ARTYKUŁY POGLĄDOWE (REVIEW PAPERS)

Cloud computing – prawne zabezpieczenia i perspektywy technologiczne

(*Cloud computing* - legal safeguards and technological prospects)

M Machota [1,A,D], S Kasza [2,A,D], A Romaszewski [2,E], Z Kopański [2,D,F], W Uracz [1,B,E], F Furmanik [1,C], S Dyl [1,B], J Tabak [1,B]

1. Collegium Masoviense – Wyższa Szkoła Nauk o Zdrowiu
2. Wydziału Nauk o Zdrowiu Collegium Medicum Uniwersytet Jagielloński

Abstract - The authors emphasized that one of the key issues of the *cloud computing* is a matter of data security. The field of information processed, in particular in health care is very wide, and the data itself has a different type of sensitivity and validity. It is believed that the safety issue must be presented as a priority for the architects of the system. This imposes an obligation to search for the right legal solutions, because at the moment both in Polish and EU legislation there are large legal gaps relating to the collection and processing of information in cloud computing, which is a serious obstacle to the further development and modernization of IT systems in health care.

Key words - cloud computing, Polish and EU legislation, data security.

Streszczenie - Autorzy podkreślili, że jednym z kluczowych zagadnień *cloud computingu* jest kwestia bezpieczeństwa danych. Pole przetwarzanych informacji, w szczególności w ochronie zdrowia jest bardzo szerokie, a same dane posiadają różny typ wrażliwości i ważności. Uważa się, że kwestia bezpieczeństwa musi przedstawiać się jako priorytet w celach architektów systemu. Nakłada to obowiązek poszukiwania właściwych rozwiązań prawnych, bowiem w chwili obecnej zarówno w ustawodawstwie polskim jak i unijnym istnieją duże luki prawne odnoszące się do gromadzenia i przetwarzania informacji w chmurach obliczeniowych, co stanowi poważną przeszkodę w dalszym rozwoju i unowocześnianiu systemów informatycznych w ochronie zdrowia.

Słowa kluczowe - chmury obliczeniowe, ustawodawstwo polskie i unijne, bezpieczeństwo danych.

Wkład poszczególnych autorów w powstanie pracy - A-Koncepcja i projekt badania, B-Gromadzenie i/lub zestawianie danych, C-Analiza i interpretacja danych, D-Napisanie artykułu , E-Krytyczne zrecenzowanie artykułu, F-Ostateczne zatwierdzenie artykułu

Adres do korespondencji — Prof. dr Zbigniew Kopański, Wydziału Nauk o Zdrowiu Collegium Medicum Uniwersytet Jagielloński, Kraków, ul. Piotra Michałowskiego 12, PL-31-126 Kraków, e-mail: zkopanski@o2.pl

Zaakceptowano do druku: 29.08.2018.

WSTĘP

W obrębie organizacji może funkcjonować jednocześnie wiele rozwiązań, a wybór konkretnej opcji zależy od rodzaju analizowanych danych. Jednym z kluczowych zagadnień *cloud computingu* jest kwestia bezpieczeństwa danych. Pole przetwarzanych informacji, w szczególności w ochronie zdrowia jest bardzo szerokie, a same dane posiadają różny typ wrażliwości i ważności. Uważa się zatem, że kwestia bezpieczeństwa musi przedstawiać się jako priorytet w celach architektów systemu. Dalszemu nierozwiązaniu podlega także kwestia ustawodawstwa, bo choć obecnie zarówno w prawie polskim jak i unii europejskiej jest regulowana kwestia danych osobowych to w tym momencie nie funkcjonują żadne przepisy odnoszące się do gromadzenia i przetwarzania podobnych informacji w chmurach obliczeniowych, a taka sytuacja stanowi poważny kłopot w dalszym rozwoju i unowocześnianiu systemów informatycznych w ochronie zdrowia. [1-4]

