Łódzkie Studia Teologiczne
35 (2026) 2

Emilia Rybicka
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

ANALIZA PRZYPADKÓW NARUSZENIA DANYCH W CHMURACH NA PODSTAWIE WYBRANYCH INCYDENTÓW W LATACH 2020–2024

1. Geneza i ewolucja chmury obliczeniowej. 2. Regulacje prawne chmury obliczeniowej. 3. Analiza wybranych incydentów naruszeń danych w chmurach

Słowa kluczowe: chmura, dane, bezpieczeństwo, ochrona, usługi, RODO

1. GENEZA I EWOLUCJA CHMURY OBLICZENIOWEJ

Chmura obliczeniowa jest jedną z kluczowych technologii współczesnej ery cyfrowej, znacząco zmieniającą sposób, w jaki społeczeństwo zarządza danymi oraz zasobami IT. W artykule przedstawiono podstawowe zagadnienia związane z definicją chmury obliczeniowej i jej rozwojem, co pozwoli zrozumieć jej funkcjonowanie. Przeanalizowano historię i ewolucję chmury obliczeniowej, uwzględniając także zmiany w mechanizmach działania oraz zastosowaniach IT. Zaprezentowano rozwiązania chmurowe różnych firm dostępnych na rynku, takich jak: Apple, Google, Microsoft oraz Amazon. Ukazane zostało, jak można wykorzystać rozwiązania, które oferują.

Wraz z rozwojem technologii informatycznych i powszechnym dostępem do Internetu pojawiły się nowe modele zarządzania danymi i zasobami IT. Jednym z najważniejszych z nich jest chmura obliczeniowa, która jest polskim odpowiednikiem angielskiego *cloud computing* i odnosi się do modelu dostarczania usług informatycznych za pośrednictwem Internetu. Nazwa ta wywodzi się z diagramów sieciowych, gdzie Internet był przedstawiony jako symbol chmury[1]. Chmura obliczeniowa jest zwykle postrzegana jako nowoczesna technologia do przechowywania, przetwarzania i zarządzania danymi, oparta na współdzieleniu zasobów, takich jak: oprogramowanie i infrastruktura. Usługi te mogą być dostarczane przez dostawcę zewnętrznego lub wewnętrznego, a dostęp do nich odbywa się przez Internet[2].

[1] Por. G. Szpor, Internet Cloud Computing, *Przetwarzanie w chmurach*.

[2] Por. Centralny Ośrodek Informatyki – POPC Wsparcie, *Co to jest chmura obliczeniowa?* Portal Gov.pl., https://www.gov.pl/web/popcwsparcie/co-to-jest-chmura-obliczeniowa (dostęp: 20.11.2024).

Kolejnym przykładem definicji chmury obliczeniowej jest innowacyjny model przetwarzania danych, który opiera się na wykorzystaniu zaawansowanej infrastruktury zdalnych serwerów połączonych w sieć za pomocą Internetu. Technologia ta umożliwia użytkownikom dostęp do zasobów obliczeniowych, przechowywania danych i aplikacji bez konieczności lokalnego posiadania sprzętu czy oprogramowania. Głównym założeniem chmury jest umożliwienie korzystania z mocy obliczeniowej oraz przechowywania danych w sposób elastyczny, skalowalny i dostępny na żądanie, co odróżnia ją od tradycyjnych rozwiązań informatycznych. Symbolizuje przejście od modelu lokalnego przetwarzania danych do modelu rozproszonego, gdzie dane i aplikacje są przechowywane na serwerach należących do dostawców usług chmurowych. Użytkownicy mogą dzięki temu korzystać z usług z dowolnego miejsca na świecie, mając dostęp do Internetu[3].

Z perspektywy prawnej, termin *chmura obliczeniowa* nie jest określony ustawowo ani w przepisach polskich, ani w aktach prawnych Unii Europejskiej wynikających z Traktatu o Funkcjonowaniu Unii Europejskiej. Przepis ten stanowi, że „w celu wykonania kompetencji Unii instytucje przyjmują rozporządzenia, dyrektywy, decyzje, zalecenia i opinie. Rozporządzenie ma zasięg ogólny i jest bezpośrednio stosowane we wszystkich Państwach Członkowskich. Dyrektywa wiąże każde Państwo Członkowskie, do którego jest kierowana, w odniesieniu do rezultatu, który ma być osiągnięty, pozostawia jednak organom krajowym swobodę wyboru formy i środków. Decyzja wiąże w całości. Decyzja, która wskazuje adresatów, wiąże tylko tych adresatów. Zalecenia i opinie nie mają mocy wiążącej”[4]. W prawie unijnym znajduje się definicja usługi ośrodka przetwarzania danych, która według art. 6 pkt 30 dyrektywy NIS 2 obejmuje „usługę chmurową”, umożliwiającą dostęp do skalowalnego i elastycznego zestawu zasobów obliczeniowych przeznaczonych do wspólnego użytkowania[5]. Zdalne serwery, na których przechowywane są dane i aplikacje, mogą być wykorzystywane przez wielu użytkowników jednocześnie.

Historia chmur obliczeniowych sięga lat 60. XX w., gdy koncepcja współdzielenia zasobów komputerowych zyskała popularność dzięki postępom technologicznym. Idea dostępu do komputerów na żądanie, rozwinięta przez wynalazców takich jak John McCarthy, wskazywała, że kiedyś przetwarzanie komputerowe stanie się usługą publiczną. Początkowo rozwój tej koncepcji był ograniczony ze względu na wysokie koszty i rozmiary ówczesnych komputerów. Pierwsze maszyny były masywne, miały niewielką moc obliczeniową i wymagały znacznych nakładów energetycznych, co sprawiało, że niewiele przedsiębiorstw mogło sobie na nie pozwolić. Dodatkowo, technologia wirtualizacji, kluczowa dla chmury obliczeniowej, była wówczas w początkowej fazie rozwoju. Wraz z rozwojem Internetu w latach 90.,

[3] Por. A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Wolters Kluwer, Warszawa 2017, 48–51.

