

**Cywilnoprawna
odpowiedzialność dostawcy
usług cloud computing
w świetle przepisów Ogólnego
Rozporządzenia o Ochronie
Danych Osobowych - wybrane
problemy**

Przejdź do produktu na **ksiegarnia.beck.pl**

Wstęp

Kiedy w 1943 r. współzałożyciel i prezes IBM, *Thomas Watson* wygłosił śmiałą tezę o tym, że „rynek światowy potrzebuje nie więcej niż pięciu komputerów”¹ nie wielu było takich, którzy przyjęli to z entuzjazmem i zaaprobowali. Co więcej, szybki rozwój technologii i branży IT², skutkujący nie tylko coraz szerszym dostępem do Internetu, ale też upowszechnieniem się dostępu do nabywania różnego rodzaju dóbr materialnych z tejże dziedziny, przez wiele kolejnych lat zdawał się przeczyć prawdziwości tego typu twierdzeń. Tymczasem obserwacja samego procesu i kierunków rozwoju usług informatycznych w ostatnich latach XX i początkach XXI w. musi i powinna implikować wniosek o słuszności przytoczonej powyżej opinii. I choć oczywiście pogląd ten należy traktować metaforycznie, trudno sobie bowiem wyobrazić dosłowne urzeczywistnienie tejże tezy, to dziś jego istota znajduje odzwierciedlenie właśnie w postaci technologii *cloud computing*, w języku polskim określanej terminem „chmury obliczeniowej” czy też „przetwarzania w chmurze”³. Idea tychże usług sprowadza się bowiem do wszechobecnego, wygodnego i możliwego na żądanie dostępu 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 dostawcy⁴, a więc – analogicznie jak w przytoczonym powyżej

¹ Y. Shen, U. Li, L. Wu, S. Liu, Q. Wen, Cloud era information hub, w: Y. Shen, U. Li, L. Wu, Q. Wen (red.), Enabling the new era of cloud computing: data security, transfer, and management, Hershey PA 2014, s. 27.

² Ang. *Information Technology*. Według Merriam-Webster Dictionary pod pojęciem tym rozumieć należy technologię obejmującą opracowywanie, utrzymywanie i wykorzystywanie systemów komputerowych, oprogramowania i sieci do przetwarzania i dystrybucji danych, [https://www.merriam-webster.com/dictionary/information technology](https://www.merriam-webster.com/dictionary/information%20technology) (dostęp: 18.3.2018 r.).

³ Podobnie również na potrzeby przedmiotowej dysertacji za zasadne uznać należy naprzemienne posługiwanie się takimi określeniami, jak *cloud computing*, przetwarzanie w chmurze, czy pojęciem chmury obliczeniowej.

⁴ P. Mell, T. Grance, The NIST Definition of Cloud Computing: Recommendations of National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, MD September 2011, s. 2, csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (dostęp: 20.1.2015 r.). Zob. także Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie wykorzystania potencjału chmury obliczeniowej w Europie, COM (2012) 529 final, s. 2; J. Byrski, A. Wachowska, Cloud computing w działalności instytucji płatniczej, MoPrBank 2012, Nr 9, s. 59; D. Szostek, Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej, Warszawa 2012, s. 56–57.

twierdzeniu – opiera się ona na dostępie do zmaksymalizowanych zasobów obliczeniowych, a nie ich rozproszeniu. W praktyce obejmuje ona swoim zakresem pojęciowym możliwość skorzystania z portali społecznościowych (np. Facebook, LinkedIn), poczty elektronicznej (m.in. Google Gmail, Yahoo!), przechowywanie i przetwarzanie plików (Dropbox, Google Drive), zdjęć, udostępnianie muzyki (Spotify) czy filmów na żądanie (Netflix), tzw. media strumieniowe (np. Youtube) czy chociażby pakiety biurowe *online* (np. Microsoft Office 365) i przynosi szereg różnego rodzaju korzyści, takich jak powszechność, funkcjonalność, elastyczność i niskie koszty dostępu.

