikowaniu przez osoby nieuprawnione danych osobowych przesyłanych drogą elektroniczną. Oznacza to konieczność przekazania informacji o tym, w jaki sposób usługodawca zabezpiecza dane, np. poprzez wykorzystanie określonych programów szyfrujących[209], podmiocie, któremu powierza przetwarzanie danych, ich zakresie, zamierzonym terminie przekazania, jeśli usługodawca zawarł z tym podmiotem umowę o powierzenie przetwarzania danych. Ustawodawca podkreślił ponadto, że wszystkie powyższe informacje mają być dla usługobiorcy stałe i łatwo dostępne.

4. Specyfika cloud computing

Powyższa analizę należy teraz odnieść do specyfiki *cloud computing*. Z uwagi na fakt przyjęcia przez ustawodawcę, omówionej już, szerokiej definicji danych osobowych, tylko nieliczne dane przetwarzane w chmurze nie będą związane z osobą fizyczną[210], i omówione przepisy u.o.d.o, określające podmioty uprawnione oraz warunki przetwarzania danych nie znajdą do nich zastosowania. Przedstawione przepisy pozwalają zauważyć kluczową rolę jaką pełni administrator danych w procesie przetwarzania danych[211], oraz, rozróżniony od niego, podmiot przetwarzający dane, stosującego się w pełni do wydanych poleceń.

W odniesieniu do *Cloud Computing* najistotniejszą kwestią okazuje się więc ustalenie czy usługodawca może być uznany za administratora czy jest jedynie podmiotem przetwarzającym dane. Grupa Robocza Artykułu 29 w opinii 5/2012 chociaż zauważa przypadki, w których dostawcę usług w chmurze można uznać za administratora danych - w sytuacji gdy dla realizacji własnych celów przetwarza dane klientów[212], to za przeważającą

[207] A.Frań-Adamek, *Komentarz… , opt.cit.*
[208] *Ibidem*
[209] *Ibidem*
[210] M.Siwicki, *Ochrona praw autorskich, bezpieczeństwa systemów informatycznych, danych osobowych i tajeminicy telekomunikacyjnej w chmurach obliczeniowych,* Prawo i Prokuratura 5,2015 s. 121.
[211] E.Molenda-Kropielnicka, *Prawne aspekty… , opt.cit.,* s.36.
[212] E.Molenda-Kropielnicka, *Cloud Computing... , opt.cit.,* s.125.

relację uznaje model administrator - klient i dostawca usług - przetwarzający, Podkreśla, że to klient usługi w chmurze jest osobą decyzyjną, jak zostało to już wspomniane - posiada władztwo, nad danymi, decyduje się powierzyć przetwarzanie przetwarzającemu - organizacji zewnętrznej, w tym przypadku dostawcy usług w chmurze oraz określa jego ostateczny cel.

Najistotniejsza jest więc decyzja podjęta przez klienta określająca formę, model, kierunek przetwarzania[213]. Takie założenie implikuje ograniczenie odpowiedzialności dostawcy usług jedynie do wypełnienia zobowiązań określonych w zawartej między stronami umowie, z kolei dla klienta - administratora konieczność realizacji szeregu obowiązków nałożonych przez przepisy prawa. Realizacja tych zadań może okazać się dla niego zadaniem niełatwym. Jednym w istotnych powodów jest fakt stosowania przez dostawców usług w chmurze standardowych umów, które ograniczają klientom margines swobody. Mimo tego Grupa Robocza w opinii 1/2010[214] wyraźnie uznaje, że nierównowaga w zakresie uprawnień między "małym administratorem a dużym usługodawcą" nie stanowi usprawiedliwienia dla przyjmowania przez administratora w umowie warunków niezgodnych z przepisami o ochronie danych osobowych. Z tego powodu to na administratorze ciąży obowiązek wyboru dostawcy usług w chmurze gwarantującego zgodność przetwarzania z przepisami o ochronie danych osobowych[215].

Pojawiającymi się w tym zakresie istotnymi problemami jest po pierwsze kwestia podmiotu pod-przetwarzającego. Wspomniane zostało już, że o ile wyraźnie w umowie nie zastrzeżono, podmiot przetwarzający dane na mocy umowy powierzenia ma możliwość przekazania przetwarzania danych innemu podmiotowi. Zjawisko to jest w usługach *Cloud Computing* niezwykle powszechne, a oznacza jednocześnie, iż mimo obowiązku przestrzegania przez przetwarzającego i pod-przetwarzających instrukcji administratora[216], jedynie w przypadku przetwarzającego, gdy ten podejmuje działania niezgodne z umową, administrator dysponuje możliwością pociągnięcia go do odpowiedzialności umownej.

Nie mniej istotnym zagadnieniem jest również obowiązek ochrony danych przed nielegalnym przetwarzaniem oraz precyzyjnego określenia jego celów nałożony na administratora - klienta. W związku z przekazaniem danych do systemu zarządzanego przez dostawcę usług w chmurze, klient może nie mieć możliwości sprawowania dalszej realnej kontroli nad danymi zwłaszcza, że po zawarciu umowy powierzenia to podmiot przetwarzający może stać się upoważnionym do wyboru metod oraz środków organizacyjnych i technicznych zapewniających ochronę przetwarzania danych osobowych, które mogą okazać się niewystarczające i umożliwić przejęcie danych przez nieuprawnione podmioty, zwłaszcza w momencie współdzierżawy umożliwiająca jednoczesne korzystanie z usługi przez wielu użytkowników. Niestety nie wyłącza to odpowiedzialności administratora, wystarczy wspomnieć art 31 ust 4 u.o.d.o, który wskazuje, że w przypadku powierzenia danych do przetwarzania, odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na administratorze danych.

---

[213] G.Karp, Cloud computing czyli przetwarzanie w chmurze przez prawników, http://www.rp.pl/artykul/769989-Cloud-computing-czyli-przetwarzanie-w-chmurze-przez-prawnikow.html, dostęp: [2.01.2016 r.]

[214] Opinia 1/2010 w sprawie pojęć "administrator danych" i "przetwarzający", http://www.giodo.gov.pl/1520057/id_art/3595/j/pl//.

[215] Opinia 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej, http://www.giodo.gov.pl/457/id_art/4760/j/pl/.

[216] Opinia 1/2010, *opt.cit.*

Należy rozważyć również kwestię usuwania danych osobowych., będącego, zgodnie z podaną definicją, formą przetwarzania danych. Ustawa o ochronie danych osobowych dopuszcza przechowywanie danych nie dłużej niż jest to niezbędne do celów przetwarzania. "Czasowym wyznacznikiem"[217] może być więc wykonanie zawartej między dostawcą usług a klientem umowy. J. Barta i R.Markiewicz wskazują, że co prawda po ustaniu celu przetwarzania danych nie trzeba usuwać, ale "powinny utracić walor danych osobowych"[218]. Dla osiągnięcia tego celu wspomniani autorzy wskazują na konieczność dokonywania przez administratora oceny zawartości swoich zbiorów, a nawet uprzednie ustanowienie okresów przetrzymywania danych[219]. Niestety, nietrudno zorientować się, że również ten przypadek znacznie komplikuje się w momencie korzystania z usług w chmurze. Powierzając dane podmiotowi przetwarzającemu będącego dostawcą usług w chmurze, administrator danych wyzbywa się bowiem faktycznej kontroli nad danymi. a więc możliwości dostępu, odzyskania po zakończeniu trwania umowy, poza tym nie wie również, czy odzyskane dane, jeśli taką możliwość przewidziała umowa, nie funkcjonują już samoistnie w chmurze, czego powodem jest istnienie łańcucha podmiotów przetwarzających oraz fakt przechowywanie danych na różnych serwerach i w różnych lokalizacjach[220]. Grupa Robocza art 29. wskazuje ponadto na zjawisko *"vendor lock-in".* Polega ono na tym, że dostawca usług w chmurze bazuje na zastrzeżonej technologii, nie mającej cechy kompatybilności z innymi systemami usługi *Cloud Computing*, co często mimo chęci, uniemożliwia przeniesienie przez klienta danych między różnymi systemami[221].

Transfer danych pomiędzy państwami stanowi kolejne pytanie o możliwość zapewnienia faktycznej ochrony przetwarzanym danym. B. Fisher i D. Karwala wskazują, że rozwój technologiczny niewątpliwie zwiększa możliwość niekontrolowanego przepływu danych między państwami, co powoduje konieczność szczególnej troski w tym zakresie[222]. Tak też jest w rzeczywistości - dostawcy usług w chmurze w sposób szczególny zainteresowani są możliwością niezakłóconego przemieszczania i powielania danych między swoimi serwerami. Chcąc zwiększyć swoją elastyczność, prędkość przetwarzania często korzystają z dowolnych, mniej przeładowanych serwerów zlokalizowanych w dowolnym miejscu na świecie[223].

Choć, zarówno u.o.d.o. jak i dyrektywa dopuszczają, a wręcz obligują państwa do niezakłócania swobodnego przepływu danych w obszarze Europejskiego Obszaru Gospodarczego(EOG), to inaczej sprawa wygląda w przypadku państw zlokalizowanych poza EOG - tzw. państw trzecich. Rozwiązanie to nie może dziwić, gdyż wynika z przyjęcia standardowego europejskiego modelu ochrony danych, czyli eliminowania dodatkowych wymogów dotyczących przetwarzania danych[224]. Inaczej wygląda natomiast kwestia przekazywania danych do państw trzecich. Następuje to w sytuacji, gdy dane faktycznie

[217] J.Barta, P.Fajgielski, R,Markiewicz, *Ochrona ..., opt.cit.*
[218] *Ibidem*
[219] *Ibidem*
[220] Opinia 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej, http://www.giodo.gov.pl/457/id_art/4760/j/pl/
[221] Opinia 5/2012, *opt.cit.*
[222] B.Fischer, D.Karwala, *Transfer danych osobowych do państw trzecich,* PiP 2007/1/ s.100.
[223] *Chmury obliczeniowe. Ekspertyza.* PE 475.104 2012
[224] B.Fischer, D.Karwala, *Transfer danych… , opt.cit.,* s.101.

„przekroczą granicę”[225]. Dopuszczalność ta jest uzależniona jest od tego czy państwa te zapewnią właściwy poziom ochrony. Oznacza to, że państwo przeznaczenia danych musi zachować chociażby takie poziom ochrony jakie zachowuje państwo pochodzenia. Należy w tym miejscu zauważyć, że ocenę zgodności standardów ochrony pozostawia się administratorowi danych[226]. I choć nasuwającą się interpretacją jest ta, że to państwo docelowe powinno dawać gwarancje ochrony[227], to jednak art 48 pkt 2 ust. 1 u.o.d.o. wprowadza konstrukcję standardowych klauzul umownych jako instrumentu umożliwiającego wprowadzenie zabezpieczenia danych osobowych, będącego jednocześnie wymogiem ich transferu do państwa trzeciego. To właśnie powoduje, że to administratorze danych ciąży wspomniany ten obowiązek. Wzory tych klauzul zostały określone w decyzjach Komisji Europejskiej, jedna z nich - decyzja Komisji 2010/87/UE z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich[228] zawiera wzory klauzul umownych do wykorzystania w przypadku zawierania umowy o powierzenie przetwarzania danych, a więc obejmuje przypadek zawarcia umowy między klientem - klientem a dostawcą usług w chmurze - podmiotem z państwa trzeciego, który przetwarza dane na zlecenie.

W nawiązaniu do wcześniejszych rozważań o *Cloud Computing* nietrudno jednak wyciągnąć wniosek, że po pierwsze ponownie pojawia się problem rozgraniczenia ról administratora a przetwarzającego, oraz kwestia możliwości wynegocjowania brzmienia zawieranej umowy i dołączenia wspomnianej klauzuli w sytuacji stosowania przez dostawców standardowych wzorców.

Podsumowując powyższe rozwiązania trudno nie zauważyć wielu trudności interpretacyjnych w zakresie obecnie obowiązujących przepisów prawa. Szybkość wprowadzania nowych rozwiązań technologicznych nie jest proporcjonalna do adekwatnych regulacji prawnych i budzi poważne wątpliwości o ich skuteczność. Niewątpliwie stoją więc przed ustawodawcami nowe wyzwania. Nie mniej istotna jest jednak również świadomość zwykłych użytkowników dotycząca zarówno mechanizmów istniejących w chmurze obliczeniowej i związanych z nimi zagrożeń dla bezpieczeństwa danych przetwarzanych w chmurze, oraz znajdujących do nich zastosowanie przepisów. Korzystanie z zasobnej w liczne zalety chmury obliczeniowej musi pozostać poparte ostrożnością oraz dbałością o ochronę własnych interesów. Tylko taka postawa może w dalszej perspektywie spowodować, że “mały administrator” nie będzie słabszy od “dużego usługodawcy”. Wreszcie to również dla dostawcy gwarancja coraz skuteczniejszej ochrony przetwarzanych danych będzie determinować wzrost zysków i zajmowaną pozycję rynkową.

[225] *Ibidem*
[226] *Ibidem*
[227] J. Barta, R. Markiewicz, *Komentarz …, opt.cit.*
[228] Dz. Urz. UE L 39/5 z 12/02.2010 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:PL:PDF

mgr Zuzanna Lisowska

Mowa nienawiści a wolność wyrażania opinii w Internecie

1. Wprowadzenie

Stopniowy rozwój koncepcji związanych z prawami człowieka na przestrzeni ostatnich lat spowodował, iż potrzeba zbalansowania wolności oraz praw gwarantowanych w wielu międzynarodowych dokumentach, takich jak chociażby Powszechna Deklaracja Praw Człowieka z 1948 roku[229] czy też Europejska Konwencja Praw Człowieka z 1950 roku[230], znacząco wzrosła. W dzisiejszych czasach, na tle coraz bardziej wielokulturowego społeczeństwa, nie sposób nie zauważyć, większej niż dawniej różnorodności związanej z stylem życia, religią, zwyczajami, czy też wyglądem poszczególnych ludzi[231]. Ze względu na te dalece widoczne różnice, ochrona praw człowieka, które nabierają coraz to nowego, często szerszego znaczenia, staje się jednym z najważniejszych wyzwań dla władz poszczególnych państw na całym świecie.

Niezmiernie szybki rozwój środków komunikacji w Internecie, takich jak chociażby portale społecznościowe, blogi, videoblogi, czy też gazety internetowe, jest dodatkowym czynnikiem, który stawia przed ochroną praw człowieka wyzwania takie jak nowe możliwości ich naruszeń. W tym kontekście, istotne jest przede wszystkim określenie granic pomiędzy poszczególnymi prawami człowieka, każdorazowo mając na uwadze poszczególny stan faktyczny. Konieczność odnalezienia odpowiedniego balansu pomiędzy wolnością słowa, prawem do poszanowania życia prywatnego oraz rodzinnego, wolnością sumienia i religii oraz zakazem dyskryminacji w świecie wirtualnym, jawi się jako rzecz kluczowa.

Jednym z głównych oraz najtrudniejszych zadań w aspekcie rozwoju społeczeństwa internetowego jest pogodzenie wolności słowa z innymi chronionymi prawami oraz wolnościami. Naruszenia wolności słowa w Internecie związane są z powszechnym przeświadczeniem o anonimowości wśród użytkowników Internetu, którą można zauważyć przede wszystkim w komentarzach pod artykułami w gazetach internetowym, blogach, forach internetowych oraz portalach społecznościowych. Rozpowszechnianie mowy nienawiści w wypowiedziach w wirtualnym świecie staje się przyczyną licznych naruszeń takich praw człowieka, jak chociażby ochrona praw mniejszości[232].

Naruszenia związane z mową nienawiści w Internecie dotyczą takich zagadnień, jak rasizm, ksenofobia, anty-semityzm, homofobia[233]. Inną, bardziej powszechną formą wyrażania

---

[229] Powszechna Deklaracja Praw Człowieka z 1948 r., zwana dalej „PDPC", http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/pql.pdf.

[230] Europejska Konwencja Praw Człowieka z 1950 r., zwana dalej "EKPC", http://www.echr.coe.int/Documents/Convention_POL.pdf.

[231] *A. Weber*, Manual of Hate Speech, Strasburg 2009, s.1.

[232] *Ibidem*, s.2.

[233] *Rada Europy*, Factsheet Hate Speech, 2008, s.1.

mowy nienawiści, jest kierowanie obraźliwych określeń w stronę danych osób, z uwagi na jakąś cechę lub sposób zachowania, które nie są powszechnie akceptowane przez osoby, które naruszeń dokonują. Należy również zaakcentować, iż głównym powodem tak szerokich naruszeń dóbr osobistych w Internecie jest różnica pomiędzy światem wirtualnym, a rzeczywistym, której użytkownicy sieci niekiedy nie dostrzegają.

Występowanie mowy nienawiści, nie jest ograniczone jedynie do strefy Internetu, a dotyczy również świata rzeczywistego. Warto jednak zauważyć, że to właśnie w Internecie, z uwagi na łatwość i szybkość przekazu możliwa skala naruszeń zdaje się przybierać rozmiary większe niż dotychczas.

Celem niniejszej publikacji jest przedstawienie problematyki związanej z ochroną wolności słowa na terenie Europy w zestawieniu mową nienawiści, która przybiera coraz to różne formy, zwłaszcza w świecie wirtualnym. Rozważania będą dotyczyć głównie tego, czy wprowadzenie ograniczeń wolności słowa, z uwagi na obecność w Internecie mowy nienawiści jest pożądane i możliwe.

2. Pojęcie „mowa nienawiści"

Na wstępie rozważań na temat pojęcia „mowy nienawiści", istotne jest określenie znaczenia terminu „wolności wyrażania opinii". Wolność wyrażania opinii na terenie większości krajów Europy zagwarantowana została przede wszystkim w artykule 10 EKPC. Zgodnie z tym przepisem, pojęcie to zawiera w sobie wolność posiadania poglądów, otrzymywania i przekazywania informacji oraz idei bez ingerencji władz publicznych, bez względu na granice państwowe. Ponadto artykuł ten podkreśla, że korzystanie z tych wolności może podlegać odpowiednim wymogom formalnym, warunkom, ograniczeniom i sankcjom, niezbędnym w społeczeństwie demokratycznym[234]. Odpowiednie ograniczenie wolności wyrażania opinii może być wprowadzone w interesie bezpieczeństwa państwowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych[235].

