Uniwersytet Jagielloński

Wydział Prawa i Administracji

Kierunek: Prawo

Ewa Molenda

Nr albumu: 1019292

Prawne aspekty Cloud Computing

Opiekun pracy magisterskiej:

Prof. dr hab. Ewa Nowińska

Instytut Prawa Własności Intelektualnej

Kraków 2012

Spis treści

Streszczenie

Kiedy na początku XXI w. znany amerykański pisarz Nicholas Carr ogłosił tezę o upadku tradycyjnego modelu świadczenia usług IT na rzecz modelu wzorowanego na dostarczaniu usług komunalnych, to przedstawiciele największych amerykańskich firm informatycznych przyjęli ją z niechęcią. Według Carr'a usługi w IT powinny być dostarczane i opłacane na takich samych zasadach jak prąd, czy woda. W chwili wydania jego drugiej książki *„The Big Switch"* (2008 r.) było już jednak wiadomo, że Carr miał rację, gdyż branża IT wkroczyła w erę Cloud Computing, tj. modelu ekspansji usług IT, który nie wymaga inwestycji w sprzęt, a tylko podłączenia do współdzielonych, wirtualnych zasobów umieszczonych na zewnętrznych serwerach. Już sam fakt transferu zasobów do podmiotu zewnętrznego musi budzić problemy prawne. Jak bowiem określić w takim przypadku lokalizację danych czy miejsce pobytu (siedziby) usługodawcy?

Celem tej pracy jest próba wyjaśnienia istoty Cloud Computing, i- co najważniejsze- poszukiwanie potencjalnych problemów prawnych, które mogą wiązać się z korzystaniem z usług dostarczanych w ramach tego modelu. Zagadnienia techniczne będą tu przedstawione tylko w zakresie niezbędnym do właściwej analizy problemów prawnych. Warto również zaznaczyć, że rozważania nie będą nakierowane na dogłębną analizę konkretnego systemu prawnego, gdyż mają one charakter uniwersalny. W celu lepszego zrozumienia istoty omawianych problemów, częstym punktem odniesienia będzie jednak prawo Unii Europejskiej oraz prawo polskie. Należy również wskazać, że w pracy zostaną przestawione tylko niektóre, choć wydaje się, iż najbardziej istotne problemy prawne.

Słowa kluczowe: chmura obliczeniowa, aspekty prawne, SaaS.

Summary

When in the beginning of XXI century, famous American writer Nicholas Carr announced the thesis that traditional model of IT delivery came to an end and makes way for the model imitating delivering municipal services, representatives of the biggest American IT companies received it reluctantly. Carr considered, that IT should be delivered in the same manner as water or electricity. While his second book "The Big Switch" was published in 2008, it was clear that he was right, because IT sector entered the era of Cloud Computing – IT propagation model which doesn't require investment in device, but just connection to a share, virtual resources place on external servers. The fact of transfer of those resources to the outer subject causes legal issues. How to set in this case the localization of data or the place of service provider's residence?

This work focuses on attempt to explain the essence of Cloud Computing and – what is the key target – to search for potential legal issues which are connected with benefitting from service provided within this model. It is necessary to point out that technical issues will only be briefly drafted to frame the main legal issues. On the other hand, deliberation will not contain deep analysis of particular legal system, because most of them are universal. For the better understanding of facts, frequent points of reference will be drawn from EU's and Polish law. It needs to be underlined, that this work will describe only some of – most important – legal issues.

Keywords: Cloud Computing, legal aspects, SaaS.

Wstęp

Branża IT (*Information Technology)* to obecnie jedna z najszybciej rozwijających się gałęzi gospodarki. Rynek usług IT i form ich dostarczania zmienia się tak dynamicznie, że przeciętny odbiorca nie jest zazwyczaj w stanie przyswoić sobie sensu tych zmian oraz skutków, które mogą wywołać (również skutków prawnych). Dla klienta (biznesowego czy indywidualnego) liczy się przede wszystkim maksymalna realizacja potrzeb przy jednoczesnej minimalizacji kosztów. O ile jednak usprawiedliwiona jest sytuacja, gdy usługobiorca zainteresuje się istotą usługi dopiero wtedy, gdy przestanie ona odpowiadać na jego zapotrzebowanie, to prawnik powinien obserwować zmiany na rynku IT i zaznajomić się przynajmniej z elementarnymi zagadnieniami, gdyż tylko w taki sposób będzie w stanie takiemu klientowi pomóc w razie zaistnienia sporu.

Kiedy na początku XXI w. znany amerykański pisarz Nicholas Carr ogłosił tezę o upadku tradycyjnego modelu świadczenia usług IT na rzecz modelu wzorowanego na dostarczaniu usług komunalnych, to przedstawiciele największych amerykańskich firm informatycznych przyjęli ją z niechęcią. Według Carr'a usługi w IT powinny być dostarczane i opłacane na takich samych zasadach jak prąd, czy woda[1]. W chwili wydania jego drugiej książki „*The Big Switch"* (2008 r.) było już jednak wiadomo, że Carr miał rację, gdyż branża (dzięki pojawieniu się usług *Google* lub *Salesforce*) IT wkroczyła w erę Cloud Computing, tj. modelu ekspansji usług IT, który nie wymaga inwestycji w sprzęt, a tylko podłączenia do współdzielonych, wirtualnych zasobów umieszczonych na zewnętrznych serwerach[2]. Już sam fakt transferu zasobów do podmiotu zewnętrznego musi budzić problemy prawne. Jak bowiem określić w takim przypadku lokalizację danych czy miejsce pobytu (siedziby) usługodawcy?

Celem tej pracy jest po pierwsze próba wyjaśnienia istoty Cloud Computing, i- co najważniejsze- poszukiwanie potencjalnych problemów prawnych, które mogą wiązać się z korzystaniem z usług dostarczanych w ramach tego modelu. Należy przy tym podkreślić, że zagadnienia techniczne będą tu przedstawione tylko w zakresie niezbędnym do właściwej analizy problemów prawnych. Warto również zaznaczyć, że rozważania nie będą skierowane

[1] Tom Sullivan, *Nichollas Carr: Jak Cloud Computing zdefiniuje IT,* computerworld.pl, 7.04.2009 r., http://www.computerworld.pl/artykuly/343055/Nick.Carr.Jak.cloud.computing.zredefiniuje.IT.html, odczyt 20 kwietnia 2012 r.

[2] Na podstawie: Nicholas Carr, *The big switch*, W.W. Norton & Company, Nowy Jork, Londyn 2008 r.

na dogłębną analizę konkretnego systemu prawnego, gdyż mają one charakter uniwersalny. W celu lepszego zrozumienia istoty omawianych problemów, częstym punktem odniesienia będzie jednak prawo Unii Europejskiej oraz prawo polskie. Należy również wskazać, że w pracy zostaną przestawione tylko niektóre, choć wydaje się, iż najbardziej istotne problemy prawne.

Niewątpliwą trudnością przy przeprowadzaniu analizy dotyczącej zagadnień prawnych w modelu Cloud Computing, będzie brak polskich publikacji o charakterze naukowym. Taki stan rzeczy może dziwić, ponieważ zasoby polskiego Internetu pełne są wielu interesujących opracowań w tym przedmiocie, autorstwa informatyków, ale również prawników. Świadczy to tym, że Cloud Computing nie jest w Polsce pojęciem niszowym.

Jednak na chwilę obecną, konieczne jest sięgnięcie do licznych naukowych publikacji anglojęzycznych oraz źródeł internetowych. Wynikną z tego dwie podstawowe trudności. Pierwsza ma charakter *stricte* techniczny. W wielu miejscach konieczne będzie posługiwanie się słownictwem angielskim, które nie zawsze znajdzie właściwe tłumaczenie w języku polskim (doskonałym przykładem jest samo wyrażenie Cloud Computing i jego odpowiednik w języku polskim- chmura obliczeniowa[3], które – jak się może wydawać- zbyt duży nacisk kładzie na aspekt techniczny, a zbyt mały na aspekt biznesowy. Ze względu na powszechne użycie, znajdzie ono jednak zastosowanie w niniejszej pracy). Ze względu na fakt, że powszechnie przyjmuje się, iż język angielski jest językiem nowych technologii, należy taką sytuację zaakceptować. Druga trudność, o charakterze merytorycznym, sprowadza się do konieczności poszukiwania odpowiedników wskazanych w zagranicznych publikacjach instytucji prawnych. To często może wywoływać zawiłości interpretacyjne.

W pierwszej części pracy zostanie podjęta próba wyjaśnienia istoty Cloud Computing, co jest niezbędnym wstępem do analizy prawnej. Na dalszym etapie zostaną przedstawione główne problemy prawne dotyczące tego modelu świadczenia usług IT powstające na gruncie prawa ochrony danych osobowych, prawa autorskiego oraz prawa międzynarodowego prywatnego. W ostatniej części (rozdział V) zostaną wskazane charakterystyczne klauzule w kontraktach na usługi Cloud Computing.

[3] Można również spotkać się z innym wyrażeniem „przetwarzanie w chmurze".

Rozdział 1. Cloud Computing – charakterystyka, definicje

1.1 Źródła i istota chmury obliczeniowej

Zagadnienia związane z Cloud Computing są w ostatnim czasie przedmiotem rozważań informatyków, prawników, publicystów. Pierwsi, widzą w Cloud Computing przede wszystkim technologicznie zaawansowany sposób rozpowszechniania swoich narzędzi informatycznych. Prawnik będzie rozpatrywał chmurę obliczeniową, jako nowy sposób świadczenia usług za pośrednictwem Internetu. Z tego względu, konieczna staje się dla niego redefinicja niektórych- dotychczas stosowanych- klauzul umownych, szczególnie w zakresie bezpieczeństwa i ochrony danych, ale także prawa autorskiego. Publicysta będzie upatrywał w Cloud Computing przede wszystkim szansę rozwoju technologicznego kraju w różnych obszarach tj. służba zdrowia, administracja publiczna[4], lub jako sposób na pobudzanie wzrostu gospodarczego[5]. W niniejszej pracy zostanie położony nacisk na kwestie prawne. Analiza w tym zakresie nie będzie jednak możliwa bez zrozumienia podstaw Cloud Computing. Warto przyjrzeć się źródłom świadczenia usług w tym modelu. W dalszej kolejności przedstawione zostaną podstawowe definicje.

Cloud Computing jest rezultatem lub, jak niektórzy podkreślają, zaledwie kolejnym etapem ewolucji technologicznej w dziedzinie IT. Autorzy książki *„Cloud Security and Privacy"* zauważają, że Cloud Computing jest kombinacją wielu technologii. Każda z nich przechodziła inną ścieżkę rozwoju i z tego względu nie można traktować ich jako całości, choć wszystkie tworzą dla Cloud Computing zaplecze technologiczne[6]. Chmura obliczeniowa jest możliwa dzięki temu, że dokonał się rozwój zarówno sprzętu komputerowego (*hardware*), połączeń internetowych czy w zakresie rodzajów usług świadczonych przez dostawców (ISP- *Internet Service Provider*). Mówiąc o sprzęcie komputerowym, należy odnotować nieprzerwany postęp, który miał swój początek w latach sześćdziesiątych XX w. Komputery typu *mainframe*[7] zostały zastąpione przez komputery osobiste (PC), które obecnie

[4] Barbara Mejssner, *Długa droga administracji publicznej do chmury*, Cyfrowa Polska, 22.05.2011 r., http://komputerwfirmie.gazeta.pl/itbiznes/1,59368,9642450,Dluga_droga_administracji_publicznej_do_chmury.html, odczyt 25.03.2012 r.

[5] Aleksandra Stanisławska, *Branża IT napędzi wzrost gospodarczy w naszym regionie*, http://www.ekonomia24.pl/artykul/769821-Branza-IT-napedzi-wzrost-gospodarczy-w-naszym-regionie.html, 14.12.2011, odczyt 25 marca 2012 r.

[6] Tim Mather, Subra Kumaraswamy, Shahed Latif, *Cloud Security and Privacy*, O'Reilly Media, 2009r. , wyd. I., str. 2.

[7] Informatyczny słownik angielsko- polski dostępny na stronie www.idg.pl definiuje komputery typu mainframe za Networld.pl jako *„wielodostępny system komputerowy przeznaczony do zarządzania dużą ilością danych i przetwarzania. Są to komputery o znacznej mocy obliczeniowej zwykle instalowane w dużych firmach,*

ustępują już miejsca urządzeniom mobilnym[8]. Rozwój tych, tak zwanych „*thin clients*"[9] niewątpliwie przyczynił się do upowszechnienia Cloud Computing. Użytkownik tabletów, czy smartfonów oczekuje bowiem, że usługi, z których korzysta za pośrednictwem Internetu, będą dostępne z każdego miejsca, na żądanie. Tego rodzaju udogodnienia nie byłyby możliwe, gdyby nie ulepszenia technologiczne w zakresie połączeń z Internetem. Rosnąca przepustowość łączy i rozwój szerokopasmowego Internetu sprawiły, że urządzenia mobline stają się podstawowym środkiem dostępu do technologii IT przez przedsiębiorców i klientów indywidualnych[10]. W ostatnich latach, można również zaobserwować przyrost zdolności sprzętów w zakresie mocy obliczeniowej (wyrażanej w jednostkach FLOPS)[11]. Nie bez wpływu na rozwój chmury obliczeniowej jest także unowocześnianie centrów danych. To bowiem na nich- jak podkreślają Arthur Mateos i Jothy Rosenberg- oparte jest bezpieczne i niezawodne przetwarzanie danych oraz skalowanie[12]. Wyzwaniem dla tych centrów są przede wszystkim kwestie fizycznego i logicznego bezpieczeństwa[13].

Także sposób organizacji przetwarzania danych znacznie się w ostatnich latach zmienił. W pierwszym chronologicznie modelu przetwarzania tj. klient- serwer, system klienta wysyłał żądanie na serwer, a odpowiedź otrzymywał za pośrednictwem sieci[14]. Kolejnym etapem był *grid computing* tj. technika polegająca na łączeniu mocy obliczeniowej różnych systemów w wirtualny superkomputer przy wykorzystaniu nieużywanych zasobów sieciowych[15]. *Grid computing* bywa mylone z późniejszą techniką, *utility computing*. O ile jednak w przypadku *grid computing*, wiele komputerów było zaangażowanych równocześnie do rozwiązania jednego problemu, to przy *utility*- dzięki zastosowaniu wirtualizacji- pracę wykonywała już tylko jedna maszyna, na której umieszczono kilka serwerów. Rozliczenie następuje tu już w modelu biznesowym, tj. za rzeczywiste zużycie[16]. Cloud Computing to model wykazujący wiele podobieństw do *ulitlity computing* z tą różnicą, że usługi *utility* są bardziej spersonalizowane i prostsze do zdefiniowania w umowach. Dostawca może tu

---

uniwersytetach (…), mogą mieć setki a nawet tysiące użytkowników", w: http://www.idg.pl/slownik/termin/33330/mainframe.html, odczyt 25.03.2012 r.

[8] Anthony Velte, Toby Velte, Robert Elsenpeter, *Cloud Computing. A Practical Approach*, wyd. MCGraw-Hill Companies, 2010, s.6-7.

[9] *Thin client* to komputer, który nie posiada dysku twardego, gdyż wszystkie operacje wykonują za niego serwery, Ibidem.

[10] T. (red.), Ibidem, s. 13.

[11] Arthur Mateos , Jothy Rosenberg, *Chmura obliczeniowa. Rozwiązania dla biznesu*, Helion S.A, 2011r., s.37.

[12] Ibidem, s.48.

[13] Ibidem

[14] Ibidem.

[15] Józef Muszyński, *Grid Computing a problem zarządzania*, 2.07.2002 r., http://www.networld.pl/news/43047/Grid.computing.a.problem.zarzadzania.html, odczyt 25.03. 2012 r.

[16] J. Muszyński, *Układanka z chmur*, 24 maja 2011 r., http://www.networld.pl/artykuly/361587_2/Ukladanka.z.chmur.html, odczyt 25.03. 2012 r.

dokładnie określić miejsce przechowywania danych i maszynę, która je przetwarza. Provider usług Cloud Computing, ze względu na rozproszenie platform, gdzie dokonywane są procesy obliczeniowe, takich gwarancji dać nie może[17].

Autorzy publikacji „*Cloud Security and Privacy"* zauważają, że chmura obliczeniowa jest kolejnym elementem w ewolucji modelów dostarczanych usług i określają ją jako ISP 5.0[18]. Historycznie pierwszą usługą świadczoną przez dostawców była poczta elektroniczna oraz możliwość przechowywania danych na udostępnianych przez nich serwerach. Na dalszym etapie zaczęto udostępniać infrastrukturę, a niedługo później zaoferowano gotowe aplikacje (od tego momentu mowa już o nowym typie ISP tj. dostawcach aplikacji- *Applications Service Providers* –ASP). Cloud Computing to zatem kolejna wersja usług świadczonych przez ASP. Różnica leży jednak w tym, że ASP gwarantują klientom dedykowaną instancję aplikacji uruchomioną na serwerze. Zamiast tego, dostawcy usług Cloud Computing (w szczególności w modelu *Software as a Service*) oferują zasoby tej samej, wspólnej (zatem nie dzielonej) infrastruktury dla wielu użytkowników jednocześnie[19].

Poczta elektroniczna oraz hosting stron WWW pozostają dziś niezmiennie najczęściej wybieranymi spośród usług Cloud Computing. Jak zaznaczono, poczta elektroniczna, czy przechowywanie danych na serwisach internetowych, nie jest niczym nowym[20]. Pojawia się zatem pytanie, czym wyróżnia się Cloud Computing i dlaczego z popularyzacją tych usług mamy do czynienia właśnie dzisiaj? Przyjmuje się, że w erę Cloud Computing branża IT wkroczyła w połowie pierwszej dekady XXI wieku. Wtedy to, zasoby centrów danych zaczęły być dostępne na żądanie. W 2007 r. Amazon uruchomił pierwszą usługę w chmurze i od tego czasu zainteresowanie zaczęło wzrastać[21]. Renzo Marchini zauważa, iż popularyzacja chmury jest związana przede wszystkim z rosnącymi potrzebami klientów oraz z atrakcyjną dla nich formą rozliczania, która idealnie wpisuje się w tendencję do minimalizacji kosztów utrzymania IT[22].

Biorąc od uwagę powyższe dywagacje należy stwierdzić, że Cloud Computing warto – z jednej strony- traktować jako osobliwy model świadczenia usług IT, a z drugiej nie można rozpatrywać go w oderwaniu od dotychczasowych sposobów dystrybucji, gdyż wiele

[17] Marcin Marciniak, *Bliższe niż chmura,* www.computerworld.pl, 6.10. 2009 r., http://www.computerworld.pl/artykuly/350736_4/Blizsze.niz.chmura.html, odczyt 25.03.2012 r.
[18] T. Mather (red.), Ibidem, s.3.
[19] Ibidem.
[20] M. Marciniak, *Chmurę już mamy, ale jej nie widzimy*, www.computerworld.pl, 6.03.2012 r., http://www.computerworld.pl/artykuly/380852/Chmure.juz.mamy.ale.jej.nie.widzimy.html, odczyt 25.03. 2012 r.
[21] A. Mateos, J. Rosenberg, Ibidem, s.34.
[22] Renzo Marchini, *A practical Introduction to the Legal Issues*, British Standards Institution 2010, s. 4.

istotnych elementów zostało z nich zaczerpniętych. Osobliwość chmury obliczeniowej może być wykazana przede wszystkim przez wskazanie cech charakterystycznych. W dalszej części zostanie dokonany przegląd przykładowych definicji oraz opis kluczowych atrybutów określających chmurę.

1.2. Definicje

Różnorodność modeli dostarczania usług oraz ich eksploatacji, a także fakt, iż wiele elementów charakterystycznych zaczerpnięto z innych usług IT, zdecydowanie utrudnia podanie precyzyjnej definicji Cloud Computing. Z tego względu, często opisuje się ten model poprzez wskazanie cech charakterystycznych. W tej części zostaną przedstawione różne sposoby wyjaśnienia pojęcia przedstawione przez autorów publikacji dotyczących chmury obliczeniowej.

W 2009 r. eksperci Narodowego Instytutu Standaryzacji i Technologii w USA opracowali często cytowaną w literaturze definicję. Zgodnie a nią, Cloud Computing jest modelem umożliwiającym wszechobecny, wygodny i możliwy na żądanie dostęp za pośrednictwem sieci do dzielonych zasobów obliczeniowych (tj. sieć, serwery, pamięć masowa, aplikacje i usługi), które mogą być szybko zapewnione 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 modele eksploatacji[23]. Modele dostarczania i rozpowszechniania usług zostaną omówione w dalszej kolejności. W tym miejscu należy zwrócić uwagę na cechy charakterystyczne, o których wspomina definicja. Są to: samoobsługa na żądanie (klient może zapewnić sobie nowe zasoby obliczeniowe, kiedy tylko ich potrzebuje bez konieczności kontaktu z dostawcą usługi), nieograniczony dostęp do sieci (dostęp do wszystkich udogodnień możliwy jest przez urządzenia z dostępem do Internetu), pula zasobów (zasoby są gromadzone i dzielone między wielu użytkowników jednocześnie tj. wielodzierżawa [ang: *multitenancy*]), szybka elastyczność (zasoby są elastycznie zapewniane i uwalniane w zależności od potrzeb), mierzalność usługi (zakres i intensywność korzystania z danej usługi musi być na bieżąco monitorowana)[24].

[23] Peter Mell, Thimoty Grance, *The NIST definition of Cloud Computing*, US. Department of Commerce, wrzesień 2011 r., odczyt 25.03.2012 r.
[24] The NIST definition of Cloud Computing, Ibidem.

Cloud Computing jako swoistą konstrukcję pozwalającą na dostęp do aplikacji z innego miejsca niż to, gdzie znajduje się *hardware* użytkownika, definiują autorzy publikacji „*Cloud Computing a Practical Approach"*[25]. Istota Cloud Computing sprowadza się według nich do tego, że podmiot trzeci gospodaruje aplikacją, która dotychczas musiała być instalowana na dysku twardym z nośnika CD czy DVD i w analogiczny sposób aktualizowana[26]. Inni autorzy- Arthur Mateos i Jothy Rosenberg wyjaśniają, że Cloud Computing to *„usługi obliczeniowe oferowane przez zewnętrzne podmioty i dostępne na życzenie w dowolnym momencie, skalujące się dynamicznie w odpowiedzi na zapotrzebowanie"*[27]. Zwracają dalej uwagę na ekonomiczny aspekt tego modelu. Ich zdaniem, Cloud Computing to nowe podejście do zasad wytwarzania systemów informatycznych, zarządzania nimi i ich obsługi, które dzięki swoim właściwościom, daje szansę na uzyskanie większych przychodów i większej elastyczności produktu.

Renzo Marchini w książce „*Cloud Computing. A practical Introduction to the legal issues*" wyjaśnia, że Cloud Computing to dostarczanie możliwości, zdolności komputerowych zdalnie, przez dostawcę bez konieczności instalacji oprogramowania (SaaS) lub infrastruktury (IaaS) w sieci klienta[28].Według niego, podanie ścisłej definicji jest trudne, dlatego należy wyróżnić zespół cech oddających istotę omawianego pojęcia. Zaliczył do nich: brak wymogu instalacji oprogramowania w sieci klienta, używanie oprogramowania zarządzanego przez dostawcę na serwerach przez niego kontrolowanych lub na rzecz dostawcy, opłata tylko za konkretne użycie, odpowiedzialność dostawcy za aktualizacje, bezpieczeństwo danych i zarządzanie sprzętem[29].

Zdefiniowanie Cloud Computing przez wskazanie najbardziej istotnych cech zaproponowali również autorzy „*Open Cloud Manifesto"* tj. zestawu zasad, które wskazują standardy zachowań w chmurze[30]. Według nich, Cloud Computing można scharakteryzować jako model zapewniający zdolność skalowania i dynamicznego zapewniania mocy obliczeniowej w sposób pozwalający ograniczyć koszty oraz dający klientowi (użytkownik końcowy, dział IT, organizacja) możliwość pełnego korzystania z udogodnień, bez konieczności zarządzania skomplikowaną technologią. Na podstawie tego opisu, skonstruowali cztery najważniejsze założenia Cloud Computing: skalowalność na żądanie

[25] A. Velte (red.), s. 4.
[26] Ibidem, s.5.
[27] A. Mateos, J. Rosenberg, Ibidem, s. 26.
[28] R. Marchini, Ibidem, s.4.
[29] Ibidem.
[30] *Open Cloud Manifesto* został sygnowany przez kilkadziesiąt firm świadczących usługi Cloud Computing w 2009 r. min. IBM, Hewlett Packard, Hitachi. Manifest dostępny jest na stronie internetowej: http://opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf, odczyt 27 marca 2012 r.

(dostosowanie zasobów obliczeniowych do potrzeb danej organizacji), uproszczenie centrów danych (klient może uprościć działanie swoich centrów danych przez skorzystanie z technologii Cloud wewnątrz organizacji lub dokonując transferu danych na zewnątrz, bez konieczności zakupu *hardware* i *software*), doskonalenie procesów biznesowych (rozwiązania w chmurze dają możliwość poświęcenia większej uwagi na działaniu organizacji, niż kwestiom organizacyjnym), minimalizacja kosztów początkowych (wybór rozwiązania Cloud Computing pozwala zaoszczędzić na zakupie całej infrastruktury niezbędnej do rozpoczęcia działalności)[31].

Wyróżnia się trzy zasadnicze sposoby implementacji rozwiązań Coud Computing: obliczenia w chmurze (*compute cloud*), przechowywanie w chmurze (*storage cloud*) oraz aplikacje w chmurze (*cloud applications*)[32]. Najczęściej wybieraną usługą jest ta, gdzie świadczenie polega na przechowywaniu danych. Klient korzysta tu z udostępnionej na zewnętrznych dyskach przestrzeni, na którą przenosi swoje dane. Największą zaletą tej usługi (i równocześnie tym, co definitywnie odróżnia tę usługę w chmurze od innych podobnych) jest sposób rozliczania. Odbiorca nie musi opłacać korzystania z całej infrastruktury, a tylko za transfer danych i ich przechowanie. Na rynku jest wielu dostawców *storage cloud* np. Google (*Google Apps, You Tube*), *Facebook, My Space* umożliwiające użytkownikom umieszczanie zdjęć oraz innych danych. Przy wyborze dostawcy takich usług, ważne jest zwrócenie szczególnej uwagi min. na kwestie bezpieczeństwa, kwestie fizycznej lokalizacji danych oraz możliwości dostępu do wykazu logowania[33].

Obliczenia w chmurze (*compute cloud*) to usługa oferowana min. przez *Amazon* (EC2) czy *Google* (*Google App Engine*). Pozwala ona na dostęp na żądanie do własnych aplikacji utrzymywanych przez providera na jego platformie, przy użyciu specjalnego kodu[34]. Taka usługa będzie właściwa dla modelu IaaS (*Infrastructure as a Servive*). Oprogramowanie jako usługa (SaaS) będzie natomiast oferować to, co określa się pojęciem *aplikacje w chmurze*. Warto w tym miejscu zauważyć, że w każdym modelu dostarczania mogą być obecne różne świadczenia charakterystyczne np. dostawca SaaS może oferować zarówno usługę korzystania z aplikacji, która jednocześnie daje możliwość przechowywania danych np. *Gmail.*

[31] Ibidem.
[32] A. Velte (red.), Ibidem, s. 25.
[33] Andrzej Maciejewski, *Fakty i mity o cloud computing*, 14.09.2010 r., http://www.computerworld.pl/artykuly/361854/Fakty.i.mity.o.cloud.computing.html, odczyt 20.04. 2012 r.
[34] A. Velte (red.), Ibidem.

Z zaprezentowanych definicji i wyróżnionych atrybutów wyłania się obraz Cloud Computing jako modelu świadczenia usług IT, który daje użytkownikowi możliwość korzystania z zasobów obliczeniowych w dowolnym miejscu i dowolnym czasie. Klient ma tu dostęp zarówno do aplikacji bez konieczności ich instalacji, jak i infrastruktury, na którą dokonuje transferu gotowych lub stworzonych przez siebie programów. Co jednak najbardziej istotne, płaci jedynie za tyle, ile rzeczywiście używa (model *pay-as-you-go* tj. płacisz za ile korzystasz) zazwyczaj w modelu abonamentowym (subskrypcyjnym). Usługi w chmurze obliczeniowej, dzięki możliwościom jakie daje skalowanie i wielodzierżawa, są elastyczne i dostosowane do zmieniających się potrzeb klientów. Klient nie musi inwestować w *hardware* i *software*, gdyż są one gwarantowane przez providera, który odpowiada za utrzymanie i bezpieczne funkcjonowanie całej infrastruktury. Cloud Computing będzie się zatem różnił od innych modeli outsourcingu IT. Na przykład, od *grid computing* chmura odróżnia się sposobem skalowania (*grid computing* w razie zmiany zapotrzebowania zakłada dołożenie nowego serwera, w Cloud Computing instancje są uwalniane dynamicznie)[35]. Cloud Computing jest również czymś innym niż model klient- serwer. Obliczenia w chmurze mogą odbywać się tu na komputerze zlokalizowanym gdziekolwiek, dzięki użyciu wirtualnych platform, podczas gdy w modelu klient- serwer komputer jest pojedynczą maszyną możliwą do zlokalizowania[36]. Od *utility computing*, Cloud Computing różni się tym, że może używać rozdzielonych zwirtualizowanych platform zamiast scentralizowanych zasobów obliczeniowych[37]. Pojawiają się również opinie, że usługi Cloud Computing mogą stanowić konkurencję na tradycyjnego outsourcingu. Ich autorzy podkreślają, że istotą outosourcingu jest przekazanie określonego procesu firmie na dłuższy okres czasu. Cloud Computig zakłada natomiast częste rozliczanie - przeważnie w systemie miesięcznym[38]. Ze względu na wskazane atrybuty, należy rozpatrywać chmurę obliczeniową jako nowe rozwiązanie o szczególnych, odmiennych właściwościach.

1.3 Cloud Computing- pojęcia kluczowe

W poprzedniej części przedstawiono próby zdefiniowania Cloud Computing. W tym miejscu, warto przyjrzeć się bliżej pojęciom, które często stosuje się opisując nowy ten model korzystania z IT, a które pozwalają lepiej zrozumieć istotę chmury obliczeniowej.