PERSPEKTYWY

Na całym świecie rośnie rola przetwarzania danych w chmurze. Dzieje się to nie tylko za sprawą indywidualnych inicjatyw, ale także projektów rządowych, które coraz śmielej wprowadzają nowoczesne rozwiązania z segmentu nowoczesnych technologii. Bardzo dobrym przykładem są Stany Zjednoczone Ameryki, gdzie całkiem niedawno podpisano umowę publiczno-prywatną na dostarczenie stronie administracji rządowej chmury obliczeniowej przez firmę Amazon. Tzw. GovCloud ma zapewnić agencją amerykańskim tańszą i bezpieczniejszą formę gromadzenia i przetwarzania danych. Skonsoliduje tym samym wszelkie istniejące do tej pory centra danych, poprawiając ogólną efektywność systemu. [4,5]

W związku z licznymi zaletami jakie niesie ze sobą cloud computing, chmury obliczeniowe wydają się niezbędne w przyszłych rozwiązaniach informatycznych, także w opiece zdrowotnej. Według Vivek Kunda dyrektora działu informatyki w tamtejszym sektorze rządowym, potrzeba nowego modelu informatycznego zmniejszającego koszty, a zwiększającego innowacyjność jest niezbędna, ponieważ rząd powinien rozwiązywać problemy, a nie prowadzić centra danych. W związku z opisanymi działaniami po stronie USA, również w Europie mówi się o potrzebie stworzenia chmur obliczeniowych dla tego regionu. W Komisji Europejskiej z inicjatywy komisarz ds. agendy cyfrowej Neelie Kroes, powstała zatem komórka, której za zadanie jest doprowadzenie do ujednolicenia i normalizacji rynku oraz prawa na terenie UE, aby urzeczywistnienie idei rozproszonych chmur na terenie unii było możliwe pod każdym względem. Projekt powstał w 2012 roku oraz został wpisany do strategii unijnej Horizon 2020 pod kategorią wspólnego rynku cyfrowego (DSM). Niestety prace, które wymagają konsultacji wszystkich członków UE trwają bardzo długo i nadal nie wiadomo jak będzie wyglądał ostateczny kształt chmur obliczeniowych w Europie. Komisarz Kroes jako podstawy nowych struktur wymieniła trzy punkty [6]:

- Standaryzacja i certyfikacja, która pomoże użytkownikom ocenić i porównać usługi
- Wzór warunków kontraktów będzie regulował, jak dane są wykorzystywane w chmurze i kto za nie odpowiada.
- Europejskie partnerstwa przyczynią się do pobudzenia siły nabywczej sektora publicznego i ukształtują rynek

Niezależnie od KE państwa takie jak Francja (Andromede), Niemcy (Trusted Cloud) czy Wielka Brytania (G-Cloud) także rozwijają swoje krajowe chmury obliczeniowe. Rozwiązania tego typu są planowane także w Polsce. W przyszłości przewiduje się Państwowej Chmury Obliczeniowej (PCO), która posłuży administracji państwowej do testowania aplikacji oraz obsługi podstawowej działalności, a także wprowadzenie licencjonowania, niektórych rozwiązań chmurowych w celu zapewnienia jak największego bezpieczeństwa i wiarygodności. W kontekście zapewnienia należytego bezpieczeństwa przewiduje się również opracowanie prawa i standardów, które zabezpieczą powierzane dane. W tym celu powołano min. niezależną grupę doradczą Parlamentu Europejskiego o nazwie Grupa Robocza Art. 29, która dyskutowała nad najważniejszymi problemami bezpieczeństwa i przetwarzania danych.[7,8] Skutkiem ich działań było nakreślenie określonych dylematów [8]:

- Brak pełnej interoperacyjność danych stanowi obecnie poważny problem na drodze do efektywnego działania systemu
- Przetwarzanie danych w różnych regionach geograficznych związane jest z prawem regionu, w którym znajdują się serwery. Oznacza to możliwość wpływania służb na udostępnienie danych zawartych na urządzeniach
- Wielość podwykonawców oraz długość łańcucha poddostawców usług skutkuje brakiem możliwości wskazania jaki podmiot przetwarza dane powierzone do chmury, w tym dane o stanie zdrowia.