Dodatkowo, Europejski Trybunał Praw Człowieka[236] wielokrotnie w swym orzecznictwie podkreślał, że wolność wyrażania opinii stanowi fundamentalną zasadę społeczeństwa demokratycznego. W związku z nieodzownym znaczeniem tej reguły, każde jej ograniczenie czy też spenalizowanie powinno być proporcjonalne do uzasadnionego celu[237].

Pomimo istnienia szeroko pojętej wolności wyrażania opinii w Internecie, rosnąca ilość jej naruszeń przybierających różne formy doprowadziła do tego, że międzynarodowe sądy i trybunały takie jak m.in. Europejski Trybunał Praw Człowieka oraz przedstawiciele doktryny stanęli przed trudnym zadaniem w postaci konieczności ustalenia pewnych ograniczeń

[234] Art. 10 EKPC.
[235] *Ibidem.*
[236] Europejski Trybunał Praw Człowieka, zwany dalej „ETPC".
[237] *Europejski Trybunał Praw Człowieka*, Factsheet Hate speech, 2015, s.1;
Wyrok ETPC w sprawie Handyside vs. Wielka Brytania z dnia 07.12.1976 r., (5493/72), http://hudoc.echr.coe.int/.

i restrykcji. Limitowanie wolności wyrażania opinii stało się bardzo istotne przede wszystkim, na zintensyfikowany rozwój tzw. „mowy nienawiści", w każdym ze środków przekazu i komunikacji.

Definicja „mowy nienawiści" przez długi czas nie była wprost sformułowana, mimo, że zjawisko to było coraz bardziej zauważalne. Z uwagi na to, przedstawiciele instytucji międzynarodowych, jak Rada Europy, Europejski Trybunał Praw Człowieka, czy też Organizacja Narodów Zjednoczonych (w tym również wyspecjalizowane organizacje działające w jej ramach jak UNESCO) zaczęły podejmować działania prowadzące ku ustaleniu głównych cech charakteryzujących to zjawisko, co rozpoczęło dyskusję na temat możliwego ograniczenia jego negatywnych skutków.

Pierwszym dokumentem, który należy przywołać na tle tematyki mowy nienawiści są Zalecenia Komitetu Ministrów Rady Europy dla krajów członkowskich dotyczące mowy nienawiści[238], który zawiera kluczowe wskazówki interpretacyjne związane ze zrozumieniem terminu „mowa nienawiści". Zgodnie z Zaleceniami termin ten, powinien być rozumiany jako zawierający wszelkie formy wyrażania opinii, które rozpowszechniają, podżegają, promują bądź też usprawiedliwiają nienawiść rasową, ksenofobię, antysemityzm, bądź też inne formy nienawiści opartej na nietolerancji wyrażanej poprzez agresywny nacjonalizm, etnocentryzm, dyskryminację czy też wrogość w stosunku do mniejszości, imigrantów lub osób obcego pochodzenia[239].

Następnie, również ETPC na tle wieloletniej praktyki orzeczniczej wypracował ogólne cechy pojęcia „mowy nienawiści", zgodnie z którą zawiera ona w sobie wszelkie formy wyrażania opinii, która promuje, podżega, rozpowszechnia bądź też usprawiedliwia nienawiść opartą na nietolerancji. W zakresie rozumienia tego terminu, ETPC umieścił również nietolerancję religijną oraz nienawiść związaną ze zjawiskiem homofobii[240].

W związku w powyższym, oczywisty zdaje się fakt, iż wyrażanie opinii, które wchodzi w zakres „mowy nienawiści" nie jest chronione poprzez artykuł 10 Europejskiej Konwencji Praw Człowieka[241].

Odnosząc się do zjawiska „mowy nienawiści" w świecie wirtualnym, należy zaznaczyć, że rozpoznanie i zakwalifikowanie go jako szkodliwego jest niezwykle trudne. Wynika to przede wszystkim z tego, że niektóre treści mogą być sklasyfikowane jako znajdujące się w zakresie terminu „mowa nienawiści" od samego początku, inne zaś, mimo że na początku zdają się być niegroźne i nieszkodliwe w swym wyrazie, po głębszej analizie mogą zostać zakwalifikowane jako dyskryminujące osoby trzecie ze względu na różne, wyżej wymienione czynniki[242].

Identyfikacja i charakteryzacja „mowy nienawiści *online"* zdaje się być istotnym punktem wyjścia do dalszych rozważań. Z uwagi na to, należy zaznaczyć, że w wielu aspektach różnica pomiędzy „mową nienawiści" w świecie rzeczywistym, a wirtualnym nie jest bardzo widoczna. Każde bowiem rozpowszechnienie mowy nienawiści i nawoływanie do dyskryminacji, czy też agresji należy klasyfikować jako naruszenie dóbr osobistych danej osoby, bez względu na

[238] *Rada Europy,* The Recommendation of the Committee of Ministers of the Council of Europe to member states on the execution on hate speech z dnia 30.10.1997 r., zwany dalej „Zaleceniami".
[239] *Ibidem.*
[240] *Europejski Trybunał Praw Człowieka*, Factsheet…, s.1.
[241] *Rada Europy,* Factsheet…, s.2.
[242] *Ibidem,* s.1.

miejsce dokonania tego naruszenia. Tego typu sytuacje, muszą być również zaliczane jako naruszające fundamentalne prawa człowieka, bez względu na miejsce i formę ich rozpowszechnienia. Odnosząc się do naruszeń dóbr osobistych w Internecie, w praktyce pojawiają się wciąż nowe wyzwania, co wzmaga konieczność uregulowania tej sfery związanej z umieszczaniem treści *online*.

Jako główne wyzwania, które związane są ze specyficznymi cechami wirtualnego świata, można zaliczyć przede wszystkim poczucie anonimowości wśród użytkowników Internetu, wielomiejscowość internetowych naruszeń oraz problem z monitorowaniem naruszeń z uwagi na ich dużą skalę. Bardzo ważnym elementem związanym z „mową nienawiści *online"* jest fakt, iż treści umieszczone w sieci internetowej mogą pozostać tam przez bardzo długi czas, w różnych formatach, na różnych serwerach oraz mogą być przekazywane sobie pomiędzy użytkownikami (tzw. „linkowanie") w niesamowicie szybki i skuteczny sposób. Dodatkowo, nawet w przypadku usunięcia treści *online*, może ona następnie pojawić się w zupełnie innym miejscu – na kolejnej stronie internetowej, innym serwerze, bądź też pod inną nazwą[243].

Jako problem jawi się również duża anonimowość użytkowników sieci wirtualnej, których zazwyczaj cechuje przeświadczenie, że nie zostaną zidentyfikowani[244]. W porównaniu ze światem rzeczywistym, użytkownicy Internetu czują się dużo bardziej komfortowo, rozprzestrzeniając mowę nienawiści, gdyż w ich przekonaniu nie będą musieli ponosić konsekwencji swoich działań.

Kolejnym kluczowym aspektem, który dotyczy rozpowszechniania „mowy nienawiści *online"* jest ponadnarodowy zasięg Internetu. Należy podkreślić, iż problematyka ta wymaga wzmożonej międzynarodowej współpracy w celu stworzenia mechanizmów prawnych odpowiednich w zwalczaniu mowy nienawiści. Ponadto, rozpowszechniając mowę nienawiści, użytkownicy Internetu krzywdzą nie tylko osoby, których dobra osobiste zostają naruszone, lecz również naruszają regulaminy serwisów społecznościowych, serwisów internetowych czy też prawa kraju, w którym się znajdują [245].

3. Zagrożenia związane z obecnością mowy nienawiści w Internecie. Przykłady naruszeń.

Ilość naruszeń dóbr osobistych użytkowników internetowych poprzez rozpowszechnianie mowy nienawiści jest ogromna i rośnie z każdym dniem. W przestrzeni wirtualnej, praktycznie na każdej stronie internetowej możliwe jest odnalezienie miejsca, w którym użytkownicy Internetu mogą wyrażać lub wymieniać opinie pomiędzy sobą. Nie ulega wątpliwości, że w dzisiejszych czasach Internet jedyną w swoim rodzaju, unikalną platformą, dzięki której społeczeństwo może zarówno rozwijać swoją osobowość, poszukiwać informacji jak i komunikować się między sobą. Niestety, również w czasie każdej z tych czynności istnieje możliwość równoczesnego rozpowszechnia treści, które można zakwalifikować jako mowę nienawiści. Najbardziej popularnym przykładem występowania mowy nienawiści są portale

[243] *I. Gagliardone, D. Gal, T. Alves, G. Martinez,* Countering Hate Speech, 2015 UNESCO, s.14-16.
[244] *Ibidem.*
[245] *Ibidem,* s.16.

społecznościowe, takie, jak chociażby Twitter, czy też Facebook (przez niektórych użytkowników Internetu nazywany "*Hatebookiem*"). Na tego typu stronach internetowych, użytkownicy mają pełną możliwość tworzenia własnej przestrzeni wirtualnej i umieszczania w niej ogromnej ilości treści wybranych przez siebie (komentarzy, zdjęć, filmów, muzyki). Każda z tych treści może stanowić potencjalny nośnik mowy nienawiści i doprowadzać do naruszeń dóbr osobistych innych użytkowników internetowych.

Bardzo interesującym zagadnieniem jest również niezwykle popularny fonemem tzw. „memów". Tworzone przez użytkowników Internetu memy, zwyczajowo składają się ze zdjęcia bądź obrazka oraz kilku słów, zdania na pierwszym planie. Głównym celem tego typu formy wyrazu jest odniesienie się do otaczającej nas rzeczywistości, zarówno politycznej, związanej z osobami powszechnie znanymi, jak i do codziennych, zwyczajnych sytuacji celem skomentowania ich. W praktyce wszystko może stać się przedmiotem, czy też „głównym bohaterem" mema. Na tle tego fenomenu należy z całą stanowczością przyznać, iż rozpowszechnianie memów bardzo często wiąże się ze zjawiskiem mowy nienawiści, ponieważ niekiedy autorzy nie znajdują właściwego balansu pomiędzy krytykowaniem, a dyskryminowaniem i oczernianiem innych osób.

Kolejnym miejscem w przestrzeni internetowej, w którym można odnaleźć przykłady naruszeń rozpowszechniania mowy nienawiści są internetowe wydania gazet i dzienników. Na takich portalach dobra osobiste mogą być naruszone zarówno poprzez umieszczenie krzywdzących określeń w samej treści artykułów oraz przez samych użytkowników, którzy komentują tego typu publikacje, o ile taka możliwość wyrażania opinii jest przez dany portal umożliwiona. W tym miejscu konieczne wydaje się przywołanie sprawy, w której ETPC musiał po raz pierwszy zmierzyć się z rozstrzygnięciem spawy dot. mowy nienawiści. Sprawa ta dotyczyła sporu pomiędzy Estonią a Delfi AS[246] odnośnie skargi o odpowiedzialności za komentarze pozostawiane przez użytkowników na internetowym portalu informacyjnym. Delfi AS jest portalem informacyjnym, na którym w 2011 roku pod jednym z artykułów pojawiło się dużo komentarzy, oceniających w sposób negatywny bohaterów artykułu – członków przedsiębiorstwa SLK Company. Mężczyzna, który stał się jednym z głównych bohaterów artykułu, początkowo zażądał od portalu usunięcia negatywnych komentarzy (co Delfi AS uczyniło bez zbędnej zwłoki) oraz odszkodowania z tytułu naruszenia jego dóbr osobistych. Z uwagi na przyznanie racji przez sąd w Estonii powodowi, na skutek skargi Delfi SA, sprawa trafiła do ETPC. Delfi SA, podnosiło, że poprzez nakazanie im zapłaty odszkodowania na rzecz powoda, naruszono i ograniczono prawo człowieka w postaci swobody wypowiedzi. Po rozpatrzeniu sprawy ETPC zdecydował, że w niniejszej sprawie artykuł 10 EKPC nie został naruszony. Trybunał orzekł również, że internetowe serwisy informacyjne, które do celów handlowych i zawodowych, stwarzają użytkownikom możliwość umieszczania komentarzy pod artykułami, muszą przyjąć na siebie obowiązki i odpowiedzialność związane z wolnością wyrażania opinii, zgodnie z artykułem 10(2) EKPC. Decyzja ETPC poparta była przede wszystkim tym, że rozpowszechnianie mowy nienawiści poprzez umieszczanie komentarzy, w sposób wyraźny podżegał do przemocy. ETPC podkreślił dodatkowo, że internetowe serwisy informacyjne są zobligowane do kontrolowania zawartość treści umieszczanych na ich stronach

[246] Wyrok ETPC w sprawie Delfi as. v. Estonia z dnia 10.10.2013 r. (App. No. 64569/09), http://hudoc.echr.coe.int/.

internetowych w sposób efektywny w celu zapobieżenia rozpowszechniania mowy nienawiści. Wyrok w omawianej sprawie wywołał kontrowersje związane z faktem, iż ETPC nie doprecyzował w sposób klarowny tego, kiedy i w jaki dokładnie sposób internetowe portale informacyjne mogą „kontrolować zawartość" treści umieszczonych na portalu w sposób nienaruszający wolności do wyrażania opinii[247].

Powyższe przykłady, ukazujące możliwość naruszenia dóbr osobistych osób poprzez mowę nienawiści w Internecie, w praktyce, poza prawnymi aspektami tego zagadnienia, mogą mieć również wywoływać negatywne skutki wobec ofiar tego zjawiska, takie jak wzrost liczby psychicznych załamań na tle nerwowym, a nawet wzrostu liczby samobójstw. Szkodliwe skutki internetowej mowy nienawiści, odzwierciedla wiele przypadków w postaci zachowań nastolatków[248], którzy ze względu na negatywne komentarze internautów na temat swojego wyglądu, wagi, stylu życia, rasy czy też wyznania decydują się na fizyczne okaleczenie swojego ciała lub samobójstwo[249].

3.1. Legalne aspekty ochrony przed mową nienawiści w Internecie w Europie.

Z uwagi na zaakcentowane powyżej przykłady naruszeń dóbr osobistych poszczególnych osób poprzez użycie mowy nienawiści w Internecie, należy zaznaczyć, że skala tego zjawiska wymaga pozytywnej reakcji zarówno instytucji, które chronią prawa człowieka, jak i władz państwowych poszczególnych krajów.

Państwa powinny przyjmować takie regulacje prawne, które powinny zapobiegać naruszaniu dóbr osobistych poprzez obecność mowy nienawiści, która jest rozpowszechniana przez osoby znajdujące się na jej terytorium. Niektóre z krajów w Europie, takich jak Szwecja[250] i Dania[251] wprowadziły do swojego systemu prawnego wyraźne regulacje penalizujące przejawy <<mowy nienawiści>>. Inne kraje europejskie, takie jak Polska czy też Chorwacja[252], zakazują mowy nienawiści poprzez regulacje, które nie określają tego zjawiska wprost, lecz poprzez przepisy, które w swoim zakresie obejmują m.in. zakaz rozpowszechniania wyrażeń, które podżegają do przemocy, rasizmu, ksenofobii, antysemityzmu, homofobii i innych tego rodzaju zjawisk.

---

[247] http://www.hfhr.pl/wielka-izba-etpc-brak-naruszenia-swobody-wypowiedzi-w-sprawie-delfi-p-estonii/ dostęp: [28.01.2016 r.]

[248] Szerzej w odniesieniu do sytuacji w Polsce: *J. Włodarczyk*, Mowa nienawiści w internecie w doświadczeniu polskiej młodzieży, Warszawa 2014; http://www.mowanienawisci.info/wp-content/uploads/2014/10/Mowa-nienawi%C5%9Bci-w-internecie-w-do%C5%9Bwiadczeniu-polskiej-m%C5%82odzie%C5%BCy.pdf, dostęp: [28.01.2016 r.]

[249] Drastyczny przykład stanowi sprawa czternastolatka Dominika z Bieżunia, który z uwagi na negatywne komentarze w Internecie na temat jego wyglądu, popełnił samobójstwo poprzez powieszenie się na sznurówkach. http://wyborcza.pl/duzyformat/1,146227,18321428,mamo-jestem-zerem.html, dostęp: [28.01.2016 r.]

[250] Szwedzki Kodeks Karny, Rozdział 16, Dział 8, http://www.government.se/contentassets/5315d27076c942019828d6c36521696e/swedish-penal-code.pdf.

[251] Duński Kodeks Karny, Dział 266 b, http://www.inach.net/content/denmark.html.

[252] Chorwacki Kodeks Karny, Artykuł 174, https://www.icrc.org/ihlnat.nsf/0/ce67fea60a8e402fc1257163002a6ea9/$FILE/Criminal%20Code%20Croatia%20ENG.pdf.

W Polsce, prawo do wyrażania opinii gwarantowane jest przede wszystkim w Konstytucji Rzeczypospolitej Polskiej poprzez określenie, iż każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji[253]. Ponadto, regulacje chroniące przed skutkami rozpowszechniania mowy nienawiści znajdują się w Kodeksie karnym[254], który penalizuje publicznie propagowanie faszystowskiego lub innego totalitarnego ustroju państwa czy też nawołuje do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość[255]. Na uwagę, w związku z tematem mowy nienawiści, zasługuje również regulacja umieszczona w k.k. dotycząca karalności publicznego znieważenia grupy lub osoby z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości lub z takich powodów narusza nietykalność cielesną innej osoby[256]. Ustawodawstwo polskie nie penalizuje wprost naruszeń związanych z rozpowszechnianiem mowy nienawiści ze względu na orientację seksualną czy też przynależność płciową. Należy również zaznaczyć, iż również naruszenia dóbr osobistych związanych z mową nienawiści mogą wchodzić w zakres regulacji polskich, jak chociażby regulacje kodeksu cywilnego[257] czy też przestępstwo zniesławienia bądź zniewagi uregulowanych w kodeksie karnym.
Pomimo drobnych różnic w podejściu różnych krajów w Europie do zjawiska mowy nienawiści, faktem jest, iż jest to zjawisko zauważalne powszechnie. Penalizacja wyrażania opinii, które mogą być uznane za mowę nienawiści zależą od podejścia danego kraju do takich czynników jak, chociażby ksenofobia i homofobia. Warto również podkreślić, iż każdy z krajów, który jest członkiem Rady Europy, czy też Organizacji Narodów Zjednoczonych, tworząc regulacje prawne dotyczące tego zjawiska, powinien mieć na uwadze wytyczne oraz zasady przyjęte przez te organizacje.