[35] A. Velte (red.), Ibidem, s.8.
[36] Ronald L. Krutz, Russel Dean Vines, *Cloud Security. A comprehensive Guide to Secure Cloud Computing*, Wiley Publishing INC, 2010, s. 7.
[37] Ibidem.
[38] A. Maciejowski, Ibidem.

Jednym z nich jest wielodzierżawa (o polskim tłumaczeniu tego zwrotu była mowa wyżej). Inne formy korzystania z IT zakładają istnienie pewnych dedykowanych dla pojedynczego użytkownika zasobów. Cloud Computing bazuje na modelu biznesowym, gdzie zasoby (sieć, hosting, aplikacja) dzielone są między wielu klientów równocześnie[39]. Renzo Marchini wyjaśnia, że wielodzierżawa to termin, który opisuje sposób wykorzystywania pojedynczej instancji przez dostawcę do dostarczania usługi do wielu klientów[40]. Ta sama kopia oprogramowania jest zatem uruchamiania przez wielu klientów w tym samym czasie. Kwestia multidzierżawy jest o tyle ważna w przypadku konstruowania umów, że dostawca - ze względu na nieokreśloną- liczbę odbiorców, będzie usiłował maksymalnie ujednolicić wzorzec w taki sposób, by odpowiadał na uniwersalne potrzeby, a przy tym był zgodny z jego celami biznesowymi.

Kolejnym terminem, który niejednokrotnie występuje przy opisie Cloud Computing jest skalowanie. Nie wnikając w kwestie techniczne, można wskazać za Arthurem Mateos' em i Jothy Rosenberg'iem, że „s*kalowalność to zdolność platformy do obsługi zwiększonej liczby użytkowników korzystających z aplikacji"*[41]. Skalowanie natężenia ruchu pozwala na uniknięcie problemów mogących prowadzić do zawieszenia pracy serwisu. Zaleta skalowalności, jaką jest automatyczna obsługa szczytów obciążenia, będzie szczególnie przydatna w sytuacji, gdy firma przewiduje intensyfikację korzystania z serwisu internetowego (np. finał kampanii marketingowej). Dzięki Cloud Computing, nie będzie musiała zgłaszać zapotrzebowania na dodatkowe zasoby, gdyż zostaną jej one przydzielone. Z pojęciem skalowania związane jest inne- elastyczność. Termin ten odnosi się do sytuacji, gdy użytkownicy mogą zwiększać i pomniejszać swoje zasoby obliczeniowe w zależności od potrzeb[42]- gdy zwiększa się obciążenie zasoby są dodawane, a gdy przestają być potrzebne - zostaną usunięte.

Zrozumienie istoty Cloud Computing nie jest możliwe bez przynajmniej zdawkowego wyjaśnienia pojęcia wirtualizacji, gdyż jest ona głównym czynnikiem technologicznym chmury obliczeniowej[43]. Arthur Mateos i Jothy Rosenberg twierdzą, że tylko dzięki wirtualizacji chmura jest opłacalna. Według nich, *„ze wszystkich rewolucyjnych technologii wykorzystywanych w chmurze to wirtualizacja i jej wdrożenie zdecydowały o przyjęciu*

[39] T. Mather, Ibidem, s.8.
[40] R. Marchini, Ibidem, s.8.
[41] A. Mateos, J. Rosenberg, Ibidem, s.30.
[42] T. Mather, Ibidem.
[43] Ibidem.

nowego trendu"[44]. Renzo Marchini tłumaczy ten termin, jako technologię umożliwiającą uruchomienie oprogramowania nie na konkretnym, fizycznym serwerze, ale wirtualnym[45]. Zalety wirtualizacji mogą zilustrować dane wskazujące, iż dzięki niej z dziesięciu komputerów wykorzystujących średnio trzydzieści procent zasobów, można zrobić czterdzieści a ich wykorzystanie zwiększyć do dziewięćdziesięciu procent[46]. Wymiernym rezultatem zastosowania tej technologii są również oszczędności, a także szansa na dzielenie zasobów w taki sposób, by znalazły się tam, gdzie są najbardziej przydatne.

1.4. Modele dostarczania usług w chmurze

Dla dalszych rozważań, elementarne znaczenie będzie miał podział modeli dostarczania usług Cloud Computing ze względu na rodzaj świadczenia. Cechy charakterystyczne każdego z nich, pozwolą bowiem na wyodrębnienie kwestii prawnych, na które należy zwrócić szczególną uwagę przy sporządzaniu umów. NIST wyróżnił trzy podstawowe modele: *Software as a Service* (SaaS) tj. oprogramowanie jako usługa[47], *Platform as a Service* (PaaS) tj. platforma jako usługa oraz *Infrastructure as a Service* (IaaS) tj. infrastruktura jako usługa[48]. Zbiorczym określeniem tych modeli jest skrót SPI (od wyrażeń *Software- Platform- Infrastructure*).

Poniżej zostaną omówione wyróżnione przez NIST modele dostarczania usług w chmurze oraz najbardziej znane przykłady ich zastosowania. Warto dodać, że kolejność omawiania jest zgodna z tą przyjętą przez Instytut. SaaS jest usługą wymagającą najmniej zaangażowania ze strony klienta, za to ciężar działania przerzucony jest na dostawcę. Z kolei IaaS daje użytkownikowi duże pole do aktywności, a rolę providera ogranicza do minimum. Stąd SaaS zostanie omówione w pierwszej kolejności, IaaS jako ostatni. Należy jednak podkreślić, że opisywane modele mają wiele cech wspólnych. Według Renzo Marchini' ego, PaaS to tak naprawdę IaaS z pewną wartością dodaną, którą jest możliwość uruchomienia usługi SaaS[49]. Dalsze rozważania mają na celu przybliżenie tych relacji.

---

[44] A. Mateos, J. Rosenberg, Ibidem, s.29.
[45] R. Marchini, Ibidem, s.8.
[46] Jakub Chabik, *Krótki przewodnik po rozwiązaniach cloud computing,* 10.10.2011 r., http://www.computerworld.pl/artykuly/375893/Krotki.przewodnik.po.rozwiazaniach.cloud.computing.html, odczyt 20.04. 2012 r.
[47] Również bezpieczeństwo jako usługa (*security as a service*). W niniejszej pracy używane będzie jednak znaczenie podstawowe.
[48] The NIST Definition of Cloud Computing, Ibidem.
[49] R. Marchini, Ibidem, s.5.

1.4.1. SaaS

Zgodnie z definicją NIST istotą SaaS jest przyznanie klientowi możliwości używania aplikacji uruchomionej w infrastrukturze Cloud przez dostawcę usługi. Dostęp do aplikacji jest możliwy z dowolnego sprzętu, przy użyciu przeglądarki lub interfejsu programu. Klient nie zarządza i nie kontroluje infrastruktury tj. sieci, serwerów, systemu operacyjnego, *storage* i innych możliwości aplikacji z wyjątkiem ewentualnych uprawnień do konfiguracji[50]. Definicja ta zwraca uwagę na pozycję klienta w usłudze SaaS. Z jednej strony, ma on uprawnienie nieograniczonego korzystania z aplikacji na żądanie, z drugiej nie ma w zasadzie żadnych możliwości ingerowania w infrastrukturę, gdyż nie jest jej właścicielem. W wielu kwestiach będzie zatem uzależniony od dostawcy, którego wybrał. Podkreśla się wiele zalet tego modelu. Sprzedawca posiada kontrolę nad dystrybucją swojego oprogramowania (ograniczona zostaje zatem liczba nielegalnych kopii) oraz ma zagwarantowany stały przychód. Po stronie klienta dochodzi z kolei do redukcji kosztów, które – kupując oprogramowanie w tradycyjny sposób- musiał wydać na drogą licencję, zakup i utrzymanie serwerów i personelu wykwalifikowanego do obsługi infrastruktury[51].

SaaS definiuje się również jako „*model hostingu aplikacji jako usługi do klientów, którzy mają dostęp do Internetu*”[52]. Autorzy tej definicji również wskazują na zalety i wady SaaS. Wśród zalet wymieniają: lepszą gwarancję ochrony własności intelektualnej dla sprzedawcy oraz stały dochód, możliwość dostosowania do potrzeb klienta czy wyższe standardy bezpieczeństwa (zastosowanie protokołu SSL tj. *Secure Socket Layer* jest tu standardem). Mówiąc o wadach wskazują min. na efekt *vendor lock-in* tj. sytuację, gdy niemożliwe jest przeniesienie aplikacji do innego dostawcy (sprzedawcy), gdyż postanowienia umowy pierwotnej w istotny sposób taką możliwość ograniczają[53]. Klient nie będzie mógł zatem dokonać prostego transferu danych, które umieścił w aplikacji lub będzie mógł to uczynić, ale po uiszczeniu dodatkowej opłaty. Według autorów publikacji „*Cloud Computing. A Practical Approach”*, najbardziej istotną różnicą między SaaS a tradycyjnym modelem hostingu aplikacji jest liczba dzierżawców. Zauważają oni również, że tradycyjny model jest „*odizolowany*” i „*jednostkowy*”[54], co oznacza, że tylko jeden klient, po zakupieniu i zainstalowaniu aplikacji na serwerze, może z niej korzystać. SaaS natomiast jest oparty na

[50] NIST Cloud Computing definition Ibidem.
[51] T. Mather, Ibidem, s. 18.
[52] A. Velte (red), Ibidem, s.18.
[53] Ibidem.
[54] Ibidem.

wielodzierżawie, co powoduje, że zaplecze infrastrukturalne dzielone jest między wielu klientów i dla każdego z nich jest unikalne.

Najbardziej znane przykłady SaaS to aplikacje oferowane przez *Google* (*Google Apps, Gmail, Picasa),* czy *Microsoft* (*Hotmail, Windows Live*). SaaS to również takie serwisy jak: *YouTube, Flickr, Facebook* (szczególnie w części, gdzie oferują możliwość przechowywania danych). Prekursorem SaaS jest firma *Salesforce.com* ze swoim systemem zarządzania relacjami z klientami (CRM). Z podstawowej aplikacji CRM dotyczącej zarządzania sprzedażą korzysta obecnie ponad milion użytkowników na całym świecie[55]. W Polsce pierwsze usługi typu SaaS zaoferowała w 2000 r. firma Heuthes w postaci produktu ISOF, czyli programu służącego do kompleksowej obsługi firmy. Rynek SaaS w Polsce wciąż się rozwija. W sektorze małych i średnich przedsiębiorstw działa około sześćdziesięciu dostawców (min. Anica System czy Mis S.A.)[56]. Wśród najchętniej wybieranych aplikacji SaaS można znaleźć te, które służą do zarządzania przedsiębiorstwem, zasobami ludzkimi, oraz księgowością, projektami etc. i- niezmiennie- poczta elektroniczna[57].

Z korzystaniem z SaaS będzie wiązać się kilka problemów prawnych, min.: konieczność zawierania umowy licencyjnej w sytuacji, gdy żaden element oprogramowania nie jest instalowany na sprzęcie klienta, problem wyboru prawa właściwego, kwestie związane z bezpieczeństwem danych użytkownika i jego klientów oaz problem ograniczenia odpowiedzialności dostawcy etc. Zagadnienia te będą przedmiotem dalszych rozważań.

1.4.2. PaaS

Kolejnym modelem świadczenia usług Cloud Computing jest PaaS tj. Platforma jako usługa. Według NIST, PaaS daje klientowi możliwość wdrożenia w infrastrukturę stworzonych przez niego lub gotowych aplikacji, przy użyciu języka i narzędzi gwarantowanych przez dostawcę. Klient nie zarządza i nie kontroluje infrastruktury tj. sieci, serwerów, sytemu operacyjnego, *storage*, ale ma kontrolę nad wdrażaną aplikacją oraz możliwość kontroli nad ustawieniami środowiska, w którym następuje hosting[58]. Wgląd w tę definicję pozwala stwierdzić, że możliwości działania klienta są w przypadku PaaS o wiele

[55] A. Velte (red.), Ibidem, s.59.
[56] Michał Małyszko, *SaaS jako metoda świadczenia e- usług,* Raport Polskiej Agencji Rozwoju Przedsiębiorczości, PARP, Warszawa 2008 r., dostępny na stronie: http://www.web.gov.pl/g2/big/2009_03/c6dfab4e6f795ca260afdc0c04f5f5c7.pdf, odczyt 22 kwietnia 2012 r., odczyt 20.03.2012 r.
[57] Ibidem.
[58] The Nist Definition of Cloud Computing, Ibidem.

wyższe niż w SaaS. Dostawca zaopatruje użytkownika w zestaw niezbędnych narzędzi, które ten może wykorzystać do budowania własnej aplikacji bez konieczności instalowania ich na dysku twardym swojego komputera. Rolą providera jest rozwijanie za pomocą przeglądarki narzędzi służących do tworzenia aplikacji, za co otrzymuje opłatę. Tworzący aplikację (developer) może wdrażać ją bez konieczności posiadania specjalistycznych umiejętności [59].

PaaS jest podobne do SaaS z tą różnicą, że usługą jest tu środowisko do tworzenia aplikacji (platforma rozwojowa), a nie aplikacja jako taka[60]. Podkreśla się, że główną zaletą PaaS jest brak konieczności nabywania przez developerów sprzętu i oprogramowania, gdyż cały cykl życia oprogramowania odbywa się w ramach platformy. Jest to szczególnie ważne dla programistów, dla których barierą dla tworzenia aplikacji były dotychczas koszty początkowe (zakup i utrzymanie sprzętu, oprogramowania)[61]. Mówiąc o wadach PaaS, należy- tak jak w przypadku SaaS- zwrócić szczególną uwagę na zjawisko *vendor lock in*. Stworzenie aplikacji (często o znacznej wartości) na platformie jednego dostawcy będzie zazwyczaj równoznaczne z brakiem możliwości przeniesienia na inną platformę lub z koniecznością uiszczenia wysokiej opłaty[62].

Lista sprzedawców usługi PaaS nie będzie tak rozległa jak w przypadku SaaS ze względu na mniejszy krąg potencjalnie zainteresowanych odbiorców. Pierwszym sprzedawcą tej usługi był również *Salesforce.com* w postaci *force.com*[63]. Obecnie najbardziej znanymi przykładami tych usług są: *Windows Azure* (kwalifikowane zarówno jako PaaS jak i IaaS) oraz *Google – AppEngine*. Arthur Mateos i Jothy Rosenberg twierdzą, iż właśnie Google AppEngine jest *„całkowicie zgodna z definicją platforma jako usługa”*[64].

Zakres problemów prawnych dla PaaS będzie pokrywał się- w większości- z zakresem problemów związanych z korzystaniem z SaaS. Istotną kwestią będzie min. rozstrzygniecie wątpliwości związanych z licencjonowaniem programów tworzonych w ramach dostarczanej infrastruktury (także składającej się z elementów licencjonowanych na zasadzie *open source*).

[59] T. Mather (red.), Ibidem. s.19.
[60] R. Krutz, Ibidem, s.39-40.
[61] Ibidem.
[62] A. Velte (red.), Ibidem, s. 13-14.
[63] Ibidem.
[64] A. Mateos, J. Rosenberg, Ibidem, s. 41.

1.4.3. IaaS

Ostatnim modelem wyróżnionym przez NIST jest Infrastruktura jako usługa tj. IaaS. Zgodnie z definicją Instytutu, IaaS to zapewnienie klientowi możliwości korzystania z przetwarzania, *storage*, sieci i innych podstawowych zasobów obliczeniowych, gdzie klient ma możliwość wdrażania i uruchamiania oprogramowania w tym system operacyjnego i aplikacji. Klient nie zarządza i nie kontroluje infrastruktury cloud, ale ma kontrolę nad systemem operacyjnym, *storage*, wdrożonymi aplikacjami a często także ograniczoną kontrolę nad wybranymi elementami sieci np. firewall[65].

Podkreśla się, że IaaS jest usługą typową jedynie dla Cloud Computing i w sposób najbardziej pełny oddaje różnice z tradycyjnymi infrastrukturami IT[66]. Renzo Marchini zwraca uwagę, iż ideą IaaS jest dostarczanie przez dostawcę *hardware*, stąd inna nazwa HaaS (*Hardware as a Infrastructure*)[67]. Po stronie dostawcy leży odpowiedzialność za wszystkie potrzeby klienta w zakresie przetwarzania: tworzy infrastrukturę, obsługuje momenty szczytu oraz wprowadza nowe funkcjonalności dostosowane do zmieniających się żądań[68]. Dzięki temu, możliwe będzie- tak jak w pozostałych modelach- użytkowanie na zasadzie *pay-per-use*[69]. Obecnie najwięcej usług IaaS oferuje Amazon- Amazon EC2. Innym przykładem tej chmury będzie Microsoft Azure, który- jak zaznaczono- zawiera zarówno elementy PaaS jak i IaaS.

Jak już wspomniano wcześniej, IaaS – zgodnie z klasyfikacją przyjętą przez NIST- jest modelem, który położony jest na przeciwnym biegunie od SaaS. Jest on przeznaczony dla użytkownika, który chce posiadać kontrolę nad oprogramowaniem, ale nie zamierza utrzymywać sprzętu. Klient otrzymuje najmniej w pełni gotowych rozwiązań w porównaniu z innymi modelami[70]. Mówi się o IaaS jako czystej kartce, którą użytkownik może zapisać w dowolny sposób- umieszczając gotowe lub własne aplikacje. W tym drugim przypadku, IaaS ewoluuje w PaaS[71]. Charakterystycznym problemem prawnym dla użytkowników modelu IaaS będzie min. licencjonowanie gotowego oprogramowania umieszczanego w infrastrukturze przez użytkownika.

---

[65] NIST definition of Cloud Computing, Ibidem.
[66] T. Mather (red.), s.22.
[67] R. Marchini, s.5.
[68] T. Mather, Ibidem.
[69] T. Mather (red.), Ibidem.
[70] A. Mateos, J. Rosenberg, Ibidem, s.39.
[71] Jeff Caruso, *Iaas vs. PaaS vs. SaaS* , 2.11.2011 r., http://www.networkworld.com/news/2011/102511-tech-argument-iaas-paas-saas-252357.html, odczyt 22 marca 2012 r.

1.5. Modele eksploatacji chmury

Na koniec rozważań teoretycznych na temat Cloud Computing, należy krótko omówić modele eksploatacji wyżej analizowanych usług. Przyjmując typologię zaproponowaną przez NIST, należy wyróżnić cztery, główne modele rozpowszechniania usług: chmura publiczna, chmura prywatna, chmura publiczna, wspólnotowa i hybrydowa[72]. Każdy model dostarczana może funkcjonować w każdym modelu eksploatacji, choć niektóre połączenia będą bardziej standardowe, np. SaaS działa przede wszystkim w chmurze publicznej[73]. Ponadto, każdy model rozpowszechniania musi być zgodny z elementarnymi zasadami Cloud Computing tj. musi zapewniać dynamiczne skalowanie zasobów, wymaga sprzętu umożliwiającego połączenie z Internetem, a użytkownicy przeważnie nie będą posiadali wpływu na stosowaną przez dostawcę technologię[74]. Organizacja nie musi ograniczać się do jednego tylko modelu. Informacje krytyczne, wymagające szczególnych zabezpieczeń, będą odpowiednie dla chmury prywatnej. Natomiast te, potrzebne tylko do projektów czasowych, mogą być eksploatowane do chmury publicznej[75]. Im bowiem chmura bardziej dostępna dla ogółu, tym większym wyzwaniem będzie zachowanie standardów bezpieczeństwa.

Pierwszorzędne znaczenie będzie miała chmura publiczna i prywatna (często zwane odpowiednio *external* i *internal*[76]*)*, gdyż to w ramach tych modeli eksploatowanych jest najwięcej usług. Chmura *community* oraz hybrydowa będą nosiły mieszane cechy- zarówno chmury prywatnej jak i publicznej.

1.5.1. Chmura publiczna

Według definicji NIST, z chmurą publiczną mamy do czynienia wtedy, gdy infrastruktura jest dostępna dla wszystkich użytkowników lub większej grupy i jest ona własnością organizacji sprzedającej usługi Cloud[77]. Decydując się na ten rodzaj chmury, klient nie musi dbać o koszty związane z zakupem i utrzymaniem serwerów. Jedynym wkładem z jego strony powinno być zapewnienie dostępu do Internetu. Jak podkreślają znawcy tematu, chmura publiczna jest zgodna z tradycyjnym rozumieniem Cloud Computing. Oddaje bowiem wszystkie cechy chmury obliczeniowej: jest obsługiwana i zarządzana przez

[72] NIST definition of Cloud Computing, Ibidem.
[73] R. Krutz (red.), Ibidem, s.33-34.
[74] Ibidem.
[75] Ibidem.
[76] Ibidem.
[77] NIST definition of Cloud Computing, Ibidem.

sprzedawcę lub dostawcę i hostowana do wielu klientów poprzez infrastrukturę[78]. Stąd, chmurze publicznej będzie poświęcona znaczna część rozważań

Przyjmuje się, że niewątpliwą zaletą tego modelu są znaczne oszczędności, które przynosi dzielona infrastruktura, zdalny hosting, dynamiczne licencjonowanie i system zabezpieczeń[79]. Kwestie związane z bezpieczeństwem danych klientów są domeną dostawcy. Brak pewności co do standardów i jakości tych zabezpieczeń będzie często czynnikiem zniechęcającym do korzystania z usług oferowanych w ramach chmury publicznej. Tym, co zachęca, są przede wszystkim koszty. Wiele usług jest darmowych (np. *Gmail* w chmurze publicznej *Google* w swej podstawowej wersji tj. bez niestandardowych wymagań co do pojemności skrzynki jest bezpłatny). Wśród przykładów chmury publicznej można odnaleźć: *Amazon Web Services, Google Apps Engine, Saleforce.com, Microsoft Azure.*

Dla chmury publicznej szczególnie istotne będą kwestie związane z ochroną danych przed niepożądaną ingerencją lub ujawnieniem. Polityka prywatności dostawcy będzie jednym z podstawowych elementów umowy na korzystanie z usług w takiej chmurze. Tym oraz innym postanowieniom (ograniczenie odpowiedzialności dostawcy, możliwość wyprowadzenia danych z chmury) warto przyjrzeć się w dalszej części pracy.

1.5.2. Chmura prywatna

Przeciwieństwem chmury publicznej (*external*) jest chmura prywatna *(internal*). Podstawową różnicą będzie liczebność grupy odbiorców, którym usługa jest oferowana oraz relacje między nimi a dostawcą. NIST zwraca uwagę, że w przypadku chmury prywatnej, infrastruktura jest obsługiwana wyłącznie dla jednej organizacji. Może być zarządzana przez tę organizację lub przez stronę trzecią i może funkcjonować wewnątrz lub na zewnątrz niej[80]. Chmury prywatne są zatem rozwiązaniem przeznaczonym dla biznesu. Jeżeli zatem firma posiada odpowiednią infrastrukturę, to wybór chmury prywatnej może być dla niej rozwiązaniem optymalnym.

Renzo Marchini opisuję *private cloud* jako chmurę wdrażaną bez konieczności korzystania z usług podmiotu trzeciego[81]. Jest to usługa dedykowana, dostarczana przez firmę w postaci oprogramowania lub infrastruktury, z której skorzystać może każdy upoważniony członek danej organizacji[82]. Ciężar odpowiedzialności za procesy zachodzące w tej chmurze

[78] T. Mather, Ibidem, s.23.
[79] Ibidem.
[80] NIST definition of Cloud Computing, Ibidem.
[81] R. Marchini, Ibidem, s.7
[82] Ibidem.

jest przerzucony na klienta[83]. Taka chmura jest hostowana w obrębie posiadanego przez klienta centrum danych oraz obsługiwana przez wewnętrzny departament IT. Zgodnie z definicją NIST, chmura prywatna może być jednak zarządzana przez podmiot zewnętrzny. Taki podmiot jest z organizacją związany klauzulami umownymi, które dotyczą przede wszystkim bezpieczeństwa.

Niejednokrotnie można spotkać się z opinią, że chmura prywatna gwarantuje wyższe standardy bezpieczeństwa. Jest on jednak często kwestionowany. Autorzy takich opinii twierdzą, że chmura prywatna będzie bardziej bezpieczna od publicznej tylko wtedy, gdy zastosowane zostaną niestandardowe środki ochrony[84]. Chmura prywatna będzie przedmiotem zainteresowania raczej większych podmiotów, gdyż początkowe wydatki na infrastrukturę wymagają znacznych inwestycji[85].

1.5.3. Chmura hybrydowa i chmura community

Chmura hybrydowa jest kombinacją wcześniej wymienionych. NIST definiuje ją jako infrastrukturę złożoną z dwóch lub więcej chmur (prywatnych, wspólnotowych lub publicznych). Barrie Sosinsky wskazuje, że chmura hybrydowa jest kombinacją chmur, gdzie składniki zachowują swoje unikalne cechy, ale jednocześnie działają ze sobą jako zespół[86]. Przykładem chmury hybrydowej jest sytuacja, gdzie zwykłe dane organizacji umieszczone są w chmurze publicznej (na przykład poczta), a krytyczne są przesunięte do chmury prywatnej, wewnątrz organizacji[87]. Cechą chmury hybrydowej jest tzw. *cloudburst* tj. zwiększona transmisja zasobów. Jeśli zatem zaistnieje deficyt zasobów wewnętrznych, to obciążenie będzie można skierować na chmurę zewnętrzną[88]. Znanym przykładem chmury hybrydowej jest oferowana przez Amazon funkcjonalność *VM Import*, która daje użytkownikom możliwość transferu obrazów maszyn wirtualnych z lokalnych centrów danych do chmury Amazon[89].

Chmura *community* leży między chmurą publiczną a prywatną. Według NIST z *community cloud* mamy do czynienia, gdy infrastruktura dzielona jest przez kilka

[83] T. Mather (red.), Ibidem, s. 23-24.
[84] R. Krutz (red.), Ibidem, s.38.
[85] Marcin Marciniak, *Cloud Computing bez tajemnic*, Computerworld, 23 czerwca 2009 r., http://www.computerworld.pl/artykuly/346686/Cloud.computing.bez.tajemnic.html, odczyt 24 marca 2012 r.
[86] Barrie Sosinsky, *Cloud Computing Bibble,* Wiley Publishing Inc., Kanada 2011, s. 22.
[87] R. Krutz (red.), Ibidem 46-48.
[88] Monika Kulesza, *Cloudburst a chmura hybrydowa,* 20.04. 2011 r. http://www.computingcloud.pl/pl/cloudprzewodnik/co-nas-czeka-wkrotce/item/349-cloudburst-a-chmura-hybrydowa, odczyt 24.03.2012 r.
[89] Janusz Chustecki, *Hybrydowe chmury obliczeniowe,* , 28.12.2010 r., http://www.networld.pl/news/365574/Hybrydowe.chmury.obliczeniowe.html, odczyt 24 marca 2012 r.

organizacji o wspólnych celach (tj. misja, standardy bezpieczeństwa, polityka). Ich realizacja ma być ułatwiona właśnie ze względu funkcjonowanie wspólnego środowiska Cloud. Taka chmura może być zarządzana przez organizacje lub podmiot trzeci oraz może funkcjonować wewnętrznie lub na zewnątrz[90]. Przykładem tej chmury jest min. *Automotive Composites Consortium* stworzone przez *Chrysler, Ford i General Motors* w celu prowadzenia programów badawczych nad wykorzystaniem komponentów polimerowych dla wykorzystania istniejących zasobów i zwiększenia konkurencyjności[91].

[90] NIST definition of Cloud Computing, Ibidem.
[91] Srinivasan Sundra Rajan**,** *The importance of community clouds*, 24.04. 2011 r., http://cloudcomputing.sys-con.com/node/1803698, odczyt 24.03.2012 r.

Rozdział 2. Bezpieczeństwo i ochrona danych użytkowników w chmurze obliczeniowej

2.1. Problemy podstawowe

Już z definicji Cloud Computing wynika, że usługi w ten sposób oferowane dają możliwość dostępu do zasobów z każdego miejsca i w każdej chwili przez wielu użytkowników równocześnie. Wirtualizacja, wielodzerżawa, skalowalność- te cechy chmury obliczeniowej wyjaśnione w poprzedniej części - będą źródłem wielu komplikacji w sferze zachowania odpowiednich, zgodnych z wymaganiami użytkowników standardów bezpieczeństwa. Dla klientów nie ma bowiem obecnie czynnika bardziej zniechęcającego do korzystania z usług Cloud Computing, niż wątpliwa polityka bezpieczeństwa i prywatności dostawców, która naraża ich dane (często niezwykle istotne) na wyciek.

Krytycy Cloud Computing często podkreślają, że ten model dostarczania usług IT powoduje znaczne ryzyko dla prywatności i bezpieczeństwa danych osobowych. Dla prawników Cloud Computing jest niczym innym, jak tylko transferem danych, który powoduje utratę kontroli[92]. Bywają jednak tacy obserwatorzy, którzy uważają, że transfer i utrzymywanie danych w chmurze obliczeniowej może być relatywnie bardziej bezpieczne, niż pozostawienie ich w wewnętrznym centrum danych[93]. Lotar Determann w artykule "*Data Privacy in the Cloud: Dozen Myths and Facts"* wskazuje na dwanaście często powtarzanych twierdzeń na temat bezpieczeństwa i prywatności Cloud Computing, które jego zdaniem nie są prawdziwe. Uważa on, że nie ma podstaw do twierdzenia, że chmura jest bardziej ryzykowna dla prywatności niż inne modele świadczenia usług IT z tego względu, że wszystkie bazują na Internecie, który powstał na fundamencie zdecentralizowanego transferu danych. Według tego autora, Cloud Computing nie niesie żadnych nowych wyzwań dla prywatności, nie dochodzi tu do przetwarzania większej ilości danych, a dostawcy mogą oferować wyższe niż dotychczas standardy bezpieczeństwa.

Wydaje się, że o ile można zgodzić się z tym autorem co do tezy, że sam transfer danych do środowiska Cloud nie musi automatycznie generować zwiększonego ryzyka dla danych użytkowników, to już trudno przystać na twierdzenie, że rozwój chmury nie niesie nowych wyzwań dla prywatności i bezpieczeństwa. Wystarczy bowiem wskazać na wielodzierżawę. W innych modelach ograniczona liczba użytkowników może korzystać

[92] Lothar Determann, *Data Privacy in the Cloud: Dozen Myths and Facts*, The Computer& Internet Lawyer, tom 28, nr 11, listopad 2011 r.
[93] A. Mateos, J. Rosenberg, Ibidem, s. 102-103.

z jednej aplikacji. W przypadku Cloud Computing, dzięki wirtualizacji, wiele osób w tym samym czasie używa zasobów. Z racji tego, że użytkownicy nie mają informacji na temat współdzierżawców, ryzyko niekontrolowanego dzielenia się danymi niewątpliwie wzrasta[94].