Dziś, przez wielu postrzegana w kategoriach technologii „jutra”, stanowiąca wyraz o ile nie prawdziwej rewolucji, to przynajmniej kolejny krok w ewolucji technologii IT, po wodzie, gazie, energii elektrycznej i telefonii, utożsamiana z „piątą użytecznością”⁵, „demokratyzuje innowacje”⁶, będąc powszechnie dostępną zarówno dla podmiotów indywidualnych, jak i różnego rodzaju organizacji czy przedsiębiorstw. Wywiera ona ogromny wpływ nie tylko na ich codziennie funkcjonowanie, ale też silnie oddziałuje na gospodarkę zarówno Polski, jak i całego świata. Z roku na rok poszerza się grono odbiorców przedmiotowych usług, a wartość światowego rynku sięga setek bilionów dolarów amerykańskich⁷.

Taki stan rzeczy, co oczywiste, powoduje, że technologia ta jest przedmiotem zainteresowania nie tylko przedstawicieli branży informatycznej, ekonomistów, ale też ustawodawców poszczególnych państw i ustawodawcy unijnego, czy przedstawicieli nauki prawa. I choć, co jest truizmem, **rzeczone prawo nie nadaje za technologią, to niemniej jednak wzajemna ich implikacja jest nie do przecenienia. Z jednej strony technologia *cloud computing*, cechująca się przecież tak dużą powszechnością, masowością i aterytorialnością, musi mieścić się w porządkach prawnych czy to poszczególnych państw, czy UE, to z drugiej strony prawo nie powinno niweczyć jej użyteczności, zapewniając chociażby możliwość jej rozwoju. Sztuką racjonalnego ustawodawstwa winno być przecież to, aby zapewnić milionom użytkowników na całym świecie możliwość takiego korzystania z technologii *cloud computing*, które o ile nie będzie stanowić swoistej ochrony przed jej negatywnymi skutkami czy ryzykiem (które to zresztą są immanentną cechą każdej technologii), to chociaż tworzyć będzie mechanizmy czy instrumenty pozwalające zrekomensować poniesione w tym zakresie straty, krzywdy czy naruszone prawa, dobra, interesy. Potrzeba taka zdaje się być zresztą tym bardziej pożądana, gdy dotyczy ona technologii, z której każdego dnia korzysta wiele milionów osób fizycznych (konsumentów), ale też wykorzystywana jest w celach związanych z działalnością gospodarczą przedsiębiorstw, organizacji itd., co ma miejsce właśnie w przypadku chmury obliczenio-**

⁵ T.J. Calloway, Cloud computing, clickwrap, agreements and limitation on liability clauses: a perfect storm?, DLTRev, vol. 11, No. 1, s. 166.

⁶ P. Szygalski, Chmura obliczeniowa demokratyzuje innowacje, <https://www.wnp.pl/tech/chmura-obliczeniowa-demokratyzuje-innowacje366752.html> (dostęp: 21.2.2020 r.).

⁷ Więcej na ten temat (w tym dane statystyczne) w dalszej części pracy.

wej. Stawianie pytania o to, jakie w aktualnym stanie prawnym obowiązują normy prawne urzeczywistniające możliwość rekompensowania naruszenia praw czy interesów użytkowników *cloud computing*, z którym to pytaniem immanentnie związane jest zagadnienie odpowiedzialności prawnej tychże podmiotów, zdaje się więc mieć nie tylko doniosłość prawną, ale też walor praktyczny. Stąd na kartach przedmiotowej pracy podjęłam się oceny istniejących w tym zakresie w prawie polskim unormowań, przy czym oczywista wydaje się być jednocześnie okoliczność, że analiza taka musiała być prowadzona na określonym polu badawczym, tak aby możliwym było nie tylko dogłębne zidentyfikowanie istniejących na tym polu rozwiązań prawnych, ale też ich szczegółowa ocena *in concreto* w odniesieniu do technologii *cloud computing*.

Dokonując więc pewnej selekcji materiału badawczego, zakres swojej analizy ograniczyłam do kwestii związanej z cywilnoprawną odpowiedzialnością dostawcy usług *cloud computing* w świetle przepisów ogólnego rozporządzenia o ochronie danych osobowych, na co wpływ miało szereg okoliczności.