3.2. Mechanizmy ochrony przed mową nienawiści wprowadzane przez Radę Europy

Rada Europy wielokrotnie wprowadzała pewne zasady oraz formułowała wytyczne w celu zapobiegania i zwalczania mowy nienawiści. W związku z tym, należy przede wszystkim przywołać, że w swych Zaleceniach, Rada Europy ustanowiła wspólne kryteria dla ustawodawstwa krajowego dotyczącego zwalczania tego zjawiska. Jednymi z głównych wytycznych jest stymulowanie i koordynacja badań nad skutecznością istniejących przepisów i praktyki prawnej oraz zapewnienie społeczeństwu i fachowcom pracującym w mediach odpowiednich informacji dotyczących przepisów prawnych[258]. Dodatkowym i ważnym tematem, który został ujęty w Zaleceniach jest fakt, że wyrażenia pełne mowy nienawiści jawią się jako bardziej szkodliwe, w sytuacji, gdy są rozpowszechniane przez media[259]. Zalecenia

[253] Art. 54 Konstytucji Rzeczypospolitej Polskiej.
[254] Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (t.j. Dz. U. z 2016 r. poz. 189 ze zm.), zwany dalej „k.k."
[255] Art. 256 k.k.
[256] Art. 257 k.k.
[257] Art.23 i n. ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny, zwana dalej „k.c.".
[258] *Rada Europy*, The Recommendation…, Principle 2.
[259] *Rada Europy*, Factsheet…, s.3-5.

zawierają zasady ukazujące w jaki sposób odróżnić odpowiedzialność autora danej treści od odpowiedzialności mediów, które dane treści rozpowszechniają i przekazują[260].
Innym ważnym dokumentem sporządzonym przez Radę Europy odnoszącym się do kwestii mowy nienawiści, jest protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości, dotyczący penalizacji czynów o charakterze rasistowskim i ksenofobicznym popełnionych przy użyciu systemów komputerowych[261]. Dokument ten doprecyzowuje kwestie penalizacji takich zachowań, jakie powinny zostać podjęte na szczeblu krajowym.
Kolejnym aktem, który należy przywołać jest Rekomendacja Zgromadzenia Parlamentarnego Rady Europy w sprawie bluźnierstwa, zniewagi religijnej i mowy nienawiści wobec bluźnierstwa, obrazy religijnej i mowy nienawiści przeciwko osobom z powodu ich wyznania[262]. W tym dokumencie podkreślona została konieczność kryminalizacji wypowiedzi, które podżegają do nienawiści, bluźnierstwa, przemocy lub dyskryminacji wobec osób lub grup religijnych bądź innych.

Istotne jest również to, że liczne Komisje działające w ramach Rady Europy odgrywają bardzo istotną rolę w zwalczaniu zjawiska mowy nienawiści. Dobrym przykładem zdaje się być Komisja Wenecka[263], która zaleca, że krytyka powinna być tolerowana do czasu, gdy nie stanowi świadomej obelgi, nienawiści lub dyskryminacji w stosunku do ludzi, którzy są wyznawcami określonych religii. Inną ważną instytucją jest Europejska Komisji przeciwko Rasizmowi i Nietolerancji[264]. Według jej zaleceń należy zabronić wyrażeń, które zawierają rasistowskie wypowiedzi, takich jak podżeganie do przemocy wobec ludzi ze względu na ich narodowość, religię, rasę, kolor skóry czy języka.

4. Ochrona przed mową nienawiści gwarantowana na gruncie orzecznictwa Europejskiego Trybunału Praw Człowieka

Odnosząc się do orzecznictwa Europejskiego Trybunału Praw Człowieka, najważniejszą kwestią tam poruszaną jest ustalenie właściwego balansu pomiędzy poszczególnymi prawami i zasadami oraz ustalenie odpowiednich granic dla każdego z nich. Europejska Konwencja Praw

[260] *Ibidem,* s.4.
[261] Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości, dotyczący penalizacji czynów o charakterze rasistowskim i ksenofobicznym popełnionych przy użyciu systemów komputerowych z dnia 28.01.2003 r., http://www.dziennikustaw.gov.pl/.
[262] The Recommendation of the Parliamentary Assembly of the Council of Europe on blasphemy, religious insults and hate speech against blasphemy, religious insult and hate speech against persons on the grounds of their religion z dnia 29.07.2007 r., http://www.venice.coe.int/webforms/documents/?pdf=CDL-STD(2010)047-e dostęp: [28.01.2016 r.]
[263] Komisja Wenecka jest organem doradczym Rady Europy, jej działalność opiera się przede wszystkim na udzielaniu porad prawnych państwom członkowskim w celu dostosowania przez nie swoich struktur prawnych i instytucjonalnych w zgodzie z europejskimi standardami i międzynarodowym doświadczeniem w dziedzinie demokracji, praw człowieka i rządów prawa; http://www.venice.coe.int/, dostęp: [28.01.2016 r.]
[264] Europejska Komisji przeciwko Rasizmowi i Nietolerancji jest niezależnym organem monitoringowym Rady Europy do spraw zwalczania rasizmu, dyskryminacji rasowej, ksenofobii, antysemityzmu i nietolerancji; http://www.strasburgre.msz.gov.pl/pl/o_re/monitoring/ecri/, dostęp: [28.01.2016 r.]

Człowieka zawiera dwie możliwe sposoby oceny, czy w danym przypadku wolność wyrażania opinii powinna być ograniczana czy też nie[265].

Pierwszy sposób, na podstawie artykułu 17 EKPC, przewiduje wyłączenie ochrony przewidzianej w EKPC w stosunku do określonego wyrażenia. Artykuł ten ustanawia zasadę zakazu nadużywania prawa w przypadku, gdy wyrażenia zawierają mowę nienawiści oraz neguje podstawowe wartości zawarte w EKPC. Drugi sposób oceny, którego podstawę stanowi artykuł 10 ustęp 2 EKPC, przewiduje ustanowienie ograniczenia ochrony w przypadku domniemanego naruszenia, z uwagi na takie elementy, jak chociażby interes bezpieczeństwa państwowego, integralność terytorialna lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu[266].

Rada Europy ustaliła szereg zasad dotyczących czynników, które powinny być brane pod uwagę w każdym przypadku przez ETPC, gdy są związane z tematem mowy nienawiści (rozgłos i potencjalny wpływ rozpowszechnianego wyrażenia), kluczowe kryteria w celu określenia czy wyrażenie stanowi przejaw mowy nienawiści i czy powinno być ograniczone (jaki był zamiar autora wypowiedzi) oraz sytuacje, gdy wolność wyrażania opinii nie powinna być ograniczona (gdy wyrażenie nie jest obraźliwe)[267]. Następnie, bardzo ważną kwestią, która została podniesiona przez Radę Europy w celu ustalenia wytycznych dla ETPC, jest możliwość wprowadzenia ograniczeń dotyczących wolności mediów. Należy podkreślić, że co do zasady prasa nie powinna przekraczać granic, ustawionych po to, by nie naruszać praw innych osób, zaś z drugiej strony, w taki sam sposób jest zobowiązana do przekazywania informacji i idei z uwagi na prawo do otrzymywania informacji przez społeczeństwo[268]. Kryteria ustalone przez Radę Europy mają zasadniczy wpływ na kształt orzeczeń ETPC dotyczących mowy nienawiści.

5. Podsumowanie

Odpowiedź na pytanie, czy mowa nienawiści z uwagi na swoje szkodliwe skutki powinna być poddana cenzurze, nie jest jednoznaczna. Wszechobecna debata dotycząca mowy nienawiści dotyczy głównie konfliktu pomiędzy wolnością wyrażania opinii, a potencjalną możliwością naruszenia dóbr osobistych innych osób. Zwolennicy poglądu, iż wolność wyrażania opinii jest najważniejszą wartością, nie popierają żadnej formy cenzury tego niezbywalnego i przyrodzonego każdej osobie prawa człowieka. Reprezentanci odmiennej opinii, według której mowa nienawiści jest jednym z poważnych zagrożeń społecznych podkreślają, że powinny istnieć regulacje penalizujące to zjawisko z uwagi na konieczność ochrony innych niż wolność wyrażania opinii praw człowieka.

W jednoznaczne udzielenie odpowiedzi na ww. pytanie, utrudnia fakt, że zazwyczaj trudno jest zdecydować, czy dane wyrażenie może być uznane za przejaw mowy nienawiści[269].

---

[265] *Europejski Trybunał Praw Człowieka*, Factsheet…, s.1.
[266] *Ibidem.*
[267] *Rada Europy,* Factsheet…, s.2-3.
[268] *Ibidem,* s.3-4.
[269] *D. Bychawska-Siniarska, D. Głowacka,* Mowa nienawiści w Internecie: jak z nią walczyć? Materiały z konferencji zorganizowanej przez Obserwatorium Wolności Mediów w Polsce, Helsińskiej Fundacji Praw

Problem ten pojawia się zwłaszcza na płaszczyźnie Internetu, gdzie z uwagi na światowy charakter tego medium, znalezienie autora szkodliwych treści umieszczonych na stronie internetowej jest bardzo trudne, niekiedy wręcz niemożliwe.

Nie ulega jednak wątpliwości, że regulacje, które już istnieją związane z penalizacją zjawiska mowy nienawiści są jak najbardziej pożądane w dzisiejszym społeczeństwie, którego wielokulturowości nie można zanegować. Próby podejmowane przez przedstawicieli Organizacji Narodów Zjednoczonych oraz Rady Europy w celu ochrony naruszeń związanych z wszechobecną mowie nienawiści należy ocenić w sposób pozytywny. Ponadto, warto również docenić wkład i zaangażowanie osób tworzących różne kampanie społeczne, które zajmują się zwalczaniem zjawiska mowy nienawiści i zmniejszeniem poziomu akceptacji społecznej jego przejawów, jak chociażby „*No Hate Speech Movement"*[270] (ang. ruch przeciwko mowie nienawiści*),* czy też „Hejtstop"[271].

Należy również podkreślić, iż w celu zwalczania obecności oraz łagodzenia skutków wywołanych przez mowę nienawiści istotne jest nieustające edukowanie społeczeństwa[272] w celu zwiększenia świadomości dotyczącej skali tego zjawiska oraz pożądanych reakcji w celu zapobieżenia licznym tragediom z nim związanych[273].

W świetle powyższego, należy zaakcentować zgodnie z internetowym sloganem głoszącym hasło, że *"hate speech is no free speech"* tj. „mowa nienawiści nie jest mową wolną". Z perspektywy ochrony praw człowieka i rosnącej ilości naruszeń dóbr osobistych innych osób, przepisy które uniemożliwiają nieograniczoną wolność wyrażania opinii powinny istnieć, ale należy wprowadzać je bardzo ostrożnie i tylko w sytuacjach koniecznych. Ograniczanie wolności wyrażania opinii nie powinno bowiem w żadnym wypadku przerodzić się w cenzurowanie tego niezbywalnego prawa człowieka.

Człowieka oraz Zakład Praw Człowieka WPiA UW i Zakład Praw Człowieka Wydziału Politologii UMCS w dniu 29 października 2012 r., Warszawa 2013, s.7.

[270]No Hate Speech Movement Youth Department of the Council of Europe, European Youth Centre, http://www.nohatespeechmovement.org/, dostęp: [28.01.2016 r.] *„No Hate Speech Movement"* poza wymienionymi już przykładami działalności, skupia się również na rozwoju uczestnictwa młodzieży w Internecie.

[271] http://www.hejtstop.pl/, dostęp: [28.01.2016 r.]

[272] *M. Bilewicz, M. Marchlewska, W. Soral, M. Winiewski,* Mowa nienawiści. Raport z badań sondażowych, Warszawa 2014, s. 4-7.

[273] *E. Junczyk-Ziomecka [w:] R. Wieruszewski, M. Wieruszewski, A. Bodnar, A. Gliszczyńska-Grabias,* Mowa nienawiści a wolność słowa. Aspekty prawne i społeczne, Warszawa 2010, s.17-18.

Anna Panek

Odpowiedzialność prawna za naruszenie ochrony danych osobowych z uwzględnieniem środków prawnych przewidzianych w RODO

1. Wstęp

Postęp gospodarczy i rozwój nowych technologii oraz związane z nimi przetwarzanie danych coraz szerszego grona osób niosą ze sobą ryzyko utraty kontroli nad zasobami informacji prywatnych, stąd niezbędna jest ich jak najlepsza ochrona. Najwłaściwszą z nich wydaje się być ochrona prawna w postaci podjęcia stałej i zorganizowanej działalności z użyciem określonych środków prawnych w celu zabezpieczenia interesu danego podmiotu.

2. Pojęcie danych osobowych

Treść artykułu 6 Ustawy o ochronie danych osobowych, dalej u.o.d.o, definiuje pojęcie danych osobowych jako wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[274]. Można więc zauważyć, że ustawodawca określił tym mianem nie tylko informacje służące samej identyfikacji, ale również te konkretyzujące tożsamość określonej osoby. Obowiązujące na terenie RP przepisy odnoszą się tak do polskich obywateli, jak i do cudzoziemców. Dla zakwalifikowania pewnych informacji jako dane osobowe nie ma znaczenia kwestia posiadania praw publicznych czy zdolności do czynności prawnych, ani status prawny i wspomniane w zdaniu poprzednim – obywatelstwo[275]. Szczególne znaczenie tych danych przekłada się na konieczność ich wyjątkowo szeroko zakrojonej ochrony. Jej źródła odnaleźć można wśród polskich, europejskich i międzynarodowych aktów prawnych.

3. Źródła prawa ochrony zdrowia

3.1. Przepisy konstytucyjne

[274] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133 poz. 883 z późn. zm.).
[275] J.Barta, P.Fajgielski, R.Markiewicz: Ochrona danych osobowych. Komentarz, Warszawa 2015, s.305.

Temat ochrony danych osobowych okazał się na tyle istotnym, iż jego uregulowania dokonano już w Konstytucji RP. Ta w sposób generalny i abstrakcyjny wyraża gwarancje poszanowania prywatności oraz normuje kwestie związane z gromadzeniem, udostępnianiem i przetwarzaniem danych osobowych. Artykuł 47 zapewnia każdemu prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowania o własnym życiu osobistym. Prywatność nie zawęża się jedynie do autonomii informacyjnej jednostki, lecz odnosi się także do instytucji małżeństwa, bowiem treść art. 47 odnosi się także do „trwałości rodziny i małżeństwa", „wolności jego zawarcia" czy „wolności wyboru małżonka"[276]. Bezpośrednim wyrazem ustanowienia prawa do ochrony danych osobowych jest artykuł 51, który w ust. 1 gwarantuje, iż nikt nie może być obowiązany do ujawniania informacji dotyczących jego osoby w inny sposób niż na podstawie ustawy. W ust. 2 ustawodawca dokonuje wyłączenia działań władz publicznych w sferze pozyskiwania, gromadzenia i udostępniania informacji o obywatelach. Owe wyłączenie nie dotyczy jednak informacji niezbędnych w demokratycznym państwie prawnym. Ust. 3 deklaruje dostęp do urzędowych dokumentów i zbiorów danych osób, których dotyczą, chyba że ustawa takie prawo ograniczy. Treść kolejnego ustępu formułuje prawo do żądania sprostowania i usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Ostatni ustęp jest przepisem odsyłającym do ustawy, która w sposób szczegółowy reguluje zasady i tryb gromadzenia i udostępnienia informacji. W obecnym porządku prawnym takim aktem jest u.o.d.o.

3.2. Ustawa o ochronie danych osobowych

Wspominana wyżej ustawa kompleksowo normuje kwestie danych osobowych, jak również ich ochrony i przetwarzania o charakterze profesjonalnym, doraźnym czy incydentalnym[277]. Na mocy u.o.d.o. ustanowiony został Generalny Inspektor Ochrony Danych Osobowych, dalej GIODO. Ponadto ustawa określa procedurę jego powołania i odwołania a także formułuje zadania oraz kompetencje. Przedmiotem regulacji są również uprawnienia i obowiązki osoby, której przetwarzane dane dotyczą oraz sposoby ich wykonywania. U.o.d.o. zawiera katalog przepisów prawnokarnych, wskazując sześć typów czynów zabronionych nieujętych w polskim kodeksie karnym[278]. Reasumując, należy podkreślić, iż omawiana ustawa wnikliwie reguluje prawo do ochrony danych osobowych, realizując tym samym postanowienia konstytucyjne.

Do polskich źródeł normujących tematykę niniejszej pracy zaliczyć trzeba również liczne przepisy wykonawcze wydawane na podstawie u.o.d.o. Większość z rozporządzeń dookreśla kwestie związane z GIODO i administratorem bezpieczeństwa informacji. Postanowienia wszystkich dotychczas wymienionych aktów prawnych można nazwać przepisami o ochronie danych osobowych sensu stricte. Miano przepisów sensu largo można

[276] M.Wild: Ochrona prywatności w prawie cywilnym (Koncepcja sfer a prawo podmiotowe), PiP 2001, nr 4, s.55.
[277] T.Banyś, E.Bielak-Jomaa, M.Kuba, J.Łuczak: Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków, 2016, s.19.
[278] Tamże.

przyznać unormowaniom odrębnym, rozproszonym wśród wielu ustaw zawierających przepisy materialne i proceduralne regulujące omawianą materię[279].

3.3. Przepisy prawa międzynarodowego

Istotnym aktem prawnym o zakresie międzynarodowym jest Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Zwięźle, aczkolwiek konkretnie wyraża najważniejsze aspekty prawa do ochrony danych. Jest wyrazem współpracy międzynarodowej państw będących jej stronami w zakresie poruszanej problematyki.

Do tej pory niezwykle ważna dla europejskiego porządku prawnego była dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/WE). Jednakże wraz z wejściem w życie Rozporządzenia PE i Rady z dnia 27 kwietnia 2016 r. (2016/679) zostanie ona uchylona ze skutkiem od dnia 25 maja 2018 r. Rozporządzenie, o którym mowa w zdaniu poprzednim zostanie szerzej omówione w dalszej części niniejszej publikacji. Pochylając się nad tematem unijnego prawa ochrony danych osobowych, nie sposób nie wymienić pozycji takich jak artykuł 8 Karty praw podstawowych Unii Europejskiej czy artykuł 16 Traktatu o funkcjonowaniu Unii Europejskiej regulujących zasady ochrony i tryb przetwarzania takich informacji.