Według Arthura Mateos'a i Jothy Rosenberg'a, to właśnie kwestie bezpieczeństwa hamują ekspansję chmury. Na potwierdzenie tej tezy wskazują dane, w których ponad siedemdziesiąt procent klientów firm informatycznych uważa, że kwestie bezpieczeństwa stanowią główną przeszkodę dla korzystania z usług Cloud Computing[95]. Także Renzo Marchini uważa, że bezpieczeństwo będzie podstawowym czynnikiem konkurencyjności na rynku usług Cloud Computing[96]. Firmy oferujące usługi w chmurze muszą mieć te opinie i przywołane dane na uwadze, gdyż wprowadzają coraz wyższe standardy bezpieczeństwa. Władze państwowe mobilizują dostawców od strony prawnej, wprowadzając - często restrykcyjne - wymogi co do gromadzenia, przechowywania i przetwarzania danych. Przykładem takiego działania jest Dyrektywa Unii Europejskiej 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Ze względu na to, że kwestie zachowania odpowiednich standardów bezpieczeństwa przez dostawcę są niewątpliwie powiązane z zagadnieniem ochrony danych i informacji na temat użytkowników (luka w systemie zabezpieczeń może bowiem prowadzić do nieuprawnionego wycieku danych ważnych dla klienta), zostaną one w tym rozdziale omówione łącznie. Pierwsza część będzie dotyczyć podstawowych zasad funkcjonowania systemu zabezpieczeń stosowanych przez usługodawców (jednak bez szczegółowej analizy kwestii technicznych). Na dalszym etapie, zostaną omówione elementarne kwestie związane z ochroną danych osobowych przez dostawców Cloud Computing- podstawowe pojęcia oraz problemy związane z przetwarzaniem danych.

2.2. Bezpieczeństwo

Wybór dostawcy będzie wiązał się z outsourcingiem kwestii związanych z bezpieczeństwem. Tym samym, użytkownik w znacznym stopniu traci kontrolę nad swoimi danymi. Często jednak potrzeba ograniczenia kosztów będzie czynnikiem determinującym i kwestie bezpieczeństwa zostaną przez klientów odsunięte na drugi plan. Jak zgodnie podkreślają autorzy publikacji dotyczących bezpieczeństwa w chmurze, dokładna analiza

[94] Józef Muszyński, *Bezpieczeństwo w chmurze*, Computerworld.pl, 10.02. 2012 r., http://www.networld.pl/artykuly/376996_1/Bezpieczenstwo.w.chmurze.html, odczyt 3.04. 2012 r.
[95] A. Mateos, J. Rosenberg za IDC, Ibidem, s. 103-104.
[96] R. Marchini, Ibidem, s. 21.

polityki bezpieczeństwa dostawcy jest podstawowym obowiązkiem podmiotu poszukującego ofert firm świadczących usługi Cloud Computing[97].

W ogólnym zarysie można stwierdzić, że źródłem problemu związanych z bezpieczeństwem jest fakt, że dane usługobiorców znajdują się w zewnętrznej pamięci masowej. Podstawowym ryzykiem związanym z taką sytuacją, jest nieodpowiednie zarządzanie systemem mogące doprowadzić do niekontrolowanego udostępnienia danych (ryzyko wewnętrzne) a także ataki hakerów (ryzyko zewnętrzne)[98]. Ponieważ infrastruktura jest współdzielona, coraz częściej pojawiają się próby przejęcia danych przez współużytkowników poprzez rozpoznawanie adresu IP i zasobów komputerowych oraz przeszukiwanie danych po zwolnieniu zasobów przez innych użytkowników. Problemem jest także kwestia uwierzytelniania tak dużej ilości klientów[99]. Ponadto, w środowisku Cloud Computing większość serwerów udostępnianych jest przez Internet. Taka sytuacja wymusza weryfikację podejścia do bezpieczeństwa także w zakresie poszerzania wiedzy na temat podstaw funkcjonowania infrastruktury.

Najpoważniejsze ryzyko związane z bezpieczeństwem dotyczy chmury publicznej i modelu SaaS (w przypadku IaaS, często - tak np. Amazon EC2 - zapewniane jest bezpieczeństwo fizyczne, środowiskowe oraz bezpieczeństwo wirtualizacji, ale nie gwarantuje się już bezpieczeństwa wirtualnych instancji, systemów operacyjnych i danych[100]). Usługi oferowane w tym modelu zakładają bowiem całkowitą kontrolę providera nad elementami infrastruktury, w tym nad bezpieczeństwem[101]. Renzo Marchini przywołuje kilka przykładów spektakularnych naruszeń bezpieczeństwa dotyczących największych dostawców usług Cloud Computing w chmurze publicznej. Jednym z nich jest sprawa *Gmail'a*. 24 lutego 2009 r. usługa poczty *Google* nie była aktywna przez ponad dwie godziny, co miało wpływ na sto milionów użytkowników na całym świecie, którzy nie mogli w tym czasie korzystać ze swojego konta (tu pojawia się również problem gwarancji dostępności usługi, który jest elementem umowy, głównie w części dotyczącej zapewnienia poziomu usług, tzw. SLA- będzie o tym mowa w dalszej części). Przyczyną awarii były rutynowe prace konserwacyjne serwerów w Europie. Innym przykładem- także dotyczącym *Google*- jest problem z marca 2009 r. Dokumenty stworzone w ramach usługi *Google Docs*, zostały udostępnione bez wiedzy użytkowników i oznaczone jako „wspólne", co dawało innym

[97] Tak min. R. Marchini, Ibidem.
[98] J. Muszyński, Ibidem.
[99] Ibidem.
[100] Ibidem.
[101] R. Krutz (red.), Ibidem, s.62.

możliwość edycji. Także *Windows Live Hotmail* miał kłopot z wyciekiem danych. W 2009 r. dane użytkowników i hasła zostały przekierowane na stronę innego podmiotu[102]. Zważając na powyższe przykłady powstaje pytanie, w jaki sposób dostawcy chronią się przed podobnymi sytuacjami?

Przede wszystkim należy wskazać, że dostawcy usług Cloud Computing muszą jednakowo dbać zarówno o bezpieczeństwo zewnętrzne (bezpieczeństwo centrów danych) jak i wewnętrzne (logiczne) tj. bezpieczeństwo sieci (np. technologie *firewall* i możliwość dostępu do danych przez pracowników dostawcy), bezpieczeństwo serwerów (sposób w jaki serwery są zabezpieczone przed atakami), sposób gromadzenia danych (np. uwierzytelnienie użytkowników), szyfrowanie danych, *back- up* (tj. jak często tworzone są kopie zapasowe) [103]. Mimo, że elementy te mają charakter ściśle techniczny, to ich zbadanie powinno być dla odbiorcy priorytetem, nawet jeśli wymaga to zaangażowania ekspertów. Arthur Mateos i Jothy Rosenberg porównują sposób fizycznego zabezpieczenia (na przykładzie *Salesforce)* do „ufortyfikowanych bunkrów"[104]. Wskazują, że firma ta (podobnie zresztą *Google* czy *Amazon*) prowadzi całodobowe patrole, posiada pięć poziomów biometrycznych skanerów a także fizyczne pułapki. Centra danych mieszczą się w zakamuflowanych budynkach (często na osiedlach mieszkalnych). Kontrola osób uzyskujących dostęp do usługi również jest zaawansowana i odbywa się min przez weryfikację tożsamości min. przez telefon, poświadczenia i logowanie, klucze dostępowe, certyfikaty X.509[105].

Renzo Marchini wskazuje na pewien elementarny zestaw pytań, które usługobiorca powinien skierować do wybranego dostawcy usług. Przede wszystkim powinien upewnić się: kto jest właścicielem oraz kto kontroluje infrastrukturę, jaki jest dokładny model rozpowszechniania i dostarczania usługi Cloud, gdzie ulokowane są elementy infrastruktury, jak zbudowana jest architektura usługi, jak wygląda kontrola bezpieczeństwa oraz kwestie raportowania o stanie wykonanych usług[106].

Większą pewność klient uzyskuje, kiedy standardy bezpieczeństwa są mierzone przez stronę trzecią, szczególnie odpowiednio akredytowaną. Uzyskanie certyfikatu daje stronom dużą pewność- provider może podnosić fakt uzyskania certyfikatu w sporach sądowych, gdzie zarzuca się mu np. brak dochowania wymogów technicznych, klient natomiast ma możliwość zweryfikowania, czy gwarancje dostawcy odpowiadają jego potrzebom. Spośród wielu

[102] Opracowane na podstawie fragmentu książki R. Marchini' ego, Ibidem, s.22-24.
[103] R. Marchini, Ibidem, s. 24-25.
[104] A. Mateos, J. Rosenberg, Ibidem, s. 104-106.
[105] Ibidem.
[106] R. Marchini, Ibidem.

standardów opracowanych przez organizacje międzynarodowe, bez wątpienia największe znaczenie mają normy Międzynarodowej Organizacji Normalizacyjnej (ISO) oraz standard Amerykańskiego Instytutu Audytorów (AICPA) tj. SAS 70.

Wśród norm ISO najważniejsze znaczenie dla omawianego zagadnienia ma rodzina norm ISO/IEC 27000 tj. standardów zarządzania bezpieczeństwem informacji. Szczególnie istotne będą dwie normy z tej grupy: ISO /IEC 27001 oraz ISO/IEC 27002. Pierwsza jest specyfikacją systemów zarządzania bezpieczeństwem informacji. Na zgodność z tą normą przeprowadzane są audyty i możliwe jest uzyskanie certyfikatu. Składa się na nią jedenaście obszarów (min.: polityka bezpieczeństwa, organizacja bezpieczeństwa informacji, zarządzanie aktywami, bezpieczeństwo zasobów ludzkich, bezpieczeństwo fizyczne, zarządzanie sieciami, kontrola dostępu etc.)[107]. Zgodność z tą normą daje pewność, że zarządzanie bezpieczeństwem informacji jest w danej organizacji wdrożone, ulepszane i przestrzegane. Uzyskanie certyfikatu ISO/IEC 27001 prowadzone jest na kilku etapach, w trakcie których dokonywany jest audyt. Organizacja musi wykazać, że deklarowane przez nią działania zostały zaimplementowane. Druga norma z grupy ISO/IEC 27000- ISO/IEC 27002 jest rozszerzeniem normy 270001 i zawiera praktyczne wskazówki do prawidłowego wdrożenia standardów bezpieczeństwa. Co ważne, norma ta zawiera tylko generalne zasady. Na zgodność z nią, nie można zatem uzyskać certyfikatu.

Drugim, wskazanym wyżej sposobem na potwierdzenie jakości kontroli wewnętrznych min. w odniesieniu do prowadzonej polityki bezpieczeństwa, jest SAS70. Należy podkreślić, że SAS70 nie jest standardem bezpieczeństwa i może być wykorzystywany do weryfikacji wielu obszarów. Najkrócej mówiąc, SAS 70 wyznacza standardy prowadzenia audytu organizacji, która świadczy usługi informatyczne. Składa się na niego: charakterystyka środowiska, gdzie prowadzona jest wewnętrzna kontrola, opis sposobów zarządzania ryzykiem i świadczonych usług, czy najważniejsze mechanizmy kontrolne[108]. Audyt, podobnie jak w przypadku ISO, przeprowadza niezależny i akredytowany podmiot. Rezultatem są dwa typy raportów. Pierwszy jest ogólnym opisem, w jaki sposób organizacja osiąga opisane przez siebie standardy. Typ drugi ma natomiast wymiar praktyczny, gdyż powstaje w wyniku obserwacji audytora pracy w organizacji przez pewien okres czasu (co najmniej sześć miesięcy). Jest on istotny o tyle, że pozwala określić rzeczywistą skuteczność działania wewnętrznych mechanizmów kontrolnych w organizacji.

[107] Na podstawie informacji dostępnych na stronie ISO w Polsce, http://www.iso27000.pl/sites/view/site=85, odczyt 23.03. 2012 r.
[108] Piotr Urban, Bezpieczny Outsourcing, outsourcing.com.pl, 28.07.2010 r., http://www.outsourcing.com.pl/17867,bezpieczny_outsourcing_czyli_sas_70.html, odczyt 23.03.2012 r.

Szczególnie ten właśnie raport powinien być przedmiotem zainteresowania firmy, która chce skorzystać z usług podmiotu świadczącego usługi informatyczne[109].

Aby zrozumieć w jaki sposób może być zorganizowany system zabezpieczeń, warto wskazać przykłady polityk dostawców usług Cloud Computing w ramach chmury publicznej. Na stronach internetowych *Oracle*, możemy przeczytać, że firma ta stosuje wiele rozwiązań mających na celu zwiększenie bezpieczeństwa danych. Wśród nich są: *„zarządzanie tożsamością (Oracle Identity Management), ochrona danych poprzez ich szyfrowanie oraz szyfrowanie kopii zapasowych, kontrola dostępu do danych (Database Firewall, Audit Vault, Database Vault) oraz możliwość maskowania danych (Data Masking)[110].”* Firma zaznacza również, że ma nowoczesne serwery, które są tak skonstruowane, by nie było mowy o przestojach[111].

Z kolei *Google*, w kontrowersyjnym dokumencie „*Polityka prywatności*” (szerzej będzie o tym mowa w dalszej części pracy) podkreśla, że *„dokłada wszelkich starań, aby chronić firmę Google i użytkowników przed nieuprawnionym dostępem, nieautoryzowaną modyfikacją, ujawnieniem oraz zniszczeniem informacji znajdujących się w posiadaniu Google*”[112]. W tym celu stosuje takie środki bezpieczeństwa jak: szyfrowanie SSL, dwuetapową weryfikację dostępu do *Gmail*, bezpieczne przeglądanie w przeglądarce *Chrome*, fizyczne środki bezpieczeństwa, limitowany dostęp do danych dla pracowników i kontrahentów[113].

Portal społecznościowy *LinkedIn* podaje na oficjalnej stronie internetowej informację, że dane osobowe chroni w ten sposób, że *„dostęp do informacji użytkownika podanych w LinkedIn możliwy jest wyłącznie po podaniu hasła, a dane poufne (takie jak informacje o karcie kredytowej) chronione są szyfrem SSL podczas ich wymiany między przeglądarką użytkownika, a witryną LinkedIn*”[114]. Dalej jednak można przeczytać, że ponieważ „ *Internet nie jest w 100% bezpiecznym środowiskiem, nie możemy zapewnić ani gwarantować ochrony informacji przekazywanych przez użytkownika do LinkedIn*”[115] i z taką klauzulą można spotkać się analizując większość udostępnianych przez dostawców dokumentów. W wielu

[109] R. Marchini, Ibidem.
[110] Opracowano na podstawie danych dostępnych na oficjalnej stronie *Oracle*, http://oracle-pl.blogspot.com/2012/04/bezpieczenstwo-w-chmurze.html, odczyt 25.03.2012 r.
[111] Ibidem.
[112] Opracowano na podstawie danych dostępnych na oficjalnej stronie *Google*, https://www.google.pl/intl/pl/policies/privacy/, odczyt 25.03.2012 r.
[113] Ibidem.
[114] Opracowano na podstawie danych dostępnych na oficjalnej stronie *LinkedIn*, http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv, odczyt 25.03.2012 r.
[115] Ibidem.

miejscach będą oni próbować ograniczyć lub wyłączyć swoją odpowiedzialność za naruszenie zasad bezpieczeństwa. Często jednak można spotkać się z opinią, że znani usługodawcy poprzez znaczne inwestycje w zachowanie wysokich standardów bezpieczeństwa, dają większe gwarancje, niż utrzymywanie danych w środowisku wewnętrznym. Małe podmioty nie posiadają środków finansowych na takie przedsięwzięcia.

Każdy użytkownik zamierzający przenieść dane do chmury, powinien skrupulatnie przeanalizować wszelkie działania podejmowane przez dostawcę zmierzające do zapewnienia bezpieczeństwa infrastruktury (min. powinien zabiegać o wgląd do uzyskanych certyfikatów, żądać udostępnienia możliwie szczegółowych parametrów technicznych). Tak zwana „*amorficzność chmury*" tj. cecha powodująca, że nie jest ona możliwa do zlokalizowania[116], będzie prowadziła do powstania wielu wątpliwości natury prawnej. Także sytuacja, gdy z tych samych zasobów korzysta wiele osób jednocześnie (wielodzierżawa) powinna być asumptem do pogłębionej weryfikacji. Od tego bowiem, w jaki sposób zabezpieczone są dane, zależeć będzie powodzenie wielu przedsięwzięć, zysk finansowy a także ochrona prywatności i ogólny komfort korzystania z usług.

2.3. Chmura obliczeniowa źródłem nowych wyzwań dla ochrony danych osobowych

2.3.1. Ochrona danych osobowych - system ochrony, podstawowe pojęcia

Ochrona danych osobowych jest jednym z najważniejszych zagadnień prawnych związanych z chmurą obliczeniową. Rozwój Internetu- coraz większa ilość transakcji i kontaktów nawiązywanych za pośrednictwem sieci - spowodował wzrost zainteresowania tematyką ochrony danych, a także prowokuje do ujęcia tego zagadnienia w nowe ramy prawne. Potrzeba zmian jest tym większa, im szybciej rozwijać będą się usługi Cloud Computing, których założeniem jest dynamiczna skalowalność zasobów w wielu centrach danych równocześnie. Stwarzać to będzie bowiem wiele trudności z określeniem miejsca faktycznego przechowywania danych. To z kolei utrudni pociągnięcie usługodawcy do odpowiedzialności za ewentualne naruszenia. Problemy pojawią się również w kwestii definiowania takich (elementarnych dla ochrony danych osobowych pojęć) jak: administrator (*data controller*), czy podmiot przetwarzający dane (*data processor*). Znaczenia nabiorą także zagadnienia dotyczące transferu danych do podmiotu trzeciego. Wielu usługodawców ma bowiem swoje siedziby np. w Stanach Zjednoczonych, które- według standardów Unii

[116] J. Muszyński, Ibidem.

Europejskiej- nie są krajem bezpiecznym. Z tych oraz innych względów, prawnicy postulują wprowadzenie zmian w obecnym systemie prawnym ochrony danych osobowych[117].

W krajach Unii Europejskiej (na ten obszar zostanie w tym miejscu położony nacisk) system ochrony danych osobowych, kształtowany jest dwutorowo. Z jednej strony funkcjonuje prawo wspólnotowe -przede wszystkim Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, a z drugiej, obowiązuje ustawodawstwo poszczególnych krajów. W Polsce jest to przede wszystkim Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (u.o.o.d.o), a także min. ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Zwracając w tym momencie szczególną uwagę na Dyrektywę 95/46 oraz ustawę z 1997 r., należy podkreślić, że choć polska ustawa najbardziej istotne zagadnienia przejmuje z Dyrektywy, to często różni się w detalach. Zakres pojęciowy i sposób definiowania jest jednak w zasadzie identyczny[118]. Aby lepiej zrozumieć najbardziej istotne zagadnienia w przedmiocie ochrony danych osobowych w chmurze obliczeniowej, należy krótko przybliżyć te podstawowe pojęcia.

W obu aktach prawnych rozumienie terminu „dane osobowe" jest analogiczne. Pojęcie to obejmuje wszystkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (art. 2 lit a Dyrektywy oraz art. 6 ust. 1 i ust. 2). Przyjmuje się, że osoba fizyczna możliwa jest do zidentyfikowania, gdy da się określić jej tożsamość, co zresztą wynika z ustępu 2 art. 6 polskiej ustawy (oraz art. 2 lit a Dyrektywy), zgodnie z którym osoba możliwa jest do zidentyfikowania, „*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"*. Uznaje się, że określenie tożsamości jest niemożliwe, jeśli wymaga to nadmiernych kosztów lub działań[119]. Za dane osobowe mogą być uznane min. PESEL, imię i nazwisko, płeć, miejsce urodzenia, sytuacja majątkowa, przejawy działalności, lub cechy nabyte tj. wykształcenie[120] oraz – przyjmując stanowisko Justyny Ożegalskiej- Trybalskiej – adres e-mail, który pozwala zidentyfikować osobę fizyczną[121] (np. imię.nazwisko@x.com).

[117] Rafał Surowiec, *Dane osobowe w chmurach*, Rzeczpospolita, 21 lipca 2011 r., odczyt 5.04. 2012 r.
[118] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, *Ochrona danych osobowych. Komentarz*, wyd. V, Lex 2011, nr.8531, rozdział II części I dotyczący prawa polskiego.
[119] Tak Sąd Najwyższy w wyroku z 5 września 2001 r., I CKN 1159/00, OSNC 2002, nr 5, poz. 67.
[120] Andrzej Drozd, *Ustawa o ochronie danych osobowych, Komentarz. Wzory pism i przepisy*, Wyd. Prawnicze Lexis Nexis, Warszawa 2004. , s. 48.
[121] Justyna Ożegalska- Trybalska, *Adresy e-mailowe a dane osobowe*, ODO 2001, nr 23, s. 10-13.

Ustawa i Dyrektywa wprowadzają także kategorię danych „wrażliwych". Zgodnie z art. 27 Ustawy *„zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, 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*". Dla tych danych osobowych wprowadzono odrębne regulacje dotyczące przetwarzania.

Ustawa definiuje również pojęcie zbioru danych. Jest to *„posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie"* (art. 7 pkt.1). Często przepisy będą odnosić się jedynie do zbioru danych.

Kolejnymi, niezwykle istotnymi pojęciami, których rozumienie wywołuje wiele niejasności w kontekście Cloud Computing są: „*administrator danych*" (*data controller*) oraz „*podmiot przetwarzający dane*" (*data processor*) tj. podmioty biorące udział w procesie przetwarzania. Dyrektywa w art.2 pkt b (analogicznie a art. 7 ust. 2 u.o.o.d.o) mówi, że przetwarzanie (*processing*) to *„operacje lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie*".

W art. 26 u.o.o.d.o. (odpowiednik art. 6 Dyrektywy) wymienione są podstawowe zasady przetwarzania danych. Zgodnie z tym przepisem, *„administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były 1) przetwarzane zgodnie z prawem, 2)zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2, 3)merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, 4)przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania"*. Dyrektywa dodaje również wymóg „rzetelności" przetwarzania danych a także „prawidłowości" i względnej aktualności danych (art. 6 lit. a oraz d). Przetwarzanie danych osobowych musi wiązać się ze spełnieniem

specjalnych wymogów określonych w art. 23 ust. 1 u.o.o.d.o[122], który powtarza regulację ujętą w Dyrektywie.

W procesie przetwarzania danych biorą udział administrator oraz podmiot przetwarzający. Według Dyrektywy (art. 2 pkt b), 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; jeżeli cele i sposoby przetwarzania danych są określane w przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe*". Określenie w polskiej Ustawie jest podobne[123].

Ustalenie, czy podmiot jest administratorem ma doniosłe konsekwencje prawne. Administratora obowiązują bowiem obowiązki min.: informacyjne, dbania o zgodność z prawem przetwarzania danych osobowych, zachowanie danych osobowych w poufności itd., których niespełnienie może skutkować nawet odpowiedzialnością karną[124]. Innym obowiązkiem administratora wynikającym z Dyrektywy (art. 18) oraz z Ustawy (art. 40 i n.) jest obowiązek notyfikacji zamiaru przetwarzania danych (a w polskiej ustawie tylko zbiorów danych) odpowiedniemu organowi (Generalny Inspektor Ochrony Danych Osobowych), który może odmówić takiej rejestracji (odpowiednio art. 20 Dyrektywy i art. 41 Ustawy). Jak podkreśla Andrzej Drozd, do oceny, czy mamy do czynienia z administratorem, zasadnicze powinno być stwierdzenie, że administrator „ponosi odpowiedzialność za przetwarzanie" (takie powinno być bowiem według niego rozumienie Dyrektywy, tak też ujęte to zostało w ustawodawstwie Niemiec czy Francji)[125].

---

[122] Zgodnie z tym przepisem: „*przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:*
1) *osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,*
2) *jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,*
3) *jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,*
4) *jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,*
5) *jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą*".

[123] Polska ustawa nie przewiduje rozwiązania przyjętego w drugiej części tego przepisu tj. w kwestii powołania administratora, gdy cele i środki są wyznaczone w odpowiednich przepisach. W pozostałym zakresie definicje się porywają.

[124] Ibidem., Kwestia odpowiedzialności karnej wynika z przepisów u.o.o.d.o.: art. 51 (jeśli administrator udostępnia dane osobom nieupoważnionym), 52 (gdy administrator- choćby nieumyślnie- zaniecha obowiązku zabezpieczenia danych), art. 54 (w sytuacji, gdy administrator nie dopełni obowiązku informacyjnego). W takich sytuacjach na administratora może być nałożona grzywna, kara ograniczenia lub pozbawienia wolności.

[125] A. Drozd, Ibidem, s. 62.

Administrator (jak wynika z przepisów) nie musi osobiście przetwarzać danych[126]. „Przetwarzającym dane" *(data processor)* wedle postanowień Dyrektywy (art. 2 lit. e) jest "*osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ przetwarzający dane osobowe w imieniu administratora danych*". Polska ustawa nie przejęła tej definicji wprost, jednak z jej postanowień wynika, że administrator może powierzyć innemu podmiotowi w drodze umowy przetwarzanie danych (art. 31 ust. 1 u.o.d.o). Podmiot, któremu powierzono przetwarzanie może to robić wyłącznie w zakresie i w celu przewidzianym w umowie (art. 31 ust. 2). Co również istotne, taka umowa nie wyłącza odpowiedzialności administratora, a przetwarzający odpowie jedynie za naruszenie przepisów umowy (art. 31 ust. 4). Podmiot przejmujący dane do przetwarzania jest jednak zobligowany min. do podjęcia odpowiednich środków organizacyjnych i technicznych zabezpieczających zbiór danych. Jeśli tego obowiązku nie spełni, będzie odpowiadał na takich samych zasadach jak administrator (art. 31 ust. 3).

Na zakończenie tej części, należy podkreślić, że z racji tego, iż umowy Cloud Computing są umowami o świadczenie usług drogą elektroniczną, to znajdzie do nich zastosowanie Ustawa o świadczeniu usług drogą elektroniczną (u.ś.u.d.e.) oraz wspomniana dyrektywa 2000/31/WE. Jest to o tyle ważne, że te akty prawne zawierają przepisy, które traktuje się jako *lex specialis* w stosunku do omówionych aktów prawnych[127] tj. u.o.o.d.o. nie znajdzie zastosowania tam, gdzie u.ś.u.de. wprowadza odrębne lub dodatkowe uregulowania. Warto w tym miejscu zwrócić uwagę tylko na te przepisy wprowadzające szczególne unormowania w stosunku do u.o.d.o.

Po pierwsze, zakresem ochrony przewidzianej w u.ś.u.d.e. objęte są dane „usługobiorców", do których ustawa zalicza także osoby prawne (art. 2 pkt 6), jednak z powodu braku odrębnej definicji danych osobowych w tej ustawie, na podstawie art. 16. ust.1 u.ś.u.d.o[128] stosowane będą przepisy u.o.o.d.o., a zatem przepis ten znajdzie zastosowanie tylko do osób fizycznych[129]. Co ważne, usługodawcy nie można automatycznie utożsamiać z administratorem w rozumieniu u.o.o.d.o. Usługodawca, który jedynie

[126] J. Barta, R. Markiewicz, P. Fajgielski, Ibidem, Komentarz do art. 7 ust.4 u.o.o.d.o.
[127] J. Barta, R. Markiewicz, P.Fajgielski, Ibidem, rozdział pt. „*Polska Ustawa o świadczeniu usług drogą elektroniczną*".
[128] Art. 16 u.ś.u.d.e. mówi, że „ *do przetwarzania danych osobowych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926), w związku ze świadczeniem usług drogą elektroniczną, stosuje się przepisy tej ustawy, o ile przepisy niniejszego rozdziału nie stanowią inaczej*".
[129] J. Barta, R. Markiewicz, P.Fajgielski, Ibidem.

pośredniczy w świadczeniu usług, nie może być uznany za administratora, gdyż nie decyduje o celach i środkach przetwarzania[130].

Ustawa o świadczeniu usług drogą elektroniczną wprowadza także własne regulacje w zakresie podstaw przetwarzania danych (przez co wyłącza stosowanie art. 23 u.o.o.d.o.). Zgodnie z art. 18 u.ś.u.d.e, podstawą przetwarzania danych są kwestie związane z istnieniem lub zmianą stosunku prawnego między usługodawcą a usługobiorcą lub pewne szczególne sytuacje po ustaniu stosunku prawnego (np. konieczność rozliczenia usługi). W niektórych przypadkach konieczna będzie zgoda usługobiorcy (art. 19 ust.2 pkt 2 wymaga zgody, gdy przetwarzanie niezbędne jest do celów reklamy, badania rynku, polepszenia usług etc.). Zgodnie z art. 4 ust. 2 u.ś.u.d.e. ciężar udowodnienia faktu udzielenia zgody ciąży na usługodawcy.

Należy pamiętać, że istnieją również inne kategorie danych, niż te objęte zakresem u.o.o.d.o. Są to min. dane chronione na podstawie ustawy o bazach danych, ustawy o zwalczaniu nieuczciwej konkurencji (tajemnice przedsiębiorstwa), czy na podstawie ustawie o ochronie informacji niejawnych. Każda z tych kategorii podlega odrębnemu reżimowi prawnemu (min. wyznacza odrębne zasady odpowiedzialności prawnej). Przedmiotem tego rozdziału pozostaną jednak zagadnienia dotyczące danych osobowych.

W trakcie dalszej analizy, rozważane będą kwestie dotyczące właściwego zdefiniowania administratora danych w chmurze obliczeniowej, gdyż ma to dla Cloud Computing znaczenie elementarne. W dalszej kolejności omówione zostanie zagadnienie transferu danych osobowych poza Unię Europejską. Warto podkreślić, że z kwestią ochrony danych osobowych związane są problemy jurysdykcji i prawa właściwego. Będą one przedmiotem kolejnego rozdziału.