31 lipca 2017 r. dokumentacja medyczna może być prowadzona w postaci papierowej lub elektronicznej.

PRAWO

11 maja 2017 r. weszły w życie zmiany przepisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, które zmieniają pewne, dotychczas

obowiązujące, zasady dostępu do dokumentacji medycznej. Od 31 lipca 2017 r. dokumentacja medyczna może być prowadzona w postaci papierowej lub elektronicznej. [9,10]. Obecnie w Polsce jak i w Unii Europejskiej nie ma regulacji dotyczących przetwarzania danych, w tym danych o stanie zdrowia z wykorzystaniem technologii chmury obliczeniowej. Nie oznacza to jednak, że nie można wykorzystać obowiązujących uogólnionych przepisów do określenia miejsca *cloud computingu* w przepisach prawa. Główne regulacje dotyczące najważniejszych kwestii związanych z gromadzeniem, analizą oraz archiwizacją danych medycznych (dane osobowe wraz z danymi o stanie zdrowia), zostały określone w ustawach [11-16]:

- systemie informacji w ochronie zdrowia o określa organizacje i zasady działania systemu informacji w ochronie zdrowia o reguluje kwestie dostępu i przetwarzania danych z zakresu ochrony zdrowia
- ochronie danych osobowych o reguluje i określa zasady postępowania z danymi osobowymi o nakłada na podmioty obowiązek rejestracji i zabezpieczenia danych osobowych o określa zasady powierzenia danych podmiotowi trzeciemu, art.31
- narodowym zasobie archiwalny i archiwach o reguluje kwestie elektronicznej dokumentacji medycznej o reguluje przepisy dla części dokumentacji medycznej podlegającej archiwizacji
- ochronie baz danych o reguluje dotyczące baz danych z uwzględnieniem danych o stanie zdrowia o chroni interes ekonomiczny właścicieli baz danych
- informatyzacji działalności podmiotów realizujących zadania publiczne o określa i ustala zasady i działania publicznych systemów informatycznych o ustala minimalne wymagania dla rejestrów oraz systemów teleinformatycznych do realizacji zadań publicznych o ustala zasady wymiany informacji pomiędzy podmiotami publicznymi o funkcjonowanie elektronicznej platformy usług administracji publicznej „ePUAP" oraz funkcjonowania centralnego repozytorium wzorów dokumentów urzędowych
- prawo telekomunikacyjne o regulacje zapewniające odpowiedni poziom integralności sieci, usług oraz przekazu komunikatów

W wyżej wymienionych aktach prawnych poruszone zostały najważniejsze kwestie dotyczące normowania problematyki elektronicznej dokumentacji medycznej, ochrony danych osobowych w tym zasad postępowania z danymi przez podmioty świadczące usługi medyczne oraz ochrony baz danych ze szczególnym uwzględnieniem informacji na temat zdrowia. W przepisach zawarte są również normy prawne odnoszące się do systemu informacji medycznej, a także informatyzacji podmiotów realizujących zadania publiczne. Finalnie uwzględnia się też fakt uczestników pośrednich wymiany i przetwarzania informacji, a są nimi podmioty świadczące usługi przesyłu danych, które także w sposób pośredni wchodzą w ich posiadanie, dlatego uregulowano odpowiedni poziom integralności sieci, usług oraz przekazów komunikatów przez dostawców usług i rozwiązań teleinformatycznych.

W zakresie regulacji podmiotów przetwarzających dane medyczne istnieje niewielka lista. Każdy z poniżej przytoczonych punktów jest obarczony odmiennymi normami prawnymi, a niejednokrotnie przepisy prawa mogą się przeplatać, utrudniając tym samym klarowne i pełne rozumienie prawa. Informacje o stanie zdrowia mogą być przetwarzane przez [9-16]:

- Pacjenta, którego dane są przetwarzane
- Podmiot udzielający świadczeń zdrowotnych
- Podmioty określone przepisami prawa (np. NFZ)
- Podmioty, które dostarczają infrastrukturę lub inne usług informatyczne
- Podmioty odpowiedzialne za przesyłanie danych w sieciach informatycznych