Mimo szerokiego unormowania materii danych osobowych zarówno w porządku krajowym, jak i międzynarodowym oraz ciągłej pracy nad udoskonalaniem spraw z tym związanych, wciąż dochodzi do naruszeń praw ochrony danych i poszanowania prywatności. Za takie naruszenia prawodawca przewiduje określone sankcje. Pod uwagę zostaną wzięte kwestie odpowiedzialności karnej i cywilnej w związku z przekroczeniem prawa ochrony danych osobowych.

4. Odpowiedzialność z tytułu naruszenia prawa ochrony danych osobowych

4.1. Odpowiedzialność karna

Rozdział VIII u.o.d.o zatytułowany „Przepisy karne" jest katalogiem sześciu typów czynów zabronionych, które mogą zostać popełnione bezpośrednio z powodu nieprawidłowości związanych z administrowaniem i przetwarzaniem danych. Wszystkie z nich ścigane są z urzędu[280]. Podstawowym źródłem procedury ścigania sprawców będzie Kodeks postępowania karnego. Przestępstwo z artykułu 49 u.o.d.o. może być popełnione w dwóch wariantach:

[279] G.Sibiga: Postępowanie w sprawach ochrony danych osobowych, Warszawa 2003, s.27.
[280] A.Drozd: Zabezpieczenie danych osobowych, Wrocław 2008, s.96.

1) gdy przetwarzanie danych jest niedopuszczalne;
2) gdy przetwarzania danych dokonuje osoba nieuprawniona do takiego działania.

Fraza „nie jest dopuszczalna" odnosi się do znamion przedmiotowych czynu, natomiast kwalifikacji podmiotowych sprawcy dotyczy określenie „nie jest uprawniony"[281]. Czyn zabroniony ma charakter powszechny, ponieważ popełniony może zostać przez każdy podmiot podlegający odpowiedzialności karnej. Niedopuszczalne przetwarzanie danych to takie, które jest niezgodne z u.o.d.o., w szczególności, gdy podmiot przetwarzający nie legitymuje się żadną z przesłanek wyłączających zakaz z art.23 i 27 lub czyni to mimo zgłoszenia sprzeciwu na podstawie art. 32 ust. 1 pkt. 8[282]. Jeżeli chodzi o przetwarzanie tzw. danych wrażliwych, to w artykule 49 ust. 2 ustawodawca zaostrza karę za nieprawne działanie z użyciem takich informacji, podnosząc górną granicę kary pozbawienia wolności do lat 3. Artykuł 49 ust. 2 wyraźnie określa rodzaj takich danych. To takie związane z:

-pochodzeniem rasowym lub etnicznym,
-poglądami politycznymi,
-przekonaniami religijnymi lub filozoficznymi,
-przynależnością wyznaniową, partyjną lub związkową,
-stanem zdrowia,
-kodem genetycznym,
-nałogami,
-życiem seksualnym.

Artykuł 51 u.o.d.o. reguluje materię czynu zabronionego związanego z nieprawnym udostępnianiem przetwarzanych danych osobowych. Przedmiotem ochrony jest tutaj poufność danych zgodna z zasadą celowości i bezpieczeństwa danych[283]. Odpowiedzialność karna wynika więc z zamachu na to prawnie chronione dobro. Podmiotem przestępstwa może być administrujący zbiorem danych oraz osoba obowiązana do ochrony danych osobowych. Administrator zbiorów danych na gruncie u.o.d.o. to w ocenie Sądu Najwyższego jedynie ten podmiot, który decyduje o celach i środkach przetwarzania tych danych (art. 7 pkt 4), natomiast pod pojęciem „administrujący zbiorem danych" należy rozumieć również taki podmiot, który zarządza, zawiaduje zbiorem danych (art. 50, 51, 54) lub danymi (art. 52) w toku ich przetwarzania, w tym powierzonego mu w trybie przewidzianym w art. 31[284]. SN dokonuje rozróżnienia pod względem pojęciowym, a także pod względem ewentualnej odpowiedzialności karnej, bowiem administrujący nie będący administratorem danych odpowiada prawnie w wypadku, gdy jego zachowanie uznane jest przez ustawę za karalne i wynika z powierzonych mu czynności przetwarzania[285]. Ustawodawca wprowadził sankcje za występek, biorąc pod uwagę możliwość jego popełnienia tak umyślnego, jak i nieumyślnego. Jeżeli sprawca działał umyślnie, to podlega karze grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. W przypadku nieumyślnego spowodowania skutków z art. 51

[281] I.Zgoliński, I.Zduński: Praktyczny komentarz do ustawy o ochronie danych osobowych, Bydgoszcz 2013, s.194.
[282] Tamże.
[283] I.Zgoliński, I.Zduński: Praktyczny komentarz …, Bydgoszcz 2013, s.196.
[284] Postanowienie SN z dnia 11 grudnia 2000 r. II KKN 438/2000, OSNKW 2001, nr 3-4, poz.33.
[285] J.Barta, P.Fajgielski, R.Markiewicz: Ochrona danych…, Warszawa 2007, s.671-672.

ust. 1 u.o.d.o. sprawca podlegać będzie karze grzywny, ograniczenia wolności albo pozbawienia wolności do roku.

Nieistotna natomiast z prawnego punktu widzenia jest kwestia umyślności popełnienia czynu zabronionego z art. 52, bowiem jest on zagrożony grzywną, karą ograniczenia wolności albo pozbawienia wolności do roku, choćby odpowiedzialny za naruszenie działał nieumyślnie. Jest to przykład tzw. hybrydalnej formy winy[286]. Zakres podmiotowy przepisu obejmuje każdą osobę, na której ciąży obowiązek zabezpieczenia danych osobowych przed zabraniem przez osobę nieuprawioną, uszkodzeniem czy zniszczeniem takich danych. O tym, czy określony podmiot takowy obowiązek posiadał rozstrzygać mogą w pierwszej kolejności regulacje związane z podstawami jego zatrudnienia[287]. Przedmiotem występku są dane osobowe, nie jest więc konieczne, by tworzyły one jakiś zbiór danych[288]. Sprawca dokonuje zamachu na atrybuty bezpieczeństwa takie jak rozliczalność i integralność danych[289].

W przepisie kolejnym odniesiono się do obowiązku zgłaszania zbioru do rejestracji. Kto nie wykonuje tej powinności, mimo, że jest do tego obowiązany, podlega karze grzywny, ograniczenia wolności albo pozbawienia wolności do roku. Strona przedmiotowa przestępstwa polega na zaniechaniu sprawcy zgłoszenia zbioru do rejestracji. Przepis ma chronić integralność tego typu zbiorów[290].

Moment popełnienia występku z artykułu 54 u.o.d.o. następuje wówczas, gdy upłynie termin na spełnienie spoczywającego na administrującym obowiązku polegającym na poinformowania osoby, której dane będą przetwarzane oraz pouczenie jej o przysługujących prawach i sposobach korzystania z uprawnień ustawowo nadanych. Chronionym przez normę prawną dobrem jest prawo do kontroli danych osobowych oraz obowiązek administratora poinformowania zainteresowanego o posiadaniu danych i wynikających z tego faktu przysługujących uprawnień[291]. Dla uniknięcia odpowiedzialności wystarczy skierowanie zgłoszenia do GIODO[292].

Artykuł 54a dodany nowelą z dnia 29 października 2010 r. reguluje materię przestępstwa powszechnego polegającego na udaremnianiu lub utrudnianiu czynności kontrolnej przeprowadzanej przez inspektora biura GIODO. Udaremnienie może mieć postać uniemożliwienia lub niedopuszczania do przeprowadzenia czynności. Utrudnianie natomiast może przejawiać się stwarzaniem przeszkód zaburzających prawidłowy tok procesu kontroli[293]. Przy interpretacji użytych w ustawie pojęć można odwołać się do dorobku doktryny prawa karnego, wypracowanego na podstawie analizy art. 255 Kodeksu karnego[294], bowiem w tym przepisie ustawodawca również posługuje się wspomnianymi terminami[295]. Celem wprowadzenia omawianego przepisu jest przede wszystkim ochrona legalnej, niczym

[286] D. Żak: Ochrona danych osobowych, Stalowa Wola 20121, s.110.
[287] A.Drozd: Zabezpieczenie…, Wrocław 2008, s. 98.
[288] Tamże.
[289] M.Polok: Bezpieczeństwo danych osobowych. Zarys prawa, 2008, s. 295.
[290] I.Zgoliński, I.Zduński: Praktyczny komentarz …, Bydgoszcz 2013, s. 198.
[291] M.Polok: Bezpieczeństwo…, 2008, s.296.
[292] T.Szewc: Publicznoprawna ochrona informacji, Warszawa 2007, s. 107.
[293] I.Zgoliński, I.Zduński: Praktyczny komentarz …, Bydgoszcz 2013, s. 200.
[294] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.).
[295] J.Barta, P.Fajgielski, R.Markiewicz: Ochrona danych…, Warszawa 2015, s.647.

niezakłóconej kontroli przeprowadzanej przez inspektora biura GIODO[296]. Występek zagrożony jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2.

4.2. Odpowiedzialność cywilna

O ile odpowiedzialność karna stała się przedmiotem działań prawodawcy przy tworzeniu ustawy o ochronie danych osobowych, o tyle zaniechał on regulacji związanych z odpowiedzialnością cywilną, pozostawiając tym samym dochodzenie roszczeń na podstawie przepisów Kodeksu cywilnego. W tym zakresie istotne będą przede wszystkim postanowienia Księgi I (części ogólnej) i Księgi III (zobowiązania). Wśród naruszeń prawa ochrony danych osobowych na gruncie prawa cywilnego najczęściej będzie chodziło o odpowiedzialność odszkodowawczą. Do możliwości zaistnienia, a następnie dochodzenia roszczeń z tego tytułu wymagane jest spełnienie trzech podanych przesłanek:
-powstanie szkody,
-zaistnienie określonego zdarzenia, które skutkuje powstaniem odpowiedzialności, jeżeli ustawa tak stanowi
-występowanie adekwatnego związku przyczynowego pomiędzy tym zdarzeniem a szkodą[297].
Kwestie odpowiedzialności *ex delicto*, czyli za czyn niedozwolony, wyznaczają artykuły Tytułu VI Księgi III Kodeksu Cywilnego. Podmiotem obciążonym takową odpowiedzialnością mogą być zarówno osoby fizyczne, jak i osoby prawne oraz jednostki organizacyjne uregulowane w art. 33^1 kc[298]. Pierwszoplanowy charakter będzie miał artykuł 415, który stanowi podstawę odpowiedzialności deliktowej i w sposób ogólny wyznacza jej zakres. Zobowiązuje on do naprawienia szkody tego, który wyrządził ją drugiemu z własnej winy[299]. Za uznaniem czynu za niedozwolony muszą przemawiać dwie przesłanki – jego bezprawność oraz wina, przy czym konieczne jest, by jako pierwsze ustalone zostało zaistnienie bezprawnego działania lub zaniechania, gdyż dopiero wtedy można rozważać wystąpienie winy[300]. Pojęcie „bezprawność" jest przedmiotem sporów w doktrynie. Jednakże przeważającym poglądem jest uznanie, że jest to sprzeczność z prawem i zasadami współżycia społecznego[301]. Termin „wina" również nie ma swojej ustawowej definicji. Dominuje teoria normatywna zakładająca, iż oznacza możność postawienia określonej osobie zarzutu, że nie zachowała się prawidłowo, to znaczy zgodnie z prawem i zasadami współżycia społecznego. Ważnym przepisem związanym z odpowiedzialnością deliktową jest także art. 439. Ma on istotne znaczenie w praktyce wykonywania prawa do ochrony danych osobowych[302]. Przepis stanowi, że temu, komu wskutek zachowania się innej osoby, zagraża bezpośrednio szkoda, przysługuje uprawnienie do żądania, by taka osoba przedsięwzięła środki

[296] I.Zgoliński, I.Zduński: Praktyczny komentarz …, Bydgoszcz 2013, s.200.
[297] T.Banyś, E.Bielak-Jomaa, M.Kuba, J.Łuczak: Prawo ochrony danych…, 2016, s.163.
[298] Kodeks cywilny. Komentarz, Jerzy Ciszewski (red.), Warszawa 2014, s. 694.
[299] T.Banyś, E.Bielak-Jomaa, M.Kuba, J.Łuczak: Prawo ochrony danych…, 2016, s.164.
[300] Kodeks cywilny. Komentarz, Jerzy Ciszewski (red.), Warszawa 2014, s. 697.
[301] Tamże.
[302] J.Barta, P.Fajgielski, R.Markiewicz: Ochrona danych…, Warszawa 2015, s.279.

niezbędne do odwrócenia grożącego niebezpieczeństwa, a jeżeli jest taka potrzeba, to również do tego, by dała odpowiednie zabezpieczenie. Sporne pozostaje określenie, czy dla wystąpienia z roszczeniem konieczne jest urzeczywistnienie przesłanek odpowiedzialności, czy wystarczające okażą się te dotyczące bezprawności zachowania grożącego powstaniem szkody[303]. Szczególny charakter prawa o ochronie danych osobowych mógłby skłaniać do uznania poglądu drugiego, jednakże pierwszy z nich jest na tyle rozpowszechnionym w doktrynie i orzecznictwie, iż kwestie niejednolitego podejścia do problemu mogą wzbudzać kontrowersje[304].

Naruszenie dóbr osobistych w związku z przetwarzaniem danych osobowych może stanowić podstawę dochodzenia roszczeń cywilnych. Wówczas zastosowanie będą miały artykuły 24 i 448 kc. Przepis pierwszy będzie przyznawać temu, czyje dobro osobiste zostaje zagrożone cudzym działaniem, legitymację do żądania zaniechania takiego postępowania. Norma nie będzie miała zastosowania w sytuacji, gdy takie działanie nie będzie bezprawne. Roszczenie o zaniechanie trwa do chwili faktycznego naruszenia dobra osobistego. W wypadku takiego naruszenia pokrzywdzony może domagać się usunięcia skutków wynikłych z pogwałcenia jego prawa[305]. Inaczej niż w przypadku odpowiedzialności deliktowej wygląda stosunek bezprawności do winy. Jeżeli chodzi o art. 24 nie wymaga się zawinienia. Należy więc przede wszystkim wykazać bezprawność działania naruszającego dobro osobiste[306]. Zgodnie z orzeczeniem Sądu Najwyższego z dnia 19 października 1989 r. pojęcie „działanie bezprawne" należy rozumieć jako każde działanie naruszające dobro osobiste, jeżeli nie zachodzi żadna ze szczególnych okoliczności usprawiedliwiająca je[307]. Na gruncie polskiego prawa przesłankami dla takiego usprawiedliwienia będą:

-zgoda uprawnionego,

-działanie na podstawie przepisu prawnego[308].

Artykuł 448 wprowadza zadośćuczynienie pieniężne za doznaną krzywdę w razie naruszenia dobra osobistego. Sąd może przyznać takowe niezależnie od innych środków niezbędnych do usunięcia skutków naruszenia[309]. Przedstawiciele doktryny prawa cywilnego precyzując cel zadośćuczynienia, wyjaśniają, iż chodzi o złagodzenie doznanych ujemnych konsekwencji, a nie stricte rekompensatę[310].

Podmiot, którego prawa do ochrony danych osobowych zostały naruszone może dochodzić roszczeń z tytułu niewykonania lub nienależytego wykonania umowy (art. 471 i następne). Jest to przykład odpowiedzialności kontraktowej dotyczącej zobowiązań pomiędzy wierzycielem i dłużnikiem. Dotyczy jedynie szkód majątkowych[311].

---

[303] Kodeks cywilny. Komentarz, E.Gniewek, P.Machnikowski (red.), Warszawa 2013, s.812.
[304] T.Banyś, E.Bielak-Jomaa, M.Kuba, J.Łuczak: Prawo ochrony danych…, 2016, s.165.
[305] T.Banyś, E.Bielak-Jomaa, M.Kuba, J.Łuczak: Prawo ochrony danych…, 2016, s.166.
[306] M. Matysiak: Odpowiedzialność cywilna z tytułu bezprawnego przetwarzania danych [w:] Prawna ochrona danych osobowych w Polsce na tle europejskich standardów, G.Goździewicz, M.Szabłowska (red.), Toruń 2008, s.304.
[307] Wyrok SN z dnia 19 października 1989 r., II CR 419/89, OSP 1990, nr 11-12, poz.377.
[308] M. Matysiak: Odpowiedzialność cywilna… [w:] Prawna ochrona…, G.Goździewicz, M.Szabłowska (red.), Toruń 2008, s.304.
[309] T.Banyś, E.Bielak-Jomaa, M.Kuba, J.Łuczak: Prawo ochrony danych…, 2016, s.167.
[310] M. Matysiak: Odpowiedzialność cywilna… [w:] Prawna ochrona…, G.Goździewicz, M.Szabłowska (red.), Toruń 2008, s.305.
[311] Kodeks cywilny. Komentarz, Jerzy Ciszewski (red.), Warszawa 2014, s. 825.

5. Wpływ rozporządzenia ogólnego o ochronie danych osób fizycznych na Polską ustawę o ochronie danych osobowych

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE to krok milowy w stronę jeszcze lepszej i bardziej skutecznej działalności związanej z tą materią. Jego postanowienia będą stosowane od dnia 25 maja 2018 r. Celem rozporządzenia ogólnego jest konieczność zapewnienia w państwach członkowskich równorzędnego uprawnienia w zakresie sprawowania kontroli i nadzoru nad utrzymywaniem odpowiedniego poziomu ochrony danych osobowych oraz wprowadzenie jednakowego egzekwowania przepisów dotyczących tej materii[312]. Znajomość przepisów RODO jest bardzo istotna, szczególnie na gruncie polskiego prawa, ze względu na fakt, iż w naszym porządku prawnym rozporządzenie będzie miało pierwszeństwo w stosowaniu wobec ustawodawstwa krajowego[313].