2.3.2. Pozycja dostawcy usług Cloud Computing

Powyższa analiza daje podstawę do twierdzenia, że w procesie przetwarzania danych osobowych szczególną rolę odgrywa administrator. To na nim spoczywa szereg obowiązków, których niedopełnienie może skutkować odpowiedzialnością, także na gruncie prawa karnego. Wyróżnia się również (zarówno w Dyrektywie jak i u.o.o.d.o.) podmioty, które przetwarzają dane (tj. dokonują operacji na danych przy pomocy środków zautomatyzowanych lub innych) w imieniu administratora, na podstawie umowy.

[130] Ibidem.

Zgodnie z twierdzeniami autorów Komentarza do u.o.o.d.o., ten kto przetwarza dane w pełni według poleceń, nie może być uznany za administratora. Kryterium decydującym o uznaniu za administratora staje się zatem samodzielność w podejmowaniu decyzji w zakresie środków i celów przetwarzania[131]. Przechodząc na grunt Cloud Computing, powstaje pytanie, czy dostawca usług może być uznany za administratora w rozumieniu przepisów Dyrektywy i u.o.o.d.o., czy jest zaledwie przedmiotem przetwarzającym, a tym samym nie musi spełniać wszystkich wymogów ustalonych we wskazanych aktach prawnych, także tych dotyczących świadczenia usług drogą elektroniczną? Definitywne rozstrzygnięcie przesądza nie tylko o przypisaniu podmiotowi określonego zestawu obowiązków, ale jest także ważne dla ustalenia, jakie prawo krajowe będzie właściwe dla przetwarzania danych[132].

Pobieżna analiza może prowadzić do wniosku, że skoro to klient jest władny podejmować decyzje dotyczące celu przetwarzania swoich danych, to spełnia przesłanki wymienione w odpowiednich przepisach i można go uznać za administratora. Dostawca usług będzie zatem podmiotem przetwarzającym, gdyż na podstawie umowy zostały mu przekazane dane, które (zgodnie z celami wyznaczonymi w umowie) mogą być przez niego przetwarzane. Zagadnienie to nie jest jednak tak oczywiste. Jak bowiem zakwalifikować podmiot, który co prawda przede wszystkim świadczy usługę, w której dane są przetwarzane, ale oprócz tego samodzielnie wyznacza zasady i sposoby przetwarzania, a także rodzaj danych, które mogą podlegać przetwarzaniu oraz wskazuje odrębne zasady bezpieczeństwa? Czy taki podmiot wciąż jest tylko przetwarzającym?

Z tym problemem zmierzyła się w 2006 r. tzw. Grupa Robocza art. 29 (ustanowiona na podstawie art. 29 Dyrektywy 95/46/WE) badając sprawę SWIFT (*Society for Wordwide Interbank Financial Telecommunication)* tj. podmiotu, który świadczy usługę przekazywania informacji finansowych umożliwiającą dokonywanie międzynarodowych przekazów pieniężnych. SWIFT, choć utrzymywał, że zajmuje się wyłącznie przetwarzaniem danych w imieniu usługodawców, to jednak samodzielnie wyznaczał zasady i standardy[133]. Według opinii Grupy Roboczej, SWIFT powinien być uznany za administratora danych w rozumieniu art. 2 lit. d. Dyrektywy ze wszystkimi tego konsekwencjami[134]. Pogląd wyrażony przez Grupę Roboczą jest kontrowersyjny. Każdy dostawca usług ma bowiem pewne standardy w przedmiocie sposobu świadczenia usługi oraz zasady polityki bezpieczeństwa. Uznanie

[131] J. Barta, R. Markiewicz, P. Fajgielski, Ibidem.
[132] Opinia 10/2006 Grupy Roboczej art.29 dostępna na stronie http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_pl.pdf, odczyt 10.04.2012 r.
[133] Opinia 1/2010 Grupy Roboczej art.29 dostępna na stronie http://www.giodo.gov.pl/1520057/id_art/3595/j/pl/, odczyt 10.04.2012 r.
[134] Ibidem.

wszystkich dostawców za administratorów, mogłoby skutkować poważnym ograniczeniem swobody prowadzenia przez nich działalności. Trzeba jednak zgodzić się z poglądem Grupy Roboczej, że takie czynności mogą być w pewnym sensie uznane za „decydowanie o środkach i celach przetwarzania danych" w rozumieniu Dyrektywy. Jak zaznacza Renzo Marchini, choć SWIFT nie może być uznany za dostawcę usług w chmurze, to istnieją pewne cechy wspólne, które nakazują stosować tutaj analogię. Autor do cech wspólnych zalicza: świadczenie usług, umieszczenie danych w wielu centrach danych, skalowalność[135].

O ile opinia 1/2006 nie przyniosła konkretnych wskazówek, w jaki sposób odróżnić administratora od podmiotu przetwarzającego w przypadku usług świadczonych za pośrednictwem Internetu, to inna opinia Grupy Roboczej nr 1/2010 idzie o krok dalej. Po dogłębnej analizie definicji administratora i przetwarzającego dane zwartych w Dyrektywie, Grupa Robocza uznała, że *„określenie „celu" przetwarzania powoduje uznanie za administratora danych (de facto). Administrator danych może natomiast przekazać określenie „sposobów" przetwarzania w odniesieniu do kwestii technicznych i organizacyjnych*"[136]. Tym samym, jeżeli uznamy, że dostawca ma decydujący wpływ na określenie „celów" przetwarzania, to – według wskazanej opinii- z całą pewnością można go uznać za administratora. Jak bowiem można przeczytać w dalszej części opinii: „*Określenie zasadniczych kwestii dotyczących sedna zgodności przetwarzania danych z prawem – takich jak dane, które należy przetworzyć, czas ich przechowywania, dostęp do nich itd. – należy do administratora danych*"[137]. Pomimo, że nie wskazano tu przykładów „celów", które mógłby określić dostawca, to zwrócono uwagę na jedną istotną kwestię: „*środki bezpieczeństwa uznaje się za podstawową właściwość określaną przez administratora danych*"[138].

Kilka praktycznych wskazówek, co do sposobu kwalifikowania dostawcy usług Cloud Computing, wymienia Renzo Marchini. Według niego, jeśli dostawca daje klientowi możliwość wyboru jakiegokolwiek elementu technicznego np. sposobu kodowania lub jeśli deleguje na klienta prawo akceptacji ewentualnych podmiotów, z którymi będzie współpracował w zakresie przetwarzania jego danych, to można przypuszczać, że będzie próbował udowadniać, że nie decyduje w pełni o celach przetwarzania, a więc nie można uznać go za administratora. Jeśli natomiast, dostawca zechce wykorzystywać dane klientów

[135] R. Marchini, Ibidem, s. 47.
[136] Opinia 1/2010 Grupy Roboczej art. 29, Ibidem.
[137] Ibidem.
[138] Ibidem.

do własnych celów, to trudno byłoby zgodzić się z argumentacją, że jest on tylko podmiotem przetwarzającym[139].

Powracając na grunt rozważań w temacie Cloud Computing, należy wskazać, że w przypadku usług SaaS np. CRM, to klient wprowadza, udostępnia i zarządza swoimi danymi tj. inicjuje i prowadzi proces decyzyjny. Jednak to dostawca decyduje o bezpieczeństwie, ulokowaniu serwerów oraz sposobie dostępu do danych. Zgodnie z przywołaną opinią, to on mógłby być zatem uznany za administratora.

Jak zatem można stwierdzić, przy sporządzaniu kontraktów z dostawcą, należy dokładnie przeanalizować wszelkie działania, które podejmuje on względem transferowanych do chmury danych. Prosty wniosek, że dostawca usług jest podmiotem przetwarzającym, nie przystaje do Cloud Computing i zważając na szybki rozwój tego modelu, należy się zgodzić z postulatem wprowadzenia zmian w przepisach. Do czasu kiedy to nastąpi, klient musi brać pod uwagę dwa sposoby rozumienia dostawcy: jako administratora i jako przetwarzającego i stosować odpowiednie standardy wynikające z Dyrektywy, a na gruncie prawa polskiego także u.o.o.d.o.

2.3.3. Transfer danych poza Unię Europejską. Zagadnienia podstawowe

Kolejną kwestią wartą rozważenia w kontekście zastosowania przepisów dotyczących ochrony danych osobowych w przypadku Cloud Computing, jest problem transferu danych poza Unię Europejską. Dyrektywa o ochronie danych osobowych a także polska ustawa, mając na uwadze konieczność ochrony osób fizycznych przed utratą kontroli nad danymi, wprowadzają bowiem ograniczenia przesyłania danych do państw trzecich. Zasada ustanowiona już w Preambule Dyrektywy 95/46/WE głosi, że przepływ danych między państwami członkowskimi powinien być swobodny i niezakłócony (punkt 9 Preambuły). Stąd transfer danych np. z Polski do Niemiec jest traktowany tak, jakby odbywał się między podmiotami z Polski. Odmienna sytuacja będzie miała miejsce, jeśli podmiot, któremu przekazywane są dane ma swoją siedzibę lub miejsce zamieszkania w państwie trzecim.

U.o.o.d.o definiuje państwo trzecie jako „*państwo nienależące do Europejskiego Obszaru Gospodarczego*" (art. 7 pkt. 7). Możliwość przekazywania danych do tych państw, będzie uzależniona od spełnienia określonych wymagań. Temu zagadnieniu poświęcony jest rozdział VII Dyrektywy. Artykuł 25 ust. 1. tego aktu wprowadza podstawową zasadę, że przekazywanie danych do państw trzecich jest dozwolone, jeśli państwo to zapewnia

[139] Ibidem.

„*odpowiedni stopień ochrony*". Przede wszystkim, należy podkreślić, że poziom ochrony w państwie przeznaczenia nie musi być identyczny, jak w kraju pochodzenia podmiotu poszukującego ochrony. Istotne jednak, by gwarancje w państwie trzecim były co najmniej takie, jak w kraju odniesienia[140]. Ocena, czy stopień ochrony jest „odpowiedni" (adekwatny) zależy przy tym od wielu elementów operacji przekazania danych, a także od charakteru danych, celu i czasu trwania przetwarzania, kraju pochodzenia, kraju przeznaczenia, przepisów szczególnych w państwie przeznaczenia (art. 25 ust. 2). Mariusz Jagielski zwraca uwagę, że *„metoda adekwatności ochrony będzie skutecznie zabezpieczać interesy jednostki jedynie wtedy, jeśli zostanie zastosowana w ramach odpowiedniego środowiska sprzyjającego respektowaniu praw podmiotu danych*"[141].

Na mocy procedury przewidzianej w dalszych ustępach tego artykułu (art. 25 ust.4), Komisja Europejska może podjąć działania uniemożliwiające transfer danych, jeśli uzna, że poziom ochrony nie jest tam odpowiedni. Artykuł 26 Dyrektywy wprowadza natomiast odstępstwa, które - w ściśle określonych przypadkach (o ile jest to zgodne z szczególnymi przepisami państw członkowskich) - umożliwiają przesłanie danych do państwa trzeciego, nawet mimo tego, że nie zapewnia ono odpowiedniego poziomu ochrony. Do takich sytuacji Dyrektywa zalicza: udzielenie wyraźnej zgody przez osobę, której dane dotyczą, przekazanie danych wiąże się z realizacją postanowień umowy z administratorem, przekazanie danych jest niezbędne do realizacji interesów osoby, której dane dotyczą, przekazanie danych jest konieczne dla zawarcia lub wykonania umowy między administratorem a stroną trzecią, przekazanie jest niezbędne do realizacji ważnych interesów publicznych a także jeśli przekazanie jest istotne dla prawidłowego funkcjonowania odpowiednich rejestrów (art. 26 ust. 1 lit a- f). Istotny wyjątek został również przewidziany w ustępie drugim. Zgodnie z nim możliwe jest przekazanie danych państwu trzeciemu niezapewniającemu odpowiedniego stopnia ochrony za zgodą państwa członkowskiego (w Polsce organem, który wydaje takie upoważnienia jest GIODO- tak art. 48 u.o.o.d.o.), jeśli administrator zapewni o wprowadzeniu dodatkowych środków zabezpieczeń.

Obecnie tylko kilka państw otrzymało pozytywną opinię w sprawie spełnienia odpowiedniego poziomu ochrony[142]. Nie ma wśród nich Stanów Zjednoczonych, co dla umów Cloud Computing ma istotne znaczenie, gdyż wielu dostawców ma swoje siedziby

[140] Piotr Drobek (op), *ABC przekazywania danych osobowych do państw trzecich,* Biuro Generalnego Inspektora Danych Osobowych, wyd. Sejmowe, Warszawa 2007 r., s. 7.
[141] Mariusz Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie,* wyd. Oficyna Wolters Kluwer Business, Warszawa 2010 r., s. 205.
[142] R. Marchini, Ibidem, s. 69.

w tym właśnie kraju. Powoduje to wiele utrudnień w handlu między podmiotami z USA i UE. Co więcej, negowane mogą być także transakcje, w których co prawda nie uczestniczy dostawca z USA, ale rozlokowane są tam serwery[143].

Aby zapobiec niekorzystnym konsekwencjom nieuznawania USA, jako kraju zapewniającego odpowiedni poziom ochrony, został pomiędzy Komisją Europejską a Departamentem Handlu USA opracowany dokument *Safe Harbor Privacy Principles*, określane jako *Zasady Safe Harbor (Zasady Bezpiecznej Przystani)*[144]. Podstawowym celem tego dokumentu jest umożliwienie podmiotom z USA przetwarzania danych pochodzących z UE, po spełnieniu określonych wymagań i uzyskaniu właściwego certyfikatu. W interesie strony, która ma zamiar zawrzeć umowę (importera danych) na usługę Cloud Computing z podmiotem z USA (eksporterem danych) będzie zatem zweryfikowanie, czy taki certyfikat został przyznany a także, czy rodzaj certyfikowanych danych odpowiada jego wymaganiom[145]. Należy jednak podkreślić, że poza spełnieniem warunków wynikających z *Safe Harbor Principles*, podmiot z USA (i każdego innego kraju, gdzie ochrona nie jest adekwatna) musi zrealizować podstawowe wymogi Dyrektywy, a - w przypadku transakcji z podmiotem z Polski- także u.o.o.d.o. oraz min. Rozporządzenia MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. Akt ten wprowadza wiele dodatkowych obowiązków podmiotu przetwarzającego. Przykładowo, powinien on udostępnić min. wykaz budynków, pomieszczeń, gdzie przetwarzane są dane (§4 pkt 1 Rozporządzenia). Jeżeli podmiot z USA (lub jakiegokolwiek kraju nieuznawanego za bezpieczny) korzysta z serwerów w wielu miejscach świata (co dla chmury jest sytuacją naturalną), to sprostanie temu wymaganiu nie będzie łatwe.

Warto również wskazać, że dla podmiotu, który nie spełnia właściwych wymagań, sposobem na przekazanie danych osobowych, jest uzyskanie zgody odpowiedniego organu. Jak wskazano, w Polsce jest to GIODO. W wyroku do sygn. II SA 3878/02 NSA uznał, że "*przy udzielaniu zgody na przekazanie danych osobowych za granicę, organ powinien kierować się oceną, czy zastosowane środki różnego typu, klauzule umowne i środki techniczne pozwalają zapewnić stopień ochrony tych danych odpowiadający*

[143] J. Barta, R. Markiewicz, P. Fajgielski, Ibidem, rozdział pt. *Przetwarzanie i ochrona danych osobowych w sieciach komputerowych*.
[144] Na podstawie tekstu pt. *Co to jest safe harbor?*,opublikowanego na stronie GIODO http://www.giodo.gov.pl/317/id_art/1500/j/pl/, odczyt 13.04.2012 r.
[145] R. Marchini, Ibidem, s. 71.

ustawodawstwu polskiemu"[146]. Przy podejmowaniu decyzji, organ może wziąć również pod uwagę zastosowanie w umowie tzw. standardowych klauzul umownych. Są one wyznaczane przez Komisję Europejską w drodze decyzji[147]. Decyzja 2001/497/WE (zmieniona przez decyzję 2004/915/WE) zawiera standardowe klauzule, które dotyczą przekazywania danych między administratorem w UE a administratorem w państwie trzecim (dwa typy klauzul). Z kolei decyzja 2010/87/UE prezentuje pakiet klauzul mogących znaleźć zastosowanie w przypadku, gdy podmiot przetwarzający jest z państwa trzeciego[148]. Prawidłowy wybór odpowiedniego zestawu klauzul będzie uzależniony od określenia funkcji podmiotu tj. czy jest on administratorem, czy przetwarzającym. Rozważania z poprzedniej części doprowadziły do wniosku, że nie zawsze będzie to proste.

2.3.4. Wykorzystanie danych użytkownika przez dostawcę

Cloud Computing niesie wiele wyzwań dla prywatności. Wraz z chmurą pojawiły się bowiem nowe postacie i formy przekazania danych: *e-maile*, edytory tekstów, magazyny plików audio lub video, prezentacji[149]. Coraz bardziej powszechną sytuacją będzie chęć wykorzystania tych danych przez dostawcę do własnych celów np. marketingowych tj. tworzenia raportów na podstawie profilu użytkowników będącego kompozycją danych zebranych na wiele sposobów. Problemy prywatności w chmurach można wyjaśnić na przykładzie *Google*, którego polityka prywatności wzbudziła w ostatnim czasie wiele kontrowersji. Podstawowym zarzutem kierowanym pod adresem tego dokumentu jest łamanie postanowień Dyrektywy 95/46/WE i zasad Safe Harbor[150].

We wstępie do polityki prywatności można przeczytać, że *„z Google można korzystać w różny sposób, np. wyszukując i udostępniając informacje, komunikując się z innymi osobami czy tworząc nowe treści. Dzięki informacjom uzyskanym od użytkowników (np. podczas tworzenia konta Google) udoskonalamy te usługi – wyświetlamy bardziej adekwatne wyniki wyszukiwania i trafniejsze reklamy, ułatwiamy kontakty ze znajomymi oraz oferujemy szybsze i prostsze sposoby udostępniania treści"*[151]. Google informuje następnie, że zamierza

[146] Orzeczenie Naczelnego Sądu Administracyjnego do sygn. II SA 3878/02 z 16 kwietnia 2003 r. ONSA 2004/1/41
[147] J. Barta, R. Markiewicz, P. Fajgielski, Ibidem, Komentarz do art.78 u.o.u.d.o.
[148] Ibidem.
[149] John W. Rittinghouse, James F. Ransome, *Cloud Computing. Implementation, Management, Security*, CRC Press Taylor&Francis Group 2010, s.147.
[150] Raport pt. *Analysis of Google's Privacy Policy and Related FAQ,* Amberhawk, marzec 2012, dostępny na stronie: http://amberhawk.typepad.com/amberhawk/, odczyt 20.04.2012 r.
[151] Polityka Prywatności Google dostępna na, http://www.google.com/intl/pl/policies/privacy/,odczyt 2.04.2012 r.

gromadzić informacje na temat użytkowników w celu udoskonalenia swoich usług, co ma dać użytkownikom większy komfort korzystania. Zbieranie informacji ma odbywać się na dwa sposoby: bezpośrednio od użytkowników (np. podając hasło do *Gmail*, numery telefony czy z kart kredytowych) a także niebezpośrednio- uzyskane w trakcie korzystania przez użytkowników z usług (np. przeglądając strony) - a więc nieświadomie. W tym drugim przypadku będą to informacje dotyczące min. rodzaju sprzętu, adres IP, informacje o lokalizacji. Dane te mogą być następie udostępniane partnerom *Google*[152].

Przeciwko postanowieniom *„Polityki Prywatności Google"* wystąpiła jednak min. Komisarz Sprawiedliwości UE oraz francuski odpowiednik GIODO[153]. Choć bowiem zbieranie informacji o użytkownikach od nich samych lub od strony trzeciej jest w UE dopuszczalne na podstawie art. 10 i 11 Dyrektywy, to jednak niezbędne jest spełnienie odpowiednich wymagań[154]. Podstawowym zarzutem podnoszonym przeciw *Google* jest posługiwanie się niespójnymi pojęciami. W jednym miejscu użyty jest zwrot „dane osobowe", w innym „informacja". To w znaczny sposób utrudnia użytkownikowi zrozumienie, które dane zostaną przez *Google* wykorzystane i czy są to jego chronione dane osobowe. Ponadto, dostrzeżono kilka przypadków naruszeń *Zasad Bezpiecznej Przystani* takich jak: konieczność akceptacji dla unijnej definicji „danych osobowych" i „poufnych danych osobowych" (Polityka Prywatności *Google* wymienia tylko wybrane dane poufne), zagwarantowanie użytkownikom prawa dostępu do danych, obowiązek posługiwania się

[152] Ibidem.

[153] Adam Golański, *Nowa polityka prywatności Google'a nielegalna w Unii Europejskiej? Francuski CNIL wszczyna śledztwo,* webhosting.pl, 6.03.2012 r., http://webhosting.pl/Nowa.polityka.prywatnosci.Googlea.nielegalna.w.Unii.Europejskiej.Francuski.CNIL.wszczyna.sledztwo, odczyt 2.04.2012 r.

[154] *Art. 10 Dyrektywy. Państwa Członkowskie zapewniają, aby administrator danych lub jego przedstawiciel miał obowiązek przedstawienia osobie, której dane dotyczą i od której gromadzone są dane, co najmniej następujących informacji, z wyjątkiem przypadku, kiedy informacje takie już posiada: a) tożsamości administratora danych i ewentualnie jego przedstawiciela; b) celów przetwarzania danych, do których dane są przeznaczone; c) wszelkich dalszych informacji, jak np.: — odbiorcy lub kategorie odbierających dane, — tego, czy odpowiedzi na pytania są obowiązkowe czy dobrowolne oraz ewentualne konsekwencje nieudzielenia odpowiedzi, — istnienie prawa wglądu do swoich danych oraz ich sprostowania, o ile takie dalsze informacje są potrzebne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą.* ***Art. 11. Ust.*** *1. W przypadku gdy dane uzyskiwane są z innych źródeł niż osoba, której dane dotyczą, Państwa Członkowskie zapewniają, aby administrator danych lub jego przedstawiciel był zobowiązany od początku gromadzenia danych osobowych lub w przypadku ujawnienia danych osobie trzeciej, nie później niż do momentu, gdy dane są ujawniane po raz pierwszy, dostarczyć osobie, której dane dotyczą, co najmniej następujące informacje, z wyjątkiem przypadku, kiedy posiada już ona takie informacje: — tożsamość administratora i ewentualnie jego przedstawiciela;— cele przetwarzania danych; — wszelkie dalsze informacji, jak np.: — kategorie potrzebnych danych, — odbiorcy lub kategorie odbierających dane, — istnienie prawa wglądu do swoich danych oraz ich prostowania, o ile takie dalsze informacje są konieczne, biorąc od uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą".*

jasnymi pojęciami, obowiązek współpracy z urzędami ochrony danych osobowych (Google potraktowało go wybiórczo)[155].

Polityka prywatności *Google* jest na tyle niejasna, że słusznie próbuje się ja kwestionować. Należy jednak pamiętać, że *Google* to tylko jeden z wielu przykładów dostawców usług, który próbuje korzystać z danych osobowych użytkowników dla swoich celów biznesowych (trudno bowiem zgodzić się z prawdziwością oficjalnie prezentowanych celów tj. ulepszenie oferowanych usług). Choć tego rodzaju nadużycia można przypisać przede wszystkim dostawcom SaaS, to klauzule zezwalające na spożytkowanie danych klientów pojawiają się również w innych modelach dostarczania usług Cloud Computing[156]. O ile zatem przy usługach SaaS, klient zazwyczaj nie będzie miał możliwości negocjacji, to zawierając umowę na usługi w innych modelach, powinien dokładnie sprawdzić, jakie dane firma może zbierać i w jaki sposób je wykorzystać.

2.3.5. Dostęp do danych i wyprowadzenie danych z infrastruktury dostawcy

Kolejnym, ważnym problemem związanym z ochroną danych osobowych w chmurze obliczeniowej jest dostęp do danych oraz odzyskanie danych po zakończeniu obowiązywania umowy. Już w pierwszej części pracy wspomniano, że z korzystaniem z usług w modelach Cloud Computing często związane będzie zjawisko *vendor lock- in* tzn. uzależnienie się od dostawcy. Jeżeli bowiem dostawca SaaS dostarcza gotową aplikację, dostawca PaaS platformę do tworzenia aplikacji, a provider IaaS kompletną infrastrukturę, to może się okazać, że efekt pracy dokonanej przy użyciu dostarczonych narzędzi nie będzie kompatybilny ze środowiskiem innego dostawcy, a zatem niemożliwe będzie wyprowadzenie i przeniesienie danych.

Dyrektywa 95/46/WE wprowadza w art. 12 generalną zasadę, że każdy może mieć dostęp do swoich danych. Postanowienia u.o.o.d.o. uznaje się za zgodne z tym postulatem[157]. Usługobiorca powinien jednak na tyle, na ile to możliwe, zadbać o postanowienia umowne, które zezwolą mu na bezproblemowe uzyskanie dostępu i przeniesienie danych do innego dostawcy. Renzo Marchini zwraca uwagę, że w umowie powinny znaleźć się klauzule

[155] Piotr Waszczuk, *Nowa polityka prywatności Google powszechnie krytykowana*, Computerworld.pl, 28.02.2012 r., http://www.computerworld.pl/news/380668/Nowa.polityka.prywatnosci.Google.powszechnie.krytykowana.html, odczyt 25.04.2012 r.

[156] Na przykład nowa przeglądarka *Amazon Silk* oferowana głównie klientom chmury Amazon EC2 pozwala na zbieranie i odszyfrowywanie danych użytkowników w: Adam Golański, *Amazon Silk. Przełomowa przeglądarka ery chmur , czy po prostu nowa Opera Mini?*, webhosting.pl, 29.09. 2011 r., http://webhosting.pl/Amazon.Silk.przelomowa.przegladarka.ery.chmur.czy.po.prostu.nowa.Opera.Mini, odczyt 10.04.2012 r.

[157] J. Barta, R. Markiewicz, P. Fajgielski, Ibidem, Komentarz do art. 32 u.o.o.d.o.

umożlwiające samo wyprowadzenie danych, a po drugie postanowienia precyzujące ich format, aby uniknąć sytuacji gdy klient co prawda otrzymał dane bez dodatkowych kosztów, ale i tak nie może z nich skorzystać[158].

Zagadnieniem problematycznym jest również możliwość wykasowania danych z baz dostawcy po rozwiązaniu umowy. Brak odpowiednich gwarancji prawnych w tym zakresie stwarza poważne problemy prawne. W prawie polskim, u.ś.u.d.o. co prawda zakazuje w art. 19. ust 1. przetwarzania danych po zakończeniu korzystania z usługi (w ust. 2 wprowadza natomiast pewne wyjątki), ale nie ma tam mowy o całkowitym wyeliminowaniu z baz danych dostawcy.

Projekt nowego Rozporządzenia Parlamentu Europejskiego i Rady z 25 stycznia 2012 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) wprowadza w art. 17 nową instytucję „*prawo do bycia zapomnianym i usunięcia danych*". Zgodnie z treścią ust. 1 tego artykułu, podmiot danych ma prawo do uzyskania od administratora usunięcia danych osobowych odnoszących się do niego oraz zaprzestania dalszego rozpowszechniania tych danych (…) jeżeli: a) dane nie są już potrzebne do celów, do których były zebrane lub przetwarzane w inny sposób; b) podmiot danych odwołuje zgodę, na której opiera się przetwarzanie (…) lub gdy minął okres przechowywania, na który wyrażono zgodę oraz jeśli nie ma już podstawy prawnej przetwarzania danych; c) podmiot danych sprzeciwia się przetwarzaniu danych osobowych(…), d) przetwarzanie danych nie jest zgodne z rozporządzeniem z innych powodów. Na podstawie ust. 3, administrator musi niezwłocznie usunąć dane (za wyjątkiem pewnych ściśle określonych przypadków). Z kolei art. 18 ustanawia prawo do uzyskania kopii danych (ust.1), a także możliwość przeniesienia danych do innego systemu bez przeszkód ze strony administratora, z którego baz dane osobowe zostają wycofane[159]. Zmiany te są przez specjalistów do spraw ochrony danych osobowych przyjmowane z entuzjazmem[160]. Z pewnością zwiększają zakres ochrony i dają usługodawcą większe gwarancje oraz mogą prowadzić do ograniczenia zjawiska „*vendor-lock-in*".

[158] R. Marchini, Ibidem. s. 101.
[159] Rozporządzenia Parlamentu Europejskiego i Rady nr 2012/0011 z 25 stycznia 2012 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), dostępne na stronie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:PL:PDF, odczyt 25.04. 2012 r.
[160] Projekt rozporządzenia pozytywnie ocenił GIODO a także min. przedstawiciele polskiego PKPP Lewiatan, tak: *PKPP Lewiatan o planowanych zmianach w ochronie danych osobowych*, 19.03.2012 r., http://www.e-ochronadanych.pl/a,1597,pkpp-lewiatan-o-planowanych-zmianach-w-ochronie-danych-osobowych.html, odczyt 25.04.2012 r.

Zagadnienie dostępu do danych w chmurze rodzi wiele problemów i wątpliwości. Wspomniana wcześniej *„Polityka Prywatności Google”* daje co prawda możliwość dostępu do danych dla osób, których te dane dotyczą, ale wprowadza zarazem wyjątki, które stawiają pod znakiem zapytania skuteczność i egzekwowalność tych postanowień[161]. Klient musi w takich wypadkach dokonać dokładnej analizy postanowień. Wtedy, kiedy możliwe są negocjacje, powinien również żądać dokładnego określenia miejsca przechowywania danych, co jest utrudnione szczególnie w sytuacji, gdy w przetwarzaniu uczestniczy wiele podmiotów podwykonawczych (np. usługodawca SaaS buduje aplikacje na platformie PaaS w ramach infrastruktury IaaS).

[161] Dla przykładu, dostęp do danych nie będzie możliwy, jeśli żądania są *„bezzasadnie wielokrotnie przesyłanych, wymagających nieproporcjonalnych nakładów prac technicznych (np. opracowania nowego systemu lub całkowitej zmiany dotychczasowej praktyki), stwarzających ryzyko naruszenia prywatności innych osób, skrajnie trudnych do zrealizowania (m.in. dotyczących informacji znajdujących się w kopiach zapasowych na taśmach)*” w: *Polityka Prywatności Google*, Ibidem.