[4] Traktat USTANAWIAJĄCY EUROPEJSKĄ WSPÓLNOTĘ GOSPODARCZĄ (Dz.U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.).

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80).

chmura obliczeniowa zaczęła nabierać praktycznego znaczenia. W 2000 r. wiele firm zaczęło inwestować w nowe technologie i poszukiwać innowacyjnych rozwiązań. To właśnie wtedy chmury obliczeniowe zaczęto tworzyć. Inspiracją nazwy *chmura obliczeniowa* były schematy i rysunki chmur, często używane w podręcznikach dotyczących *business computingu* do przedstawiania złożonych systemów sieciowych. W miarę postępu technologicznego, wirtualizacja zasobów stała się bardziej dostępna, a rozwój szybkich i rozległych sieci umożliwił efektywne przetwarzanie danych na odległość[6].

Pierwszą na świecie usługą chmury obliczeniowej, która zapoczątkowała rozwój tej technologii, był Amazon. Jako pionier w handlu elektronicznym potrzebował skalowalnej i elastycznej infrastruktury, aby sprostać rosnącemu zapotrzebowaniu na zasoby obliczeniowe i przechowywanie danych. Pierwsze kroki powstania Amazon Web Services[7] podjęto na początku lat 2000, kiedy Amazon dostrzegł, że rozwój własnej infrastruktury IT jest kosztowny i czasochłonny. Firma postanowiła zbudować uniwersalny system do zarządzania zasobami i wdrażania usług. W 2003 r. inżynierowie Amazonu, w tym Andy Jassy, opracowali koncepcję platformy usługowej, która umożliwiłaby innym firmom korzystanie z tej samej infrastruktury, na której działa Amazon. Przełomowym momentem był 2006 r., kiedy Amazon uruchomił AWS, który zmienił model dostarczania usług IT na oparty o *pay-as-you-go*, co oznacza, że użytkownicy płacą tylko za wykorzystane zasoby. Początkowo składała się z kilku kluczowych usług, takich jak Amazon S3, czyli Amazon Simple Storage Service, który umożliwiał przechowywanie danych w chmurze, oraz Amazon Elastic Compute Cloud[8], pozwalający na uruchamianie skalowalnych maszyn wirtualnych. Te usługi zrewolucjonizowały rynek IT, dając firmom możliwość korzystania z zaawansowanej infrastruktury bez konieczności inwestowania w sprzęt i jego utrzymanie. Do 2010 r. AWS stało się liderem na rynku chmury obliczeniowej, obsługując klientów z różnych branż. Jednym z kluczowych elementów strategii AWS była globalna ekspansja. Firma zaczęła budować centra danych w różnych regionach świata, aby zapewnić niskie opóźnienia, wysoką dostępność i spełnić lokalne wymagania regulacyjne dotyczące przechowywania danych. AWS wprowadziło koncepcję regionów i stref dostępności, umożliwiając klientom wybór lokalizacji zasobów w zależności od potrzeb[9].

W 2011 r. AWS wprowadziło AWS Marketplace, platformę, która umożliwiła firmom sprzedaż i zakup oprogramowania oraz aplikacji działających w chmurze. Rok później, w 2012 r., zaprezentowano Amazon Glacier, usługę przeznaczoną do archiwizacji dużych ilości danych niskim kosztem. W 2014 r. AWS zrewolucjonizowało rynek baz danych, wprowadzając Amazon Aurora, relacyjny silnik baz danych, oferujący wydajność porównywalną z komercyjnymi systemami. Bezpieczeństwo w AWS jest jednym z kluczowych elementów platformy, zapewniającym ochronę

[6] EY Polska, *Co to jest chmura obliczeniowa? Definicja, przykłady, zalety;* https://www.ey.com/pl_pl/insights/digital-first/co-to-jest-chmura-obliczeniowa (dostęp 21 listopada 2024).

[7] Od tego momentu będzie używany skrót tej nazwy AWS.

[8] Od tego momentu będzie używany skrót tej nazwy Amazon EC2.

[9] Amazon Web Services, About AWS, https://aws.amazon.com/about-aws/ (dostęp: 24.11.2024).

danych, aplikacji i infrastruktury. Platforma wdraża wielopoziomowe mechanizmy bezpieczeństwa, które obejmują zarówno aspekty fizyczne, jak i wirtualne, tworząc kompleksowe środowisko chroniące przed zagrożeniami. Fizyczne bezpieczeństwo centrów danych AWS to pierwszy poziom ochrony. Centra są zabezpieczone za pomocą zaawansowanych systemów monitoring, wieloczynnikowych systemów kontroli dostępu oraz całodobowej obecności wykwalifikowanego personelu ochrony. Dane centra są zlokalizowane w niskiego ryzyka obszarach sejsmicznych i zalewowych, a niezbędne systemy zasilania i chłodzenia zapewniają ciągłość działania. Na poziomie wirtualnym AWS zapewnia izolację danych między klientami, wysoką dostępność usług oraz zaawansowane metody szyfrowania danych zarówno w spoczynku, jak i w ruchu. Klienci mogą też korzystać z usługi AWS Key Management Service[10] do zarządzania własnymi kluczami szyfrującymi, z wykorzystaniem modułów bezpieczeństwa sprzętowego. AWS Identity and Access Management[11] umożliwia precyzyjne zarządzanie dostępem, obsługuje także uwierzytelnianie wieloskładnikowe i pozwala na zarządzanie dostępem na podstawie zasad opartych na tożsamości użytkownika, zasobach oraz działaniach. Monitoring i audyt są realizowane przez usługi, takie jak AWS CloudTrail i Amazon CloudWatch. AWS CloudTrail zapisuje wszystkie operacje API[12], interfejsu programowania aplikacji, umożliwiając szczegółową analizę działań oraz identyfikowanie potencjalnych zagrożeń. Z kolei Amazon CloudWatch monitoruje wydajność i stan zasobów w czasie rzeczywistym, pozwalając na definiowanie alarmów i automatyczne reakcje na problemy. Platforma spełnia wymagania wielu standardów, takich jak: ISO 27001, PCI DSS, SOC 1/2/3, HIPAA oraz FIPS 140-2. Klienci mogą korzystać z informacji dostępnych w raportach i certyfikatach AWS, aby zapewnić zgodność własnych aplikacji z przepisami prawnymi i branżowymi. Sieciowa izolacja jest realizowana przez Amazon Virtual Private Cloud[13], umożliwiający tworzenie prywatnych środowisk z kontrolą dostępu, trasowaniem i integracją z lokalną infrastrukturą za pomocą szyfrowanych połączeń VPN lub dedykowanych połączeń AWS Direct Connect. Narzędzia, takie jak AWS Config i Trusted Advisor, wspierają automatyzację i bezpieczeństwo, oferując monitoring konfiguracji oraz rekomendacje. W przypadku ochrony danych platforma stosuje szyfrowanie oparte na standardach branżowych, takich jak Advance Encryption Standard – 256[14], którego klucze szyfrowania i deszyfrowania są takie same, oraz umożliwia klientom korzystanie z dedykowanych modułów bezpieczeństwa. Dane są bezpiecznie przechowywane w wielu lokalizacjach, co minimalizuje ryzyko ich utraty. Praktykowana jest również stała inwestycja w rozwój systemów bezpieczeństwa, przy współpracy z najlepszymi ekspertami oraz wdrażanie najnowszych technologii. Dzięki temu klienci mogą budować swoje aplikacje w środowisku, które jest zarówno elastyczne, jak i wysoce bezpieczne, spełniając oczekiwania najbardziej wymagających sektorów, takich jak: finanse, opieka zdrowotna czy