Przed wszystkim analiza cech charakterystycznych chmury obliczeniowej pozwala na metaforyczne i ogólne ujęcie jej istoty jako przetwarzanie różnego rodzaju danych/informacji, które to w ujęciu normatywnym mogą być różnie klasyfikowane i pomiędzy którymi mogą zachodzić różnego rodzaju korelacje. Jedną z takich kategorii danych, które poddawane są procesom przetwarzania w chmurze obliczeniowej, są dane osobowe. I choć oczywiście w ramach *cloud computing* dojść może jeszcze do przetwarzania takich kategorii danych, jak dobra osobiste, treść cyfrowe czy tajemnice prawnie chronione, to niemniej jednak odniesienie się do danych osobowych zdaje się być, zwłaszcza po 25.5.2018 r., konieczne i potrzebne. Otóż od tego czasu zastosowanie mają przepisy RODO, które po niemal 25 latach obowiązywania Dyrektywy 95/46/WE⁸ na nowo ukształtowały przestrzeń prawa ochrony danych osobowych w państwach członkowskich UE, implikując przy tym konieczność rozstrzygnięcia wielu prawnie relewantnych wątpliwości i poszukiwania odpowiedzi na szereg pytań. Mimo że dorobek judykatury i piśmiennictwa z biegiem czasu staje się coraz bardziej obszerny, to nadal jednak pozostaje szereg zagadnień, które wymagają szerszej analizy, a uzyskanie konkretnych wniosków w tym zakresie – tak jak w przypadku *cloud computing* – może mieć praktyczne implikacje dla ogromnej rzeszy podmiotów indywidualnych.

I tak, z całą pewnością do tego typu zagadnień, które wymagają głębszej refleksji zaliczyć można to dotyczące cywilnoprawnej odpowiedzialności dostawcy usług w chmurze obliczeniowej w świetle przepisów RODO. Poza wskazaną już wcześniej okolicznością ważkości tego zagadnienia dla olbrzymiej rzeszy użytkowników tejże technologii w Polsce, dla których analiza ta może okazać się pomocna w dochodzeniu roszczeń odszkodowawczych od interesujących nas dostawców, równie istotna zdaje się być uwaga,

⁸ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L z 1995 r. Nr 281, s. 31 ze zm.).

iż to właśnie w przepisach rozporządzenia ogólnego o ochronie danych osobowych – inaczej niż to miało wcześniej miejsce w przypadku Dyrektywy 95/46/WE – zawarto *stricte* prywatnoprawną regulację dotyczącą odpowiedzialności z tytułu naruszenia jego przepisów. Tego typu *novum*, co oczywiste, musi implikować szereg kolejnych wątpliwości i pytań natury prawnej, dla których poszukiwanie odpowiedzi zwięzłone powinno zostać o ile nie rozstrzygnięciem, to przynajmniej stanowić początek pewnego dyskursu naukowego w tym zakresie.

Biorąc pod uwagę wszystkie te okoliczności, za zasadne uznałam podjęcie się próby analizy zagadnienia cywilnoprawnej odpowiedzialności dostawcy usług *cloud computing* w kontekście naruszenia ochrony danych osobowych i dalej, próby odpowiedzi na pytanie: czy, a jeśli tak, to na ile normy rozporządzenia ogólnego o ochronie danych osobowych kształtujące mechanizmy cywilnoprawnej odpowiedzialności *in abstracto* sprawdzają się w kształtowaniu odpowiedzialności dostawców usług *cloud computing in concreto*?

Ponadto osiągnięcie wskazanego powyżej celu badawczego wymagało także określenia, a następnie osiągnięcia pośrednich celów badawczych, które to sformułowane w postaci pytań brzmią następująco:

- 1) Jakie kategorie danych/informacji (prawnie relewantnych) przetwarzane są w ramach *cloud computing* i jak należy je klasyfikować prawnie oraz czy, a jeśli tak, to jakie zachodzą pomiędzy tymi kategoriami korelacje mogące mieć wpływ na kształtowanie się odpowiedzialności dostawcy usług w chmurze obliczeniowej?
- 2) Jak – biorąc pod uwagę złożoność regulacji dotyczących *cloud computing* i ich multiplikacje – owy *cloud computing* identyfikować prawnie, tj. w szczególności jak na gruncie przepisów RODO identyfikować dostawcę usług w chmurze obliczeniowej i dalej umowę o świadczenie przedmiotowych usług? Uzyskanie odpowiedzi na to pytanie pozwoli m.in. na doprecyzowanie, jakie obowiązki spoczywają na dostawcy usług w chmurze obliczeniowej z tytułu przepisów ogólnego rozporządzenia o ochronie danych osobowych, co jest okolicznością niezbędną dla określenia zakresu jego odpowiedzialności.
- 3) Jaką koncepcję odpowiedzialności cywilnej (tj. zakres i zasady) przyjął ustawodawca unijny w ramach przepisów RODO, w tym także jak kształtował się zakres odpowiedzialności dostawcy usług w chmurze obliczeniowej w polskim porządku prawnym pod rządami Dyrektywy 95/46/WE?
- 4) Jak odpowiedzialność dostawcy *cloud computing* będzie się kształtowała na gruncie przepisów KC zarówno w kontekście regulacji przyjętej w RODO, jak – co ma charakter rozważań uzupełniających – chociażby w przypadku odpowiedzialności kontraktowej czy na podstawie art. 415 i n. KC?

Przedmiotowa analiza prowadzona była przy wykorzystaniu następujących metod porządkowania czynności badawczych tj.: metody formalno-dogmatycznej, a także w charakterze metod uzupełniających metody historycznej oraz porównawczej.

Pierwsza ze wskazanych powyżej metod, tj. metoda formalno-dogmatyczna, ma podstawowe znaczenie dla efektywności poszukiwania odpowiedzi na stanowiące trzon dysertacji pytania badawcze. Jej istota bowiem sprowadza się do egzegezy treści norm prawnych i ustalenia ich znaczenia, co – głównie z uwagi na złożoność regulacji dotyczących *cloud computing* – miało fundamentalne znaczenie nie tylko dla uzyskania odpowiedzi na pytanie dotyczące możliwości identyfikacji prawnej *cloud computing* na gruncie prawa prywatnego, ale też dla wyznaczenia pola badawczego.

Wreszcie też, w charakterze metod uzupełniających, wykorzystane zostały metody historyczna i porównawcza, których to zastosowanie sprowadzało się głównie do dwóch celów, tj. do wykazania, jak na przestrzeni ostatnich lat kształtowały się – zwłaszcza te mające znaczenie w kontekście chmury obliczeniowej – regulacje prawne z zakresu prawa ochrony danych osobowych, a także jak sama koncepcja odpowiedzialności dostawcy tychże usług ewoluowała w prawie UE i prawie krajowym.

Realizacja przywołanych powyżej celów badawczych implikowała także systematykę i strukturę pracy, która to została podzielona na część wprowadzającą, cztery rozdziały i część podsumowującą.

W rozdziale pierwszym, mającym charakter wprowadzający i porządkujący, przybliżona została istota usług *cloud computing*, a także proces tworzenia i ewolucji tejże technologii na przestrzeni ostatnich lat. Ta część dysertacji, ograniczona jedynie do najistotniejszych aspektów, stała się następnie preludium do kolejnych rozważań, tym razem jednak dotyczących kwestii zasadniczych, a więc czym owy *cloud computing* w istocie jest oraz jak rozumienie tegoż pojęcia ewoluowało i nadal ewoluuje. Następnie zaprezentowana i omówiona została także typologia usług i modeli chmury, a zamknięcie rozważań w niniejszym rozdziale stanowiło zaprezentowanie korzyści i potencjalnych zagrożeń, jakie niesie ze sobą korzystanie z usług przetwarzania w chmurze.

W rozdziale drugim, również mającym charakter wprowadzający, wskazane i wyodrębnione zostały poszczególne kategorie danych, jakie mogą być przetwarzane w ramach *cloud computing*. Powyższe pozwoliło nie tylko na dookreślenie i sprecyzowanie – stanowiącej *clou* rozważań niniejszego opracowania – kategorii danych osobowych, ale też na ukazanie wzajemnych korelacji pomiędzy poszczególnymi kategoriami danych i tym samym również wynikających z tego implikacji prawnych. I tak analizie, oprócz danych osobowych, poddane zostało zagadnienie przetwarzania w chmurze obliczeniowej dóbr osobistych, treści cyfrowych, tajemnic prawnie chronionych (jak np. tajemnica adwokacka) czy wreszcie też danych nieosobowych.