Treść RODO normuje również kwestie związane ze środkami ochrony prawnej. Poza przyznaniem organowi nadzorczemu kompetencji do nakładania administracyjnych kar pieniężnych ustawodawca uregulował następujące prawa:
-do wniesienia skargi do organu nadzorczego;
-do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu oraz przeciwko administratorowi lub podmiotowi przetwarzającemu;
-do odszkodowania za poniesioną szkodę w wyniku naruszenia przepisów RODO[314].

Prawo do wniesienia skargi do organu nadzorczego uregulowane w art. 77 RODO to instytucja znana także przepisom u.o.d.o., bowiem artykuł 18 tejże ustawy daje ku temu podstawy prawne. GIODO po przeprowadzeniu postępowania wyjaśniającego w oparciu o zebrane informacje podejmuje z urzędu autonomiczną decyzję w sprawie skorzystania z uprawnień przyznanych mu na mocy art. 12 pkt 5, art. 17, a także art. 19 u.o.d.o. GIODO w drodze decyzji administracyjnej nakazuje przywrócenie stanu zgodnego z prawem[315]. Organ nadzorczy może również wnieść o wszczęcie postępowania dyscyplinarnego czy innego przewidzianego prawem przeciwko osobom, które dopuściły się naruszenia ochrony danych osobowych w procesie ich przetwarzania albo może zawiadomić odpowiedni organ ścigania o podejrzeniu popełnienia przestępstwa[316]. Po 25 maja 2018 r. osoba upoważniona do wniesienia takiej skargi będzie mogła zadecydować, według jakiej właściwości miejscowej złoży skargę, bowiem do wyboru, w szczególności w państwie członkowskim, będzie miała następujące warianty:

[312] A.Dmochowska, M.Zadrożny: Unijna reforma ochrony danych osobowych. Analiza zmian, Warszawa 2016, s.153.
[313] D.Wocióra: Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego, Warszawa 2016, s.XXIX.
[314] A.Dmochowska, M.Zadrożny: Unijna reforma…, Warszawa 2016, s.154.
[315] A.Dmochowska, M.Zadrożny: Unijna reforma…, Warszawa 2016, s.154.
[316] A.Dmochowska, M.Zadrożny: Unijna reforma…, Warszawa 2016, s.155.

-właściwość swojego zwykłego pobytu,
-właściwość swojego miejsca pracy,
-właściwość miejsca popełnienia domniemanego naruszenia[317].

Do złożenia skargi do organu nadzorczego wystarczające jest samo przekonanie osoby, której dane dotyczą, o naruszeniu postanowień RODO. Obowiązkiem organu nadzorczego, wynikającym z art. 78 będzie poinformowanie skarżącego o postępach i efektach postępowania oraz pouczenia go o przysługującym mu uprawnieniu do skutecznego środka ochrony prawnej przed sądem przeciwko temu organowi.

Uprawnieniem przysługującym osobom fizycznym jest także prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu, wyrażone w art. 78 RODO. Możliwość wniesienia odwołania do sądu od decyzji organu administracyjnego stanowi jeden z elementów fundamentalnej zasady demokratycznego państwa prawa. Standardy owej zasady pełnią nadrzędną rolę wśród podstaw funkcjonowania Unii Europejskiej, stąd też uregulowanie tej kwestii w RODO wydaje się w pełni uzasadnione. Samo rozporządzenie nie rozstrzyga o tym, do jakiego sądu należy skierować odwołanie. Ma to związek ze zróżnicowaniem strukturalnym sądownictwa w poszczególnych państwach członkowskich. Ustawodawca unijny ograniczył się wyłącznie do wskazania, iż sądem właściwym będzie sąd na terenie państwa, w którym mieści się siedziba organu nadzorczego.
Co do sytuacji polskiej – kwestia ta będzie zależna od tego, jak uregulowany zostanie status prawny GIODO. Obecnie, jest to organ administracyjny, zatem kierowane do niego skargi wszczynają postępowanie administracyjne. Przy okazji wejścia w życie RODO pojawiają się postulaty o zmianę pozycji GIODO i nadanie mu bardziej „rzecznikowskiego" charakteru, podobnie jak UOKiK. Wówczas, GIODO nie byłby zobligowany do wszczęcia postępowania w razie wpłynięcia skargi, zostając wyposażonym w możliwość weryfikacji jej zasadności. Ze strony przedsiębiorców (w związku z obawami o kary finansowe) pojawiają się głosy w sprawie możliwości odwołania od decyzji GIODO do sądów cywilnych, co jednak wiązałoby się z koniecznością tworzenia dodatkowej, odrębnej od istniejących, procedury. Opinie na temat właściwości sądów są podzielone, podobnie jak ma to miejsce w dyskusji nad administracyjno-sądową procedurą kontroli decyzji Prezesa UOKiK. W przypadku GIODO, właściwszym wydaje się jednak skierowanie uwagi w stronę sądownictwa administracyjnego. Nie tylko czyniłoby to większym stopniu za dość założeniom Konstytucji RP w kwestii rozdzielenia kompetencji orzeczniczych sądów administracyjnych oraz powszechnych, ale także unikałoby rozbieżności proceduralnych – wynikających chociażby z faktu, iż postępowanie administracyjne oparte jest na zasadzie prawdy obiektywnej, a cywilne na zasadzie kontradyktoryjności[318].
W art. 79 RODO przyznane zostało analogiczne uprawnienie przeciwko administratorowi lub podmiotowi przetwarzającemu.
RODO dopuszcza możliwość reprezentowania osób, których dane dotyczą przez określone w art. 80 podmioty. Umocowanie obejmuje samo wniesienie skargi, jak również wykonywanie w imieniu mocodawcy innych praw, przewidzianych w art. 78 i 79 – podmiot, organizacja lub zrzeszenie, niemające charakteru zarobkowego, a realizujące cele statutowe, które leżą w

[317] Tamże.
[318] Tamże.

interesie publicznym oraz działające w sprawie ochrony praw i wolności innych osób. Poza umocowaniem osobistym ze strony osoby, której dane dotyczą, upoważnienie do podjęcia działań w problematycznej materii może także nastąpić z inicjatywy samych podmiotów – o ile rozwiązanie takie zostanie przewidziane w państwie członkowskim. Kompetencja im przyznana ma zastosowanie wtedy, gdy naruszone zostaną prawa osoby, której dane dotyczą[319].

Wraz z wejściem w życie nowych przepisów pojawia się wyjście naprzeciw prawom osób, których dane dotyczą – w stosunku do u.o.d.o. Mowa o prawie do odszkodowania w razie naruszenia dla osoby, której dane dotyczą. Każda osoba, która poniosła szkodę w wyniku niezgodnego z RODO przetwarzania danych, ma prawo uzyskać z tego tytułu odszkodowanie od administratora lub podmiotu przetwarzającego. W przypadku administratora odpowiedzialność obejmuje wszelkie szkody wynikające z niezgodnego z prawem przetwarzania danych, z kolei, jeżeli chodzi o podmiot przetwarzający, to będzie on odpowiadał za szkody tylko wówczas, gdy nie dopełnił obowiązków nałożonych na niego bezpośrednio przepisami RODO lub gdy działał poza zgodnymi z przepisami instrukcjami administratora albo wbrew nim. Wykazanie przez administratora lub podmiot przetwarzający braku winy z zdarzenie, które spowodowało szkodę jest przesłanką do uwolnienia się przez nich od odpowiedzialności. W sytuacji, gdy odpowiedzialnych jest kilka podmiotów jednocześnie, odpowiadają oni solidarnie. Administratorowi lub podmiotowi przetwarzającemu, który wypłacił poszkodowanemu pełną kwotę odszkodowania przysługuje roszczenie regresowe względem reszty zobowiązanych.

Postępowanie sądowe w sprawie odszkodowania wszczynane jest przed sądem właściwym według przepisów prawa państwa członkowskiego[320].

6. Zakończenie

Niewątpliwie prawo do ochrony danych osobowych należy do grupy praw szczególnych. Szeroko pojęta informatyzacja, a co za tym idzie zwiększenie ilości przetwarzanych danych, zwiększa ryzyko naruszenia dóbr osobistych. Wymusza to na ustawodawcy podejmowanie takich rozwiązań prawnych, które w jak największym stopniu zabezpieczałyby poufne informacje. Skuteczna ochrona wiąże się również z odpowiednim systemem kontroli i nadzoru, a także z ustanowieniem takich środków prawnych, które pozwolą na pociągnięcie do odpowiedzialności osób naruszających prawa drugiego.

[319] Tamże.

[320] D.Wocióra: Ochrona danych osobowych…, Warszawa 2016, s.36-37.

mgr Anna Pyka

Monitoring – problematyka funkcjonowania w Polsce

1. Wstęp

Zastanawiając się nad rozwojem życia społecznego i gospodarczego w XXI wieku, można jednoznacznie stwierdzić, że jedną z najprężniej rozwijających się dziedzin życia w ostatnich latach jest rozwój nowych technologii. Z dnia na dzień koncerny prześcigają się w tworzeniu co raz to nowszych urządzeń technologicznych mających na celu poprawę i wzbogacenie naszego życia. Na tle ogromnego rozwoju pojawiają się jednocześnie nowe aspekty prawne, wymagające niekiedy szczegółowej interpretacji a często również wprowadzenia zupełnie nowych unormowań. Niewątpliwie kwestię istotną i nierozwiązaną do dnia dzisiejszego, jest kwestia monitoringu. Jesteśmy przyzwyczajeni, że wchodząc do różnych obiektów, jeżdżąc komunikacją miejską, spacerując po parku czy ulicach miasta napotykamy kamery, nie zważając tak naprawdę kto nas obserwuje za ich pośrednictwem, co z takimi nagraniami się dzieje i czemu szczegółowo mają służyć.

Pod ogólnym pojęciem „monitoringu" kryją się urządzenia rejestrujące obraz, czyli kamery CCTV[321] oznaczają telewizję zamkniętego obiegu – określenie na tradycyjne, analogowe systemy monitoringu wizyjnego. Systemy CCTV składają się z kamer oraz rejestratorów obrazu, połączonych ze sobą funkcjonalnie za pomocą przewodów lub bezprzewodowo. Synonimem do anglojęzycznego terminu CCTV są: monitoring video [monitoring wizyjny] oraz telewizja przemysłowa. Aby mieć możliwość prowadzenia skutecznej obserwacji system telewizji przemysłowej powinien być wyposażony w kamery CCTV o odpowiednich parametrach, dobranych do danego planu obserwacyjnego, rodzaju oraz intensywności oświetlenia i innych warunków środowiskowych.

W niniejszym artykule przybliżona zostanie problematyka formalnoprawna prawa do prywatności, jak również zagrożenia wynikające z braku ustawy kompleksowo traktującej o monitoringu.

2. Monitoring a prywatność

Marek Safjan sformułował tezę zgodnie z którą „prywatność ma podlegać ochronie właśnie dlatego i tylko dlatego, że przyznaje się każdej osobie prawo do wyłącznej kontroli tej sfery życia, która nie dotyczy innych, a w której wolność od ciekawości innych jest swoistą conditio

[321] Skrót od ang. Closed Circuit Television.

sine qua non swobodnego rozwoju jednostki”[322]. Istnieje wiele koncepcji traktujących o prywatności, jednakże ze względu na jej płynne granice nie jest możliwe skonstruowanie jednej definicji prywatności. Szczególnie jest to utrudnione ze względu na wspomniany, utrzymujący się w XXI rozwój technologiczny, co raz to nowe innowacje tworzone w celu ułatwienia życia jego odbiorcom z jednej strony, kosztem ograniczenia ich prywatności, zbierania o nich danych i przetwarzania ich dla zróżnicowanych celów. Co w takim razie z naszą prywatnością – jak się kształtuje i jaki jest jej stosunek do czynników zewnętrznych na nią wpływających? Prywatność można określić jako sferę osobistą człowieka, sferę indywidualności, która jest wolna od ingerencji innych osób i jako taka podlega ochronie. Ramy prawne ochrony prywatności można rozpatrywać na czterech szczeblach: krajowym systemie prawnym, prawie europejskim, prawie międzynarodowego oraz kodeksach dobrych praktyk i kodeksach etyki zawodowej[323]. Aktualnie dąży się do ujednolicenia prawodawstw państw członkowskich Unii Europejskiej zarówno gdy chodzi o przesłanki ochrony prywatności jak i wyjątki od niej.

W Polsce prawo do prywatności sformalizowane zostało dopiero wraz z uchwaleniem Konstytucji RP w 1997 r[324]., stanowiąc w art. 47, iż „każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”. Prawo sformułowane w art. 47 ma bezpośredni związek zaś z art. 51 ust. 1 Konstytucji „nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.” Oprócz wspomnianego art. 47, kolejne artykuły dotyczące wolności i ochrony tajemnicy komunikowania się, nienaruszalności mieszkania czy wolności wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji stanowią niejako konkretyzację prawa do prywatności[325]. Regulacje dotyczące prywatności funkcjonują w układzie wertykalnym państwo-jednostka[326], gdzie z jednej strony zabrania się ingerencji państwa w ustalony prawnie zakres życia człowieka, zaś w przypadku naruszenia tej sfery nakazuje państwu zapewnić ochronę jednostce[327]. W literaturze można wyróżnić dwa aspekty podejścia do prawa do prywatności. Pierwsze akcentuje konieczność zwiększenia form i zakresu poziomu ochrony prywatności. Wynika to przede wszystkim z liberalnego poglądu, że istnieje różnie definiowana sfera życia niepodlegająca kontroli ze strony państwa oraz innych osób. Drugie podejście pragnie ograniczyć sferę prywatności, uzasadniając to działalnością wyspecjalizowanych instytucji państwowych, zwalczających zagrożenia wymierzone w bezpieczeństwo społeczeństwa i całego państwa[328]. Nie inaczej jest w przypadku monitoringu. Człowiek ze swej natury ma potrzebę zachowania pewnych spraw dla siebie, zachowania pewnej autonomii, osobistej przestrzeni czy anonimowości, podczas gdy

[322] M. Safjan, *Prawo do ochrony życia prywatnego* (w:) *Podstawowe prawa jednostki i ich ochrona*, pod red. L. Wiśniewskiego, Warszawa 1998, s. 128.
[323] J. van Dijk, *Społeczne aspekty nowych mediów. Analiza społeczeństwa nowych mediów*, Wydawnictwo Naukowe PWN, Warszawa 2010, s. 210.
[324] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483).
[325] J. Braciak, *Prawo do prywatności*, [w:] S. Pajączkowski, A. Preisner (red.), *Praktyczne i teoretyczne problemy współczesnego państwa. Wybrane zagadnienia*, Zeszyty Luksemburskie 1, Lublin 2012, s. 80-81.
[326] J. Braciak, *Prawo do prywatności,* Wydawnictwo Sejmowe, Warszawa 2004, s. 168.
[327] W. Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Lex 2013.
[328] J. Braciak, *Prawo do prywatności*, [w:] B. Banaszak, A. Preisner (red.), *Prawa i wolności obywatelskie w Konstytucji RP*, Warszawa 2002, s. 278.

różne podmioty mogą kontrolować to co robimy i przetwarzać te informacje innym. Niewątpliwie to w interesie jednostek jaki i całych społeczeństw jest, aby mieć kontrolę nad informacjami ich dotyczącymi. M. Ossowska wśród aspektów obrony przed zagrożeniem naruszenia prywatności wymienia m.in.: zabezpieczenie się przed obcą kontrolą, szczególnie we własnym domu czy obronę prywatności przed nieuprawnioną poufnością[329]. Gdyby zastanowić się w jakich przestrzeniach można spotkać się z zainstalowanymi kamerami CCTV, można by wymienić: osiedla mieszkaniowe, ulice, komunikację miejską, miejsca pracy, dworce, banki, centra handlowe, placówki oświaty, placówki ochrony zdrowia czy parki. Nie każdy natomiast wie, że kamery instalowane nawet w lasach. Hipotetycznie możliwym jest, że cała trasa, którą pokonuje w ciągu dnia przeciętny człowiek oraz miejsca które odwiedza, a nawet w ograniczony sposób – co w nich robi – mogą być nagrane i połączone w jedną spójną całość. Oczywiście byłoby to działanie utrudnione ze względu na fakt, że „właścicielami" kamer mogą być różne podmioty, nie tylko podmioty publiczne jak policja, staż miejska, ale i osoby prywatne jak wspólnoty i spółdzielnie mieszkaniowe, przedsiębiorcy a nawet zwykli ludzie. Można mieć poczucie, że każdy powyższy podmiot monitoruje tylko to w czym ma interes, jednakże w dzisiejszych czasach każdy może zainstalować kamerę w dowolnym miejscu i „szpiegować" innych. Brak odpowiednich regulacji bez wątpienia powoduje, że w obecnym stanie nasza prywatność jest naruszana. Każdego dnia obserwują nas dziesiątki urządzeń, o których nie mamy żadnych informacji: kto jest ich właścicielem, kto może mieć dostęp do tych nagrań ani w jakim celu jesteśmy nagrywani. Podczas gdy cele mogą być różne.

3. Monitoring a ochrona danych osobowych

Rozważając kwestię - czy fakt bycia nagrywanym może prowadzić do naruszenia prywatności nagrywanego w przypadku braku uregulowania tej kwestii, punktem wyjścia, mogą być przepisy ustawy o ochronie danych osobowych[330], bowiem w pewnych warunkach nagranie z monitoringu można uznać za zawierające dane osobowe. Danymi takimi, zgodnie z art. 6 u.o.d.o. są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, tzn. której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Numerami identyfikacyjnymi, o których mowa w komentowanym przepisie, są: numer PESEL, numer NIP, dokument tożsamości (dowód osobisty oraz paszport). Czynnikami indywidualizującymi daną osoby mogą być m.in.: cechy fizyczne, cechy fizjologiczne, cechy ekonomiczne, pochodzenie, poglądy polityczne, przekonania religijne lub filozoficzne oraz przynależność wyznaniowa, partyjna lub

[329] M. Ossowska, *Normy moralne*, PWN, Warszawa 2000, s. 107.
[330] Ustawa z dnia 03.09. 2014 r. o ochronie danych osobowych (Dz.U. 1997 nr 133, poz. 883), dalej u.o.d.o.

związkowa[331]. Wymienione elementy umożliwiające identyfikację stanowią przykład, nie wyczerpują one jednak katalogu z art. 6 u.o.d.o.