[10] Od tego momentu będzie używany skrót KMS.

[11] Od tego momentu będzie używany skrót tej nazwy IAM.

[12] Application Programming Interface.

[13] Od tego momentu będzie używany skrót tej nazwy VPC.

[14] Od tego momentu będzie używany skrót AES-256.

administracja publiczna. Usługi obliczeniowe obejmują przede wszystkim Amazon EC2, który dostarcza skalowalne jednostki obliczeniowe w chmurze, umożliwiając elastyczne uruchamianie aplikacji. AWS Lambda pozwala na wykonywanie kodu w odpowiedzi na zdarzenia bez potrzeby zarządzania infrastrukturą. Amazon Elastic Beanstalk to usługa ułatwiająca wdrażanie i zarządzanie aplikacjami, a Auto Scaling oraz Elastic Load Balancing automatycznie dostosowują zasoby do zmieniających się potrzeb. Przechowywanie danych jest realizowane przez usługi, takie jak Amazon S3, oferujący bezpieczne i skalowalne przechowywanie obiektów, oraz Amazon Elastic Block Store, który dostarcza wydajną pamięć blokową instancji EC2. Amazon Glacier zapewnia niskokosztowe archiwizowanie danych, a AWS Storage Gateway umożliwia integrację lokalnych systemów z chmurą. Bazy danych to kluczowy obszar AWS, obejmujący Amazon RDS, który zarządza relacyjnymi bazami danych, oraz Amazon DynamoDB, elastyczną bazę NoSQL zoptymalizowaną pod kątem niskich opóźnień i wysokiej dostępności. Amazon Aurora to relacyjny silnik baz danych, kompatybilny z MySQL i PostgreSQL, oferujący wydajność porównywalną z komercyjnymi rozwiązaniami. Amazon Redshift dostarcza hurtownię danych do analizy na dużą skalę, a Amazon ElastiCache wspiera aplikacje przez szybkie przetwarzanie w pamięci podręcznej. Analizy i big data wspierane są przez Amazon EMR, który wykorzystuje Hadoop do przetwarzania dużych zbiorów danych, oraz Amazon Kinesis, umożliwiający przetwarzanie strumieni danych w czasie rzeczywistym. AWS Data Pipeline automatyzuje proces przesyłania i przetwarzania danych między różnymi usługami i środowiskami. Sieci w AWS obejmują Amazon VPC, który pozwala na tworzenie prywatnych sieci w chmurze, oraz Amazon Route 53, skalowalny system Damain Name System, wspierający routing użytkowników do odpowiednich zasobów. AWS Direct Connect umożliwia ustanawianie dedykowanych połączeń sieciowych między infrastrukturą lokalną a chmurą AWS, co zwiększa przepustowość i redukuje opóźnienia. Aplikacje mobilne wspierane są przez Amazon Simple Notification Service, który umożliwia wysyłanie powiadomień *push* na różne urządzenia, oraz Amazon Cognito, ułatwiający zarządzanie danymi użytkowników. Amazon Mobile Analytics pozwala na szybkie analizowanie danych aplikacji mobilnych. Zarządzanie i wdrażanie usług w AWS jest uproszczone dzięki AWS CloudFormation, które automatyzuje tworzenie i zarządzanie zasobami w chmurze, oraz AWS OpsWorks, służącemu do zarządzania aplikacjami. AWS CodeDeploy, CodeCommit i CodePipeline wspierają procesy CI/CD, umożliwiając szybkie i niezawodne wdrażanie nowych wersji aplikacji. Bezpieczeństwo w AWS jest zapewniane przez takie usługi jak AWS IAM, pozwalający na kontrolowanie dostępu użytkowników oraz AWS KMS, zarządzający kluczami szyfrowania. AWS CloudTrail rejestruje wszystkie operacje API, a Amazon CloudWatch monitoruje zasoby i wydajność aplikacji, dostarczając alarmy w czasie rzeczywistym. Oferowane są także usługi specyficzne przedsiębiorstwom, takim jak Amazon WorkSpaces, które umożliwiają uruchamianie wirtualnych biurek w chmurze, oraz Amazon Zocalo, wspierający współdzielenie i przechowywanie plików w sposób bezpieczny i efektywny[15].