Najważniejszym zagadnieniem prawnym istotnym z punktu widzenia pracy jest określenie regulacji dla analizy zgromadzonych informacji medycznych w planowanym systemie informacji o ochronie zdrowia. Jednym ze sposobów realizacji tego zadania jest zwrócenie uwagi na rejestry medyczne, które gromadzą różne dane na wspomniany cel. W ustawie o systemie informacji w ochronie zdrowia są zdefiniowane jako „tworzone zgodnie z prawem rejestry, ewidencje, listy, spisy albo inne uporząd-

kowane zbiory danych osobowych, jednostkowych danych medycznych lub danych niebędących danymi osobowymi, służący do realizacji zadań publicznych, prowadzony przez podmiot funkcjonujący w systemie ochrony zdrowia" [17]. Uporządkowane zbiory pełnią zatem funkcję rozległych baz danych z informacjami dotyczącymi zachorowań, chorób, stanu zdrowia, metodach leczenia, diagnozowania, monitorowania postępów w leczeniu oraz zagrożeniach związanych z występowaniem niektórych chorób. Ustawodawca przewidując zapotrzebowanie na ten celuregulował także zasady zarządzania zbiorami. Główną osoba odpowiedzialną i sprawującą nadzór nad rejestrami jest właściwy minister do spraw zdrowia. Mogą być wykorzystywane do [9-17]:

1. monitorowania zapotrzebowania na świadczenia opieki zdrowotnej,
2. monitorowania stanu zdrowia usługobiorców,
3. prowadzenia profilaktyki zdrowotnej lub realizacji programów zdrowotnych.

Obok rejestrów medycznych powołano do życia rejestry o kluczowym znaczeniu dla funkcjonowania systemu [9-17]:

1. Centralny Wykaz Usługobiorców, zawierający dane dotyczące pacjentów;
2. Centralnym Wykazem Usługodawców, w którym są przetwarzane dane świadczeniodawców i aptek;
3. Centralnym Wykazem Pracowników Medycznych.

Dane do rejestrów są przekazywane przez:

- świadczeniodawców oraz apteki;
- podmioty prowadzące rejestry publiczne i rejestry medyczne.

Obecne funkcjonujące prawo prowadzenia rejestrów w Polsce, zostało jednak podważone przez Trybunał Konstytucyjny. Zakwestionowane metodologie na podstawie której rejestry medyczne były tworzone przez ministra zdrowia. Działanie i gromadzenie takich rejestrów jak np. dawców szpiku jest w pełni legalne, lecz niezgodne jest dopuszczanie do danych ministra zdrowia bądź Krajowej Radzie Transplantologicznej. Dodatkowo Rzecznik Praw Obywatelskich zgłosił kolejny wniosek do Trybunału o rozpatrzenie zasadności tworzenia rejestrów przez ministra zdrowia. Według RPO obecne uprawnienia interpretuje się zbyt szeroko, a wytyczne zawarte zarówno w treści upoważnienia, jak i w całej ustawie są zbyt ogólne, aby przesądzić o wykonawczym charakterze rozporządzenia. W związku z powyższymi problemami, prowadzenie rejestrów w ramach chmury obliczeniowej, będzie wymagało wdrożenia na poziomie ustawy. [9]

Ostatnim zagadnieniem w ramach bezpieczeństwa danych w części prawnej jest przekazywanie danych osobowych do chmury w Stanach Zjednoczonych. Kraje wymieniające informacje w ramach Unii Europejskiej są związane dyrektywą 95/46/WE oraz implementacjami krajowymi, jednak te akty prawne nie odnoszą się do wymiany międzynarodowej z krajami z poza UE, a szczególnie dotyczy to USA. [18,19] Do niedawna dane osobowe zabezpieczało porozumienie Safe Harbor jednak po uznaniu go niezgodnym z unijnymi przepisami przez Trybunał Europejski, porozumienie upadło i zostało zastąpione prze Standardowe Klauzury Umowne i Wiążące Reguły Korporacyjne, czyli pierwotne umowy międzynarodowe krajów członkowskich. W odpowiedzi na powstały chaos prawny UE oraz USA wypracowały nowe porozumienie określane mianem Privacy Shield, która według legislatorów lepiej chroni prawa obywateli dotyczące danych osobowych przy transferach do Stanów Zjednoczonych z UE i vice versa [20].