Rozdział 3. Wybrane problemy prawa autorskiego a chmura obliczeniowa

3.1. Prawo autorskie w chmurze obliczeniowej- charakterystyka problemu

Rozwój Internetu przynosi nowe wyzwania dla prawa autorskiego - pojawiły się nowe metody rozpowszechniania, a tym samym nowe typy naruszeń. Charakterystyczny dla takich spraw będzie szeroki, często nieograniczony krąg odbiorców, a co za tym idzie- szkody powodowane przez działanie naruszyciela są bardziej dotkliwe, niż miało to miejsce dotychczas. Internet wymusza zmianę poglądu w kwestii interpretacji podstawowych pojęć prawa autorskiego tj. egzemplarz, kopia, utrwalenie, zwielokrotnienie etc. Problemy te będą analogiczne w przypadku Cloud Computing. Dostrzegalne są jednak pewne odmienności, choćby w tak podstawowej dla prawa autorskiego kwestii, jak licencjonowanie.

Zagadnienia prawnoautorskie będą obecne w chmurze obliczeniowej w kilku aspektach. Niezwykle istotną kwestią będą problemy związane z umowami na korzystanie z programów komputerowych udostępnianych przez dostawcę lub transferowanych do chmury przez użytkownika. Pojawi się tu szereg wątpliwości, które – ze względu na specyficzne, omówione wcześniej cechy Cloud Computing- należy rozpatrywać w sposób odmienny niż dotychczasowy, właściwy dla tradycyjnych licencji. Interesującym zagadnieniem jest również wpływ postanowień odpowiednich dla licencji typu GNU na możliwości korzystania z aplikacji w środowisku Cloud. Na gruncie prawa polskiego, do oceny tego typu zagadnień odpowiednie będą przede wszystkim przepisy Ustawy prawo autorskie i prawa pokrewne z 1994 r. (pr. aut.) oraz Kodeksu cywilnego (k.c.). Należy jednak zaznaczyć, że w wielu miejscach (np. dla licencji *open source*) polska ustawa dotycząca ochrony praw twórców w obrocie internetowym będzie anachroniczna[162].

Problemy prawa autorskiego będą obecne w chmurze także ze względu na możliwości jakie daje ona w zakresie magazynowania danych. Zdjęcia umieszczane w programie *Google Picasa* lub w galerii *Facebook*'a mogą być przedmiotem autorskich praw majątkowych lub naruszać dobra osobiste (głównie w postaci wizerunku). Nie można też zapomnieć, że Cloud Computing to również usługi oferujące gromadzenie i wymianę plików tzw. *peer-to-peer*. Tu również pojawi się konieczność wyznaczenia zakresu odpowiedzialności dostawcy.

Analizując opracowania dotyczące praw autorskich w chmurze obliczeniowej, można spotkać się również z interesującą tezą, że Cloud Computing może stanowić remedium na zjawisko piractwa komputerowego. Zwolennicy tej tezy wysuwają argument, że dzięki

[162] E. Traple, *Umowy o eksploatację utworów w prawie polskim,* wyd. Oficyna, Warszawa 2010, s. 297-301.

udostępnianiu aplikacji w chmurze, a co za tym idzie stopniowemu eliminowaniu materialnych nośników, dochodzi to ograniczenia liczby nielegalnych kopii[163]. Przeciwnicy natomiast podkreślają, że zjawisko piractwa wynika z braku respektu dla własności intelektualnej. Trudno zatem oczekiwać, że zaledwie zmiana modelu świadczenia usług doprowadzi do zmiany mentalności (czego najlepszym przykładem może być sytuacja, gdy prowadzono telewizję kablową- użytkownicy w dalszym ciągu wzajemnie udostępniają sobie sygnał)[164]. *Business Software Alliance* (BSA) w raporcie *„09 Piracy Study"* sugeruje, aby powstrzymać się od skrajnych opinii na temat wpływu Cloud Computing na ograniczenie piractwa. Zdaniem autorów raportu, wciąż jest jeszcze zbyt wcześnie (usługi nie są jeszcze wystarczająco spopularyzowane), aby takie skutki zmierzyć[165]. Do tej opinii należy się przychylić.

W niniejszej pracy zostaną omówione jedynie wybrane zagadnienia związane z stosowaniem prawa autorskiego w modelu Cloud Computing. Ponieważ największe, praktyczne znaczenie dla obrotu prawami autorskimi mają dla Cloud Computing kwestie licencjonowania, stąd w tej części zostanie zwrócona uwaga na kilka zagadnień z tego zakresu. Należy podkreślić, że będą one omawiane ze szczególnym uwzględnieniem przepisów polskiej ustawy pr. aut. Warto jednak zauważyć, że choć w innych systemach prawnych uregulowania mogą diametralnie różnić się od tych zawartych w przepisach prawa polskiego, to - ze względu na umiędzynarodowienie prawa autorskiego - problemy pozostaną aktualne.

3.2. Zagadnienia licencjonowania w modelu Cloud Computing

3.2.1. Specyfika umów licencyjnych- zarys problematyki

W tradycyjnym modelu licencjonowania programów komputerowych program sprzedawany jest na nośnikach lub udostępniany *online*[166]. Stronami takiej umowy są: licencjodawca tj. podmiot, któremu przysługują autorskie oraz licencjobiorca (organizacja, podmiot indywidualny) zainteresowany korzystaniem z oprogramowania. Jeśli dochodzi do

[163] Pankai Lakhotia, *Microsoft says Cloud computing can end software piracy,* stockwatch.com, 6.03.2010 r., http://www.stockwatch.in/microsoft-says-cloud-computing-can-end-software-piracy-26613, odczyt 5.04.2012 r.
[164] Kacey Weinberg, *Will the cloud eradicate software piracy?,* enterprisecioforum.com, 5.04 2011 r., http://www.enterprisecioforum.com/en/blogs/kweinberg/will-cloud-eradicate-software-piracy, odczyt 2.04. 2012 r.
[165] Raport *Business Software Aliance*, *09 Software Piracy*, BSA, maj 2010 r., http://portal.bsa.org/globalpiracy2009/studies/globalpiracystudy2009.pdf, odczyt 5.04.2012 r.
[166] E. Traple, Ibidem, s. 277.

sprzedaży oprogramowania, to licencja zazwyczaj obejmuje jedno lub kilka stanowisk[167]. Zarówno fizyczna wersja programu jak i wersja *online* wymagają w takim modelu licencjonowania, instalacji określonych komponentów oprogramowania na dysku twardym użytkownika. Licencja, w okresie jej obowiązywania, zakłada pewien poziom wsparcia ze strony dostawcy. Po upływie terminu na jaki została zawarta, wsparcie naturalnie wygasa, ale użytkownik w dalszym ciągu może korzystać z oprogramowania. Ponadto, kiedy dystrybutor wprowadza na rynek nową wersję, użytkownik nie jest zobowiązany do jej zakupu. Co jednak z perspektywy klienta najbardziej istotne, w tym tzw. tradycyjnym modelu, opłaca on ustaloną przez sprzedawcę kwotę w momencie zakupu. Na przykład, kupując program antywirusowy uiszcza on konkretną kwotę za dany okres korzystania np. 360 dni.

Cloud Computing w istotny sposób modyfikuje tradycyjne podejście do licencjonowania. Na wstępnie należy podkreślić, że w każdym modelu świadczenia usług w ramach Cloud Computing, mamy do czynienia z programami komputerowymi. W przypadku SaaS będą to aplikacje umieszczone na serwisach dostawców, do których użytkownik otrzymuje dostęp przez Internet i ma możliwość określonej interakcji z tymi aplikacjami (np. edycji dokumentów w *Google Docs*). W modelach IaaS i PaaS, oprogramowanie może być wykorzystywane przez dostawców jako element infrastruktury lub przez użytkowników, którzy posługują się narzędziami udostępnionymi przez providera do budowania lub transferu własnych albo zakupionych aplikacji. Model licencjonowania właściwy dla usług w chmurze będzie wykazywał wiele odmienności w stosunku do tego tradycyjnego. Ponieważ jednak cele podmiotów zaangażowanych w obrót nie będą w sposób zasadniczy odbiegać od tych w modelu dotychczas stosowanym, warto przyjrzeć się tym odmiennościom osobno analizując sytuację każdego z nich. Tak jak bowiem w przypadku tradycyjnych licencji, licencjodawca będzie poszukiwał możliwości maksymalnego zwiększenia swoich zysków, dostawca prawa, które pozwoli mu przygotować najlepszą ofertę dla klientów, a użytkownikowi końcowemu zależeć będzie na maksymalnej realizacji oczekiwań przy minimalizacji kosztów[168].

Analizując nowy typ licencjonowana z perspektywy licencjodawcy należy stwierdzić, że Cloud Computing będzie od niego wymagał nowego podejścia ze względu na fakt, że wielu, często niemożliwych do zidentyfikowania użytkowników będzie chciało równocześnie korzystać z oprogramowania (wielodzierżawa), a provider będzie dążył do instalowania tego

[167] Ibidem, s.280.
[168] H. Ward Classen, Marie Fogarty, *Avoiding Turbulence in the Cloud: Licensing and Contractual Issues for Licensor, Cloud Provider and End User*, The Computer & Internet Lawyer, tom. 19, nr 2, luty 2012.

oprogramowania na kilu serwerach (co umożliwi mu wirtualizacja). W interesie licencjodawcy leżeć musi uzyskanie pełnej rekompensaty za każdego użytkownika. Tym samym, będzie on starał się dobrać odpowiedni model opłaty np. jedna opłata dla całej infrastruktury (bez względu na ilość korzystających)[169].

Specyfika umów Cloud Computing sprowadza się min. do tego, że licencjobiorcą przeważnie będzie provider (chyba, że dostawca będzie równocześnie licencjodawcą. Przykładem takich podmiotów jest *Google* czy *Microsoft*, które oferują usługi bezpośrednio do użytkownika końcowego). Licencjobiorca, jeśli jest nim provider, będzie dążył do możliwie szerokiej ekspansji oprogramowania, gdyż jest to jego źródłem zysków. Musi więc zadbać, aby w umowie z licencjodawcą przewidziana była możliwość dystrybucji. Dla przykładu, polska ustawa pr. aut wskazuje art. 67 ust. 3, że *„jeżeli umowa nie stanowi inaczej, licencjobiorca nie może upoważnić innej osoby do korzystania z utworu w zakresie uzyskanej licencji"*. Prawa do udzielenia sublicenji, nie można zatem domniemywać. W umowach Cloud Computing taka klauzula powinna być umieszczona. Ze względu jednak na znaczną ilość zawieranych sublicencji, licencjobiorca zazwyczaj nie będzie miał możliwości kontroli każdej takiej umowy- stąd częstą praktyką będą wzorce umowne.

Licencja nie powinna także zawierać ograniczeń terytorialnych. Ponownie posiłkując się przykładem z polskiej ustawy, została tu ustanowiona zasada, że jeśli w licencji nie określono terytorium, na którym umowa obowiązuje, to należy przyjąć, że będzie to terytorium państwa, gdzie licencjobiorca ma swoją siedzibę (art. 66 ust.1). Jedną z podstawowych cech Cloud Computing jest brak ograniczeń terytorialnych jeśli chodzi o miejsca, gdzie przechowywane są dane (centra danych). Każde umowne zawężenie będzie zatem na niekorzyść licencjobiorcy i może prowadzić do wkroczenia w zakres autorskich praw majątkowych.

W kwestii opłaty licencyjnej, dostawcy będzie zależało, by model naliczania odpowiednio współgrał z potrzebami użytkowników końcowych. Coraz częściej będzie to model abonamentowy (subskrypcyjny) lub opłata wyliczana na podstawie łącznego (liczonego w godzinach) dostępu do oprogramowania. Istotną kwestią, na którą zwracają uwagę autorzy publikacji „*Avoiding turbulence in the Cloud*: *Licensing and Contractual Issues for Licensors, Cloud Providers and End Users*" jest także umożliwienie dostępu do oprogramowania przez klientów użytkownika końcowego. Ich zdaniem, umożliwienie takim użytkownikom korzystania z aplikacji powinno być traktowane, jako część ogólnego zużycia przez użytkownika końcowego[170]. Takie postanowienie powinno jednak stać się częścią

[169] Ibidem.
[170] H. Ward Classen, Marie Fogarty, Ibidem.

umowy, by nie doprowadzić do sytuacji, gdy krąg odbiorców oprogramowania zostanie maksymalnie poszerzony, bez zapewnienia odpowiedniej gratyfikacji dla licencjodawcy.

Analizując kwestię licencjonowania z perspektywy użytkownika końcowego należy stwierdzić, że dla niego najważniejsze będzie zagwarantowanie przez dostawcę poziomu usługi, który w pełni odpowiada jego potrzebom i jest przy tym atrakcyjny finansowo. Tak jak wspomniano, w umowach Cloud Computing użytkownik końcowy zazwyczaj nie będzie otrzymywał licencji na korzystanie z oprogramowania, ale usługę polegającą na świadczeniu tego oprogramowania przez dostawcę. Opłata będzie odpowiadała rzeczywistemu zużyciu (*pay-as-you-go*). Przedmiotem transakcji jest tu zatem usługa, nie licencja.

W tym miejscu przedstawione zostaną zaledwie wybrane zagadnienia z zakresu licencjonowania w chmurze obliczeniowej. Przeprowadzona zostanie analiza problemów charakterystycznych dla licencji w usługach SaaS, IaaS a także interesującego zagadnienia, jakim jest licencjonowanie oprogramowania udostępnionego w chmurze na zasadzie *open-source* (tu pojawi się przede wszystkim problem *copyleft*).

3.2.2. Licencje na programy udostępniane w modelu SaaS na gruncie prawa polskiego

Istota SaaS została przybliżona w części dotyczącej modeli dostarczania usług Cloud Computing. Warto w tym miejscu jedynie przypomnieć, że SaaS tj. oprogramowanie jako usługa, zakłada udostępnienie użytkownikom gotowych programów na serwerach dostawcy, z których użytkownik może korzystać w dowolnym miejscu i czasie bez konieczności instalowania oprogramowania na dysku twardym. SaaS jest najczęściej wybieranym modelem spośród SPI. Flagowym przykładem takiej usługi jest CRM oraz poczta *e-mail*, gdzie klient korzysta z infrastruktury i aplikacji dostawcy. Także *Facebook* czy *nk.pl* to *storage cloud* tj. chmura dająca użytkownikom możliwość gromadzenia danych na udostępnianej przez providera platformie.

Prawne aspekty Cloud Computing są dla polskiej doktryny prawa autorskiego zagadnieniem wciąż nowym, jednak kwestia umów licencyjnych na oprogramowanie udostępniane w ramach SaaS, już dziś wywołuje wiele kontrowersji. Tłem dla nich jest brzmienie przepisów dotyczących ochrony programów komputerowych w polskiej ustawie prawo autorskie i prawa pokrewne z 1994 r. (pr. aut.). Przepis art. 74 ust. 4 pkt. 1 mówi, że do autorskich praw majątkowych do programu komputerowego zalicza się prawo do *„trwałego i czasowego zwielokrotnienia programu komputerowego w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie w zakresie, w którym dla wprowadzania,*

wyświetlania, stosowania, przekazywania i przechowywania programu komputerowego niezbędne jest jego zwielokrotnienie, czynności te wymagają zgody uprawnionego". Oznacza to, że każde zwielokrotnienie programu komputerowego, który jest przedmiotem prawa autorskiego, tj. nosi cechy utworu w rozumieniu ustawy, wymaga zgody twórcy.

Jak już kilkakrotnie podkreślono, w przypadku SaaS użytkownik korzysta z oprogramowania na serwerach dostawcy. Nie dochodzi tym samym do reprodukcji tj. zwielokrotnienia, gdyż klient nie powiela żadnych komponentów na swoim dysku twardym. To prowadzi do wniosku, że zawarcie umowy licencyjnej nie jest konieczne, ponieważ samo takie używanie nie będzie wkraczało w domenę autorskich praw majątkowych twórcy. Taki pogląd – choć nie odnosi się bezpośrednio do Cloud Computing- został zaprezentowany w Komentarzu do ustawy pr. aut. pod redakcją Janusza Barty i Ryszarda Markiewicza. Podjęto tu próbę odpowiedzi na pytanie, czy *„wyświetlenie, stosowanie, przekazywanie i przechowywanie programu komputerowego same w sobie stanowią reprodukcję*"? tj. czy czynności te naruszają autorskie prawa majątkowe nawet, gdy nie dochodzi do fizycznego zwielokrotnienia? Autorzy Komentarza udzielają odpowiedzi przeczącej[171]. Przenosząc te rozważania na grunt SaaS można zatem stwierdzić, że samo wyświetlenie czy stosowanie aplikacji umieszczonej na platformach dostawcy, nie wkracza w zakres praw autorskich i z tego względu nie będzie wymagane zawarcie licencji.

Pojawia się jednak stanowisko, że użytkownik co prawda nie powiela aplikacji, ale i tak dokonuje pewnych czynności, z tym że w systemie informatycznym providera[172]. Taki pogląd jest zgodny z szerokim rozumieniem art. 74 ust. 4 pkt 1, gdzie nie fizyczna lokalizacja programu, a faktyczny zakres korzystania powinien decydować o konieczności udzielenia licencji[173]. Przyjęcie tego stanowiska doprowadziłoby do sytuacji, gdzie każda umowa dotycząca usługi oferowanej w ramach SaaS, powinna zawierać postanowienia właściwe dla licencji. To bez wątpienia w lepszy sposób gwarantuje prawa twórcy, jednak komplikuje obrót i mogłoby przyczynić się do mniejszego zainteresowania Cloud Computing.

Można także spotkać się próbą zakwalifikowania użytkownika SaaS jako „legalnego posiadacza"[174] z art. 75 ust. 1 pr. aut. Zgodnie treścią tego przepisu, *„jeżeli umowa nie*

[171] J. Barta (red.), R. Markiewicz (red.), M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, K. Felchner, E. Traple, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, wyd. V*, LEX 2011, nr 8545, Komentarz do art. 74 ust. 4 pkt. 1.
[172] Roman Bieda, *Prawne aspekty SaaS*, http://prawnik.net.pl/content/view/108/6/, odczyt 25.04.2012 r.
[173] Raport: Cloud Computing i jego aspekty prawne., Ibidem.
[174] Ibidem.

stanowi inaczej, czynności wymienione w art. 74 ust. 4 pkt 1 i 2[175] *nie wymagają zgody uprawnionego, jeżeli są niezbędne do korzystania z programu komputerowego zgodnie z jego przeznaczeniem, w tym do poprawienia błędów przez osobę, która legalnie weszła w jego posiadanie*". Problemem, jaki tutaj powstaje jest stwierdzenie, czy użytkownika takiego oprogramowania można uznać jako „posiadacza"? Tradycyjne rozumienie będzie wskazywało w tym wypadku bardziej na posiadacza nośnika oprogramowania. Wykładnia celowościowa, zakładająca, że „posiadanie" nie musi się tu wiązać z nabyciem materialnego nośnika, mogłoby prowadzić do przyjęcia, że przepis ten znajdzie zastosowanie do użytkownika oprogramowania oferowanego jako SaaS. To powodowałoby brak konieczności zawierania umowy licencyjnej. Z racji jednak faktu, że przywołany przepis ma na celu wprowadzenie absolutnych wyjątków ograniczających autorskie prawa majątkowe (których zakres dla programów komputerowych został w ustawie określony dość szeroko), to jego stosowanie w tym przypadku wydaje się wątpliwe.

Są jednak przypadki, gdy uruchomienie danej aplikacji będzie wymagało zainstalowania jego komponentów[176] na przykład w postaci tzw. wtyczek (*plug-in*) na komputerze. Wydaje się, że w takim wypadku nie powinno być wątpliwości co do konieczności zawarcia licencji.

Powyższe rozważania są istotne nie tylko ze względów prawnoautorskich. Uznanie, iż na oprogramowanie udostępniane w ramach SaaS konieczna jest licencja, będzie miało znaczenie z punktu widzenia prawa podatkowego. Zakup licencji, zgodnie z treścią art. 16b ust.1 pkt.5 ustawy o podatku dochodowym od osób prawnych[177], jako jeden z elementów należących do kategorii wartości niematerialnych i prawnych, podlega amortyzacji tak jak koszty trwałe, z zastrzeżeniem, że przewidywany czas używania jest dłuższy niż rok. Jeśli nie dojdzie do zawarcia licencji, SaaS może być traktowane wyłącznie jako usługa korzystania z oprogramowania, która podlegać będzie rozliczeniu jako koszt uzyskania przychodów na podstawie wskazanej ustawy.

[175] Punkt pierwszy tego przepisu cytowano wcześniej. W punkcie 2 mowa o *„tłumaczeniu, przystosowaniu, zmianach układu lub jakichkolwiek innych zmianach w programie komputerowym, z zachowaniem praw osoby, która tych zmian dokonała*"

[176] Raport Kancelarii Radcy Prawnego Stefan Cieśla: *Cloud Computing i jego aspekty prawne.*, Warszawa, 2011

[177] Art. 16b ust.1 lit.5 Ustawy o podatku dochodowym od osób prawnych mówi, że *„Amortyzacji podlegają, z zastrzeżeniem art. 16c, nabyte nadające się do gospodarczego wykorzystania w dniu przyjęcia do używania: licencje o przewidywanym okresie używania dłuższym niż rok, wykorzystywane przez podatnika na potrzeby związane z prowadzoną przez niego działalnością gospodarczą albo oddane przez niego do używania na podstawie umowy licencyjnej (sublicencji), umowy najmu, dzierżawy lub umowy określonej w art. 17a pkt 1, zwane wartościami niematerialnymi i prawnymi*".

3.2.3. Licencje software w ramach IaaS

Interesujące zagadnienia związane z licencjonowaniem pojawiają się również w środowisku IaaS. W tym wypadku, dostawca udostępnia klientom całą infrastrukturę obejmującą system operacyjny oraz możliwość eksploatowania własnego, gotowego oprogramowania. Aplikacje przeniesione do infrastruktury przez użytkownika, mogą być przedmiotem umów o eksploatację utworów, w tym umów licencyjnych. Można zatem wyobrazić sobie sytuację, że umowa licencyjna nie będzie przewidywać możliwości umieszczenia oprogramowania w infrastrukturze dostawcy usługi, gdyż sytuacja taka może być uznana jako nowa forma eksploatacji utworu. Korzystając z oprogramowania w środowisku IaaS, użytkownik może wkroczyć tym samym w zakres praw autorskich twórcy oprogramowania. Rozstrzygnięcie, czy klient IaaS dopuścił się naruszeń w dużej mierze zależeć będzie od zbadania postanowień konkretnej umowy.

Analizując wskazaną sytuację na gruncie polskiego prawa autorskiego pojawia się tu problem pola eksploatacji, w tym pola nieznanego w chwili zawarcia umowy. Pierwsze pytanie, jakie się w tej sytuacji może nasuwać, to czy korzystanie z oprogramowania w infrastrukturze IaaS jest nowym polem eksploatacji, czy jest to zaledwie pewna forma dotychczasowego używania, z tym tylko założeniem, że centrum danych (a tym samym aplikacja) znajduje się nie wewnątrz, a na zewnątrz organizacji. IaaS jest bowiem sposobem outsourcingu potrzeb klienta w zakresie działania centrum danych, gdzie dostęp do danych odbywa się przez Internet.

Wydaje się, że o uznaniu korzystania z oprogramowania w środowisku IaaS za odrębne pole eksploatacji może decydować fakt, że udostępnienie odbywa się w sposób technicznie odmienny[178]. Ze względów technicznych, czym innym jest bowiem sytuacja, gdy posiadacz praw autorskich do oprogramowania sprzedaje je z licencją na kilka stanowisk komputerowych, gdzie oryginał będzie fizycznie zainstalowany wewnątrz organizacji, a czym innym jeśli program transferowany jest do infrastruktury zewnętrznej a użytkownik uzyskuje do niego dostęp przez Internet. Choć z perspektywy użytkownika końcowego, sposób dostępu do aplikacji nie będzie miał znaczenia, to wydaję się, że dla właściciela praw autorskich może to oznaczać odmienną formę korzystania z utworu, a więc odmienne pole eksploatacji.

Do podobnych rezultatów może doprowadzić przyjęcie stanowiska, że o ustaleniu czy mamy do czynienia z odrębnym polem eksploatacji decydować będzie stwierdzenie, że

[178] J. Barta i R. Markiewicz „*odmienność technicznego sposobu zwielokrotnienia lub rozpowszechnienia dzieła*" traktują jako jedno z kryteriów uznania, iż pojawiło się nowe lub odrębne pole eksploatacji, Janusz Barta, Ryszard Markiewicz, *Prawo autorskie*, wd. Oficyna 2010 r., s.118-119.

„następuje znaczne zwiększenie się dostępności utworu, poszerzenie możliwości zapoznawania się z nim przez odbiorców, czemu towarzyszy osiągnięcie istotnych korzyści majątkowych przez osoby trzecie"[179]. Za *„zwiększeniem dostępności*" utworu może w tym wypadku przemawiać fakt, że celem umieszczenia go w infrastrukturze IaaS jest uczynienie go kompatybilnym z całym systemem i osiągalnym na żądanie użytkownika w każdej chwili, a więc łatwiej dostępnym. „Korzyści" są udziałem zarówno użytkownika, który dokonuje transferu w celu oszczędności związanych z brakiem konieczności zakupu *hardware* i *software*, dzięki czemu korzystanie z oprogramowania staje się dla niego prostsze, jak i dostawcy, który otrzymuje opłatę za udostępnienie infrastruktury.

Przyjęcie jednoznacznego poglądu w tej kwestii jest o tyle ważne, że zgodnie z opinią niektórych autorów, nieobjęcie pola eksploatacji umową skutkuje nieudzieleniem licencji na tym polu eksploatacji, gdyż nie zostaje zrealizowany obowiązek z art. 41 ust. 2 pr. aut mówiący, że *„umowa o przeniesienie autorskich praw majątkowych lub umowa o korzystanie z utworu zwana dalej licencją, obejmuje pola eksploatacji wyraźnie w niej wymienione"*[180]. Wydaje się jednak, że w tym wypadku należy– zgodnie z liberalną wykładnią- posłużyć się klauzulą interpretacyjną z art. 65 (k.c.)[181] i na jej podstawie ocenić zgodny zamiar stron[182]. W umowie powinno znaleźć się jednak postanowienie dotyczące możliwości zwielokrotnienia oprogramowania w środowisku zewnętrznym. Ewentualne wątpliwości powinny być natomiast rozstrzygane na podstawie ogólnych reguł interpretacyjnych z k.c.

Renzo Marchini wskazuje kilka klauzul interpretacyjnych, które mogą być przydatne przy ocenie umowy licencyjnej pod kątem ewentualnej możliwości korzystania z programu komputerowego w infrastrukturze IaaS. Według niego, postanowienie wskazujące, że oprogramowanie może być użyte na tylko jednym, określonym komputerze wyklucza możliwość korzystania w wirtualnym środowisku. Podobnie, jeśli w umowie znajdzie się klauzula mówiąca, że program może być użyty wyłącznie w konkretnej lokalizacji, to korzystanie z niego w chmurze (co wynika z istoty chmury) nie jest dozwolone. Inną klauzulą

[179] J. Barta (red), R. Markiewicz (red.) komentarz do art. 17 ustawy pr. aut., Ibidem.
[180] J. Barta, R. Markiewicz, *Prawo Autorskie*, Ibidem, s.207-211.
[181] Art. 65 Kodeksu cywilnego określa, że *„§ 1. Oświadczenie woli należy tak tłumaczyć, jak tego wymagają ze względu na okoliczności, w których złożone zostało, zasady współżycia społecznego oraz ustalone zwyczaje. § 2. W umowach należy raczej badać, jaki był zgodny zamiar stron i cel umowy, aniżeli opierać się na jej dosłownym brzmieniu".*
[182] Taki pogląd E. Traple, Ibidem, s 39-40.

uniemożliwiającą korzystanie z *software* w chmurze będzie taka, która zaznacza, że oprogramowanie jest poufne[183].

Marchini zwraca też uwagę na sytuację dostawcy. Przyjęcie założenia, że dostawca „korzysta" z oprogramowania objętego licencją umieszczonego w infrastrukturze przez użytkownika, a więc na polach eksploatacji wymienionych w licencji, prowadziłoby do uznania, że -zgodnie z przywołanym wcześniej przepisem art. 67 ust. 3 pr. aut.- powinna zostać udzielona sublicencja. W tym wypadku wątpliwe byłoby jednak uznanie, że dostawca „korzysta" z programu. W dalszym ciągu to licencjobiorca jest podmiotem korzystającym, a provider tylko udostępnia infrastrukturę ułatwiającą to korzystanie. Konieczność udzielania sublicencji dostawcy jest zatem dyskusyjna. Nie powinno budzić jednak wątpliwości, że w umowie licencyjnej musi być przynajmniej zawarte stwierdzenie, że licencjodawca wyraża licencjobiorcy zgodę na „udostępnianie" programu komputerowego.

3.3. Cloud Computing a oprogramowanie Open Source- problem *copyleft*

Dostawcy usług w chmurze obliczeniowej często korzystają z aplikacji lub narzędzi rozwoju opartych na licencjach *open source.* Programy udostępniane w ramach modelu SaaS oraz platforma PaaS mogą być zatem zbudowane z komponentów, co do których licencja wskazuje, że powinny być one udostępniane razem z kodem źródłowym tj. zrozumiałym dla człowieka ciągiem poleceń i instrukcji, które odczytuje komputer.

Za Januszem Bartą i Ryszardem Markiewiczem należy przyjąć, że licencja *open source* jest *„kategorią zbiorczą obejmującą różne postacie umów dotyczących programów komputerowych, charakteryzujące się udostepnieniem programu także w wersji źródłowej (obok wersji „maszynowej"), połączone z upoważnieniem do wprowadzania zmian do programu i dalszego jego rozpowszechniania na podstawie tej licencji"*[184]. Podstawowym elementem takiej licencji jest zatem *„zobowiązanie użytkownika do udostępnienia modyfikacji programu (…) na takich samych warunkach jak określone w licencji, z której skorzystał (tzw. oprogramowanie copyleft)"*[185]. Zasada *copyleft* stanowi, że udostępniając program nie mogą być ograniczone wolności, które wraz z programem otrzymano[186]. Z racji tego, że porównuje się ekspansję wolności oprogramowania do rozprzestrzeniania się wirusa, *copyleft* jest czasami określane jako *„viral effect"* (efekt wirusowy)- użytkownik, który wnosi do

[183] R. Marchini, Ibidem, s. 92.
[184] J. Barta, R. Markiewicz (red.), s.234.
[185] E. Traple, Ibidem, s.295.
[186] Joanna Kulesza, *Ius Internet. Między prawem a etyką*, Wyd. Akademickie, Warszawa 2010, s. 173.

programu swój wkład intelektualny, nie może tego efektu pracy twórczej licencjonować na tradycyjnych zasadach[187].