[15] Por. S. Mathew, AWS Overview, listopad 2014, https://www.sysfore.com/Assets/PDF/aws-overview.pdf (dostęp: 24.11.2024).

Kolejną znaną platformą oferującą usługi chmurowe jest OneDrive. W odróżnieniu od usług AWS, które oferują rozwiązania chmurowe głównie firmom i deweloperom, OneDrive jest usługą konsumencką, skierowaną w szczególności do użytkowników indywidualnych. Jako usługa chmurowa od Microsoftu, oferuje zaawansowane mechanizmy ochrony danych, obejmujące szyfrowanie, kontrolę dostępu, refundację danych oraz monitorowanie aktywności. Jednym z najważniejszych elementów zabezpieczeń OneDrive jest szyfrowanie danych. Pliki przesyłane do chmury są chronione za pomocą protokołu Transport Layer Security[16], co zapobiega ich przechwyceniu w trakcie przesyłania. Dodatkowo, pliki przechowywane na serwerach są szyfrowane za pomocą standardów AES-256, co zapewnia wysoki poziom ochrony przed nieautoryzowanym odczytem. Pliki są dzielone na mniejsze fragmenty, które są indywidualnie szyfrowane. W zakresie ochrony przed nieautoryzowanym dostępem, OneDrive stosuje uwierzytelnianie dwuskładnikowe[17] oraz zarządzanie tożsamościami, co pozwala administratorom na dostosowanie poziomów dostępu do danych. Dodatkowo, użytkownicy indywidualni mogą korzystać z osobistego sejfu, który wymaga dodatkowego uwierzytelnienia przy każdym dostępie. OneDrive wdraża środki ochrony danych przed utratą, takie jak rozproszenie danych, czyli przechowywanie kopii zapasowych w różnych lokalizacjach. Zapewnia to dostępność danych nawet w przypadku awarii serwerów. W ramach ochrony przed zagrożeniami, takimi jak *ransomware*[18], OneDrive umożliwia przywrócenie wcześniejszych wersji plików oraz całych bibliotek danych. Dodatkowo funkcja wykrywania zagrożeń ransomware automatycznie ostrzega użytkowników w przypadku podejrzenia ataku i prowadzi ich przez proces odzyskiwania plików. Microsoft stosuje również ciągłe monitorowania,analizy danych i sztucznej inteligencji do szybkiego wykrywania podejrzanej aktywności. Zespół ekspertów ds. bezpieczeństwa stale monitoruje środowisko OneDrive. Microsoft przestrzega rygorystycznych standardów zgodności, takich jak Rodo, ISO/IEC 27001 oraz HIPAA, zapewniając użytkownikom pełną kontrolę nad danymi i transparentność w zakresie ich przechowywania i przetwarzania. informacji zdrowotnych pacjentów. Firma zapewnia użytkownikom pełną kontrolę nad ich danymi oraz transparentność w zakresie tego, jak dane są przechowywane i przetwarzane[19].

Przykładem innej znanej platformy jest Google Drive. To popularna usługa chmurowa uruchomiona 24 kwietnia 2012 r. przez Google. Opiera się na wcześniejszych rozwiązaniach Google, takich jak Google Docs, i pozwala użytkownikom na przechowywanie, udostępnianie oraz synchronizowanie plików między urządzeniami. Użytkownicy mogą korzystać z 15 GB darmowej przestrzeni, którą można rozszerzyć poprzez płatne plany. Google Drive obsługuje różnorodne formaty plików

[16] Od teraz będzie używany skrót tej nazwy TSL

[17] Od teraz będzie używany skrót tej nazwy 2FA (ang. Two Factor Authentication)

[18] Ransomware to rodzaj złośliwego oprogramowania, które blokuje dostęp do systemu lub szyfruje pliki i żąda okupu w zamian za przywrócenie dostępu.

[19] Por. Microsoft Support, How OneDrive Safeguards Your Data in the Cloud, https://support.microsoft.com/en-us/office/how-onedrive-safeguards-your-data-in-the-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1 (dostęp: 20.11.2024).