Rozdział trzeci, zatytułowany „Aspekty prawne *cloud computing* – złożoność regulacji i ich multiplikacja”, miał fundamentalne znaczenie dla osiągnięcia głównego celu badawczego pracy. Jego istota sprowadzała się do odpowiedzi na jedno z przywołanych powyżej pytań, a mianowicie jak *cloud computing* identyfikować prawnie, a także do określenia prawnego statusu dostawcy usług chmury obliczeniowej. W kontekście określonego wcześniej kierunku analizy całość poczynionych w tym względzie uwag ograniczona zostanie do prawa ochrony danych osobowych.

Identyfikacja umowy *cloud computing* na gruncie prawa ochrony danych osobowych wiązała się nie tyle z określeniem formy, elementów i przedmiotu takiej umowy, choć oczywiście powyższe aspekty również zostały w dysertacji omówione, ale przede wszystkim z oceną charakteru tejże umowy w kontekście przepisów prawa ochrony danych osobowych oraz koniecznością analizy statusu podmiotów uczestniczących w przetwarzaniu danych osobowych w chmurze obliczeniowej, tj. z analizą pojęcia administratora danych i podmiotu przetwarzającego. Powyższe rozważania tym samym stanowiły istotną część całej rozprawy i przy tym ważny punkt odniesienia dla przedstawionych w dalszej części pracy analiz. Całość przeprowadzonej w tym zakresie analizy uzupełniona została dodatkowo m.in. o kwestie związane z transferem danych do państw trzecich, co jest zrozumiałe, jeżeli weźmie się pod uwagę aterytorialny charakter chmury obliczeniowej, a także o kwestie związane z podpowierzaniem danych osobowych.

Meritum rozprawy stanowi rozdział czwarty zatytułowany „Kształtowanie się odpowiedzialności dostawcy usług *cloud computing* – rozważania cywilnoprawne”.

W tej części pracy w pierwszej kolejności odniosłam się do koncepcji i zakresu cywilnoprawnej odpowiedzialności dostawcy usług *cloud computing* jaka obowiązywała w prawie polskim w świetle Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Powyższe było bowiem niezbędne nie tylko dla zrozumienia doniosłości zmian, jakie za sprawą rozporządzenia ogólnego o ochronie danych osobowych w tymże zakresie nastąpiły, ale też dla formułowania ocen tychże zmian *in concreto* w odniesieniu do dostawców usług w chmurze obliczeniowej.

Następnie analizie poddane zostały te regulacje rozporządzenia ogólnego o ochronie danych osobowych, które to stanowią o istocie dysertacji i bezpośrednio dotyczą odpowiedzialności, tj. art. 79 i 82 RODO.

I tak, w pierwszej kolejności dokonano egzegezy treści art. 79 rozporządzenia ogólnego o ochronie danych osobowych, po czym płynące z tej teoretycznoprawnej analizy wnioski stały się podstawą do formułowania implikacji art. 79 RODO dla usług *cloud computing*. W tym zakresie nieodzownym elementem było nadto odniesienie się do koncepcji ustawodawcy polskiego co do urzeczywistnienia uprawnień zagwarantowanych podmiotowi danych na gruncie art. 79 RODO, a także oceny trafności tejże koncepcji z punktu widzenia skuteczności dochodzenia przez podmioty danych ich prawa. Stąd też kolejne rozważania dotyczyły przepisów rozdziału 10 OchrDanOsobU 2018⁹, a ściślej normy art. 92 OchrDanOsobU 2018 stanowiącej w istocie realizację podstawy kompetencyjnej wskazanej w art. 79 RODO. W związku z tym, że w treści rzeczowej regulacji art. 79 RODO ustawodawca europejski uregulował także kwestie związane z właściwością miejscową postępowania przeciwko administratorowi lub podmiotowi przetwarzającemu, również i te

⁹ Ustawa z 10.5.2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781).