Do kategorii licencji *open source* należą min. licencje GNU[188]. Jedna z najczęściej stosowanych- GNU GPL 3.0. wskazuje, że można kopiować i rozpowszechniać program lub opartą na nim pracę, ale konieczne jest dołączenie do niego odpowiadającego mu, kompletnego i możliwego do odczytania przez urządzenia cyfrowe kodu źródłowego[189]. Są jednak przypadki licencji typu *open source*, gdzie użytkownik może tworzyć nowe lub modyfikować oprogramowanie, bez konieczności udostępniania kodu źródłowego. Przykładem jest licencja MIT (X11)[190]. Obowiązkiem użytkownika, jeśli chce uniknąć konieczności udostępnienia pełnego kodu źródłowego, powinno być zatem, dokładne przestudiowanie umowy na oprogramowanie, z którego zamierza skorzystać.

Warto jednak zauważyć, że w licencji GPL 3.0 mowa jest o rozpowszechnianiu programu lub zmodyfikowanej wersji w tym znaczeniu, że użytkownik z założenia otrzymuje dostęp do pełnego kodu źródłowego. W SaaS nie ma jednak mowy o udostępnianiu kodu, a tylko jego używaniu lub uruchamianiu w postaci gotowej aplikacji zazwyczaj bez możliwości modyfikacji[191]. Z tego względu, SaaS zostało poddane wielowątkowej krytyce ze strony *Free Software Foundation* (FSF) jako szkodzące idei *open source*[192].

Niedługo po opublikowaniu licencji GNU GPL w wersji 3.0 (2007 r.) zaczęły pojawiać się na rynku usługi SaaS (np. *Google Apps*), które nie są kompatybilne z licencją GNU GPL, właśnie ze względu na brak udostępnienia całości kodu źródłowego. W specjalnym manifeście *„Komu tak naprawdę służy ten serwer”*[193] Richard Stallman (założyciel FSF, twórca GNU i zasady *copyleft*) zdecydowanie skrytykował SaaS. Według niego, SaaS jest problemem, który prowadzi do ograniczenia wolności w Internecie ze względu na nieudostępnienie użytkownikowi kodu źródłowego i kodu wykonalnego. Głównym problemem SaaS jest jednak- według niego- fakt, że SaaS działa tak jak program

[187] Wojciech Machała, *Licencja mieszana? Prawnoautorskie aspekty obrotu programami komputerowymi stworzonymi przy wykorzystaniu oprogramowania o otwartym kodzie*, Zeszyty Naukowe UJ, zeszyt 110, 2007 r.
[188] Inną licencją copyleft jest Mozzilla Public License, dostępna na stronie http://www.mozilla.org/MPL/1.1/, odczyt 30.03. 2012 r.
[189] Licencja GNU GPL 2.0 dostępna na stronie http://www.gnu.org/licenses/gpl.html, odczyt 30.03.2012 r.
[190] Z treści licencji MIT dostępnej na stronie http://www.opensource.org/licenses/mit-license.php (odczyt 30.03.2012 r.) wynika, że osoba, która weszła w posiadanie oprogramowania może go wprowadzać do obrotu bez ograniczeń także w zakresie modyfikacji.
[191] William Judd, *SaaS Threatens Open Source*, 28.01. 2011 r., http://williamjudd.com/2011/01/28/the-threat-of-saas-to-open-source/, odczyt 30 .03.2012 r.
[192] *Free Software Foundation* została założona w 1985 r. przez Richarda Stallmana zajmująca się promocją idei tzw. „projektu GNU” tj. projektu zakładającego wymianę idei bez ograniczeń wprowadzanych przez właścicieli oprogramowania, w: Joanna Kulesza, Ibidem, s. 142-143.
[193] Polskie tłumaczenie (oryginał „*Who does that server really serve*”) jest dostępne na stronie http://www.gnu.org/philosophy/who-does-that-server-really-serve.html, odczyt 30 03.2012 r.

typu *spyware* tj. program komputerowy, który poza swoją podstawową funkcją, zbiera również informacje o użytkownikach[194]. Za typowy przykład SaaS, Stallman uznaje *Google Docs*, gdyż podstawowym celem tej aplikacji jest umożliwienie użytkownikom edycji plików (przy jednoczesnym przetwarzaniu danych przez tą aplikację).

Reakcją Fundacji na popularyzację Cloud Computing, był nowy typ licencji *GNU Afferro GPL* (AGPL). Zakłada ona, że jeżeli dochodzi do uruchomienia programu na serwerze i zezwolenia innym na korzystanie z niego, to musi istnieć możliwość pobrania kodu źródłowego do tego programu. Co więcej, każda modyfikacja powinna być udostępniona z kodem źródłowym[195]. Licencja AGPL nie weszła jednak do powszechnego użytku[196]. Trudno bowiem spodziewać się, że samo udostępnienie kodu źródłowego może być sposobem na zwalczanie podstawowego (według FSF) problemu (zgodnie z przedstawionym poglądem Stallmana) dotyczącego SaaS tj. niekontrolowanego przetwarzania danych.

Na koniec tej części warto również wspomnieć, że problem *copyleft* będzie dotyczył także innych usług z modelu SPI. Jak się może wydawać, z perspektywy użytkownika SaaS jest on najmniej dotkliwy, gdyż w zasadzie nie ma on żadnego wpływu na kształt środowiska, w którym umieszczona jest aplikacja. W przypadku PaaS i IaaS problem ma o wiele większą wagę, gdyż wpływ klienta na infrastrukturę jest znaczny. Źródłem tych zagadnień sytuacja, gdy element infrastruktury (np. oprogramowanie) udostępniany użytkownikowi jest zbudowany na bazie licencji *open source*. W tym wypadku, takie udostępnienie może być traktowane jako „*dystrybucja*" i nowa aplikacja, budowana w oparciu o to oprogramowanie, będzie objęta *viral effect*[197]. Po stronie użytkownika takich usług powstaje zatem ryzyko konieczności udostępnienia kodu źródłowego. Szczególnie klient PaaS będzie narażony na tego rodzaju problem, gdyż nie kontroluje on platformy służącej do wdrażania aplikacji[198]. Jeśli zatem składa się ona z komponentów licencjonowanych na zasadzie *open source*, to deweloper powinien – zgodnie z założeniem *copyleft*- udostępnić pełny kod źródłowy stworzonego programu (niejednokrotnie o znacznej wartości).

W ogólnym jedynie zarysie należy dodać, że na gruncie prawa polskiego zagadnienie *copyleft* będzie problematyczne, jeżeli jego zastosowanie będzie gwarantować więcej, niż wynika to z monopolu autorskiego. Do takiej sytuacji może dojść, jeżeli licencjobiorca zostanie zobowiązany do udostępnienia kodu źródłowego programu, który jest na gruncie pr.

[194] Ludwik Krakowiak, *Spyware coraz groźniejszy*, www.pcworld.pl, 12.08. 2005 r., http://www.pcworld.pl/news/81989/Spyware.coraz.grozniejszy.html, odczyt 30 .03.2012 r.
[195] Licencja AGPL dostępna na stronie http://www.gnu.org/licenses/agpl.html , odczyt 30 .03.2012 r.
[196] W. Judd, Ibidem.
[197] R. Marchini, Ibidem, s. 93-94.
[198] Bradley J. Waltz, *Open Source Software in the Cloud*, Intellectual Property Litigation, tom 23, nr 1

aut. tylko inspiracją[199] (pojawia się pytanie, gdzie kończy się inspiracja a zaczyna opracowanie)[200]. Według Krzysztofa Siewicza, rozważaniom na temat *copyleft* w prawie polskim, powinna przyświecać teza, o niemożliwości rozszerzania monopolu autorskiego w przedmiocie ochrony programów komputerowych[201]. Wątpliwości pojawiają się także na tle rozróżnienia idei niepodlegającej ochronie i sposobu wyrażania tej idei. Najkrócej mówiąc, na gruncie prawa polskiego, trudno przesądzić o naturze *copyleft*. Jeżeli zatem deweloper aplikacji w środowisku PaaS korzysta z narzędzi do jej budowy objętych licencją c*opyleft*, to prawo polskie nie przesądza jednoznacznie o konieczności udostępnienia kodu źródłowego do stworzonego programu. Wobec tego, w każdym, jednostkowym przypadku, konieczne będzie dokonanie odrębnej oceny.

Powyższe rozważania a także dane wskazujące, że aż dziewięćdziesiąt procent oprogramowania Cloud Computing opiera się na licencjach *open source*, uprawniają do przyjęcia wniosku, że użytkownik usługi w modelu SPI, a w szczególności odbiorca usług zakładających udostępnienie infrastruktury i możliwość budowania własnych (często wartościowych) aplikacji, powinien zwrócić szczególną uwagę na system licencjonowania poszczególnych elementów infrastruktury. Straty, również finansowe, spowodowane przez nieuwagę odbiorcy, mogą być znaczne.

[199] Przez pojęcie utworu inspirowanego na gruncie pr.aut rozumie się: „*Utwór powstały z podniety twórczej innego utworu jest objęty prawem autorskim niezależnym. Przez utwór inspirowany należy rozumieć zaczerpnięcie wątku cudzego utworu, a zgoda autora dzieła inspirującego jest zbędna*", opracowania tj. „*tak zwane „dziełami z drugiej ręki", pozostają w tak ścisłym związku z przynajmniej niektórymi elementami utworu wcześniejszego, że ich rozpowszechnianie zawsze wkracza w sferę osobistych i majątkowych praw twórcy utworu pierwotnego*" tak w: J. Barta, R. Markiewicz, Komentarz do art.2 pr.aut., Ibidem. Ponadto, SN w orzeczeniu z dnia 10 maja 1963 r., II CR 128/63, OSNC 1964, nr 4, poz. 74 stwierdził, że „*jeżeli twórczość została tylko podbudowana przez cudze dzieło, lecz autor nie przejmuje do swego utworu ani treści, ani formy cudzego dzieła, to ma się wtedy do czynienia z twórczością samodzielną w rozumieniu art. 3 § 4 prawa autorskiego*".

[200] Krzysztof Siewicz, *Zakres klauzuli copyleft w prawie polskim*, Prace Instytutu Prawa Własności intelektualnej UJ, zeszyt 93, s.251.

[201] Ibidem.

Rozdział 4. Jurysdykcja i prawo właściwe. Problemy prawa prywatnego międzynarodowego w chmurze obliczeniowej

4.1. Problemy podstawowe

Istotą Cloud Computing jest, jak już wielokrotnie wspominano, świadczenie usług w Internecie, z których odbiorca może korzystać w dowolnym miejscu, w dowolnym czasie i dowolnym zakresie. Trudno tu zatem o sprecyzowanie zarówno miejsce świadczenia usługi, miejsce odbioru lub miejsce powstania szkody. Z takim problemem, sądy na całym świecie spotykają się od dawna. Fragmentacja elementów stanu faktycznego jest bowiem charakterystyczna dla wszystkich spraw związanych z usługami, do których klient ma dostęp za pośrednictwem Internetu. Do tej pory nie udało się stworzyć uniwersalnych reguł prawa prywatnego międzynarodowego, które znalazłyby zastosowanie dla tych kontraktów. W Unii Europejskiej opracowano szereg dokumentów, które ułatwiają kontakty handlowe (min. Dyrektywa o handlu elektronicznym, Rozporządzenie Rzym I, Rzym II, Bruksela I). Także w Stanach Zjednoczonych można zaobserwować kształtowanie się jednorodnej linii orzeczniczej. Są to jednak w dalszym ciągu regulacje jedynie wewnętrzne, które nie eliminują wątpliwości pojawiających się przede wszystkim w sytuacji, gdy prawo dwóch państw odmiennie reguluje właściwość prawa i sądu, strony nie dokonały stosownego wyboru w umowie lub, gdy zobowiązanie ma charakter pozaumowny.

W umowach na usługi Cloud Computing – ze względu na ich złożoność- zazwyczaj każdy element będzie wymagał odrębnej analizy[202]. Znajdą się tu zarówno uregulowania prawnoautorskie, kwestie związane z przetwarzaniem danych osobowych, świadczeniem usług drogą elektroniczną etc. Także delikty w chmurze mogą mieć różnorodny charakter np. naruszenia prawa do prywatności, wizerunku, niedozwolone wkroczenie w zakres autorskich praw majątkowych. Dodatkowo sprawę komplikuje fakt, że w dostarczaniu usług do klienta końcowego może brać udział kilka podmiotów. Jak się wydaje, z tymi problemami doktryna i orzecznictwo do tej pory się nie uporały.

Kwestia ustalenia sądu właściwego do rozstrzygania potencjalnych sporów ma w umowach Cloud Computing duże znaczenie ze względu na element transgraniczości. Strony zazwyczaj korzystają z przywileju wyboru sądu i prawa, obie kwestie przeważnie wiążąc ze sobą w ten sposób, że ustalony zostaje sąd i prawo właściwe dla siedziby dostawcy (tak będzie przede wszystkim w sytuacji, gdy provider przedstawia wzorzec umowny).

[202] J. Burke, Ibidem.

Jednak ze względu na odmienne uregulowania i problemy odnoszące się do tych dwóch elementów, warto przyjrzeć się im z osobna. Poniżej zostaną poddane analizie zasady dotyczące określania prawa i sądu właściwego, ze szczególnym naciskiem na prawo Unii Europejskiej oraz prawo polskie.

4.2. Oznaczenie sądu właściwego dla umów w modelu Cloud Computing

Ustalenie sądu, który będzie właściwy do orzekania w kwestii dotyczącej Cloud Computing związane jest z problematyką jurysdykcji sądowej. W tym znaczeniu, jurysdykcja to *„prawo", „kompetencja" lub „upoważnienie", które przynależne jest państwu do stosowania prawa i utrzymywania porządku prawnego na swoim terytorium we wszystkich dziedzinach"*[203]. Innymi słowy, jurysdykcja to zdolność państwa do poddania stron sporu pod właściwość znajdujących się na jego terytorium organów (sądów, trybunałów) prawnie umocowanych do prowadzenia postępowań[204]. O tym, czy dana sprawa będzie powiązana z terytorium państwa, będą decydować łączniki. Dla przykładu, polski Kodeks postępowania cywilnego (k.p.c.) w art. 1103 wskazuje, że takim podstawowym łącznikiem jest miejsce zamieszkania (odpowiednio stałego pobytu czy siedziby) pozwanego. W dalszej części Działu VI k.p.c., wskazanych zostało kilka sytuacji, które stanowią odstępstwo od tej zasady, a w których znalazł zastosowanie łącznik miejsca np. miejsca wykonania zobowiązania, powstania deliktu, działalności oddziału etc.

Powyższe, klasyczne (gdzie podstawowym łącznikiem jest terytorium) rozumienie jurysdykcji niejednokrotnie będzie problematyczne dla stron zaangażowanych w spory dotyczące usług dostarczanych za pośrednictwem Internetu. W przypadku tego rodzaju stosunków, podział terytorialny i samo pojęcie „miejsca" tracą na znaczeniu. Cyberprzestrzeń ma bowiem charakter aterytorialny i dlatego- jak twierdzi Joanna Kulesza- nie wywołają skutku wysiłki zmierzające do podporządkowania stosunków prawnych powstających za pośrednictwem sieci do terytorium danego państwa[205]. Innego zdania są jednak autorzy publikacji *„Prawo Internetu"*, którzy twierdzą, że choć tradycyjne rozumienie „miejsca" stopniowo traci na znaczeniu, to wciąż możliwe jest stosowanie kryteriów związanych z terytorium[206].

[203] Paweł Grzegorczyk, *Jurysdykcja krajowa w sprawach z zakresu prawa własności przemysłowej*, wyd. Oficyna, Lex nr 65056.
[204] Kurt Wimmer, Eve Pogoriler, Stephen Sattarfield, *International Jurisdiction and the Internet in th Age of Cloud Computing,* The Bureau of National Affairs, Washington 2011, http://www.cov.com/files/Publication/, odczyt 20.03. 2012 r. .
[205] Ibidem, s.227.
[206] Paweł Podrecki (red.), *Prawo Internetu*, wyd. Lexis Nexis, Warszawa 2006, s. 114.

Prawidłowe rozstrzygnięcie w kwestii sądu właściwego dla stosunku prawnego będzie miało dla stron niebagatelne znaczenie. Postępowanie, które toczy się przed organem, który nie jest upoważniony do jego prowadzenia, będzie zazwyczaj dotknięte poważną wadą. K.p.c. w art. 1099 §2 stanowi, że postępowanie toczące się mimo braku jurysdykcji krajowej jest nieważne. Jurysdykcja jest zatem w polskim systemie prawnym przesłanką o charakterze bezwzględnym.

W przypadku konieczności ustalenia sądu właściwego, wewnętrzne uregulowania prawne państw, często muszą ustąpić uniwersalnym zasadom wyznaczonym przez międzynarodowe traktaty. Dla przykładu, w Polsce, prymat umów międzynarodowych przewidziany został w Rozdziale III Konstytucji[207]. Tym samym, w kwestii wyboru sądu właściwego zastosowanie znajdą przepisy Rozporządzenie Rady (WE) nr 44/2001 w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Bruksela I) dla spraw dotyczących obywateli 27 państw Unii oraz Konwencja z Lugano z 16 września 1988 r.[208] zmieniona nową Konwencją z 30 października 2007 r. zawarta w celu wzmocnienia współpracy między państwami UE a Norwegią, Szwajcarią i Islandią. Dopiero w przypadku, gdy wskazane akty nie znajdą zastosowania, należy sięgnąć po przepisy Działu VI k.p.c.

Najbardziej istotną kwestią, którą przewidują Rozporządzenie i Konwencja, jest reguła, że zamieszkały na terytorium państwa- strony może być pozywany przed sądy tego państwa niezależnie od obywatelstwa (odpowiednio art. 2 Rozporządzenia i art.2 Konwencji[209]). W rozumieniu tych przepisów, spółki i osoby prawne mają miejsce zamieszkania w miejscu, w którym znajduje się ich siedziba lub organ zarządzający lub główne przedsiębiorstwo. Dla roszczeń wynikających z umowy, osobę zamieszkałą na terytorium państwa członkowskiego można pozwać również przed sąd państwa, gdzie zobowiązanie zostało lub miało zostać wykonane (art. 5 ust.1a Rozporządzenia oraz art. 5 ust. 1a Konwencji[210]). Aby uniknąć częstych wątpliwości, w artykule tym zostało także przedstawione szczególne rozumienie

[207] Przepis art. 87 ust.1 Konstytucji RP wskazuje, że: „*Źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia*", z kolei zgodnie z treścią art. 91 ust. 1 „*Ratyfikowana umowa międzynarodowa, po jej ogłoszeniu w Dzienniku Ustaw Rzeczypospolitej Polskiej, stanowi część krajowego porządku prawnego i jest bezpośrednio stosowana, chyba że jej stosowanie jest uzależnione od wydania ustawy*". W ust. 2 tego art. ustanowiona jest reguła, że „*Umowa międzynarodowa ratyfikowana za uprzednią zgodą wyrażoną w ustawie ma pierwszeństwo przed ustawą, jeżeli ustawy tej nie da się pogodzić z umową*".

[208] Maksymilian Pazdan, *Prawo prywatne Międzynarodowe*, Wyd. Lexis Nexis, wyd. XIII, s.313.

[209] Konwencja z Lugano z 30 października 2007 r. dostępna na stronie: http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/l16029_pl.htm oraz Rozporządzenie Rady Bruksela I dostępne na stronie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:19:04:32001R0044:PL:PDF, odczyt 30.03.2012 r.

[210] Ibidem.

miejsca wykonania zobowiązania, którym – dla świadczenia usług- będzie miejsce, w którym usługi były lub miały być świadczone. Wskazane akty poruszają również zagadnienie sądu właściwego dla zobowiązań pozaumownych. Wedle przepisów art. 5 ust. 3 w takich przypadkach pozew można wnieść do sądu właściwego ze względu na miejsce, gdzie nastąpiło lub może nastąpić zdarzenie wywołujące szkodę. Nie wchodząc w szczegółowe dywagacje, warto dodać, że zarówno w Rozporządzeniu jak i w Konwencji, identycznie potraktowano kwestie jurysdykcji wyłącznej (kwestie związane z nieruchomościami, spółkami prawa handlowego, wpisów do rejestrów, praw własności intelektualnej etc.).

Szczególnie ważna regulacja dotyczy tzw. *prorogatio fori* tj. umowy o jurysdykcję. Wskazane akty prawa międzynarodowego przewidują, że strony mają dowolność co do wyboru sądu, który będzie umocowany do orzekania w razie zaistnienia sporu, jeśli co najmniej jedna z nich ma miejsce zamieszkania na terytorium państwa- strony Konwencji (art.23) lub Rozporządzenia (art.18). W sprawach konsumenckich, klient został uprzywilejowany, poprzez umożliwienie mu złożenia pozwu zarówno przed sąd miejsca zamieszkania kontrahenta, jak i przed sąd właściwy ze względu na swoje miejsce zamieszkania (art. 16 Rozporządzenia oraz art. 16 Konwencji). Warto wspomnieć, że powołane akty nie przewidują szczególnych wymogów co do formy umowy o jurysdykcję. Może być ona zawarta w formie pisemnej lub innej formie, która odpowiada praktyce przyjętej między stronami lub zwyczajom handlowym.

Przywilej wyboru sądu przez strony, nabiera w umowach szczególnego znaczenia, gdyż pozwala im to uniknąć często długich i kosztownych sporów[211]. Takie klauzule można odnaleźć w większości kontraktów. Tak jak wspomniano, przeważnie uprzywilejowują one dostawcę poprzez wskazanie sądu właściwego dla jego miejsca zamieszkania lub siedziby. Jak również wskazano, zazwyczaj wybór ten będzie połączony z określeniem prawa właściwego. Taką klauzulę można odnaleźć min. dla usług oferowanych przez *Google* w ramach *Google App*s: *„Wszelkie spory, które wynikły z niniejszych warunków lub usług bądź w związku z nimi, podlegają prawu stanu Kalifornia w Stanach Zjednoczonych, z wyjątkiem norm kolizyjnych obowiązujących w tym stanie. Wszystkie roszczenia powstałe na skutek tych warunków lub Usług bądź z nimi związane będą rozpatrywane wyłącznie w sądzie federalnym lub stanowym w hrabstwie Santa Clara w stanie Kalifornia w Stanach Zjednoczonych. Użytkownik i Google zgadzają się na osobistą jurysdykcję tych sądów”*[212]. W interesujący sposób skonstruowane są postanowienia w umowach na usługi świadczone

[211] Raport Cloud Computing. Aspekty prawne, Ibidem.
[212] Polityka prywatności Google, http://www.google.com/intl/pl/policies/terms/, odczyt 20.03.2012 r.

przez *Salesforce.com*. W zależności od miejsca zamieszkania użytkownika i oddziału firmy, który jest stroną umowy, wzorzec przewiduje inny sąd właściwy (np. dla klienta z Polski stroną umowy jest oddział *Salesforce.com* w Szwajcarii i tym samym sądem właściwym będzie sąd szwajcarski i prawem właściwym prawo szwajcarskie)[213]. Tego rodzaju klauzule, co prawda dają stronom pewność, jednak nie muszą być zgodne z interesem klienta, dla którego prowadzenie postępowania w często odległych miejscach, może być uciążliwe i kosztowne.

Problem pojawia się w sytuacji, gdy strony zaniechają wyboru sądu właściwego. Wracając na grunt prawa europejskiego, art. 4 Rozporządzenia Bruksela I wskazuje, że w sytuacji, gdy pozwany nie ma miejsca zamieszkania na terytorium państwa członkowskiego, jurysdykcję sądów będzie określać prawo wewnętrzne każdego z tych państw. Z perspektywy podmiotów z państw trzecich, Bruksela I może być zatem traktowana jedynie jako regulacja wewnętrzna UE, która nie stanowi dla nich ułatwienia[214]. Na przykład, gdy powód z Polski zamierza wytoczyć pozew przeciwko kontrahentowi z USA, zastosowanie znajdą przepisy polskiego k.p.c. W sprawach z zakresu zobowiązań, polski sąd będzie właściwy jeżeli: zobowiązanie z czynności prawnej zostało wykonane lub miało być wykonane na terytorium RP lub jeżeli delikt powstał na terytorium RP a także, jeśli roszczenie dotyczy działalności zakładu lub oddziału pozwanego (art. 1103 pkt. 1,2,3 k.p.c.). Jeśli stroną umowy jest konsument, to sprawa będzie należeć do jurysdykcji sądu polskiego, gdy klient będzie miał miejsce zamieszkania lub stałego pobytu w RP oraz, gdy spełnione są te warunki i podjął czynności niezbędne do zawarcia umowy. Kontrahent konsumenta będzie w takich sytuacjach traktowany tak jakby miał miejsce zamieszkania lub siedzibę w Polsce, jeśli czynność prawna została podjęta przez niego w związku z poradzeniem filii lub oddziału znajdujących się w Polsce (art. 1103^6 k.p.c.).

Szczególne wątpliwości w kontekście umów Cloud Computing, budzić będzie uregulowanie dotyczące miejsca wykonania usługi. Powyżej omówione postanowienia wskazują bowiem, że jurysdykcja sądów będzie zależna od miejsca spełnienia świadczenia (wykonania usługi) lub miejsca, gdzie świadczenie miało być spełnione. Istotą SaaS jest możliwość korzystania z oprogramowania ze sprzętu znajdującego się w dowolnej lokalizacji. Zasadne staje się zatem pytanie, czy miejscem wykonania będzie państwo- siedziba sprzedawcy (providera), państwo, gdzie aplikacja zostaje umieszona na serwerach, czy kraj

[213] *Saslesforce Master Subscription Agreement Developer Service*, http://www2.sfdcstatic.com/assets/pdf/misc/salesforce_Developer_MSA.pdf, odczyt 20.03. 2012 r.
[214] K. Wimmer, Ibidem.

odbiorcy? Najczęściej będzie to miejsce, gdzie sprzedawca lub provider podjął działanie zmierzające do umieszczenia informacji na serwerach tj. jego siedziba. Miejsce odbioru może być w tym przypadku dowolne[215].

Analogiczne rozważania można podjąć w kwestii sądu właściwego dla deliktów. Dla zdefiniowania deliktu można posłużyć się definicją przedstawioną przez Marka Świerczyńskiego. Według niego deliktem jest *„czyn niedozwolony popełniony na odległość w związku z Internetem w szczególności przy wykorzystaniu stron internetowych, poczty elektronicznej, bądź innych środków porozumiewania się na odległość. Tego typu czyny stanowią rodzaj deliktów informacyjnych tj. deliktów popełnianych w drodze transmisji danych[216]"*. Przykładami takich zachowań w chmurze mogą być czyny nieuczciwej konkurencji czy naruszenia dóbr osobistych i praw autorskich (np. w serwisach *peer2peer*) na udostępnianych przez dostawcę platformach. Sformułowanie, że dla roszczeń z tytułu czynów niedozwolonych jurysdykcję ma *„sąd miejsca, gdzie nastąpiło lub może nastąpić zdarzenie wywołujące szkodę*" (tak wyżej wskazane przepisy Rozporządzenia, Konwencji a także- w podobnym brzmieniu- k.p.c.) nie będzie dla umów zawieranych za pośrednictwem Internetu relewantne. Deliktom takim można bowiem przypisać cechę *„wielomiejscowości*", która oznacza *„rozproszenie elementów stanu faktycznego, w szczególności skutków czynu niedozwolonego (szkód) pomiędzy różne państwa"*[217].

W literaturze jak i orzecznictwie podejmowane są próby sprecyzowania pojęcia miejsca zdarzenia wywołującego szkodę. Na gruncie prawa polskiego przyjmuje się, że będzie to miejsce zarówno miejsce, w którym wystąpiła szkoda a także miejsce, w którym nastąpiło zdarzenie ją powodujące. Za miejsce, w którym szkoda nastąpiła uznaje się natomiast to, w którym nastąpiły szkodliwe skutki zdarzenia[218]. Trybunał Sprawiedliwości w wyroku dotyczącym połączonych spraw C-509-09 i 161/10 Trybunał orzekł, że art. 5 ust.3 Rozporządzenia Bruksela I należy interpretować tak, że *„w wypadku naruszenia dóbr osobistych za pośrednictwem treści opublikowanych w witrynie internetowej, osoba, która uważa się za poszkodowaną, może wytoczyć (…) bądź przed sądami państwa członkowskiego, w którym wydawca tych treści ma swoją siedzibę, bądź przed sądami państwa członkowskiego, w którym znajduje się centrum jej interesów życiowych. Osoba ta może również, zamiast powództwa dotyczącego odpowiedzialności za całość doznanych krzywd*

[215] P. Poderecki (red.), Ibidem.
[216] Marek Świerczyński, *Delikty internetowe w prawie międzynarodowym prywatnym*, wyd. Zakamycze 2006, s.19.
[217] Ibidem, s. 25.
[218] Henryk Dolecki (red.), *Kodeks postępowania cywilnego. Komentarz. Tom V*, wyd. I, Lex 2012.

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"[219].

W Stanach Zjednoczonych, sądy wielokrotnie wypowiadały się na temat tego zagadnienia. Na bazie tych wyroków, można mówić o wykształceniu się tam linii orzeczniczej, gdzie właściwość sądu w przypadku deliktów internetowych jest zależna od woli i aktywności podmiotu, który dokonał naruszenia na danym terenie. Ważne staje się zatem określenie strony będącej adresatem tych naruszeń[220]. Przy takim podejściu należy uwzględnić świadomość sprawcy co do możliwości odbioru treści w danym miejscu tj. kryterium „nakierowania przekazu" (np. język strony internetowej, domenę, używany adres strony czy charakter treści)[221]. A zatem, swoich praw dochodzić można wszędzie tam, gdzie naruszyciel skierował swoją działalność[222]. Mówiąc o jurysdykcji sądów w USA należy także wskazać, że istnieje tam zasada, iż podmiot zagraniczny może być pozwany przed sąd amerykański jeśli zostanie wykazany znaczny wpływ na handel[223].