i integruje się z ekosystemem Google, w tym z Gmail i aplikacjami Google Workspace. Został stworzony jako platforma umożliwiająca dostępne i efektywne przechowywanie oraz edytowanie plików. Początkowo, usługa oferowała funkcje edycji dokumentów w czasie rzeczywistym poprzez Google Docs, a z czasem rozwinięto ją o zaawansowane opcje synchronizacji. Dodano również możliwość edycji offline, co zwiększyło jej użyteczność. Działa on na bazie infrastruktury chmurowej, umożliwiając przechowywanie i pobieranie plików za pośrednictwem Internetu. Pliki można przesyłać ze swoich urządzeń lub tworzyć je bezpośrednio w aplikacjach: takich jak Google Docs, Sheets czy Slides. Pliki są przechowywane na serwerach Google i dostępne z przeglądarek internetowych, aplikacji desktopowych oraz mobilnych. Zmiany w dokumentach są zapisywane automatycznie w chmurze, a funkcja synchronizacji zapewnia dostępność najnowszych wersji plików na wszystkich urządzeniach. Dzięki współdzieleniu plików i folderów Google Drive wspiera pracę zespołową w czasie rzeczywistym. Firmy i administracje publiczne korzystają z Google Drive jako platformy do bezpiecznego udostępniania dokumentów i usprawniania procesów pracy, eliminując konieczność utrzymywania kosztownych serwerów. Dla użytkowników indywidualnych stanowi niezastąpione narzędzie do tworzenia kopii zapasowych zdjęć, dokumentów i innych plików, zapewniając ich bezpieczeństwo i dostępność. Integracja z Google Photos pozwala na wygodne zarządzanie multimediami, co jest szczególnie cenione przez osoby przechowujące duże kolekcje zdjęć i filmów. Google Drive zapewnia wysoki poziom bezpieczeństwa danych dzięki zastosowaniu zaawansowanych rozwiązań technicznych i organizacyjnych. Dane przesyłane do i z platformy są szyfrowane przy użyciu protokołu TLS, co chroni je przed przechwyceniem. Pliki przechowywane na serwerach Google są zabezpieczone szyfrowaniem AES – 256, które jest powszechnie uznawane za jedno z najbezpieczniejszych rozwiązań. Oferuje także mechanizmy kontroli dostępu, które umożliwiają użytkownikom precyzyjne zarządzanie tym, kto może przeglądać, edytować lub udostępniać ich pliki. Udostępnianie może być ograniczone tylko do wybranych osób, a dodatkowo użytkownicy mogą decydować, czy odbiorcy mają możliwość edycji plików, czy jedynie ich przeglądania. Funkcja ta pozwala zminimalizować ryzyko nieautoryzowanego dostępu do wrażliwych danych. Dodatkowym zabezpieczeniem jest system wykrywania zagrożeń i ochrony przed złośliwym oprogramowaniem. Mechanizmy oparte na sztucznej inteligencji analizują przesyłane pliki, identyfikując wirusy i inne potencjalne zagrożenia jeszcze przed ich pobraniem. W przypadku podejrzanych plików użytkownik otrzymuje ostrzeżenie. Prywatność użytkowników jest jednym z kluczowych priorytetów Google. Dane przechowywane nie są wykorzystywane do celów reklamowych bez wyraźnej zgody użytkownika, a dostęp mają jedynie uprawnione osoby. Google przestrzega rygorystycznych przepisów dotyczących ochrony danych, takich jak europejskie RODO czy kalifornijskie CCPA, co daje użytkownikom pewność, że ich dane są odpowiednio zabezpieczone. Dodatkowe bezpieczeństwo zapewnia także 2FA, co znacznie utrudnia potencjalnym atakującym dostęp do konta użytkownika. Proces ten wymaga podania dodatkowego kodu weryfikacyjnego przy logowaniu, który może być generowany przez aplikację lub wysyłany na telefon. Ważnym aspektem jest także

odporność na awarie. Google Drive korzysta z rozproszonych centrów danych, co minimalizuje ryzyko utraty danych w przypadku awarii jednego z nich. Dodatkowo, platforma regularnie wykonuje kopie zapasowe danych, co zapewnia ich dostępność nawet w sytuacjach kryzysowych[20].

Przykładem konkurencyjnej platformy do Google Drive platformy jest iCloud. Jest to zintegrowana z ekosystemem urządzeń Apple, pozwala na wygodne przechowywanie, synchronizację i zarządzenie danymi na iPhone'ach, iPadach, Macach, komputerach z systemem Windows oraz w przeglądarkach internetowych. Działa w tle, automatycznie synchronizując dane, dzięki czemu użytkownik ma dostęp do plików, zdjęć i dokumentów z każdego urządzenia. ICloudDrive umożliwia tworzenie folderów, organizowanie plików i ich udostępnianie. Synchronizacja odbywa się automatycznie, co zapewnia wygodny dostęp z dowolnego miejsca. Funkcja Zdjęcia iCloud służy do przechowywania zdjęć i filmów w pełnej jakości, optymalizując przy tym miejsce na urządzeniach. Dodatkowo usługa optymalizuje miejsce na dysku urządzeń, przechowując lżejsze wersje zdjęć lokalnie, a oryginały w chmurze. Kopia zapasowa iCloud regularnie tworzy automatyczne kopie zapasowe danych, takich jak: kontakty, wiadomości, aplikacje, ustawienia czy historia przeglądania, co ułatwia odtwarzanie zawartości w przypadku utraty urządzenia lub przeniesienia na nowe. Funkcja ta działa w tle i nie wymaga dodatkowej konfiguracji. Znajdź mój[21] to narzędzie lokalizacyjne, które umożliwia śledzenie zgubionych lub skradzionych urządzeń Apple, ich blokowanie, odtwarzanie dźwięku lub wyświetlanie wiadomości na ekranie. Funkcja ta pozwala także na śledzenie lokalizacji swoich bliskich. Usługa Rodzinna Chmura umożliwia dzielenie się zakupami z App Store, iTunes i Apple Books, subskrypcjami, np. Apple Music, Apple TV+ czy iCloud+ oraz przestrzenią dyskową w ramach jednej grupy rodzinnej. Użytkownicy mogą również ustawić kontrolę rodzicielską i ograniczenia iCloud+ to rozszerzona wersja usługi, która oferuje dodatkowe funkcje, takie jak Private Relay, zapewniający większą prywatność podczas przeglądania Internetu. Ukryj mój e-mail, pozwalający tworzyć tymczasowe adresy e-mail w celu ochrony prywatności oraz wsparcie dla HomeKit Secure Video, umożliwiające zapis wideo z kamer w chmurze. iCloud+ oferuje także większą przestrzeń dyskową: 50 GB, 200 GB lub 2 TB.Integracja z aplikacjami Apple, takimi jak: Pages, Numbers i Keynote, pozwala na współpracę w czasie rzeczywistym, przechowywanie projektów w chmurze i udostępnianie ich innym użytkownikom. iCloud obsługuje również aplikacje innych firm, co zwiększa jego uniwersalność[22].

Apple oferuje dwie opcje ochrony danych przechowywanych w iCloud. Pierwszą z nich jest standardowa ochrona danych. Jest to domyślne ustawienie dla wszystkich kont. Dane są szyfrowane podczas przesyłania oraz w stanie spoczynku na serwerach Apple. Klucze szyfrowania są przechowywane w centrach danych Apple, co umożliwia firmie pomoc w odzyskiwaniu danych w sytuacjach awaryjnych, takich jak zapomniane hasło. Należy jednak zauważyć, że tylko niektóre kategorie danych,

[20] Por. Google Support, About Google Drive, https://support.google.com/drive/answer/10375054?hl=en (dostęp: 24.11.2024).

[21] Ang. Find My.