PROCEDURY

W planowanym systemie informatycznym ochrony zdrowia w Polsce, opartym na chmurze obliczeniowej, planowało się wprowadzenie pozyskiwania informacji z kliku źródeł. Były to świadczone usługi medyczne, działające bazy danych, elektroniczna dokumentacja medyczna, a także rejestry medyczne. Rozważano dwa systemy analizujące dane o stanie zdrowia.

Pierwszym z nich miał być system informacji o ochronie zdrowia obowiązkowy dla wszystkich podmiotów uczestniczących w opiece zdrowotnej za wyjątkiem usługodawców, którzy wykonują świadczenia na rzecz osób pozbawionych wolności. W ramach tego systemu funkcjonuje System Informacji Medycznej (SIM).[21] Dane są przekazywane przynajmniej raz dziennie. Po drugiej stronie miał funkcjonować system informacyjny RUM-NFZ, schemat umożliwia obowiązkowe

przekazywanie informacji o wykonanych świadczeniach i wypełnionych usługach przez świadczeniodawców i apteki, którzy mają umowę na realizacje zadań ze środków publicznych. W tym wypadku dane są przekazywane co kalendarzowy, lecz nie później niż 10 dni od jego zakończenia. W związku z funkcjonowaniem systemu informacji o ochronie zdrowia, podmioty biorące udział w ramach systemu są zobligowane do prowadzenia baz danych obejmujących [17]:

- udzielone, udzielane i planowane świadczenia opieki zdrowotnej;
- usługodawców i pracowników medycznych;
- usługobiorców.

„*Podmioty prowadzące bazy danych są uprawnione do przetwarzania zgromadzonych danych w zakresie niezbędnym do realizacji wykonywanych przez nie zadań. Są zobowiązane do przekazywania i udostępniania zgromadzonych danych na zasadach określonych w przepisach prawnych. Do ich obowiązków należy również sprawdzanie kompletności, poprawności i zgodności ze stanem faktycznym gromadzonych i udostępnianych danych* .” [17]

Równie ważnym aspektem w kontekście stworzenia pełnoprawnej chmury obliczeniowej w ramach ochrony zdrowia jest kwestia wyboru miejsca przechowywania danych o stanie zdrowia. Obecnie decyzja odnośnie miejsca przechowywania jest podejmowana przez kierownika, co ważne nie ma w tym momencie przepisu zabraniającego składowania danych w miejscu poza ośrodkiem medycznym. Ministerstwo Spraw Wewnętrznych uszczegółowiło, że miejsca wytworzonej dokumentacji powinno być w zakładzie, lecz jednocześnie dopuściło jego archiwizacje w innym podmiocie pod warunkiem jej należytego zabezpieczenia przed zniszczeniem, uszkodzeniem, utratą i dostępem osób nieupoważnionych. Standardy określono dość szczegółowo. Równie ważnym punktem jest instytucja powierzenia danych o stanie zdrowia. Administrator danych może przetwarzać samodzielnie bądź powierzyć ich przetwarzanie innemu podmiotowi.

WYMAGANIA I STANDARDY

Wprowadzenie chmury obliczeniowej na polski rynek usług zdrowotnych niesie ze sobą również wiele wymagań i standardów, które ta musi spełnić. Przepisy ustawy o ochronie danych osobowych wraz z rozporządzeniami implikują wiele skutków prawnych, które muszą być przestrzegane.[22] Chodzi miedzy innymi o zachowanie poufności, integralności czy też rozliczalności danych, aby dokonać obowiązku prawnego podmiot przetwarzający dane musi stworzyć i prowadzić dokumentacje bezpieczeństwa. Dodatkowo jest on zobligowany do spełnienia szeregu wymagań dotyczących systemu informatycznego, a także poziomu bezpieczeństwa (wysokiego), które również zostały określone ustawą. Rzeczą kluczową jest ustanowienie w podmiocie systemu zarządzania bezpieczeństwem informacji. Na szczęście i w tym przypadku podmioty wdrażające rozwiązania typu chmurowego nie są pozostawione same sobie, bowiem może choć nie musi skorzystać z opracowania systemu na podstawie wskazanych norm tj. Polskiej Normy PN-ISO/IEC 27001.