Ustalenie sądu właściwego dla zobowiązań i deliktów dokonanych w związku z funkcjonowaniem usług w chmurze obliczeniowej nie jest proste. Sprawy tego rodzaju nie będą jednak istotnie różnić się od problematycznych zagadnień pojawiających się wcześniej na wokandach odnośnie min. działania dostawców usług hostingowych. Głównym problemem w obu odmianach świadczenia usług w Internecie, będzie bowiem ustalenie miejsca świadczenia lub miejsca naruszenia. W przypadku usług Cloud Computing, problem ten również jest obecny i pozostanie aktualny aż do czasu wypracowania jednolitych reguł działalności w cyberprzestrzeni.

4.3. Wyznaczenie prawa właściwego dla umów w chmurze obliczeniowej

Przy ustalaniu prawa właściwego dla zobowiązań umownych lub pozaumownych będą obecne podobne problemy, co przy ustalaniu sądu właściwego, stąd część ogólna rozważań

[219] Orzeczenie TS UE z dnia 25.10.2011 r., w sprawie *eDate Advertising GmBH* przeciwko *X. MGN Limited*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:370:0009:0010:PL:PDF, odczyt 20.03.2012r.
[220] Mateusz Kondrat, Ochrona znaków towarowych przed naruszeniami w Internecie, wyd. Oficyna, Lex nr. 81492.
[221] P. Podrecki, Ibidem.
[222] K. Wimmer, Ibidem.
[223] M. Kondrat, Ibidem.

zostanie w tym miejscu pominięta. Przede wszystkim, kwestią sporną będą łączniki oparte na zasadzie terytorialności. Naturze umów zawieranych przy pomocy Internetu sprzyja doktryna prawa „najściślej związanego z umową", nakazująca stosować system prawny państwa, z którym umowa ma naturalny, ścisły związek[224]. Podobnie, jak w przypadku ustalenia sądu, tak w przypadku prawa właściwego dąży się do przyznawania stronom prawa wyboru, a dopiero w razie nieskorzystania z tego przywileju przyjmuje się, że dla stron mających miejsce zamieszkania (pobytu, stałego pobytu) w tym samym państwie, właściwe dla stosunku prawnego je łączącego będzie prawo tego państwa[225].

W dziedzinie prawa właściwego dla zobowiązań umownych, zasady postępowania na terytorium UE wyznacza Rozporządzenie 293/2008 tzw. Rzym I z 17 czerwca 2008 r. Zastąpiło ono Konwencję Rzymską z 1980 r. w zakresie umów zawartych po 17 grudnia 2009 r. Rozporządzenie Rzym I w art. 3 określa zasady umownego określenia prawa właściwego. Strony mogą dokonać wyboru dla całej umowy lub jej części w sposób wyraźny lub taki, aby jednoznacznie z treści umowy lub okoliczności sprawy wynikało, jakie prawo jest właściwe. Zasada powszechnego stosowania Rozporządzenia, którą wprowadza art. 2 daje stronom możliwość wyboru prawa państwa trzeciego dla ich stosunku zobowiązaniowego[226]. Jeżeli strony pozostaną bierne i nie dokonają wyboru reżimu prawnego właściwego dla ich stosunku prawnego, to zastosowanie znajdzie jedna z zasad przewidzianych w art. 4 Rozporządzenia. Szczególne znaczenie dla Cloud Computing mają postanowienia odpowiednio ust.1 lit. a, b tego przepisu. Zgodnie z ich treścią, umowa sprzedaży i umowa świadczenia usług podlega prawu państwa, w którym sprzedawca lub usługodawca ma siedzibę. Ustęp 2 znajdzie natomiast zastosowanie do innych typów umów. Istotą będzie tu wyodrębnienie świadczenia charakterystycznego, co pozwala ustalić, iż prawem właściwym dla stosunku prawnego będzie prawo miejsca zamieszkania zobowiązanego do takiego świadczenia. Jeśli natomiast umowa wykazuje bardziej ścisły związek z innym państwem, to stosuje się prawo tego państwa (art. 4 ust. 3).

Rozporządzenie wprowadza również przepisy szczególne dotyczące umów, których stroną jest konsument. Znajdzie tu zastosowanie łącznik miejsca zwykłego pobytu konsumenta jednak pod warunkiem, że przedsiębiorca prowadzi działalność w tym miejscu lub w jakikolwiek sposób kieruje tam swoją działalność (art. 6) i umowa wchodzi w zakres tej działalności. Zasadę tę wyłącza min. przepis wskazujący, że nie może być ona

[224] P. Podrecki, Ibidem.
[225] Ibidem.
[226] Ibidem, s. 153

wykorzystywana do umów o świadczenie usług, jeśli mają być one świadczone na rzecz konsumenta wyłącznie w państwie innym niż to, w którym konsument ma miejsce stałego pobytu (art. 6 ust.4 lit a).

Rozporządzenie definiuje w rozdziale III „miejsce zwykłego pobytu" osoby prawnej, spółek, podmiotów nieposiadających osobowości prawnej. Jest nim miejsce siedziby ich głównego organu zarządzającego (art. 19 ust.1), a jeśli umowa została zawarta w ramach działalności filii, agencji lub innego oddziału, to miejscem zwykłego pobytu będzie siedziba tych podmiotów. Istotne jest również, że prawo wskazane na podstawie Rozporządzenia będzie miało zastosowanie bez względu na to, czy jest to prawo Państwa Członkowskiego (art. 2 wz. z art. 1 ust.1). Tym samym, nawet jeśli na podstawie Rozporządzenia zostanie ustalone, że prawem właściwym jest prawo USA, to sąd będzie musiał to prawo stosować[227].

W przedmiocie zobowiązań pozaumownych (min. *culpa in contrahendo*, prowadzenie cudzych spraw bez zlecenia, bezpodstawne wzbogacenie- art.1) cywilnych i handlowych dla Państw Członkowskich UE zastosowanie znajdzie Rozporządzenie nr 864/2007 z dnia 11 lipca 2007 r. tj. Rzym II. Układ i struktura tego aktu jest podobna do wcześniej omówionego Rozporządzenia w sprawie zobowiązań umownych. Zasada ogólna tego Rozporządzenia wskazuje, iż prawem właściwym będzie prawo kraju gdzie szkoda powstała lub (jeśli miejsca tego nie da się ustalić) prawo kraju, w którym poszkodowany i naruszający mając miejsce zwykłego pobytu w chwili powstania szkody lub prawo kraju, z którym sytuacja ma ściślejszy związek (art. 4). Akt ten zawiera także pewne szczegółowe regulacje w kwestii naruszeń praw własności intelektualnej i czynów nieuczciwej konkurencji. Art. 8 nakazuje poszukiwać prawa właściwego dla zobowiązań pozaumownych dla naruszeń praw własności intelektualnej jest prawo państwa na podstawie którego dochodzi się ochrony. Art. 6 określa natomiast, iż prawo państwa, w którym występuje lub jest prawdopodobne wystąpienie naruszenia stosunków konkurencyjnych lub zbiorowych interesów konsumentów będzie właściwe dla czynów nieuczciwej konkurencji. Podobnie jak Rzym I, Rozporządzenie nr 864/2007 w art. 3 wprowadza zasadę, iż znajdzie ono zastosowanie bez względu na to, czy prawem właściwym będzie prawo Państwa Członkowskiego czy państwa trzeciego.

Należy podkreślić, że polska ustawa prawo prywatne międzynarodowe z 2011 r. w zakresie zobowiązań odsyła bezpośrednio do obu Rozporządzeń (art.28).

[227] Alexander J. Belohlavek, *Rozporządzenie Rzym I. Konwencja Rzymska*, *Komentarz,* Tom 1, wyd. C.H. Beck, Warszawa 2010.

4.4. Prawo właściwe dla umów na usługi w chmurze obliczeniowej. Zagadnienia szczególne

Z dotychczasowych rozważań wynika, że umowy na usługi Cloud Computing zawierają postanowienia z wielu obszarów prawa. Zagadnienia dotyczące licencji, przetwarzania danych osobowych, czy obowiązki dostawcy usług świadczonych drogą elektroniczną, są uregulowane w kilku odrębnych aktach prawnych, których postanowienia dają asumpt do oddzielnego spojrzenia na zagadnienie prawa właściwego. Może bowiem dojść do sytuacji, gdy każda klauzula będzie wymagała odrębnej analizy.

Art. 4 ust. 1 Rozporządzenia Rzym I nie wprowadza dodatkowej, odrębnej kategorii dla umów prawnoautorskich. Stąd pojawiają się wątpliwości, co do poprawnego ustalenia prawa właściwego dla licencji, czy umów przenoszących autorskie prawa majątkowe. Dla Cloud Computing będzie to miało doniosłe znaczenie, gdyż często przedmiotem transakcji jest program komputerowy objęty licencją. Według Elżbiety Traple, jeżeli dochodzi tylko do sprzedaży nośnika materialnego lub programu w wersji *online* (według tej autorki rozróżnienie w tym wypadku nie ma żadnego znaczenia gospodarczego) wraz z licencją, to zastosowanie może znaleźć art. 4 ust. 1 lit. a, a tym samym prawem właściwym będzie prawo państwa, gdzie sprzedawca ma siedzibę lub miejsce stałego pobytu[228]. W chmurze obliczeniowej, jak ustalono, przedmiotem umowy nie jest sprzedaż programu, a usługa korzystania z niego. Można zatem argumentować, że – analogicznie do sprzedaży- prawem właściwym będzie siedziba usługodawcy (art. 4 ust.1 lit. a).

Janusz Barta i Ryszard Markiewicz uważają jednak, że do licencji należy stosować ust. 2 wskazanego artykułu[229], a tym samym należy określić „świadczenie charakterystyczne"[230]. W przypadku umów licencyjnych uznaje się, że świadczeniem charakterystycznym jest świadczenie licencjodawcy, gdyż to na nim spoczywa ciężar związany z realizacją postanowień umowy[231]. Wydaje się, że o ile w przypadku SaaS można przyjąć, że to na udostępniającym aplikację spoczywa obowiązek świadczenia (jest odpowiedzialny za wszystkie aspekty funkcjonowania usługi), to już mówiąc o IaaS lub PaaS

[228] E. Traple, Ibidem, s.198-199

[229] Art. 4. Ust 2 Rozporządzenia Rzym I mówi, że „*Umowa, która nie jest objęta ust. 1 lub której składniki byłyby objęte zakresem więcej niż jednego z przypadków określonych w ust. 1 lit. a) h), podlega prawu państwa, w którym strona zobowiązana do spełnienia świadczenia charakterystycznego dla umowy ma miejsce zwykłego pobytu*".

[230] J. Barta, R. Markiewicz, *Prawo Autorskie*, Ibidem, s. 400-401.

[231] Katarzyna Grzybczyk, *Prawo właściwe dla autorskoprawnej umowy licencyjnej*, wyd. Oficyna, Warszawa 2010, s.132-135.

można mieć pewne wątpliwości. Jak bowiem wyjaśniono wyżej, rola usługodawcy zostaje tu ograniczona do udostępnienia infrastruktury, której częścią są objęte licencją aplikacje. Jednak to usługobiorca przejmuje większość obowiązków w zakresie utrzymania i prawidłowego działania udostępnionego środowiska[232]. W takim wypadku, godne rozważenia jest zastosowanie art. 4 ust.3 i 4. Rozporządzenia, które – w braku ustalenia prawa właściwego na zasadach przewidzianych w ust.1 i 2. tego artykułu- zezwala na stosowanie prawa najściślej związanego z umową. Może się zatem okazać, że w rezultacie analizy prawnej, prawem właściwym będzie prawo miejsca zamieszkania lub siedziby licencjobiorcy.

Powyższe rozważania będą w części relewantne w przedmiocie ustalenia prawa właściwego dla usług świadczonych drogą elektroniczną. W punkcie 19 Preambuły Dyrektywy 2000/31 wskazano, że jej przedmiotem „*nie jest ustanowienie dodatkowych reguł prawa prywatnego międzynarodowego odnoszących się do konfliktów prawa ani regulowanie właściwości sądów*". Z tego względu, zastosowanie znajdą przepisy art. 4 tego aktu. Podobnie jak w przypadku licencji, podkreśla się, że (przy braku wyboru prawa właściwego) umowę taką należy oceniać przez pryzmat ust. 2,3 i 4 art. 4[233]. Dwie kwestie wymagają wyjaśnienia: pojęcie „świadczenia charakterystycznego" oraz „siedziby usługodawcy" (jak bowiem wskazano wcześniej, miejscem zwykłego pobytu dla osób prawnych lub podmiotów nie posiadających osobowości prawnej jest ich siedziba, a dla osób prowadzących działalność gospodarczą- miejsce głównego przedsiębiorstwa - art. 3 Rozporządzenia Rzym I). Uznaje się bowiem, że dla tego rodzaju umów „świadczeniem charakterystycznym" jest świadczenie usługodawcy[234]. Dyrektywa 2000/31 w art. 2 wyjaśnia, że pod pojęciem usługodawcy należy rozumieć „*każdą osobę fizyczną lub prawną, która świadczy usługę społeczeństwa informacyjnego*". Natomiast „usługodawca mający siedzibę" to „usługodawca, który „*prowadzi faktycznie działalność gospodarczą przez czas nieokreślony z wykorzystaniem stałej siedziby. Obecność oraz używanie środków technicznych oraz technologii wymaganych do świadczenia usług jako takie nie oznaczają istnienia siedziby usługodawcy*". Rozumienie siedziby w tej Dyrektywie jest stosunkowo szerokie, gdyż kładzie nacisk na „faktyczny" aspekt prowadzenia działalności. Jak jednak podkreśla Jacek Gołaczyński, ponieważ w umowach o świadczenie usług droga elektroniczną, mogą mieć przejściowe znaczenie

[232] Szereg obowiązków np. odpowiedzialność za jakość i rzetelność danych wprowadzanych do infrastruktury, za ewentualne naruszenia autorskich praw majątkowych osób trzecich, etc. Wymienia umowa na usługę PaaS udostępniona przez jednego z dostawców PaaS – WOLF na stronie internetowej: http://www.wolfframeworks.com/licenseagreement.asp

[233] J. Gołaczyński, *Umowy elektroniczne w prawie prywatnym międzynarodowym*, Rozdział VI, do Oficyna 2007, Lex. Rozważania autora dotyczą Konwencji Rzymskiej, jednak wydaje się, że w zakresie, w którym Rozporządzenie Rzym I nie wprowadziło odrębnych regulacji, pozostają one aktualne.

[234] Ibidem.

także takie łączniki jak: miejsce zawarcia umowy, miejsce lokalizacji serwera (przy czym, jak zaznacza autor nie może być to czynnik decydujący), miejsce pobytu usługodawcy w chwili zamieszczenia produktu na serwerze lub miejsce pobrania produktu cyfrowego przez odbiorcę, to bardziej należy się skłaniać- tak jak w przypadku licencji- do zastosowania reguły najściślejszego związku[235]. Wydaje się, że takie rozumowanie przystaje do istoty umów Cloud Computing.

Odrębną regulację w zakresie prawa właściwego wprowadza również Dyrektywa 95/46/WE. W art. 4. określono, że państwo członkowskie będzie stosować w odniesieniu do danych osobowych swoje prawo, jeżeli: administrator prowadzi na terytorium tego państwa członkowskiego działalność gospodarczą lub jeżeli prawo tego państwa obowiązuje na danym terytorium z mocy międzynarodowego prawa publicznego, a także, gdy administrator wykorzystuje środki techniczne znajdujące się na terytorium tego państwa (w takiej sytuacji musi wyznaczyć w tym państwie swojego przedstawiciela). Wskazówki interpretacyjne pojęcia „środki techniczne" wskazują autorzy Komentarza do art. 3 polskiej u.o.o.d.o. Według nich, w przepisie tym chodzi o środki zarówno tradycyjne, jak i elektroniczne służące do przetwarzania danych. Jak również podkreślają, do realizacji tej przesłanki, wystarczy występowanie na danym terenie nawet jednego środka, choć sama obecność środków „transmisyjnych" nie może być przesądzająca[236]. Regulacje te obowiązują również podmioty z państw trzecich. Jeżeli na podstawie tych uregulowań nie będzie możliwe ustalenie prawa właściwego, to zastosowanie znajdą przepisy ogólne dotyczące prawa właściwego dla zobowiązań umownych, o których była mowa w poprzedniej części.

[235] Ibidem.
[236] J. Barta, R. Markiewicz, P. Fajgielski, Ibidem, Komentarz do art. 3 u.o.o.d.o.

Rozdział 5. Cloud Computing- zarys zagadnień dotyczących kontraktowania

5.1. Charakter umowy na usługi Cloud Computing

Na zakończenie rozważań na temat Cloud Computing, warto poruszyć kilka kwestii dotyczących kontraktowania. Dotychczasowa analiza pozwala stwierdzić, że kontrakty na usługi w chmurze obliczeniowej będą złożone i wieloaspektowe. Poza ogólnymi postanowieniami, muszą się w nich znaleźć takie, które oddadzą specyfikę chmury tj. zachowanie odpowiedniego poziomu bezpieczeństwa, określenie obowiązków w zakresie przetwarzania danych, kwestie związane z prawami autorskimi do oprogramowania, czy klauzule dotyczące wyboru sądu i prawa właściwego dla zobowiązania. Dobrze przygotowana umowa musi zawierać wszystkie te elementy, aby zapewnić podstawowe gwarancje dla obu stron.

Z racji tego, iż zasadą Cloud Computing jest stworzenie możliwości dla wielu użytkowników do korzystania z usług, to umowy nie będą zazwyczaj indywidualnie dopasowane pod potrzeby konkretnego klienta. Ten masowy charakter chmury sprawi, że kontrakty będą też krótkie (co zresztą odróżnia je od innych umów outsourcingowych)[237]. Klient zazwyczaj otrzyma powszechnie stosowany przez dostawcę wzorzec. Przeważnie zatem nie ma miejsca na negocjacje, a klient – poprzez akceptację wzorca- bierze na siebie całą odpowiedzialność za dokonany wybór. To powoduje, że takie umowy można określić jako mało elastyczne[238]. Ponadto, kształt tych kontraktów będzie zdeterminowany - z jednej strony - przez specyficzne właściwości (np. wielomiejscowość, wielodzierżawność, amorficzność), a z drugiej przez przepisy prawa.

Jak już wielokrotnie podkreślano, umowy Cloud Computing są umowami o świadczenie usług, w których jedna ze stron poszukuje rozwiązań SaaS, PaaS lub IaaS a druga oferuje aplikację, platformę lub infrastrukturę. Na gruncie prawa polskiego, znajdą więc do niej zastosowanie przepisy o zleceniu. W art. 750 Kodeksu cywilnego wskazano, że *„do umów o świadczenie usług, które nie są uregulowane innymi przepisami, stosuje się odpowiednio przepisy o zleceniu”*. Umowa o świadczenie usług Cloud Computing jest bez wątpienia umową nienazwaną[239], a tej kategorii odpowiada przywołany przepis, a zatem

[237] Raport *Cloud Computing i jego aspekty prawne*, Ibidem.
[238] Ibidem.
[239] Zgodnie z Komentarzem do art. 750 KC pod redakcją A. Kidyby, umowy nienazwane charakteryzują się tym, *”że ich przedmiotem jest świadczenie usług, przy czym umowa taka może dotyczyć dokonania jednej usługi,*

- poprzez odpowiednie stosowanie - przepisy tytułu XXI k.c. dotyczącego zlecenia mogą zostać aplikowane do umów Cloud Computing.

Z uwagi na to, że świadczenie usług w chmurze obliczeniowej odbywa się drogą elektroniczną (dostęp do usług ma miejsce przede wszystkim za pośrednictwem Internetu), należy mieć na uwadze przepisy szczególne przewidziane w u.ś.u.d.e. Ustawa znajduje zastosowanie do określenia obowiązków usługodawcy związanych ze świadczeniem usług drogą elektroniczną oraz wprowadza szczególne zasady wyłączenia odpowiedzialności z tytułu takiego świadczenia a także zasady ochrony danych osobowych. Działalność dostawcy usług Cloud będzie polegać przede wszystkim na *„przechowywaniu informacji przekazanych przez usługobiorcę, przy czym przechowywanie to ma miejsce na żądanie usługobiorcy"*[240](*storage cloud*), tym samym – zgodnie z przepisami u.ś.u.d.e. usługę przez niego świadczoną można zakwalifikować jako *hosting* (z tym związane będą pewne, szczególne unormowania dotyczące wyłączenia odpowiedzialności za przechowywane dane- tak w art. 14 u.ś.u.d.e.[241]).

Dla struktury umowy na usługi w chmurze, znaczenie będzie miał obowiązek usługodawcy do przedstawienia regulaminu świadczenia usług drogą elektroniczną (art. 8 u.ś.u.d.e.). Ponadto, powinien go nieodpłatnie udostępnić usługobiorcy jeszcze przed podpisaniem umowy na świadczenie usług, a w czasie jej obowiązywania - okazywać na żądanie. Zgodnie z treścią ust. 3 wskazanego przepisu, regulamin powinien w szczególności określać: rodzaje i zakres świadczonych usług, warunki świadczenia (wymagania techniczne niezbędne do korzystania, zakres dostarczania treści o bezprawnym charakterze), warunki zwierania i rozwiązywania umów, tryb reklamacji. Przepis ten został przejęty z Dyrektywy 2000/31. Z tego względu, obowiązek przygotowania i przedstawienia regulaminu dotyczy wszystkich podmiotów świadczących usługi droga elektroniczną

większej - określonej liczby usług, bądź też dotyczyć stałego świadczenia usług określonego rodzaju" w: A. Kidyba (red.)*Kodeks Cywilny. Komentarz Tom III. Zobowiązania- część szczególna*, Lex 2010.

[240] Jacek Gołaczyński (red.), *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz,* wyd. Oficyna 2009 r., wyd. I, Komentarz do art. 1., Lex.

[241] Art. 14 u.ś.u.d.e mówi, że „ *Nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych. 2. Usługodawca, który otrzymał urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie ponosi odpowiedzialności względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych. 3. Usługodawca, który uzyskał wiarygodną wiadomość o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie odpowiada względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych, jeżeli niezwłocznie zawiadomił usługobiorcę o zamiarze uniemożliwienia do nich dostępu.4. Przepisów ust. 1-3 nie stosuje się, jeżeli usługodawca przejął kontrolę nad usługobiorcą w rozumieniu przepisów o ochronie konkurencji i konsumentów*".

w państwach członkowskich UE. W praktyce, to właśnie w regulaminie zawarte będą zawarte takie postanowienia jak: zasady płatności, licencje, zasady odpowiedzialności usługodawcy[242]. Elementem umowy są także zobowiązania usługodawcy do zapewniania odpowiedniego poziomu usług (ang. *Service Level Agreement*) tj. dostępność, wydajność, poziom wsparcia (*suport*)[243].

W wielu miejscach w tej pracy zwrócono uwagę na postanowienia charakterystyczne dla umów Cloud Computing. W tej części, nie będą one powtarzane (np. kwestie wyboru prawa i sądu właściwego zostały omówione wcześniej), a jedynie wzbogacone o inne, najbardziej charakterystyczne klauzule, które są często stosowane w kontraktach na świadczenie usług w tym modelu.

5.2. Wybrane klauzule z umów na usługi Cloud Computing

5.2.1. Ograniczenie odpowiedzialności usługodawcy

W umowach na usługi Cloud Computing często stosowana jest klauzula przewidująca ograniczenie lub wyłączenie odpowiedzialności dostawcy w przypadku wystąpienia szkód spowodowanych błędami w działaniu systemu[244]. Do takich nieprawidłowości należą min.: przerwy w dostępności systemu (np. opisany przykład przerw w pracy *Gmail*), problemy z funkcjonowaniem (np. błąd programu), naruszenia standardów bezpieczeństwa[245]. Takie sytuacje mogą powodować dla klientów poważne szkody, często finansowe.

Istotną cechą chmury obliczeniowej jest wielodzierżawa. Zdarzenie wywołujące szkodę, może rodzić konsekwencje, nie dla pojedynczego, ale dla wielu usługobiorców. Z tego względu, dostawcy będą próbowali możliwie maksymalnie ograniczyć swoją odpowiedzialność. Na gruncie polskiego prawa, umowne ograniczenie odpowiedzialności za delikt jest dopuszczalne ze względu na obowiązywanie zasady swobody umów (art. 353^1 k.c.)[246]. Ocena takiego stosunku podlegać będzie weryfikacji pod kątem zgodności z zasadami współżycia społecznego[247]. Zazwyczaj usługodawcy będą stosować klauzulę ograniczającą odpowiedzialność do pewnej granicy finansowej (np. *Salesforc*e nie odpowiada

[242] Roman Bieda, *Prawne aspekty SaaS*, Ibidem.
[243] Raport Cloud Computing i jego aspekty prawne, Ibidem.
[244] Simon Bradshaw, Christopher Millard, Ian Walden, *Contracts for clouds: comparison and analysis of Terms and Conditions of cloud computing services*, International Journal of Law and Information Technology, Queen Mary University of London, tom. 19, nr 3, 20 .07.2011 r. , s.212.
[245] R. Marchini, Ibidem, s.126.
[246] Artykuł 353^1 k.c.: *:"strony zawierające umowę mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości (naturze) stosunku, ustawie ani zasadom współżycia społecznego"*
[247] A. Kidyba (red), Ibidem, Komentarz do art. 443.

za szkody, których wartość jest niższa niż 500.000 dolarów lub równowartości dwunastomiesięcznej odpłatności za usługi[248]).

Odrębnym zagadnieniem jest kwestia ograniczenia odpowiedzialności za szkodę wywołaną nieodpowiednim przetwarzaniem danych np. ich usunięcia lub wycieku, a także naruszeniem zasad bezpieczeństwa. Sytuacje takie nie będą dla usługobiorcy przeważnie szkodliwe, dopóki nie chodzi o dane krytyczne, została sporządzona kopia oraz jeżeli nie będzie to powodowało odpowiedzialności wobec strony trzeciej (np. jego klientów)[249]. Dyrektywa 95/46/WE w art. 23 pkt. 2 przewiduje, że administrator może być zwolniony z odpowiedzialności za takie zdarzenie w całości lub w części, jeśli udowodni, że nie jest odpowiedzialny za działanie lub zaniechanie, które spowodowało szkodę. W polskiej ustawie brak podobnego przepisu. Stosowanie wskazanych reguł k.c. budzi liczne wątpliwości[250].

Należy także mieć na uwadze, że skuteczność klauzul zawężających lub wyłączających odpowiedzialność jest istotnie ograniczona, jeśli stroną umowy jest konsument[251] (klientami chmury SaaS są przede wszystkim konsumenci). Na gruncie prawa polskiego, postanowienie wyłączające lub istotnie ograniczające odpowiedzialność względem konsumenta za niewykonanie lub nienależyte wykonanie zobowiązania mogą na podstawie art. 385 (3) pkt. 2 zostać uznane za abuzywne.

5.2.2. Prawo zmiany świadczonej usługi i opłat

Postanowieniem umownym, często stosowanym w kontraktach Cloud Computing jest prawo do zmiany opłat lub zakresu usługi. W przeciwieństwie do tradycyjnych umów outsourcingowych, w przypadku Cloud Computing uprawnienia usługodawcy w tym zakresie są daleko idące. Często bowiem ograniczy się on zaledwie do poinformowania o wprowadzanej podwyżce[252]. Przykład *Google Apps Engine*, gdzie w 2011 r. została wprowadzona odpłatność za korzystanie z usług wyższa o sto (a w niektórych przypadkach ponad trzysta) procent pokazuje, że takie sytuacje mogą stwarzać dla klienta poważne problemy. O planowanych zmianach Google poinformował bowiem dwa tygodnie przed ich wprowadzeniem, co uniemożliwiło wielu deweloperom PaaS oszacowanie ewentualnych strat

[248] Umowa Salesforce Master Subscription Agreement, dostępna na stronie https://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf,
[249] R. Marchini, Ibidem. S.39-40.
[250] J. Barta, R. Markiewicz, P. Fajgielski, Ibidem, Komentarz do rozdziału Prawo polskie a prawo unijne (zgodność polskiego ustawodawstwa z dyrektywą 95/46/WE)
[251] W rozumieniu k.c. konsumentem jest "*osoba fizyczna dokonująca czynności prawnej niezwiązanej bezpośrednio z jej działalnością gospodarczą lub zawodową*" (art. 22 k.c.)
[252] Raport Cloud Computing i jego aspekty prawne, Ibidem.

i przeniesienie aplikacji na inne platformy[253].

Postanowienie umożliwiające zmiany zakresu świadczonych usług jest o tyle problematyczne, gdyż z jednej strony klient oczekuje gwarancji niezmienności usługi, którą opłaca, z drugiej jednak strony, dostawca chce zarezerwować sobie możliwość ulepszania przedmiotu świadczenia, co często będzie związane ze wzrostem cen. Stąd, musi zapewnić sobie w umowie możliwość *upgrade'*ów (ang. ulepszania) często bez konieczności wcześniejszego informowania klienta. Uzyskanie w modelu multidzierżawy zgody od każdego klienta, wiązałoby się bowiem z nadmiernymi trudnościami[254]. Ponieważ jednak klient nie ma (w przeciwieństwie do np. tradycyjnych umów licencyjnych) możliwości odmowy akceptacji zmian (szczególnie w przypadku kontraktów długoterminowych), to powinien zabiegać, aby umowa dokładnie przewidywała zakres prawdopodobnych modyfikacji i ich przyczynę (np. poprawa funkcjonowania). Ekonomika chmury zakłada, że takie zmiany są nieuniknione. Jak wskazuje R. Marchini, główny nacisk powinien być zatem położony nie na pytanie „czy w ogóle" a „jak długo wcześniej oraz w jakiej formie wystosowana zostanie do klienta odpowiednia informacja"[255]. Musi mieć on bowiem czas na podjęcie decyzji w kwestii ewentualnego zmiany providera. Odpowiednim rozwiązaniem może być w takim przypadku możliwość zagwarantowania klientowi prawa wcześniejszego rozwiązania umowy na wypadek, gdyby zakres zmian okazał się sprzeczny z jego celami. Takie postanowienie będzie jednak elementem przede wszystkim umów odpłatnych[256].