[22] Por. Apple, iCloud Overview, https://www.apple.com/icloud/ (dostęp: 24.11.2024).

takie jak aplikacja Zdrowie czy hasła w Pęku kluczy iCloud, są chronione szyfrowaniem end-to-end, co oznacza, że tylko użytkownik ma do nich dostęp. Drugą opcją jest zaawansowana ochrona danych. Jest to opcjonalne ustawienie dostępne od wersji iOS 16.2, iPadOS 16.2 oraz macOS 13.1. Po jej włączeniu większość danych w iCloud jest chroniona szyfrowaniem end-to-end, w tym kopie zapasowe, zdjęcia, notatki i inne. W tym trybie klucze szyfrowania są przechowywane wyłącznie na zaufanych urządzeniach użytkownika, co oznacza, że nawet Apple nie ma dostępu do tych danych. W przypadku ich utraty, odnalezienie jest możliwe tylko za pomocą kodu urządzenia, hasła, kontaktu lub klucza odzyskiwania[23].

Technologie chmurowe odgrywają kluczową rolę w nowoczesnym zarządzaniu danymi i infrastrukturą IT, oferując organizacjom elastyczność, skalowalność oraz możliwość optymalizacji kosztów. W zależności od potrzeb, firmy mogą korzystać z różnych modeli chmury, takich jak: chmura publiczna, prywatna czy hybrydowa, z których każda ma swoje unikatowe zalety i ograniczenia. Chmura publiczna to usługa dostarczana przez zewnętrznych dostawców, takich jak: Amazon Web Services, Google, Cloud czy Microsoft Azure. Usługi te są hostowane poza infrastrukturą użytkownika, a dostęp do nich odbywa się za pośrednictwem Internetu. Zasoby w chmurze publicznej są współdzielone przez wielu użytkowników, co pozwala na redukcję kosztów. Dostawca jest odpowiedzialny za utrzymanie, bezpieczeństwo i zarządzanie infrastrukturą. Charakteryzuje się ona elastycznością i skalowalnością. Organizacje mogą płacić tylko za te zasoby, które faktycznie wykorzystują, co pozwala na znaczne oszczędności w porównaniu z tradycyjnymi centrami danych. Warto jednak zwrócić uwagę na pewne ograniczenia, takie jak mniejsza kontrola nad danymi i infrastrukturą oraz potencjalne obawy dotyczące bezpieczeństwa, zwłaszcza w przypadku przechowywania wrażliwych danych. Zaletą tego rozwiązania jest przede wszystkim niski koszt początkowy i model rozliczeniowy pay-as-you-go, dzięki któremu koszty usług naliczane są dopiero po jej wykonaniu. Chmury publiczne są również wyjątkowo skalowalne – pozwalają na szybkie zwiększenie lub zmniejszenie dostępnych zasobów w zależności od potrzeb. Dodatkowo dostawcy chmur publicznych zapewniają automatyczne aktualizacje i zarządzanie infrastrukturą, co zmniejsza obciążenie działów IT. Wadą natomiast jest ograniczona kontrola nad danymi i infrastrukturą. Organizacje muszą polegać na dostawcy usług w zakresie bezpieczeństwa i ochrony danych, co może budzić obawy, zwłaszcza w przypadku przechowywania danych wrażliwych. Dodatkowo wydajność może być uzależniona od jakości połączenia internetowego, a brak pełnego dostosowania infrastruktury do specyficznych potrzeb firmy może stanowić wyzwanie dla organizacji o unikatowych wymaganiach. Kolejnym rozwiązaniem jest chmura prywatna. Rozwiązanie to jest dedykowane konkretnej organizacji, które może być hostowane wewnętrznie lub zlecane na zewnątrz. W tym modelu zasoby są przeznaczone wyłącznie jednej firmie, co daje większą kontrolę nad danymi i infrastrukturą. Często stosowane są przez organizacje o wysokich wymaganiach dotyczących bezpieczeństwa i zgodności z regulacjami, na przykład w sektorach finansowym czy medycznym.

[23] Por. Apple Support, Security and Privacy of Apple iCloud, 16 września 2024, https://support.apple.com/en-us/102651 (dostęp: 24.11.2024).

Budowa chmury prywatnej wymaga większych nakładów inwestycyjnych, ponieważ organizacja musi zainwestować w sprzęt, oprogramowanie i zasoby ludzkie. Jednak pozwala to na lepsze dostosowanie infrastruktury do specyficznych potrzeb oraz zapewnienie większej wydajności dzięki lokalnemu zarządzaniu zasobami. Oferuje większą kontrolę i bezpieczeństwo, ponieważ zasoby są dedykowane wyłącznie jednej organizacji. Dzięki temu firmy mogą lepiej dostosować infrastrukturę do swoich potrzeb, zachować zgodność z regulacjami oraz utrzymać pełną kontrolę nad danymi. Chmura prywatna zapewnia także wyższą wydajność, ponieważ działa w ramach infrastruktury wewnętrznej lub w dedykowanym centrum danych. To idealne rozwiązanie dla organizacji o wysokich wymaganiach dotyczących bezpieczeństwa, takich jak: banki, instytucje rządowe czy firmy z sektora medycznego. Wadą jej są wyższe koszty początkowe i operacyjne. Model ten jest mniej elastyczny w porównaniu z chmurą publiczną, jeśli chodzi o szybkie skalowanie zasobów w sytuacjach nagłego wzrostu zapotrzebowania. Ostatnim rozwiązaniem jest chmura hybrydowa, która łączy zalety obu poprzednich modeli. Dzięki swojej skalowalności, umożliwia organizacjom łatwe dostosowywanie infrastruktury do rosnącego zapotrzebowania na zasoby. Jednak zarządzanie tym modelem wymaga synchronizacji różnych środowisk, co wiąże się z koniecznością zastosowania zaawansowanych narzędzi[24].