zostały poddane krótkiej analizie. W tym miejscu poczynić należy jednak bardzo ważną uwagę, a mianowicie, że odniesienie się w przedmiotowej pracy do zagadnień *stricto* prawnomiedzynarodowych (jak np. kwestia jurysdykcji sądowej czy prawa właściwego) miało jedynie charakter ogólny i uczynione zostało tytułem zasygnalizowania problemów, jakie mogą w praktyce w tym kontekście mieć miejsce. Decyzja o takiej redukcji materiału badawczego podyktowana została przede wszystkim względami praktycznymi, tj. oceną, iż czynienie w tym zakresie szerszych uwag znacznie wykraczałoby poza przyjętą w pracy tematykę, a nadto jej obszerność i złożoność skutecznie uniemożliwiałaby wyczerpujące odniesienie się do tego tematu. Z tych też względów przyjęto założenie, że wszelkie analizy i wnioski czynione będą w tej pracy przy założeniu, że prawem właściwym będzie prawo polskie, a jurysdykcja sądowa ograniczona została do sądów polskich.

Pozostając w obszarze uregulowań RODO w dalszej części pracy podjęta została analiza treści jego art. 82, który to określa zasady odpowiedzialności odszkodowawczej administratora lub podmiotu przetwarzającego za poniesioną przez osobę, której dane dotyczą, szkodę majątkową lub niemajątkową w związku z naruszeniem przepisów RODO. Poza oczywistą koniecznością podjęcia się analizy takich kwestii, jak zasady, zakres czy przesłanki tejże odpowiedzialności oraz zagadnień związanych z wyłączeniem tej odpowiedzialności, odpowiedzialnością solidarną czy sposobem naprawienia szkody, za szczególnie istotną uznać należy ocenę charakteru tejże regulacji i jej umiejscowienie w kontekście przepisów KC – co w dalszej kolejności implikowało także konieczność doprecyzowania, które przepisy KC odnoszące się do odpowiedzialności odszkodowawczej winno się i należy stosować w kwestiach nieuregulowanych w art. 79 i 82 RODO¹⁰ – do czego obliży także i ustawodawca krajowy mocą przepisów ustawy o ochronie danych z 2018 r.

Następną część pracy stanowią rozważania prowadzone na gruncie KC. W pierwszej kolejności, nawiązując do przywołanej w rozdziale drugim pracy relacji pomiędzy danymi osobowymi a dobrami osobistymi, przeprowadzono analizę zagadnienia odpowiedzialności dostawcy usług *cloud computing* z tytułu naruszenia dóbr osobistych. Ponadto poruszono kwestię dopuszczalności dochodzenia roszczeń odszkodowawczych od dostawcy usług *cloud computing* na podstawie art. 415 KC w świetle przepisów RODO, przy czym sformułowane na tym polu oceny potraktować należy jako pewien przyczynek do szerszej w tym zakresie dyskusji.

Wreszcie też, przeanalizowane zostały zagadnienia dotyczące kontraktowej odpowiedzialności dostawcy usług *cloud computing*. Biorąc jednak pod rozległość tematyki odpowiedzialności kontraktowej *in extenso*, w pracy poruszone zostały te z nich, które, jak wynika z obserwacji praktyki kontraktowania usług *cloud computing*, są w tym zakresie charakterystyczne, a dotyczą m.in. umownych modyfikacji podstaw odpowie-

¹⁰ M. Gumularz, Wpływ regulacji odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich, EPS 2017, Nr 5, s. 31 i n.

działności dostawcy usług w chmurze obliczeniowej, kwestii kary umownej czy odpowiedzialności dostawcy interesujących nas usług za działania lub zaniechania osób trzecich.

W rezultacie więc tak przeprowadzona analiza wyznaczyła podstawy do formułowania wniosków i pytań o odpowiedzialność dostawcy usług *cloud computing* na gruncie prawa prywatnego i tym samym umożliwiła osiągnięcie głównego celu badawczego rozprawy.

Podsumowanie stanowi zakończenie prezentowanych rozważań i analiz i odnosi się do stopnia realizacji założonych celów badawczych.

Najważniejszymi źródłami stanowiącymi podstawę prowadzonych rozważań badawczych były przede wszystkich akty normatywne. Zważywszy na fakt, że dorobek polskich przedstawicieli doktryny w tym zakresie, choć coraz większy i znaczący, nie objął jeszcze wielu ważnych kwestii, w dysertacji znajdują się liczne odwołania do literatury zagranicznej.

Przejdź do księgarni →



ksiegarnia.beck.pl