5.2.3. Obowiązek zachowania odpowiedniego poziomu usług

Tak jak wspomniano, postanowienia dotyczące zachowania odpowiedniego poziomu usług (SLA) są ważnym elementem umów na usługi Cloud Computing, gdyż wskazują na faktyczny zakres możliwości działania providera oraz możliwości dostępu do usługi przez klienta[257]. SLA to zatem zobowiązanie dostawcy do dołożenia wszelkich starań w kwestii zapewnienia wysokiego poziomu dostępności, reakcji oraz innych dających się zmierzyć standardów[258]. Podstawową potrzebą klienta- poza zapewnieniem odpowiedniego poziomu bezpieczeństwa- będzie niezakłócony dostęp do usługi *on- demand.* Przeważnie dostawcy

[253] A. Golański, *Nowy cennik Google App Engine. Deweloperzy zdesperowani. Kogo będzie na to stać?* 2.09.2011 r., http://webhosting.pl/Nowy.cennik.Google.App.Engine.Deweloperzy.sa.zdesperowani.kogo.bedzie.na.to.stac odczyt 10.04.2012 r.
[254] R. Marchini, s. 109.
[255] Ibidem, s.110.
[256] S. Brideshaw, Ibidem.
[257] H. Ward Classen, Marie Fogarty, Ibidem.
[258] R. Marchini, Ibidem.

będą określali dostępność swoich usług w procentach. W typowych umowach dostępność wynosi od 95 – 99,9 procent[259]. Celem wielu dostawców jest doprowadzenie do sytuacji, gdzie przerwa w dostępnie wynosić będzie mniej niż jedną godzinę w roku[260].

Typowymi elementami SLA są zatem kwestie dotyczące: dostępności usługi, czasu odpowiedzi, czasu na rozwiązanie problemu, elastyczności (szybkość dostarczenia zasobów do klienta)[261]. Przeważnie dostawcy poprzestają na określeniu w umowie tylko pierwszego z wymienionych elementów tj. dostępność usługi (*availability).* Często stosowaną klauzulą będzie taka, która ogólnie określa, że czas przestoju wynosi kilka godzin w roku. Usługobiorca powinien dążyć do sprecyzowania takiego postanowienia, gdyż czym innym będzie dla niego, gdy cały ten czas zostanie wykorzystany na przestrzeni kilkunastu miesięcy, a czym innym, gdy nastąpi to łącznie w ciągu jednego dnia[262].

W umowie *Master Subscription Agreement, Salesforce.com* poprzestaje (co jest dość częstą praktyką) na określeniu, że dołoży wszelkich starań, aby usługa byłą dostępna siedem dni w tygodniu przez 24 godziny na dobę. Jeśli natomiast planowane jest wstrzymanie pracy, to klient zostanie uprzedzony osiem godzin wcześniej[263]. Użytkownik powinien zwrócić szczególną uwagę na sposób mierzenia dostępności (inne rezultaty przyniesie mierzenie dostępności w dniach roboczych, w dniach tygodnia a czym innym w godzinach)[264]. W ramach rekompensaty za niedogodności wyrządzone przerwą w pracy serwisu, providerzy oferują zazwyczaj tak zwane „kredyty". Będą to przeważnie odpowiednio obliczone bonifikaty na zakup innej usługi lub możliwość darmowego dostępu do dodatkowych usług[265].

Niezwykle istotnym elementem SLA powinno być również określenie zakresu udziału osób trzecich w świadczeniu usług i ich odpowiedzialności. W prawie polskim, należy zwrócić uwagę na treść art. 738 § 1 k.c., który mówi, że „ *przyjmujący zlecenie może powierzyć wykonanie zlecenia osobie trzeciej tylko wtedy, gdy wynika to z umowy lub ze zwyczaju albo gdy jest do tego zmuszony przez okoliczności. W wypadku takim zobowiązany jest niezwłocznie zawiadomić dającego zlecenie o osobie i o miejscu zamieszkania swego zastępcy i w razie zawiadomienia odpowiedzialny jest tylko za brak należytej staranności w wyborze zastępcy. §2 Zastępca odpowiedzialny jest za wykonanie zlecenia także względem*

[259] R. Marchini, Ibidem.
[260] Marcin Marciniak, *Trudna droga do chmury*, Computerworld.pl, 27.09.2011 r. http://www.computerworld.pl/artykuly/375301/Trudna.droga.do.chmury.html, odczyt 10.04.2012 r.
[261] R. Marchini s. 114-115.
[262] Raport Cloud Computing i jego aspekty prawne, Ibidem.
[263] Salesforce Master Agreement, Ibidem.
[264] R. Marchini, Ibidem.
[265] R. Marchini, Ibidem s.117-118.

dającego zlecenie. Jeżeli przyjmujący zlecenie ponosi odpowiedzialność za czynności swojego zastępcy tak jak za swoje własne czynności, ich odpowiedzialność jest solidarna". Z przepisu tego wynika zatem generalna możliwość wyboru podwykonawców przez usługodawcę, jednak tylko za zgodą usługobiorcy. W usługach Cloud Computing będzie to sytuacja częsta, ze względu na konieczność obsłużenia dużej ilości sprzętu i zasobów. Usługodawcy w razie niedopełnienia obowiązków przez podwykonawców, będą się starać wykazać, że choć ich usługa jest zależna od prawidłowego działania partnerów, to całkowita kontrola nad nimi nie jest możliwa. Znajduje to odbicie w klauzulach umownych.

Jak wspomniano, umowa o zachowanie określonego poziomu usług jest niezwykle złożona. Można tu znaleźć także wszystkie szczegóły dotyczące zachowania bezpieczeństwa (zewnętrznego i wewnętrznego) także bezpieczeństwa przetwarzania danych (np. uregulowania odpowiedzialności na wypadek wycieku danych- może to prowadzić zarówno do utraty cennych informacji, jak i naruszenia dóbr osobistych osób trzecich np. klientów). Istotną częścią będą również postanowienia dotyczące wsparcia. Na przykład, w SLA firmy *GoGrid* określono, że zespół inżynierów w centrum danych jest gotowy do szybkiej reakcji na usterki i powinien je rozwiązać w czasie do 120 minut. Klientom zaoferowano także pomoc telefoniczną i przez *e –mail*[266]. W tej części mogą się również znaleźć postanowienia co do odzyskiwania danych po awarii czy zasady tworzenia kopii zapasowych (często za dodatkową opłatą). Umowa SLA może być częścią omowy podstawowej lub odrębnym dokumentem.

5.2.4. Wypowiedzenie umowy

W umowach na usługi Cloud Computing może się znaleźć postanowienie, które w istotny sposób ogranicza możliwość rozwiązania umowy na wypadek powtarzających się problemów w działaniu systemu, co – po raz kolejny- wskazuje na istnienie zjawiska *vendor-lock- in*. Polski k.c. art. 746 daje możliwość wypowiedzenia umowy przez dającego zlecenie w każdym czasie, pod warunkiem (w przypadku zlecenia odpłatnego) uiszczenia przyjmującemu zlecenie części wynagrodzenia odpowiadającą jego dotychczasowym czynnościom, a jeżeli wypowiedzenie nastąpiło bez ważnego powodu, dający zlecenie powinien także naprawić szkodę. W umowach Cloud Computing problemem w takiej sytuacji będzie przede wszystkim ekonomiczna nieopłacalność wypowiedzenia, szczególnie jeśli kontrakt zawarty został na dłuższy czas.

[266] GoGrid SLA, http://www.gogrid.com/legal/sla.php, odczyt 12.04. 2012 r.

Niejednokrotnie umowy będą przewidywać możliwość wypowiedzenia, ale tylko na wypadek istnienia oznaczonego rodzaju naruszeń w określonym czasie. Podstawowym problemem jaki się tu pojawi, będzie sprecyzowanie o jakie naruszenia będące podstawą wypowiedzenia może chodzić. W kontraktach często umieszcza się stwierdzenie, że przyczyną rozwiązania umowy może być tylko naruszenie jej istotnych postanowień (*material breach*)[267]. Jak zauważa Renzo Marchini, problematyczne będzie ustalenie, czy np. gwarancje odpowiedniego poziomu usług, mogą zostać uznane za „istotne postanowienie"[268]? Jeśli odpowiedź na tak postawione pytanie będzie pozytywna, to pojawia się wątpliwość czy, uwzględnienie w umowie postanowienia o przyznaniu kredytów na wypadek naruszenia gwarancji odpowiedniego poziomu usług, nie wyłączy stosowania klauzuli o wypowiedzeniu? Można przypuszczać, że dostawcy będą taką argumentację forsować. Aby uniknąć ewentualnych sporów, kontrakt powinien wprost przewidywać możliwość wypowiedzenia w sytuacji, gdy zostanie przyznana już maksymalna liczba kredytów przewidziana w umowie. Świadczy to bowiem o powtarzających naruszeniach, którym dostawca nie jest w stanie sprostać[269]. Należy przy tym zauważyć, że są w obrocie również takie przykłady umów, gdzie prawo wypowiedzenia nie jest ograniczone niczym, poza koniecznością pisemnej notyfikacji[270].

Z zagadnieniem wypowiedzenia umowy na usługę Cloud Computing związane jest jeszcze jedna interesująca kwestia. W wielu umowach z dostawcami ze Stanów Zjednoczonych (np. w omawianej już wielokrotnie umowie na usługi w chmurze *Salesforce.com*[271]) zawarta jest klauzula, że wypowiedzenie jest możliwe w przypadku ogłoszenia upadłości jednej ze stron. Na gruncie polskiego prawa, taka sytuacja jest niedopuszczalna, co wynika wprost z treści art. 83 ust.1 Ustawy prawo upadłościowe i naprawcze, który mówi, że „*nieważne są postanowienia umowy zastrzegające na wypadek ogłoszenia upadłości zmianę lub rozwiązanie stosunku prawnego, którego stroną jest upadły*". W takich wypadkach, istotnego znaczenia nabierają klauzule umowne dotyczące wyboru sądu i prawa właściwego.

[267] Tak w umowie Salesforce, Ibidem.
[268] R. Marchini, s.124.
[269] Ibidem.
[270] Amazon Web Service, Customer Agreement, http://aws.amazon.com/agreement/, odczyt 10.04. 2012 r.
[271] Umowa Salesforce, Ibidem.

Zakończenie

Celem powyższych rozważań było przybliżenie istoty Cloud Computing i – przede wszystkim- poszukiwanie potencjalnych problemów prawnych, które mogą pojawić się w trakcie korzystania z usług dostarczanych w ramach tego modelu.

Przeprowadzona analiza pozwala stwierdzić, że Cloud Computing jest modelem świadczenia usług IT, który –choć w wielu miejscach jest zaledwie udoskonaleniem dotychczasowych metod rozpowszechniania- to można go rozpatrywać, jako zagadnienie odrębne. O odmienności pozwalają mówić swoiste właściwości chmury obliczeniowej tj. wirtualizacja, skalowalność, wielodzierżawa, dostęp na żądanie, model opłat na zasadzie *pay-as-you-go.*

Na rozwój Cloud Computing miało wpływ wiele czynników technologicznych. Bez wątpienia, do najważniejszych z nich należy progres w zakresie środków umożliwiających dostęp do Internetu. Użytkownik urządzeń mobilnych oczekuje, że jego zasoby będą dostępne w każdej chwili i z każdego miejsca. Nie musi przy tym dokonywać wydatków na *hardware i software*, co sprawia, że rozwiązania w chmurze stają się coraz bardziej atrakcyjne już nie tylko dla klientów biznesowych, ale także indywidualnych. Mówi się nawet o „konsumeryzacji" IT tj. sytuacji, gdy konsument będzie oczekiwał, że sprzęt codziennego użytku tj. tablet czy *smartfon* będzie mógł zostać wykorzystany także w organizacji, w której pracuje. Tym samym, to użytkownicy, a nie działy IT będą decydować o wykorzystaniu IT[272].

W pierwszej części wyróżniono również podstawowe modele świadczenia usług w chmurze oraz modele ich ekspansji wyróżnione przez NIST. Na podstawie tych rozważań można stwierdzić, że każdy model SPI będzie łączyć się ze swoistymi problemami prawnymi. Dla umów SaaS będzie to min. kwestia konieczności licencjonowania, przy braku spełnienia ustawowych przesłanek do udzielenia licencji na gruncie pr.aut. Dla dewelopera PaaS, problemem będzie tworzenie aplikacji na platformie, której komponenty objęte są licencją *open source*. Z kolei użytkownik IaaS spotka się z koniecznością zweryfikowania umowy na oprogramowanie, które przenosi do infrastruktury, pod kątem uzyskania możliwości na korzystanie w środowisku zewnętrznym. Dla wszystkich tych modeli, wspólne będą zagadnienia bezpieczeństwa i ochrony danych osobowych, choć – jak zaważono- problem ten

[272]Andrzej Maciejeski, *Konsumeryzacja. Pracownicy będą rządzić firmowym IT*, Computerworld.pl, 6.03.2012, http://www.computerworld.pl/artykuly/380831/Konsumeryzacja.Pracownicy.beda.rzadzic.firmowym.IT.html, odczyt 20.04.2012 r.

dotyczy przede wszystkim chmury publicznej. Problemem elementarnym będzie również określenie prawa i sądu właściwego dla stosunku prawnego, jeżeli strony nie dokonały wyboru w umowie.

Ustalono również, ze kształt kontraktów na usługi Cloud Computing oraz klauzule w nich zawarte, będą często w znaczący sposób odbiegać o tych, które umieszcza się w umowach dotyczących innych modeli outsourcingowych. Ze względu na wielodzierżawę, kontrakty zazwyczaj będą krótkie, oparte na wzorcach- przez co mało elastyczne i najczęściej niedające możliwości negocjacji warunków. Wielodzierżawa spowoduje również, że usługodawca będzie dążył w umowach do możliwie najbardziej szerokiego wyłączenia odpowiedzialności za ewentualne błędy w działaniu systemu. W niewielu przypadkach, umowa będzie przewidywać możliwość wypowiedzenia na wypadek powtarzających się naruszeń ze strony dostawcy. To z kolei związane jest z charakterystycznym dla Cloud Computing zjawiskiem maksymalnego uzależnienia od jednego dostawcy tzw. *vendor- lock-in.*

W pracy zostały przedstawione tylko niektóre, istotne zagadnienia prawne związane z Cloud Computing. Ta pobieżna nawet analiza daje jednak podstawy do twierdzenia, że są to problemy na tyle interesujące i istotne, że powinny stać się przedmiotem większej uwagi ze strony prawników, także w Polsce. Można oczekiwać, że zainteresowanie wzrośnie, gdyż - jak prognozują analitycy amerykańskiej firmy Gartner - „ *usługi w chmurze staną się częścią życia ludzi, a producenci urządzeń i platform będą musieli integrować je z usługami typu Cloud Computing w celu zdobycia klientów*”[273]. Wydaje się, że jeżeli ta zapowiedź się sprawdzi (a zważając na spełniające się – przywołane we wstępie- prognozy Nicholasa Carr’a, z dużą dozą prawdopodobieństwa można stwierdzić, że tak będzie), to chmura obliczeniowa będzie dla prawnika zajmującego się branżą IT wyzwaniem elementarnym.

[273] Radosław Szpunar, Gartner: prywatne chmury w 9 urządzeniach na 10 przed rokiem 2015, IDG News Service, 7.03.2012 r., http://www.pcworld.pl/news/380944/Gartner.prywatne.chmury.w.9.urzadzeniach.na.10.przed.rokiem.2015.html, odczyt 20.04.2012 r.

Bibliografia

Wykaz skrótów:

k.c. - Ustawa Kodeks cywilny z dnia 23 kwietnia 1964 r., Dz.U.1964.16.93

k.p.c. - Ustawa Kodeks postępowania cywilnego z dnia 17 listopada 1964 r., Dz.U.1964.43.296

p.m.p. - Ustawa prawo międzynarodowe prywatne z dnia 15 kwietnia 2011 r., Dz.U.2011.80.432

pr.aut. - Ustawa prawo autorskie i prawa pokrewne z dnia 4 lutego 1994 r., Dz.U.2006.90.631

u.o.o.d.o. - Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r., Dz.U.2002.101.926

u.ś.u.d.e. - Ustawa o świadczeniu usług drogą elektroniczną z dnia 9 września 2002 r., Dz.U. 2002 nr 144 poz. 1204

Akty prawne:

Akty prawa polskiego:

1. Konstytucja RP z dnia 2 kwietnia 1997 r., Dz.U. 1997, NR 78 poz. 483
2. Ustawa Kodeks cywilny z dnia 23 kwietnia 1964 r., Dz.U.1964.16.93
3. Ustawa Kodeks postępowania cywilnego z dnia 17 listopada 1964 r., Dz.U.1964.43.296
4. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r., Dz.U.2002.101.926
5. Ustawa o świadczeniu usług drogą elektroniczną z dnia 9 września 2002 r., Dz.U. 2002 nr 144 poz. 1204
6. Ustawa prawo autorskie i prawa pokrewne z dnia 4 lutego 1994 r., Dz.U.2006.90.631
7. Ustawa prawo międzynarodowe prywatne z dnia 15 kwietnia 2011 r., Dz.U.2011.80.432
8. Ustawa prawo upadłościowe i naprawcze z dnia 18 lutego 2003 r., Dz.U.2009.175.1361
9. Ustawa o podatku dochodowym od osób prawnych z dnia 15 lutego 1992 r., Dz.U.2011.74.397
10. Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U.2004.100.1024

Akty prawa europejskiego i międzynarodowego:

1. Rozporządzenie Rady (WE) nr 44/2001z dnia 22 grudnia 2000 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych
2. Rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I)
3. Rozporządzenie (WE) nr 864/2007 Parlamentu Europejskiego i Rady (WE) nr 864/2007
4. Rozporządzenie z dnia 11 lipca 2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych („Rzym II")
5. Projekt Rozporządzenia Parlamentu Europejskiego i Rady nr 2012/0011 z 25 stycznia 2012 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)
6. Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)
7. 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 danych
8. Decyzja Rady 2007/712/WE z dnia 15 października 2007 r. dotycząca podpisania Konwencji o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń w sprawach cywilnych i handlowych
9. Decyzja Komisji Europejskiej nr 2000/520/WE w sprawie zatwierdzenia Programu Safe Harbor z dnia 26 lipca 2000 r. (O.J. L 215, 25.08.2000 s. 0007 – 0047)
10. Opinia Grupy Roboczej art.29 nr 20/26 z 22 listopada 2006 r.
11. Opinia Gruby Roboczej art.29 nr 1/2010 z 16 lutego 2010 r.

<u>Orzecznictwo:</u>

Orzecznictwo sądów polskich:

1. Wyrok Sądu Najwyższego z 5 września 2001 r., I CKN 1159/00, OSNC 2002, nr 5, poz. 67
2. Orzeczenie Naczelnego Sądu Administracyjnego do sygn. II SA 3878/02 z 16 kwietnia 2003 r. ONSA 2004/1/41
3. SN w orzeczeniu z dnia 10 maja 1963 r., II CR 128/63, OSNC 1964, nr 4, poz. 74

Orzecznictwo sądów i trybunałów międzynarodowych:

Orzeczenie TS UE z dnia 25.10.2011 r., w sprawie *eDate Advertising GmBH* przeciwko *X. MGN Limited.*

Publikacje zwarte:

1. Barta Janusz (red.), Markiewicz Ryszard (red.), Czajkowska-Dąbrowska Monika, Ćwiąkalski Zbigniew, Felchner Krzysztof, Traple Elżbieta, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, wyd. V*, LEX 2011, nr 8545
2. Barta Janusz, Fajgielski Paweł, Markiewicz Ryszard, *Ochrona danych osobowych. Komentarz*, wyd. V, Lex 2011, nr.8531
3. Barta Janusz, Markiewicz Ryszard, *Prawo autorskie*, wyd. Oficyna, Warszawa 2010
4. Belohlavek Alexander J., *Rozporządzenie Rzym I. Konwencja Rzymska, Komentarz*, Tom 1, wyd. C.H. Beck, Warszawa 2010
5. Carr Nicholas, *The big switch*, W.W. Norton & Company, Nowy Jork, Londyn 2008
6. Dolecki Henryk (red.) , *Kodeks postępowania cywilnego. Komentarz. Tom V*, wyd. I, Lex 2012
7. Drozd Andrzej, *Ustawa o ochronie danych osobowych, Komentarz. Wzory pism i przepisy*, Wyd. Prawnicze Lexis Nexis, Warszawa 2004.
8. Gołaczyński Jacek (red.), *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, wyd. Oficyna 2009, wyd. I
9. Grzegorczyk Paweł, *Jurysdykcja krajowa w sprawach z zakresu prawa własności przemysłowej*, wyd. Oficyna, Lex numer publikacji 65056
10. Grzybczyk Katarzyna, *Prawo właściwe dla autorskoprawnej umowy licencyjnej*, wyd. Oficyna, Warszawa 2010
11. Gołaczyński Jacek (red.), Kowalik-Bańczyk Krystyna, Majchrowska Agata, Świerczyński Marek, *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, wyd. Oficyna 2009, Lex nr 7900
12. Jagielski Mariusz, *Prawo do ochrony danych osobowych. Standardy europejskie*, wyd. Oficyna Wolters Kluwer business, Warszawa 2010 r.
13. Kidyba Andrzej (red.), *Kodeks Cywilny. Komentarz Tom III. Zobowiązania- część szczególna*, Lex 2010
14. Kondrat Mateusz, *Ochrona znaków towarowych przed naruszeniami w Internecie*, wyd. Oficyna, Lex nr. 81492
15. Krutz Ronald L., Vines Russel Dean, *Cloud Security. A comprehensive Guide to Secure Cloud Computing*, Wiley Publishing INC, 2010
16. Kulesza Joanna, *Ius Internet. Między prawem a etyką*, Wyd. Akademickie, Warszawa 2010
17. Marchini Renzo, *A practical Introduction to the Legal Issues*, British Standards Institusion 2010
18. Mateos Arthur, Rosenberg Jothy, *Chmura obliczeniowa. Rozwiązania dla biznesu*, Helion S.A, 2011
19. Mather Tim, Kumaraswamy Subra, Latif Shahed, *Cloud Security and Privacy. An enterprise perspective on Risk and Compliance*, O'Reilly, 2009
20. Ożegalska- Trybalska Justyna, *Adresy e-mailowe a dane osobowe*, ODO 2001, nr 23, s. 10-13
21. Pazdan Maksymilian, *Prawo prywatne międzynarodowe*, Wyd. Lexis Nexis, wyd. XIII
22. Podrecki Paweł (red.), *Prawo Internetu*, wyd. Lexis Nexis, Warszawa 2006
23. Rittinghouse John W., Ransome James F., *Cloud Computing. Implementation, Management, Security*, CRC Press Taylor&Francis Group 2010

24. Sosinsky Barrie, *Cloud Computing Bible.* Wiley Publishing Inc, 2011
25. Świerczyński Marek, *Delikty internetowe w prawie międzynarodowym prywatnym*, wyd. Zakamycze 2006
26. Traple Elżbieta, *Umowy o eksploatację utworów w prawie polskim*, wyd. Oficyna, Warszawa 2010
27. Velte Anthony, Velte Toby, Elsenpeter Robert, *Cloud Computing. A Practical Approach*, MCGraw-Hill Companies, 2010

Artykuły naukowe:

1. Bradshaw Simon, Millard Christopher, Walden Ian, *Contracts for clouds: comparison and analysis of Terms and Conditions of cloud computing services,* International Journal of Law and Information Technology, Queen Mary University of London, tom. 19, nr 3, 20 lipca 2011
2. Classen H. Ward, Fogarty Marie, *Avoiding Turbulence in the Cloud: Licensing and Contractual Issues for Licensor, Cloud Provider and End User, The Computer & Internet Lawyer*, tom. 19, nr 2, luty 2012
3. Determann Lothar, *Data privacy in the Cloud: A dozen Myths and Facts,* The Computer& Internet Lawyer, vol.28, nr 11, listopad 2011
4. Machała Wojciech, *Licencja mieszana? Prawnoautorskie aspekty obrotu programami komputerowymi stworzonymi przy wykorzystaniu oprogramowania o otwartym kodzie*, Zeszyty Naukowe UJ, zeszyt 110, 2007
5. Małyszko Michał, *SaaS jako metoda świadczenia e- usług,* Raport Polskiej Agencji Rozwoju Przedsiębiorczości, PARP, Warszawa 2008
6. Mell Peter, Grance Thimoty, *The NIST definition of Cloud Computing,* US. Department of Commerce, wrzesień 2011
7. Siewicz Krzysztof, *Zakres klauzuli copyleft w prawie polskim*, Prace Instytutu Prawa Własności intelektualnej UJ, zeszyt 93
8. Ward T. Burke, Sipior Janice C., *The Internet Jurisdiction Risk of Cloud Computing,* Taylor&Franciss Group
9. Wimmer Kurt, Pogoriler Eve, Sattarfield Stephen, *International Jurisdiction and the Internet in th Age of Cloud Computing,* The Bureau of National Affairs, Washington 2011, http://www.cov.com
10. Wittow Mark H., Buller Daniel J., *Cloud Computing: Emerging legal issues for acces to data anywhere, anytime,* Internet Law, vol.14, nr 1, lipiec 2010.
11. Raport Kancelarii Radcy Prawnego Stefan Cieśla: *Cloud Computing i jego aspekty prawne.*, Warszawa, 2011

Publikacje internetowe:

1. Austien Ian, *A liabel case raises a tricky question of Jurisdiction*, The New York Times, 14.03. 2005 r., http://www.nytimes.com/
2. Bieda Roman, *Prawne aspekty SaaS,* http://prawnik.net.pl
3. Butterworth Siobhain, *The not so world wide web*, 27 września 2005 r., http://www.guardian.co.uk
4. Caruso Jeff, *Iaas vs. PaaS vs. SaaS* , 2.11.2011 r., www.networkworld.com

5. Chabik Jakub, *Krótki przewodnik po rozwiązaniach cloud computing,* 10.10.2011 r., www.computerworld.pl
6. Chustecki Janusz, *Hybrydowe chmury obliczeniowe,* , 28.12.2010 r., www.networld.pl
7. Downie Andrew, *Google and the pedophiles*, wrzesień 2006 r., www.time.com
8. Drobek Piotr (op), *ABC przekazywania danych osobowych do państw trzecich,* Biuro Generalnego Inspektora Danych Osobowych, wyd. Sejmowe, Warszawa 2007 r.
9. Gienias Krzysztof, *Aukcje internetowe a odpowiedzialność ISP*, maj 2002 r., http://prawnik.net.pl/
10. Golański Adam, *Amazon Silk. Przełomowa przeglądarka ery chmur , czy po prostu nowa Opera Mini?,* 29.09. 2011 r.,www.webhosting.pl.
11. Golański Adam, *Nowa polityka prywatności Google'a nielegalna w Unii Europejskiej? Francuski CNIL wszczyna śledztwo,* 6.03.2012 r., www.webhosting.pl
12. Golański Adam, *Nowy cennik Google App Engine. Deweloperzy zdesperowani. Kogo będzie na to stać?* 2.09.2011 r., www.webhosting.pl
13. Judd William, *SaaS Threatens Open Source,* 28.01. 2011 r., http://williamjudd.com
14. Krakowiak Ludwik, *Spyware coraz groźniejszy,* 12.08. 2005 r., www.pcworld.pl
15. Kulesza Monika, *Cloudburst a chmura hybrydowa,* 20.04. 2011 r., www.computingcloud.pl
16. Lakhotia Pankai, *Microsoft says Cloud computing can end software piracy,* 6.03.2010 r., www.stockwatch.com
17. Maciejewski Andrzej, *Fakty i mity o cloud computing,* 14.09.2010 r., www.computerworld.pl
18. Malcolm Dave, *The five defining characteristics of Cloud Computing,* 9.04.2009 r., www.zdnet.com
19. Marciniak Marcin, *Bliższe niż chmura,* 6.10. 2009 r., www.computerworld.pl
20. Marciniak Marcin, *Chmurę już mamy, ale jej nie widzimy,* 6.03.2012 r., comuterworld.pl
21. Marciniak Marcin, *Cloud Computing bez tajemnic,* 23.06. 2009 r., www.computerworld.pl
22. Marciniak Marcin, *Policz ukryte koszty w chmurze,* 17.01.2012 r., www.computerworld.pl
23. Mejssner Barbara, *Długa droga administracji publicznej do chmury,* 22.05.2011 r., www.cyfrowapolska.pl
24. Muszyński Józef, *Bezpieczeństwo w chmurze,* 10.02.2012 r., www.computerworld.pl,
25. Muszyński Józef, *Grid Computing a problem zarządzania*, 2.07.2002 r., www.networld.pl.
26. Muszyński Józef, *Układanka z chmur,* 24.05.2011 r., www.networld.pl.,
27. Salkever Alex, *5 ways to protect against vendor lock- in in the cloud,* 24.09.2011 r., http://gigaom.com
28. Srinivasan Sundra Rajan**,** *The importance of community clouds,* 24.04.2011r., www.cloudcomputing.sys-con.com
29. Stanisławska Aleksandra, *Branża IT napędzi wzrost gospodarczy w naszym regionie,* 14.12.2011 r.www.ekonomia24.pl
30. Sullivan Tom, *Jak Cloud Computing zdefiniuje IT,* 7.04.2009 r., www.computerworld.pl
31. Surowiec Rafał, *Dane osobowe w chmurach,* 21 lipca 2011 r., www.rp.pl
32. Urban Piotr, *Bezpieczny Outsourcing,* 28.07.2010 r., www.outsourcing.com.pl
33. Urbańska Kamila, *Bezpieczeństwo IT w chmurze,* 15.10.2011 r., http://www.egospodarka.pl

34. Waszczuk Piotr, *Nowa polityka prywatności Google powszechnie krytykowana,* 28.02.2012 r., www.computerworld.pl
35. Waszczuk Piotr, *Wirtualizacja coraz bardziej dojrzała,* 7.12.2010 r., www.computerworld.pl
36. Weinberg Kacey, *Will the cloud eradicate software piracy?,* 5.04 2011 r., www.enterprisecioforum.com
37. *PKPP Lewiatan o planowanych zmianach w ochronie danych osobowych,* 19.03.2012 r., http://www.e-ochronadanych.pl
38. Raport pt. *Analysis of Google's Privacy Policy and Related FAQ,* Amberhawk, marzec 2012, http://amberhawk.typepad.com/
39. Raport *Business Software Aliance, 09 Software Piracy*, BSA, maj 2010 r., http://portal.bsa.org