W zrozumieniu powyższych modeli, istotna jest wiedza na temat ich budowy. Architektura chmurowa składa się z dwóch głównych komponentów: front-endu i back-endu, które współpracują ze sobą, by dostarczać użytkownikowi końcowemu usługi w modelu chmurowym. Front-end to część widoczna przez użytkownika, obejmująca interfejsy użytkownika oraz aplikacje niezbędne do dostępu do usług chmurowych. Jest to środowisko, w którym użytkownicy wchodzą w interakcje z usługami chmury, korzystając z przeglądarek internetowych, aplikacji mobilnych lub innych narzędzi. Z kolei back-end to zaplecze technologiczne chmury, które zarządza całym ekosystemem obliczeniowym. W jego skład wchodzą serwery, systemy pamięci masowej, bazy danych, sieci oraz oprogramowanie do zarządzania. Kluczowym elementem back-endu jest oprogramowanie pośredniczące, zwane middleware, które odpowiada za alokację zasobów, zarządzanie dostępem oraz zapewnienie odpowiedniego środowiska do uruchamiania aplikacji. Middleware umożliwia efektywne wykorzystanie zasobów i zapewnia ich dynamiczne skalowanie w zależności od potrzeb użytkowników. Architektura chmury obejmuje różne modele usług, które dostosowują się do potrzeb użytkowników i organizacji. Pierwszym z nich jest SaaS (Software as a Service), który umożliwia dostęp do oprogramowania za pośrednictwem przeglądarek internetowych bez konieczności instalowania go na lokalnych urządzeniach. Przykładami takich usług są Google Apps czy Salesforce. Model ten charakteryzuje się brakiem konieczności zarządzania infrastrukturą przez użytkownika końcowego, automatycznymi aktualizacjami oraz elastycznością w dostosowywaniu zasobów do bieżących potrzeb. Kolejnym modelem jest Platform as a Service[25], który dostarcza

[24] Por. M. Amini, N.S. Safavi, S.M. Dashti Khavidaki, A. Abdollahzadegan, *Type of Cloud Computing Public and Private That Transform The Organization More Effectively*, https://shorturl.at/wdDYT (dostęp: 19.11.2024).

[25] Od tego momentu będzie używany skrót tej nazwy PaaS.

platformę do tworzenia, testowania i wdrażania aplikacji, eliminując potrzebę zarządzania bazową infrastrukturą sprzętową i systemową. Platformy. takie jak Google App Engine czy Microsoft Azure, pozwalają na szybki rozwój aplikacji dzięki gotowym narzędziom, które wspierają procesy programistyczne. Ostatnim modelem jest Infrastructure as a Service[26], który oferuje podstawowe zasoby chmurowe, takie jak: moc obliczeniowa, pamięć i sieci, dostępne na żądanie. Użytkownicy mają pełną kontrolę nad konfiguracją wirtualnych maszyn i infrastrukturą, co zapewnia dużą elastyczność w dostosowywaniu środowiska do wymagań projektów. Przykładami usług tego typu są Amazon EC2 i RackSpace. Połączenie front-endu i back-endu jest realizowane za pomocą sieci, najczęściej Internetu, co umożliwia komunikację między komponentami. Architektura chmurowa zapewnia również pięć podstawowych cech zdefiniowanych przez NIST: samodzielną obsługę na żądanie, szeroki dostęp sieciowy, wspólne zasoby, szybkie skalowanie oraz usługi mierzone, co czyni ją elastycznym i efektywnym modelem dostarczania zasobów i aplikacji[27].

Przedstawiono podstawowe zagadnienia dotyczące chmury, jej genezy, ewolucji oraz cechy. Przybliżono historyczne tło rozwoju chmury obliczeniowej, od pierwszych koncepcji współdzielenia zasobów w latach 60. XX w. po przełomowe zmiany wprowadzone przez Amazon Web Services w 2006 r. Dokonano analizy różnych modeli chmur, takich jak publiczne, prywatne i hybrydowe, pod kątem ich zastosowań w różnych sektorach. Zwrócono uwagę na brak jednolitej definicji chmury obliczeniowej ze strony prawnej oraz omówiono kluczowych dostawców usług chmurowych, takich jak: AWS, Microsoft OneDrive, Google Drive i Apple iCloud. Przedstawiono również różnice w ich podejściu do bezpieczeństwa i zarządzania danymi, co pozwoli w dalszej części pracy na dokładniejszą analizę rozwiązań proponowanych przez dane firmy.

2. REGULACJE PRAWNE CHMURY OBLICZENIOWEJ

Rozporządzenie ogólne o ochronie danych osobowych, obowiązujące od 2018 r., stanowi kluczowy element ochrony prywatności w Unii Europejskiej. Natomiast rozwój chmur obliczeniowych, które umożliwiają przechowywanie i przetwarzanie danych na globalną skalę, wprowadził nowe wyzwania w zakresie zgodności z tym rozporządzeniem. Chmury obliczeniowe oferują wiele korzyści, takich jak: elastyczność, skalowalność i redukcja kosztów, ale jednocześnie stwarzają złożone problemy związane z transgranicznym przepływem d anych, współdzieloną odpowiedzialnością oraz konfliktami jurysdykcyjnymi. Aby zapewnić bezpieczeństwo w chmurze przy jednoczesnym przestrzeganiu przepisów RODO, organizacje muszą podejmować szereg działań oraz wdrażać skuteczne strategie zarządzania danymi. RODO wprowadza rygorystyczne wymagania dotyczące ochrony danych osobowych,

[26] Od tego momentu będzie używany skrót tej nazwy IaaS.

[27] Por. B.K. Rani, B.P. Rani, A.V. Babu, *Cloud Computing and Inter-Clouds – Types*, Topologies and Research Issues., 8 maja 2015, https://www.sciencedirect.com/science/article/pii/S1877050915005074 (dostęp: 24.11.2024).

które mają na celu zabezpieczenie prywatności użytkowników oraz zwiększenie odpowiedzialności firm za przetwarzanie danych. Niezastosowanie się do przepisów może prowadzić do poważnych konsekwencji, takich jak: wysokie kary finansowe, utratę zaufania klientów czy uszczerbku na reputacji. Niniejszy rozdział analizuje te kwestie, skupiając się na ryzykach związanych z lokalizacją danych, wymogach bezpieczeństwa w architekturze chmur oraz podziale odpowiedzialności prawnej, a także przedstawia rekomendacje i perspektywy na przyszłość. Wprowadza to kontekst prawny i ryzyka związane z naruszeniami danych w chmurze, które są przedmiotem analizy wybranych incydentów opisanych w pracy.