PIŚMINNICTWO

1. Kroes N. Setting up the European Cloud Partnership. Speech at the World Economic Forum, Davos 2012.
2. Burnejko M. Kto korzysta z chmury w Polsce (i na świecie). Blog ekspertów IT . 04 września 2015. [cytowany 8 sierpnia 2016]. Adres: Chmurowisko.pl, http://chmurowisko.pl/
3. Mapping the cloud maturity curve: The Economist Intelligence Unit. 2015. 18 luty 2016. [cytowany 8 sierpnia 2016].http://www.corporate leaders.com/ sitescene/custom/userfiles/file/White_Papers/Mapping %20the%20cloud%20maturity%20curve.pdf, 25.08.2016. 34.
4. Mell P, Grance T. The NIST Definition of Cloud Computing. 2011. 18 luty 2016. [cytowany 8 sierpnia 2016]. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication80.-145.pdf,
5. Kielar M, Romaszewski A, Trąbka W. Perspektywy wprowadzenia modelu chmury obliczeniowej w ochronie zdrowia w świetle istniejących rozwiązań prawnych i organizacyjnych. Zesz Nauk WSZIB 2014;33:20-35.
6. European Cloud Strategy. 04 września 2016. [cytowany 20 września 2016] Adres: https://ec.europa.eu/digitalsingle-market/en/european-cloud-computing-strategy
7. Uptake of Cloud in Europe. Raport IDC na zlecenie Komisji Europejskiej, 2013. 18 luty 2016. [cytowany 8 sierpnia 2016].https://ec.europa.eu/digital-single-

market/en/news/final-report-study-smart-20130043uptake-cloud-europe.
8. Parlament Europejski. Chmury obliczeniowe. [cytowany 20 września 2018] Adres: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf
9. Wchodzi w życie nowelizacja ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. [cytowany 20 września 2018] Adres: https://jamano.pl/2017/05/11/prawa-pacjenta-i-nowelizacja-ustawy/
10. USTAWA z dnia 26 czerwca 2014r. o zmianie ustawy o systemie informacji w ochronie zdrowia. Dz.U. 2014 poz. 998.
11. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia Dz.U. 2011 nr 113 poz. 657
12. Art. 27. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883
13. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. Dz.U. 1983 nr 38 poz. 173 wraz z rozporządzeniami wykonawczymi
14. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych. Dz.U. 2001 nr 128 poz. 1402
15. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne Dz.U. 2005 nr 64 poz. 565
16. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne Dz. U. 2004 nr 171 poz. 1800
17. Ustawa z dnia 26 czerwca 2014 r. o zmianie ustawy o systemie informacji w ochronie zdrowia Dz.U. 2014 poz. 998
18. Dyrektywa 95/46/We Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych
19. Unijne rozporządzenie o ochronie danych osobowych. [cytowany 22 września 2016] Adres: http://e-ochronadanych.pl/unijne-rozporzadzenie-o-ochronie-danych-osobowych/
20. 6 rzeczy o Privacy Shield o których powinno się wiedzieć. [cytowany 22 września 2016] Adres: http://e-ochronadanych.pl/6-rzeczy-o-privacy-shield-o-ktorych-powinno-sie-wiedziec/
21. Romaszewski A, Trąbka W. Procedury przetwarzania danych medycznych w aspekcie wykorzystania chmury obliczeniowej. Zesz Nauk WSZIB 2014;33:55-70.
22. Romaszewski A, Trąbka W. Wymagania I standardy związane z przetwarzaniem danych medycznych. Zesz Nauk WSZIB 2014;33:71-80.