Zważając na powyższe można by rozpatrzeć sytuację, kiedy nagrywanie CCTV może naruszać prywatność nagrywanych. Samo nagranie przechodniów: niewykorzystywane w celu identyfikacji osób, nieupublicznione i nieprzekazywane w żaden sposób, o ile jest bez wątpienia swego rodzaju ograniczeniem prywatności, o tyle nie powinno co do zasady naruszać prywatności osób nagrywanych. Zakresem ochrony, wynikającym z artykułu 1 u.o.d.o. są dane osobowe. Danymi osobowymi są zaś wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Wizerunek nagrywanej osoby, sam w sobie, nie będzie prowadził do naruszenia jej prywatności ze względu na to, że w wyżej wymienionych warunkach nie prowadzi on do zidentyfikowania osoby fizycznej. Jednakże w przypadku, w którym dojdzie do jego utrwalania, przechowywania a tym bardziej wykorzystywania w określonym celu. O ile ludzi przewijających się na ulicach miast czy w komunikacji miejskiej bez uzyskania dodatkowych informacji nie sposób zidentyfikować, o tyle w przypadku monitorowania pracowników w miejscu pracy - jest to już możliwe. Podobnie będzie możliwym zidentyfikowanie osoby rezerwującej imiennie miejsce w pociągu. Kamera nakierowana na konkretne siedzenia, w połączeniu z informacją, kto dane miejsce na danym kursie zarezerwował - łącznie - tworzy bez wątpienia dane osobowe umożliwiające zidentyfikowanie osoby fizycznej.

Nagranie z monitoringu będą podlegały regulacjom u.o.d.o, gdy będzie traktowany jako zbiór danych osobowych, co będzie miało miejsce, gdy:

1) zestaw danych został poddany opracowaniu (skatalogowaniu), gdzie możliwe jest dotarcie do zapisu danych konkretnej osoby;

2) system informatyczny stosowany w związku z monitoringiem wyposażony został w mechanizmy umożliwiające automatyczne wyszukanie w zarejestrowanych nagraniach danych dotyczących konkretnej osoby, w oparciu o podane kryterium (np. mechanizm rozpoznawania kształtu twarzy, siatkówki oka, głosu);

3) dotarcie do danych konkretnej osoby jest możliwe na podstawie innego zbioru danych osobowych, w którym rejestrowane są w sposób tradycyjny zdarzenia z udziałem konkretnej osoby, zarejestrowane równocześnie w zapisie z monitoringu (np. wpisanie się listę w księdze wejść w pracy)[332].

Zgodnie z u.o.d.o., zgłoszenie zbioru do rejestracji jest obowiązkowe za wyjątkiem wskazanych przypadków zwolnienia. Wśród zwolnień nie ma monitoringu miejskiego, co oznacza, że zbiór danych osobowych powstały w związku z monitoringiem powinien zostać zgłoszony do rejestracji.

[331] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych, Komentarz, s. 346.
[332] GIODO, *Wymagania w zakresie regulacji monitoringu*, www.giodo.gov.pl/plik/id_p/2363/j/pl/, s. 28, dostęp: [15.01.2016 r.]

Wraz z uznaniem, że zapis z monitoringu, w konkretnie rozpatrywanym przypadku, można przypisać przymiot danych osobowych, odnosi to ogromny skutek w świetle u.o.d.o. Poczynając od obowiązku spełnienia przesłanki legalizującej przetwarzanie danych (art. 23 u.o.d.o.), poprzez obowiązek informacyjny administratora danych, w zależności od formy powzięcia informacji o danych konkretnej osoby (art. 24, 25 u.o.d.o.), prawo kontroli jednostki dotyczących jej danych (art. 32 u.o.d.o), czy na obowiązku należytego zabezpieczenia danych osobowych kończąc (art. 36 u.o.d.o.).

4. Próba uregulowania materii

Pod koniec 2013 r. Minister Spraw Wewnętrznych przedstawił projekt założeń do projektu ustawy o monitoringu wizyjnym. Projekt ten spotkał się krytycznym odbiorem zainteresowanych środowisk. Opinie wskazywały prawidłowość założeń projektu co do zasady, jednak niedoskonałość w kwestiach już szczegółowych. Projekt w takiej wersji, wymagał jeszcze znacznej poprawy w kwestiach sztandarowych. Przykładowo Krajowa Rada Sądownictwa[333], która zaaprobowała sam zamysł uregulowania owej materii i jej zasadniczość, uznała jednocześnie zaproponowane w projekcie uregulowania za budzące poważne wątpliwości co do ich zgodności z Konstytucją. Generalny Inspektor Ochrony Danych Osobowych[334] zwrócił uwagę na brak przepisów, które wyraźnie zabraniałyby udostępniania nagrań podmiotom innym niż wymienione w projekcie lub osobom upoważnionym przez administratora oraz w jakich sytuacjach administrator może upoważnić do wglądu w nagrania w przypadku wątpliwości czy osoba, która jest objęta monitoringiem może żądać dostępu do zarejestrowanych danych, które to kwestie wydają się być zasadniczymi w omawianej ustawie. Zastrzeżenia skierowane były też m.in. co do braku regulacji dotyczących instalowania monitoringu wizyjnego w placówkach oświatowych czy niekompletności regulacji w kwestii monitoringu wizyjnego w zakładach pracy[335].

Wobec krytycznego odbioru projektu założeń, w lipcu 2014 r. przedstawiono kolejną jego wersję[336], biorąc pod uwagę sugestie, uwagi i propozycje zmian sformułowane w wyniku konsultacji społecznych. Spotkał się on z zasadniczo lepszą oceną, choć ze względu na złożoność tej materii prawnej, część opiniujących wciąż sugerowała dalsze rozważania i poprawki uznając przedstawiony projekt za wymagający dalszego dopracowania. Kompleksową opinię do ów wersji przedstawiła m.in. Fundacja Ponoptykon, która oceniła, iż „zaproponowana koncepcja – mimo wprowadzenia wielu pozytywnych zmian – wymaga dalszej rewizji i dopracowania. (…) perspektywa ochrony praw jednostki jest w projekcie wciąż niedostatecznie obecna, co znajduje odzwierciedlenie zarówno w ograniczonym katalogu

[333] Opinia Krajowej Rady Sądownictwa z dnia 17.01.2014 r. w przedmiocie projektu założeń projektu ustawy o monitoringu wizyjnym, Lex 2016.
[334] Zwany dalej GIODO.
[335] Stanowisko GIODO z dnia 13.08.2014 r. http://bip.mswia.gov.pl/bip/projekty-aktow-prawnyc/2013/22768,Projekt-zalozen-do-projektu-ustawy-o-monitoringu-wizyjnym.html, dostęp: [12.01.2016 r.]
[336] Drugi projekt założeń do projektu ustawy o monitoringu wizyjnym http://legislacja.rcl.gov.pl/docs//1/200701/200707/200708/dokument119053.pdf.

uprawnień osób poddanych monitoringowi, jak i braku zasad prowadzenia monitoringu, które stanowiłyby ich gwarancję”[337]. Pomimo zapewnień Ministerstwa Spraw Wewnętrznych, iż ustawa wejdzie w życie, po etapie konsultacji nie nadano sprawie dalszego biegu w żaden sposób, tzn., że nie powstał ani projekt ustawy ani nie poczyniono kroków do opracowania kolejnej wersji projektu założeń uwzględniającego istotne głosy krytyki ze strony podmiotów opiniujących.

5. Regulacje traktujące o monitoringu

Jak już zostało wspomniane, brak jest przepisów kompleksowo traktujących o materii monitoringu wizyjnego. Niemniej jednak wśród obowiązujących przepisów znajdujemy szczątkowe regulacje odnoszące się do niej bezpośrednio.

Ustawą, która daje upoważnienie do rejestrowania zarówno obrazu jak i dźwięku jest ustawa o bezpieczeństwie imprez masowych[338]. Artykuł 11 oprócz bezpośredniego wskazania możliwości monitorowania obiektu, a w szczególności zachowania się osób uczestniczących w imprezie masowej zawiera również dyspozycję co do czasu przechowywania zgromadzonych materiałów z przebiegu imprezy masowej, procedurze ich niszczenia i organie odpowiedzialnym w zakresie zapewnienia wykonywania zadań związanych z bezpieczeństwem imprez masowych. I tak w pkt. 3 tego przepisu „zgromadzone podczas utrwalania przebiegu imprezy masowej materiały, niezawierające dowodów pozwalających na wszczęcie postępowania karnego albo postępowania w sprawach o wykroczenia lub dowodów mających znaczenie dla toczących się takich postępowań, organizator przechowuje po zakończeniu imprezy masowej przez okres co najmniej 30 dni, a następnie komisyjnie je niszczy”. W przypadku zaś, gdy materiały zawierają dowody mogące stanowić podstawę do wszczęcia postępowania karnego bądź wykroczeniowego, albo mające dla już toczącego postępowania „(…) organizator niezwłocznie przekazuje prokuratorowi rejonowemu właściwemu ze względu na miejsce przeprowadzonej imprezy masowej lub właściwemu terytorialnie komendantowi powiatowemu (miejskiemu, rejonowemu) Policji, w razie potrzeby z wnioskiem o wszczęcie postępowania karnego lub z wnioskiem o ukaranie, chyba że sam zawiadomi o przestępstwie albo wystąpi z wnioskiem o ukaranie w sprawach o wykroczenia. Ustawa w art. 3 pkt. 6 definiuje również czas trwania imprezy masowej wskazując na okres od chwili udostępnienia obiektu lub terenu uczestnikom imprezy masowej do chwili opuszczenia przez nich tego obiektu lub terenu. Ma to istotne znaczenie z punktu widzenia możliwości rejestrowania obrazu i dźwięku, gdyż wyrazie wskazuje jej ramy ustalając je na czas zarówno przed zasadniczą imprezą masową, co oczywiste – w czasie jej trwania, jak i okres po jej zakończeniu. W art. 11 ust. 4 wspomnianej ustawy znajduje się również przepis statuujący kompetencję wojewody do sporządzenia wykazu stadionów, obiektów lub terenów, na których utrwalanie

[337] Stanowisko Fundacji Panoptykon dnia 14.08.2014 r. http://bip.mswia.gov.pl/bip/projekty-aktow-prawnyc/2013/22768,Projekt-zalozen-do-projektu-ustawy-o-monitoringu-wizyjnym.html, dostęp: [12.01.2016 r.]
[338] Ustawa z dnia 20.03.2009 r. o bezpieczeństwa imprez masowych (Dz.U. 2009 nr 62 poz. 504).

przebiegu imprezy masowej za pomocą urządzeń rejestrujących obraz i dźwięk jest obowiązkowe, zaś umieszczenie w wykazie określonego stadionu, obiektu lub terenu następuje w drodze decyzji administracyjnej.

Na podstawie wyraźnego upoważnienia zawartego w ustawie, wydane zostało rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 10 stycznia 2011 r. w sprawie sposobu utrwalania przebiegu imprezy masowej[339]. Rozporządzenie to określa sposób utrwalania przebiegu imprezy masowej, a w szczególności:

1) miejsca na stadionach, w obiektach lub na terenach, umieszczonych w wykazie[340], o którym mowa w art. 11 ust. 4 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, w których utrwalanie przebiegu imprezy masowej za pomocą urządzeń rejestrujących obraz i dźwięk jest obowiązkowe;
2) minimalne wymagania techniczne dla urządzeń rejestrujących obraz i dźwięk;
3) sposób przechowywania materiałów zgromadzonych podczas utrwalania przebiegu imprezy masowej.

W rozporządzeniu wskazano na obowiązek umieszczenia przy wejściu na teren imprezy masowej informacji o prowadzonej w trakcie trwania tej imprezy rejestracji obrazu i dźwięku. Gdy chodzi o wymagania techniczne, do rejestracji dopuszcza się:

1) wykorzystanie kamer analogowych i jednoczesne wykorzystanie przetworników analogowo-cyfrowych, tak aby obraz zarejestrowany kamerą analogową został przetworzony do postaci cyfrowej;
2) stosowanie kamer rejestrujących obraz kolorowy, które w przypadku spadku natężenia oświetlenia rejestrowanego obszaru automatycznie przełączają się w tryb monochromatyczny z wykorzystaniem ruchomego filtra podczerwieni.

Rozporządzenie w sposób wyraźny różnicuje wymagania techniczne jakie powinny spełniać urządzenia rejestrujące obraz podczas imprezy masowej od przyjętej kategorii obrazu. Wprowadza się 4 różne kategorie ze względu na ich znaczenie dla operatora, która kształtują się następująco:

1) dla obrazu I kategorii[341] i II kategorii[342] - w zakresie rejestrowania stabilnego obrazu z częstotliwością nie mniejszą niż 12 klatek na sekundę, przy wysokości obrazu nie mniejszej niż 950 pikseli i czasie migawki nie dłuższym niż 1/125 sekundy dla każdej kamery;

[339] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 10.01.2011 r. w sprawie sposobu utrwalania przebiegu imprezy masowej (Dz.U. 2011, nr 16, poz. 73).
[340] Wykaz stadionów, obiektów lub terenów, na których utrwalanie przebiegu imprezy masowej za pomocą urządzeń rejestrujących obraz i dźwięk jest obowiązkowe.
[341] Obraz I kategorii — należy przez to rozumieć rejestrację obrazu umożliwiającą określenie tych cech osób lub rzeczy, które pozostają w zainteresowaniu operatora w związku z zabezpieczeniem imprezy masowej, w celu wykorzystania do ustalenia tożsamości osób lub przynależności rzeczy.
[342] Obraz II kategorii — należy przez to rozumieć rejestrację obrazu umożliwiającą dozorowanie miejsca, wskazanego przez operatora, w celu określenia cech grupowych osób lub rzeczy.

2) dla potrzeb rejestracji obrazu III[343] i IV[344] kategorii — w zakresie rejestrowania obrazu z częstotliwością nie mniejszą niż 6 klatek na sekundę, przy wysokości obrazu nie mniejszej niż 500 pikseli dla każdej kamery.

Gdy zaś chodzi o rejestrację dźwięku, to urządzenia podczas imprezy masowej powinny umożliwić zrozumienie treści nagranych haseł i okrzyków oraz określenie sposobu zachowywania się uczestników imprezy masowej. Parametry tych urządzeń powinny zapewniać rejestrację sygnału akustycznego w paśmie częstotliwości od 300 Hz do 4 000 Hz, przy minimalnej dynamice 50 dB[345].

Wśród pozostałych przepisów istotne są kwestie, iż zarejestrowany obraz utrwalany powinien być w niezmienionej postaci, zarejestrowany obraz i dźwięk podlegają archiwizacji na elektronicznym nośniku informacji, jak również warunki zabezpieczenia i przechowywania nośnika informacji.

Wśród innych regulacji znajdziemy również uprawnienie do obserwowania i rejestrowania przy użyciu środków technicznych przez służby mundurowe, takie jak: Policja, Straż Gminna, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego. Policja w celu wykonywania czynności: operacyjno-rozpoznawczych, dochodzeniowo-śledczych i administracyjno-porządkowych, ma prawo do:

1) obserwowania i rejestrowania przy użyciu środków technicznych obrazu z pomieszczeń przeznaczonych dla osób zatrzymanych lub doprowadzonych w celu wytrzeźwienia, policyjnych izb dziecka, pokoi przejściowych oraz tymczasowych pomieszczeń przejściowych;
2) obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych, a w przypadku czynności operacyjno-rozpoznawczych i administracyjno-porządkowych podejmowanych na podstawie ustawy - także i dźwięku towarzyszącego tym zdarzeniom[346].

Straż gmina w celu realizacji zadań wymienionych w ustawie straży gminnej ma prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych w przypadku, gdy czynności te są niezbędne do wykonywania zadań oraz w celu:

1) utrwalania dowodów popełnienia przestępstwa lub wykroczenia;
2) przeciwdziałania przypadkom naruszania spokoju i porządku w miejscach publicznych;
3) ochrony obiektów komunalnych i urządzeń użyteczności publicznej.

Straż gminna prowadzi ewidencję środków technicznych służących do obserwowania i rejestrowania obrazu zdarzeń w miejscach publicznych, pojazdów. Nadzór nad działalnością straży polegającą na wymianie informacji w zakresie obserwowania

[343] Obraz III kategorii — należy przez to rozumieć ciągłą rejestrację obrazu umożliwiającą wykrycie osób lub rzeczy, w miejscu dozorowanym przez kamerę, w celu przekazania operatorowi informacji o ujawnieniu osoby lub rzeczy, przy czym jednoczesna rejestracja obrazu z całego miejsca dozorowanego przez kamery nie jest wymagana.

[344] obrazu IV kategorii — należy przez to rozumieć ciągłą rejestrację obrazu, a w obszarach, w których jest to wymagane — także dźwięku, pozwalającą operatorowi wykryć występujące zagrożenie w miejscu dozorowanym przez kamerę, w celu przekazania informacji o stanie bezpieczeństwa.

[345] Poziom natężenia dźwięku.

[346] Art. 14 ust 1 pkt 4a, 5a ustawy z dnia 6.04.1990 r. o Policji (Dz. U z 1990 r. nr 30 poz. 179).

i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych sprawuje wójt, burmistrz (prezydent miasta). Kwestię prawa straży gminnych do obserwowania i rejestrowania przy użyciu środków technicznych uszczegóławia rozporządzenie w sprawie sposobu obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną (miejską)[347]. Gdy chodzi o funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego to w celu: rozpoznawania, zapobiegania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa mają prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom w trakcie wykonywania czynności operacyjno-rozpoznawczych podejmowanych na podstawie ustawy[348].

6. Złożoność zagadnienia

Problematyka monitoringu jest niewątpliwie kwestią zawiłą nie tylko pod względem prawnym. Świadomość funkcjonowania i zagrożeń płynących z „podglądania" innych wśród społeczeństwa jest znikoma. Dochodzi do konfrontacji ze sobą dwóch odrębnych stanowisk. Z jednej strony władza dąży do rozbudowy systemu monitorującego obywateli i przekonując o zwiększeniu poczucia ich bezpieczeństwa, a z drugiej strony faktyczny brak kontroli nad monitoringiem i monitorującymi oraz zawodność monitoringu w stosunku do celów dla jakich został powołany. Jak wskazują badania, monitoring wizyjny ma więcej zwolenników niż przeciwników. Aż 61% badanych opowiedziało się za zwiększeniem liczby kamer. Badani mają bardzo ograniczoną wiedzę na temat monitoringu i sposobu jego działania. Nie orientują się, kto może mieć dostęp do nagrań z kamer i mają na ten temat różnorodne teorie. Zdaniem badanych monitoring może być wykorzystywany do wielu celów, ale hasłem które najczęściej pojawia się w debacie publicznej jest „bezpieczeństwo"[349]. Społeczeństwo nie zdaje sobie sprawy z tego, że w codziennym życiu może być obserwowane nie tylko przez kamery miejskiego monitoringu należące do instytucji publicznych, ale też przez osoby prywatne, których celem monitorowania przypuszczalnie nie jest „bezpieczeństwo" obywateli. Dla przeciętnego człowieka, który nie miał styczności z sprzętem do monitoringu nie jest możliwe również odróżnienie kamer miejskich od kamer należących do podmiotów prywatnych. Funkcjonują również kamery na tyle precyzyjne, że mogą odczytać treść pisanego na telefonie sms-a, lub numery kodu PIN wpisywanego w bankomacie, które to dane w rękach nieodpowiednich podmiotów mogą stanowić istotne zagrożenie dla prywatności

[347] Rozporządzenie Rady Ministrów z 16.12.2009 r. w sprawie sposobu obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych przez straż gminną (miejską) (Dz. U z 2009 r. nr 220 poz. 1720).
[348] Art. 23 ust. 1 pkt 6 ustawy z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2002 r. nr 74 poz. 676).
[349] Fundacja Ponoptykon, *Monitoring w polskich miastach i w oczach społeczeństwa,* http://panoptykon.org/biblio/monitoring-w-polskich-miastach-i-w-oczach-spoleczenstwa, s. 3, dostęp: [15.01.2016 r.]

obserwowanych i być wykorzystane przeciwko nim. Przykładowo również - w opinii GIODO „emitowanie podglądu z kamer osiedlowego monitoringu w telewizji kablowej rodzi zagrożenia dla naszej prywatności. Najbardziej niebezpieczne jest to, że transmitowanie podglądu z kamer osiedlowego monitoringu wizyjnego do sieci kablowych umożliwia nagrywanie go i analizowanie. Pozwala to m.in. na ocenę zachowań poszczególnych osób, np. tego, kiedy przychodzimy do domu, a kiedy z niego wychodzimy, czy wnieśliśmy właśnie nowy telewizor, czy wynosimy jakieś rzeczy na śmietnik, jakim samochodem jeździmy, jak bawią się nasze dzieci, które dzieci są czyje. Choć są to informacje, które i tak możemy zaobserwować przebywając na osiedlu, ale czym innym jest obserwowanie tego na osiedlu, a zupełnie czym innym obserwowanie, nagrywanie i przetwarzanie tego na domowym magnetowidzie”[350]. Innym zagrożeniem dla prywatności jest popyt na dane jak najbardziej indywidualizujące daną osobę. W handlu funkcjonuje rynek informacji osobowych, który odznacza się tym, że firmy oferujące swe produkty i usługi chcą trafić do określonej grupy klientów, która może być potencjalnie nimi zainteresowana. Dzięki informacjom osobowym mogą one wyodrębnić tę grupę spośród szerszego grona (profilowanie). Jak twierdzi M. Chrabonszczewski jeszcze dokładniej można wyodrębnić docelową grupę klientów na podstawie danych wrażliwych (np. firmy farmaceutycznych oferujące lek dla osób cierpiących na daną chorobę)[351]. Powszechnie znanym jest również publikowanie nagrań z monitoringu w Internecie a nawet w telewizji, najczęściej bez zgody osób, których dotyczą, jak również bez ich wiedzy, że są nagrywane. Zdarza się, że kamery CCTV instalowane są w miejscach, w których powinna zostać zachowana intymność jak toalety czy sklepowe przymierzalnie.

Biorąc pod uwagę ilość zainstalowanych w miastach kamer należałoby stwierdzić, że proporcjonalnie do ilości kamer wzrosło bezpieczeństwo obywateli i spadła przestępczość. Najwyższa Izba Kontroli w raporcie o monitoringu wizyjnym przedstawia jednak zdecydowanie krytyczne wyniki. „W latach 2010 - 2013 w skontrolowanych miastach operatorzy zaobserwowali ponad 152 tys. zdarzeń, w zdecydowanej większości wykroczeń drogowych. Poważne przestępstwa (rozboje, włamania, kradzieże i niszczenie mienia) dostrzeżone i udokumentowane dzięki monitoringowi stanowiły jedynie 5 proc. wszystkich zaobserwowanych zdarzeń[352]”. Co jeszcze bardziej druzgocące „połowa spośród osiemnastu skontrolowanych jednostek prowadzących miejski system monitoringu wizyjnego nie przestrzegało przepisów dotyczących ochrony danych osobowych. Jednostki te nie zgłosiły zbiorów danych osobowych z systemu monitoringu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Zgłoszenie takie w świetle u.o.d.o. warunkuje legalność rozpoczęcia przetwarzania danych osobowych w systemie monitoringu wizyjnego. Zdarzały się również nieprawidłowości polegające na niezapewnieniu ochrony przetwarzanych danych osobowych uzyskanych w ramach miejskiego systemu monitoringu wizyjnego”[353]. Konkluzja jest jednoznaczna – nie tylko wykorzystywanie monitoringu przez podmioty prywatne jest

[350] http://www.giodo.gov.pl/1520001/id_art/8162/j/pl/, dostęp: [14.01.2015 r.]
[351] M. Chrabonszczewski, *Prywatność. Teoria i praktyka*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2012, s. 145.
[352] Raport NIK z dnia 25.03.2014 r., http://www.nik.gov.pl/plik/id,6400,vp,8169.pdf, s. 8, 15.01.2015 r.
[353] Ibidem.

zagrożeniem dla prywatności. Ograniczone zaufanie należy mieć również wobec instytucji publicznych, które jak widać, mogą zaniedbać swe obowiązki i narazić dane obywateli na niebezpieczeństwo.

Wyeksponować powinno się także koszty jakie generuje monitoring. Niskiej jakości kamery CCTV nie stanowią dużego wydatku, jednakże oprócz samych kamer do prawidłowego funkcjonowania potrzebny jest jeszcze inny niezbędny sprzęt oraz obsługa. Na przykładzie Warszawy samo utworzenie zintegrowanego systemu kosztowało stolicę prawie 59 mln złotych, a jego utrzymanie przez 10 lat (2003–2012) pochłonęło około 104 mln złotych. Koszt utrzymania jednej kamery to prawie 3 tys. złotych na miesiąc[354]. Nie wspominając już o jakości zakupywanych kamer CCTV, które są wysoko awaryjne i najczęściej nieprzystosowane technicznie do warunków, w których mają funkcjonować.

W kwestii monitoringu, oprócz wspomnianej już w tekście materii, została wydana również opinia Grupy Roboczej Art. 29 do spraw ochrony danych[355], w której poruszono tematykę monitoringu wizyjnego, m.in. w powiązaniu z zasadą proporcjonalności wskazując, że systemy te mogą być zastosowane, gdy inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, nie wymagające pozyskiwania obrazu (np. wykorzystywanie drzwi antywłamaniowym służące zapobieganiu aktom wandalizmu, instalacja automatycznych bramek i urządzeń kontroli dostępu, wspólnych systemów alarmowych, ulepszone i wzmocnione oświetlenie ulic w nocy, etc.) okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami[356]. Warto by się zatem zastanowić, biorąc pod uwagę ogromne wydatki ponoszone w związku z funkcjonowaniem monitoringu i jego zasadniczą słabą efektywnością, czy nie lepiej byłoby zainwestować w doraźne formy zwiększające bezpieczeństwo w miejscach publicznych.

7. Zakończenie

Konfrontując ze sobą interes jednostki i jej prawo do prywatności z interesem publicznym jakim jest bezpieczeństwo dochodzi do konfliktu. Niestety rozwój nowych technologii coraz silniej ingeruje w naszą prywatność, a przy braku środków umożliwiających ich kontrolę nieuchronnie kroczymy w kierunku systemu orwellowskiego, zagrażającemu nie tylko interesowi jednostek, ale już całych społeczeństw.

System monitoringu wizyjnego okazuje się być systemem zawodnym, technicznie nieprzystosowanym do warunków w jakich ma funkcjonować i nieodpowiedni jakościowo.

[354] Fundacja Ponoptykon, *Życie wśród kamer*, http://zycie-wsrod-kamer.panoptykon.org, s. 19, dostęp: [15.01.2015 r.]
[355] Opinia 4/2004 w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer video, opracowana przez Grupę Roboczą Art. 29 do spraw ochrony danych, przyjęta 11.02. 2004 r, http://www.giodo.gov.pl/1520189/id_art/7146/j/pl/, dostęp: [05.12.2015 r.]
[356] www.giodo.gov.pl/457/id_art/7146/j/pl/, s. 23, dostęp: [15.01.2016 r.]

Monitoring okazuje się też być mało przydatny w kwestii zwalczania przestępstw i zapewnienia ładu publicznego. Z prawnego punktu widzenia istotny jest utrzymujący się stan bezprawności, prowadzący do nadużyć ze strony podmiotów obserwujących, brak ochrony danych osób nagrywanych, przetwarzanie danych osób nagrywanych czy brak kontroli nad działaniami podmiotów korzystających z urządzeń rejestrujących obraz. Niewątpliwym jest oczekiwanie powstania kompleksowej ustawy traktującej o monitoringu celu zapewnienia ochrony danych osobowych oraz zwiększenia bezpieczeństwa obywateli przed nadmiernym jego stosowaniem w przestrzeni publicznej Im dłużej kwestia ta pozostanie nieuregulowana, tym dłużej podstawowe prawa obywateli do prywatności, poszanowania autonomii informacyjnej czy godności człowieka mogą być łamane. Aktualnie funkcjonujemy w warunkach, w których każdy może nagrywać każdego w dowolnym miejscu i w dowolnym czasie, a następnie wykorzystywać nagrania wedle własnej woli, bez niczyjej kontroli. Taki stan rzeczy należy oceniać jak najbardziej krytycznie.

mgr Anna Sojat

Problematyka wielomiejscowości naruszenia dóbr osobistych – delikty internetowe

1. Wstęp

Ochrona dóbr osobistych to współcześnie tematyka aktualna przede wszystkim z praktycznego punktu widzenia. Powszechna globalizacja i komercjalizacja w połączeniu z ogólnym dostępem do sieci Internet wpływają na mnogość przypadków, w których mamy do czynienia z koniecznością ochrony dóbr osobistych. Sieć Internet charakteryzuje się trwałością, co oznacza, że każda zamieszczona w Internecie treść jest zapisywana i archiwizowana, replikowalnością, czyli łatwością kopiowania, wyszukiwalnością, czemu sprzyja duża ilość wyszukiwarek internetowych i skalowalnością, czyli nieograniczonym dostępem do tychże informacji i treści[357]. Dzielenie się informacjami przez niezidentyfikowanych (anonimowych) użytkowników, swobodny przepływ informacji i jednocześnie bardzo uproszczony system korzystania z nich, prowadzi do sytuacji powstawania deliktów internetowych. W takich przypadkach aktualizuje się problem ochrony dóbr osobistych. Nie sposób pominąć w tym miejscu faktu, iż polska ustawa Prawo prywatne międzynarodowe z 2011 r.[358] wprowadza w art. 16 odrębną regulację dotyczącą problematyki prawa właściwego dla dóbr osobistych i ich ochrony, czym daje wyraz, że poprzednio obowiązujące, ogólne uregulowania znajdujące się w ustawie Prawo prywatne międzynarodowe z 1965 r.[359] nie były wystarczające przy obecnym rozwoju cywilizacyjnym i technologicznym państw. Warto podkreślić, że ustawa z 1965 r. w art. 9 ust. 1 określała jedynie prawo właściwe dla zdolności prawnej osoby fizycznej, co analogiczne stosowane było do dóbr osobistych. Problem poszukiwania prawa właściwego dla ochrony dóbr osobistych wiąże się z faktem, że coraz częściej mamy do czynienia ze zdarzeniami wielomiejscowymi, które wywołują skutki w skali globalnej. Przyczyną tego zjawiska jest między innymi rozwój sieci Internet.

2. Pojęcie dóbr osobistych

W polskim systemie prawa, legalna definicja dóbr osobistych nie funkcjonuje, choć pojęcie to można odnaleźć w wielu aktach normatywnych. Podstawę prawną do konstruowania instytucji dóbr osobistych ustawodawca zawarł w Konstytucji Rzeczypospolitej Polskiej. Art.

[357] Ł. Kołodziejczyk, Prywatność w Internecie, Warszawa 2014, s. 36.
[358] Ustawa z dnia 4.02.2011 r. Prawo prywatne międzynarodowe (Dz.U. 2011 Nr 80 poz. 432), dalej: p.p.m.
[359] Ustawa z dnia 12.11.1965 r. Prawo prywatne międzynarodowe (Dz.U. 1965 Nr 46 poz. 290).

30 ustawy zasadniczej podkreśla, iż przyrodzona i niezbywalna godność człowieka stanowi źródło wolności i praw człowieka i obywatela. Co więcej ustawodawca wymienia obowiązek władz publicznych do poszanowania i ochrony tej wartości, ponieważ jest nienaruszalna[360]. Art. 23 Kodeksu cywilnego[361] stanowi, iż dobrami osobistymi człowieka są w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska. Dodaje również, że pozostają one pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Przepisu tego nie można jednak traktować jako definicji. Występuje w nim jedynie przykładowe wyliczenie dóbr osobistych. Jak zaznacza wielu autorów w tym Z. Radwański, katalog ten nie ma charakteru zamkniętego[362]. Taki pogląd widoczny jest także w orzecznictwie sądowym, które często wskazuje na dobra osobiste, niezapisane literalnie w ustawie takie jak prawo do pochowania[363], więź z osobą najbliższą[364] czy poczucie przynależności narodowej[365]. Rozwój cywilizacyjny prowadzi do tego, iż procesy dotyczące dóbr osobistych polegają na odkrywaniu już istniejących dóbr, a nie na tworzeniu nowych[366] , przez doktrynę czy orzecznictwo. Otwarta lista dóbr osobistych wiąże się z odkrywaniem ich nowych postaci lub bardziej uszczegółowionych odmian dóbr, które zostały zawarte w przepisie 23 k.c.[367]. Nie sposób odmówić racji właśnie takim poglądom, szczególnie w kontekście deliktów internetowych. W przypadku dóbr osobistych w Internecie będziemy mieli do czynienia zazwyczaj z naruszeniem prywatności czy prawa do wizerunku, czyli tych rodzajów dóbr, które zostały w ustawie wymienione lub są przez praktykę orzeczniczą znane. *Novum* w tej dziedzinie, będzie stanowiła forma i skala ich naruszenia, dzięki czemu będziemy mieli do czynienia właśnie z odmianą do tej pory nieznaną czy nową postacią takiego dobra. Dobra osobiste są materią płynną, przechodzącą obecnie przez kolejne stadia rozwoju, co uniemożliwia ścisłą ich klasyfikację. Biorąc pod uwagę funkcje, jakie mają pełnić dobra osobiste we współczesnym świecie, nie wydaje się koniecznym i celowym umieszczanie ich w sztywno zarysowanych ramach.

3. Specyfika deliktów internetowych

Delikt, czyli czyn niedozwolony, w polskim prawie cywilnym określany jest jako zdarzenie powodujące odpowiedzialność deliktową. By uznać dane zdarzenie za delikt należy sprawdzić, czy spełnia on cechy kwalifikujące jako czyn niedozwolony. Po pierwsze, z danym faktem ustawa musi wiązać obowiązek naprawienia szkody. Po drugie, powstanie obowiązku

[360]Konstytucja Rzeczypospolitej Polskiej z dnia 2.04.1997 r. (Dz.U. Nr 78, poz. 483).
[361]Ustawa z dnia 23.04.1964 r. Kodeks cywilny (Dz.U. z 2014 r. poz. 121), dalej: k.c.
[362] Z. Radwański [w:] Z. Radwański, A. Olejniczak, Prawo cywilne – część ogólna, Warszawa 2011, s. 158.
[363] Wyrok Sądu Apelacyjnego w Łodzi I Wydział Cywilny z dnia 8.10.2015 r., I ACa 439/15, Legalis nr 1370763.
[364] Wyrok Sądu Apelacyjnego w Krakowie I Wydział Cywilny z dnia 23.07.2015 r., I ACa 621/15, Legalis nr 1370725.
[365] Wyrok Sądu Apelacyjnego w Białymstoku I Wydział Cywilny z dnia 30.09.2015 r., I ACa 403/15, Legalis nr 1352336.
[366] I. Lewandowska – Malec [w:] I. Lewandowska-Malec (red.), Dobra osobiste, Warszawa 2014, s. 44.
[367] M. Safjan (red.), System Prawa Prywatnego, Prawo cywilne – część ogólna, t. 1, Warszawa 2007, s. 1118.

naprawienia szkody nie może wynikać z wcześniej łączącej strony więzi prawnej, która mogłaby taki obowiązek kreować. Po trzecie, by można mówić o delikcie, zdarzenie musi wywołać skutki ex lege, a co więcej świadczenie odszkodowawcze powinno być świadczeniem głównym. Delikt internetowy musi dodatkowo zostać popełniony „na odległość" w związku z siecią Internet, co oznacza, że doszło do niego przy wykorzystaniu strony internetowej, poczty elektronicznej, czy - współcześnie stanowiących nieodłączny element aspektu socjologicznego życia – portali społecznościowych. Przykładami naruszenia dóbr osobistych w Internecie, które wypełniają cechy deliktu internetowego są sytuacje, gdy bez zezwolenia danej osoby fizycznej posłużono się jej nazwiskiem w celach reklamowych czy, gdy mamy do czynienia z bezprawnym używaniem oznaczenia (firmy) osoby prawnej w domenie lub adresie poczty elektronicznej. Jeśli zaś chodzi o krąg przeciętnych użytkowników Internetu, często mamy do czynienia z naruszeniem prawa prywatności, nie tylko poprzez umieszczanie czy rozpowszechnianie informacji na temat danej osoby, ale także choćby poprzez spamming, czyli przesyłanie na adresy elektroniczne spersonalizowanych, niezamawianych informacji.

Idea spamming'u realizuje się w sytuacjach wykorzystywania poczty elektronicznej do celów reklamowych. Niezamówione treści, zazwyczaj nie spełniają swojego podstawowego celu. Jeśli przeznaczone są dla szerokiego grona anonimowych odbiorców, w większości przypadków będą charakteryzowały się nieodpowiedniością treści do potrzeb odbiorcy. Pomijając w tym artykule, oczywiste wady spamming'u tj. uciążliwość, zbyt dużą ilość wiadomości czy opóźnianie korespondencji pożądanej, warto wspomnieć o dwóch podejściach do sposobu rozsyłania niezamawianych informacji. Obecnie wyróżnić można dwa systemy: opt-in oraz opt-out. System opt-in uzależnia możliwość przesyłania informacji od wyrażenia zgody przez użytkownika sieci. Obecnie, biorąc pod uwagę polskie regulacje, art. 10 ust. 2 ustawy o świadczeniu usług drogą elektroniczną stanowi, iż z informacją handlową zamówioną mamy do czynienia tylko w sytuacji, gdy użytkownik sieci wyraził zgodę na otrzymywanie tego typu informacji. Zgoda ta w szczególności występuje w sytuacji, gdy użytkownik udostępnia identyfikujący go adres elektroniczny, np. adres e-mail. Art. 10 ust. 1 ustawy o usługach elektr. stanowi ponadto, że przesyłanie niezamówionej informacji handlowej do oznaczonego odbiorcy będącego osobą fizyczną jest zakazane. Analizując powołane przepisy, dojść można do konkluzji, iż w pełni realizują one postulaty systemu opt-in. System opt-out charakteryzuje się zaś, postępowaniem użytkownika dającym możliwość wycofania się z otrzymywania danej niezamówionej informacji. W odniesieniu do poczty elektronicznej, schemat postępowania mający na celu rezygnację z otrzymywania informacji, powinien być umieszczony w każdej niezamówionej wiadomości i stanowić pełną, jasną i zrozumiałą instrukcję postępowania. System ten opiera się na automatycznym przesyłaniu niezamówionej informacji, do chwili wyrażenia rezygnacji przez odbiorcę. Opt-out jest zdecydowanie bardziej uciążliwym schematem postępowania. Biorąc pod uwagę regulacje europejskie, jest on także niezgodny z przepisami prawa w większości państw członkowskich UE, określającymi zasady świadczenia usług droga elektroniczną. Dyrektywa unijna nr 2000/31/WE zdelegalizowała spam komercyjny, a co więcej zdecydowanie obostrzyła funkcjonowanie systemu opt-out, na rzecz systemu opt-in.

Biorąc pod uwagę, iż sieć Internet sama w sobie jest bytem niematerialnym, to również identyfikacja miejsca wystąpienia zdarzenia w sieci, będzie o tyle niemożliwa, co niecelowa ze względu na wielomiejscowość wystąpienia takiego zdarzenia. Aspekt wielomiejscowości przyjmuje się w kontekście skutków czynu niedozwolonego, jakim jest szkoda. Rozproszenie elementów stanu faktycznego pomiędzy różne państwa, obliguje do podjęcia próby ustalenia prawa właściwego, które w danej sprawie najlepiej zrealizuje cele ochrony dóbr osobistych.

4. Znaczenia wielomiejscowości w deliktach internetowych

Wielomiejscowość charakteryzuje się powiązaniem stanu faktycznego deliktu z terytoriami różnych państw[368]. Dochodzi wtedy do sytuacji, gdy czyn powodujący odpowiedzialność deliktową i szkoda wynikła z tegoż czynu, zlokalizowane są na obszarze kilku państw[369]. Niewątpliwie pojawia się pytanie, które z możliwych państw będzie miejscem deliktu. Ponadto, jak autorka wspomniała wcześniej, określenie jednoznacznej lokalizacji deliktów internetowych stwarza trudności ze względu na ich wielomiejscowe wystąpienie w cyberprzestrzeni.

Polska doktryna wypracowała podział zjawiska wielomiejscowości, polegający na wyróżnieniu prostej i złożonej wielomiejscowości stanu faktycznego deliktu[370]. Deliktom internetowym przypisywana jest wielomiejscowość złożona, która charakteryzuje się tym, iż skutki działań sprawcy czynu niedozwolonego występują na różnych obszarach prawnych. Przykładem takiego zjawiska w kontekście ochrony dóbr osobistych jest umieszczenie informacji naruszającej dobra osobiste danego podmiotu na stronie WWW, która ze względu na nieograniczone możliwości Internetu, dostępna jest dla wszystkich użytkowników tej sieci. Jak trafnie zauważa O. Cachard, wielomiejscowość w przypadku deliktów internetowych nie może jednak oznaczać, że określenie prawa właściwego w danym stanie faktycznym, będzie możliwe dla każdego państwa, w którym można uzyskać dostęp do zasobów internetowych[371].

Prawo prywatne międzynarodowe operuje pojęciem najściślejszego związku z okolicznościami sprawy. Odnosząc się do polskiej ustawy Prawo prywatne międzynarodowe, w art. 10 tej ustawy została przyjęta regulacja, zgodnie z którą w sytuacji, gdy nie można ustalić okoliczności, od których zależy właściwość prawa, stosuje się prawo najściślej związane z danym stosunkiem prawnym. Jest to łącznik elastyczny, który był również brany pod uwagę podczas prób jednoznacznego określenia prawa właściwego, w celu umożliwienia dość szerokiego wyboru, pozwalającego na zrealizowanie praw w państwie, które strona uznała za najodpowiedniejsze. Jednak i w tym przypadku stwierdzono, iż strona nie będzie miała pewności, jakie prawo ostatecznie zastosuje sąd, a co za tym idzie, pewność dochodzenia praw przysługujących stronie zostanie zachwiana.

[368] M. Świerczyński, *op. cit*., s. 55.
[369] *Ibidem.*
[370] M. Sośniak, Zobowiązania niewynikające z czynności prawnych w prawie prywatnym międzynarodowym, Katowice 1971, s. 30-31.
[371] O. Cachard, *La régulation internationale du marché électronique*, Paryż 2002, s. 24.

Analizując wszelkie proponowane rozwiązania kwestii wielomiejscowości deliktu, w każdym przypadku zauważano, iż wybór jednego, konkretnego łącznika zawsze budzi wątpliwości. W każdej sytuacji można znaleźć wyjątek, w którym zastosowanie danego łącznika nie rozwiązywało kwestii prawa właściwego, a co więcej powodowało kolejne zastrzeżenia, co do idei wypracowania jednego stanowiska, które korespondowałoby z każdym możliwym przypadkiem.

5. Prawo właściwe dla naruszenia dóbr osobistych

W prawie prywatnym międzynarodowym w dziedzinie deliktów, fundamentalne znaczenie miał łącznik miejsca deliktu, który był stosowany w większości państw członkowskich Unii Europejskiej przed wejściem w życie rozporządzenia Rady (WE) Nr 864/2007/WE Parlamentu Europejskiego i Rady z dnia 11 lipca 2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych „Rzym II”[372]. Choć mogłoby wydawać się, że łącznik miejsca czynu jest kryterium wystarczającym, spełniającym swój cel, to w sytuacji praktycznego jego zastosowania, budził wiele wątpliwości. Łącznik miejsca deliktu nie sprawdza się w sytuacji, gdy czyn niedozwolony wystąpi w cyberprzestrzeni. Zasada terytorialności aktualna kilkadziesiąt lat temu, obecnie nie spełnia swojej pierwotnej roli, szczególnie w sytuacji, gdy elementy stanu faktycznego danej sprawy powiązane są z wieloma państwami[373].

Do momentu wejścia w życie rozporządzenia „Rzym II” doktryna podejmowała próby wypracowania jednego łącznika właściwego dla naruszenia dóbr osobistych. Jedną z pierwszych propozycji, która zyskała szerokie grono zwolenników, było zastosowanie łącznika personalnego w postaci miejsca zamieszkania lub zwyczajnego pobytu poszkodowanego. Wybór ten argumentowano tym, iż szkodę niematerialną powinno się lokalizować w miejscu zamieszkania poszkodowanego, a co więcej podnosząc aspekt socjologiczny, podkreślano, iż miejsce zamieszkania stanowi centrum stosunków społecznych poszkodowanej osoby[374].

Przywołane powyżej łączniki nie rozwiązały jednak wątpliwości dotyczących prawa właściwego dla naruszenia dóbr osobistych. Kolejnym krokiem w tej kwestii miało być wypracowanie odpowiednich łączników w ramach Unii Europejskiej i wspomnianego już wcześniej rozporządzenia „Rzym II”. Rozporządzenie to zawiera ogólną zasadę odnoszącą się do czynów niedozwolonych, a mianowicie, że prawem właściwym dla zobowiązania pozaumownego wynikającego z czynu niedozwolonego jest prawo państwa, w którym powstaje szkoda, niezależnie od tego, w jakim państwie miało miejsce zdarzenie powodujące szkodę, oraz niezależnie od tego, w jakim państwie lub państwach występują skutki pośrednie tego zdarzenia[375]. Jak wynika z powyższego, rozporządzenie dało pierwszeństwo zasadzie *lex loci damni*. Niemniej jednak wypracowanie zasady ogólnej względem deliktów, nie spowodowało tego, iż kwestia prawa właściwego dla naruszenia dóbr osobistych została rozwiązana.

[372]Rozporządzenie (WE) Nr 864/2007 Parlamentu Europejskiego i Rady z dnia 11.07.2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych („Rzym II”), (Dz.Urz. UE L z 2007r., Nr 199, s.40), dalej „Rzym II”.
[373] J. Gołaczyński, Prawo prywatne międzynarodowe, Warszawa 2011, s. 229.
[374] M. Świerczyński, *op. cit*., s. 229.
[375] Art. 4 ust. 1, rozporządzenie „Rzym II”.

Rozporządzenie „Rzym II" określając prawo właściwe dla zobowiązań pozaumownych wyłączyło z zakresu zastosowania, zobowiązania pozaumowne wynikające z naruszenia prawa do prywatności i innych dóbr osobistych, w tym zniesławienie[376]. Wyłączenie z zakresu zastosowania rozporządzenia „Rzym II" tego rodzaju deliktów ma znaczenie przy wyborze prawa właściwego, ze względu na konieczność stosowania norm krajowych. Należy dodać, iż próba wspólnego uregulowania prawa właściwego dla naruszenia dóbr osobistych, ukazała jedynie słabość systemu legislacyjnego Unii Europejskiej oraz podatność na wpływy grup interesów[377].

Biorąc pod uwagę fakt braku wspólnej regulacji, pojęcie dóbr osobistych powinno być oderwane od konkretnego porządku prawnego[378], by idea prawa kolizyjnego mogła być w pełni realizowana. Znaczenie przyznane dobrom osobistym w danym, krajowym porządku prawnym w większości przypadków jest punktem wyjścia dla organu rozpatrującego sprawę, gdyż zazwyczaj jest to jedyne, znane mu i stosowane pojęcie. Polska regulacja kwestii dóbr osobistych w ustawie p.p.m., odwołując się do prawa właściwego dla ich ochrony stworzyła zasadę opartą na łącznikach *lex loci delicti* albo *lex loci damni*, dając poszkodowanemu wybór. Takie rozwiązanie pokrywa się z większością krajowych norm kolizyjnych innych państw członkowskich. Unia Europejska pozostawiając tą kwestię do uregulowania w krajowych porządkach prawnych, dała możliwość wypracowania zasad, które najlepiej korespondują z danym porządkiem prawnym. Nie bez przyczyny, analiza rozwiązań kolizyjnych tej kwestii w pozostałych państwach członkowskich Unii Europejskiej, była konieczna. Okazało się, co zostało już wcześniej wspomniane, że zdecydowana większość państw należących do Unii Europejskiej wykorzystała przy tworzeniu własnych regulacji, założenia projektu rozporządzenia „Rzym II", który kwestię deliktów dóbr osobistych proponował uregulować w sposób jaki został powyżej wspomniany.

W tym miejscu godzi się również wspomnieć o wyroku Trybunału Sprawiedliwości Unii Europejskiej[379], który porusza kwestię prawa właściwego dla naruszenia dóbr osobistych w Internecie. Trybunał podkreślił, że osoba, która uważa się za poszkodowaną może wytoczyć powództwo dotyczące odpowiedzialności za całość doznanych krzywd i poniesionych szkód na zasadach przyjętych przez większość państw Unii Europejskiej. Jednakże, co stanowiło *novum* w kwestii prawa właściwego dla deliktów internetowych, Trybunał w wyroku stwierdził, że osoba poszkodowana może również, zamiast powództwa dotyczącego odpowiedzialności za całość doznanych krzywd i poniesionych szkód, wytoczyć powództwo przed sądami każdego państwa członkowskiego, na którego terytorium treść umieszczona w sieci jest lub była dostępna. Sądy te są właściwe do rozpoznania jedynie krzywdy lub szkody spowodowanych na terytorium państwa członkowskiego sądu, przed którym takie powództwo zostało wytoczone[380]. Bez wątpienia zaprezentowane stanowisko Trybunału Sprawiedliwości Unii Europejskiej, dało początek możliwości dochodzenia swych

[376] Art. 1 ust. 2 pkt g, rozporządzenie „Rzym II".
[377] J. Balcarczyk [w:] M. Pazdan (red.), System Prawa Prywatnego, Prawo prywatne międzynarodowe, tom 20a, Warszawa, s. 709.
[378] M. Wałachowska, Kolizyjnoprawne aspekty naruszenia dóbr osobistych [w:] J. Balcarczyk (red.), Dobra osobiste w XXI w. Nowe wartości, zasady, technologie, Warszawa 2012, s. 255.
[379] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 25.10.2011 r., C-509/09, Legalis nr 381630.
[380] Teza 1, Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 25.10.2011 r., C-509/09, Legalis nr 381630.

praw na wielu obszarach prawnych, nie korzystając przy tym z *forum shopping*, czyli wyboru najkorzystniejszego dla powoda prawa bez względu na stan faktyczny sprawy i skutki czynu niedozwolonego[381]. Tym bardziej orzeczenie to przyczyniło się do eliminowania zjawiska turystki zniesławieniowej, które po wejściu w życie rozporządzenia „Rzym II" było skutkiem negatywnym wyłączenia spod regulacji, zobowiązań pozaumownych dotyczących dóbr osobistych.

6. Podsumowanie

Aspekt wielomiejscowości naruszenia w kwestii deliktów internetowych obecnie zaczyna tracić na znaczeniu. Jest to zdecydowanie pozytywny skutek wieloletnich prób wypracowania łączników, które w pełni pozwolą na realizację praw do ochrony dóbr osobistych. Oczywiście nie można zapominać o ciągłym rozwoju cywilizacyjnym i technologicznym, który z każdym rokiem przynosi nowe rozwiązania techniczne, równocześnie stwarzając nowe wyzwania w kwestiach prawnych.

Biorąc pod uwagę, iż nin. artykuł odnosi się do deliktów powstałych przy użyciu sieci Internet, należałoby również zastanowić się czy odrębna regulacja prawna dot. cyberprzestrzeni rozwiązałaby wątpliwości interpretacyjne jakie pojawiają się na gruncie prawa prywatnego międzynarodowego. Konieczność indywidualnego uregulowania świata wirtualnego, kilkukrotnie już podnoszono w doktrynie europejskiej jak i na gruncie krajowym. Oczywiście, realizacja tego postulatu ma także swoich przeciwników, którzy pozostają wierni stanowisku, iż twór jakim jest cyberprzestrzeń nie istnieje jako przestrzeń wyodrębniona[382]. Zwolennicy zaś, upatrują sensu autonomicznej regulacji dla cyberprzestrzeń szczególnie w kontekście prawa prywatnego międzynarodowego, gdyż możliwe byłoby wypracowanie łączników właściwych dla stanów faktycznych związanych z siecią Internet, dzięki czemu uniknięto by wątpliwości interpretacyjnych czy dopasowania łączników, które sprawdzają się tylko w przypadkach jednomiejscowości stanu faktycznego, czyli w typowych, znanych prawu międzynarodowemu sytuacjach. Obecnie, na gruncie europejskim obejmującym państwa członkowskie Unii Europejskiej, niektóre dziedziny związane z funkcjonowaniem sieci Internet zostały uregulowane odrębnie, biorąc pod uwagę ich specyfikę. Można wskazać choćby powoływaną powyżej dyrektywę o handlu elektronicznym, której regulacje zostały implementowane do porządku prawnego państw członkowskich Unii Europejskiej. Zdecydowanie widoczny jest pozytywny kierunek rozwoju prawa Internetu, co jest pierwszym, dobrym krokiem do wypracowania autonomicznej regulacji właściwej w kontekście dóbr osobistych w nowych technologiach, które już nieodwracalnie funkcjonują we współczesnych społeczeństwach.

Opierając się na wypracowanych do tej pory rozwiązaniach, a jednocześnie dążąc do ciągłego udoskonalania prawa na poziomie międzynarodowym we wszelkich jego aspektach, jesteśmy w stanie doprowadzić do sytuacji, w których to nie technologia będzie wyprzedzała

[381] J. Balcarczyk, Prawo właściwe dla dobrego imienia osoby fizycznej i jego ochrony, Warszawa 2014, s. 298.
[382] M. Świerczyński [w:] P. Podrecki (red.), *op. cit.*, s. 164.

jej uregulowanie prawne, lecz obie te dziedziny będą tworzone jednocześnie, uzupełniając się nawzajem.

Autorzy publikacji:

1. Mgr Berenika Czerwińska – doktorant w Zakładzie Postępowania Administracyjnego i Sądownictwa Administracyjnego;
2. Mgr Maria Dymitruk – doktorant w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej;
3. Mgr Aleksandra Godek – absolwentka Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego;
4. Mgr Paweł Janiec – absolwent Wydziału Prawa i Administracji Uniwersytetu Opolskiego;
5. Mgr Agata Kowalska - absolwentka Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego;
6. Mgr Zuzanna Lisowska - absolwentka Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego;
7. Anna Panek – studentka Wydziału Prawa i Administracji Uniwersytetu Opolskiego;
8. Mgr Anna Pyka - absolwentka Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego;
9. Mgr Anna Sojat - doktorant w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej;

Wrocław 2018

ISBN 978-83-928515-9-2