Jednym z największych wyzwań związanych z wykorzystaniem chmur obliczeniowych w kontekście RODO jest kwestia lokalizacji danych. Zgodnie z art. 3 RODO, przepisy mają zastosowanie do przetwarzania danych obywateli UE, niezależnie od tego, gdzie znajduje się siedziba dostawcy usług. W praktyce oznacza to, że firmy korzystające z globalnych dostawców chmur, takich jak: Amazon Web Services czy Microsoft Azure, muszą zapewnić, że dane nie opuszczają Europejskiego Obszaru Gospodarczego[28] bez odpowiednich gwarancji. Problem polega na tym, że infrastruktura chmurowa często opiera się na serwerach rozsianych po całym świecie, co utrudnia kontrolę nad fizyczną lokalizacją danych. Przykładem są centra danych w Stanach Zjednoczonych, gdzie obowiązuje CLOUD Act, umożliwiający organom ścigania dostęp do danych przechowywanych przez amerykańskie firmy, nawet jeśli znajdują się poza USA. Anonimizacja danych, kluczowa dla zasady minimalizacji, opisanej w art. 5 RODO, staje się szczególnie problematyczna w środowisku chmurowym. Tradycyjne metody, takie jak usuwanie imion czy numerów PESEL, są niewystarczające w kontekście zaawansowanych technik łączenia zbiorów danych. Algorytmy uczenia maszynowego mogą zidentyfikować osoby na podstawie pozornie anonimowych metadanych, takich jak wzorce korzystania z aplikacji. Rozwiązaniem może być pseudonimizacja dynamiczna, gdzie klucze deszyfrujące są przechowywane lokalnie, a nie w chmurze, co ogranicza ryzyko reidentyfikacji. W odpowiedzi na te wyzwania, niektórzy europejscy dostawcy, jak Deutsche Telekom, rozwijają „suwerenne chmury", które gwarantują przechowywanie danych wyłącznie w EOG. Model ten łączy zalety chmury publicznej z kontrolą charakterystyczną rozwiązaniom oprogramowaniom lokalnym, ale generuje wyższe koszty i ogranicza skalowalność[29].

W art. 32 RODO nałożony jest obowiązek wdrożenia „odpowiednich środków bezpieczeństwa", jednak w chmurze odpowiedzialność dzieli się między dostawcę a klienta. W modelu współdzielonej odpowiedzialności, dostawca chmury odpowiada za bezpieczeństwo fizyczne serwerów, podczas, gdy klient musi samodzielnie konfigurować firewalle, zarządzać dostępem i szyfrować dane. Błędy po stronie klientów usług chmurowych stanowią jedną z najczęstszych przyczyn naruszeń bezpieczeństwa. W 2022 r. aż 73% incydentów dotyczących chmur publicznych było spowodowanych niewłaściwą konfiguracją zasobów, na przykład przez

[28] Od teraz będzie używany skrót EOG.

[29] Por. M.E. Cambronero, M.A. Martínez, L. Llana, R.J. Rodríguez, A. Russo, dostępne na: https://pmc.ncbi.nlm.nih.gov/articles/PMC11041943/ (dostęp: 7.01.2025).

pozostawienie baz danych MongoDB otwartych i dostępnych publicznie, co umożliwiało nieautoryzowany dostęp do wrażliwych informacji. Aby spełnić wymogi RODO, kluczowe jest wdrożenie szyfrowania danych zarówno w spoczynku, jak i podczas transmisji. Szyfrowanie w bezruchu może być realizowane za pomocą narzędzi, takich jak AWS KMS, gdy szyfrowanie podczas transmisji wymaga stosowania protokołów, takich jak TLS 1.3. Dodatkowo, polityka zero trust, gdzie każda próba dostępu jest weryfikowana nawet wewnątrz sieci, może znacząco zmniejszyć ryzyko naruszeń. Przykładem jest szpital w Finlandii, który po wdrożeniu tej polityki zmniejszył liczbę incydentów o 40%. Automatyzacja narzędzi do monitorowania, takich jak Azure Security Center, pozwala na wykrywanie anomalii w czasie rzeczywistym, np. nieautoryzowane kopiowanie dużych zbiorów danych. Przedsiębiorstwa korzystające z wielu chmur, np. AWS i Google Cloud, muszą dostosować audyty do specyfiki każdej platformy, w czym mogą pomóc narzędzia, takie jak CloudHealth czy Prisma Cloud, które umożliwiają zbieranie i analizowanie danych z różnych środowisk chmurowych oraz automatyczne generowanie raportów zgodności z przepisami, takimi jak RODO. Wymaga ono także odpowiedzialności za cały cykl życia danych, od momentu ich zbierania aż po ich usunięcie. W chmurze oznacza to zapewnienie możliwości trwałego usunięcia danych na żądanie użytkownika oraz dokładne śledzenie, gdzie dane są przechowywane i przetwarzane. Przedsiębiorstwa muszą także zadbać o procedury związane z wykrywaniem, zgłaszaniem i zarządzaniem naruszeniami ochrony danych w określonych ramach czasowych[30].

Kluczowym elementem zgodności z RODO jest wdrożenie odpowiednich zabezpieczeń technicznych i organizacyjnych. W kontekście chmury oznacza to m.in. stosowanie szyfrowania danych zarówno w trakcie ich przesyłania, jak i przechowywania. Kodowanie uniemożliwia dostęp do danych osobom nieuprawnionym, nawet w przypadku naruszenia bezpieczeństwa. Ważne jest również zarządzanie dostępem do danych przez mechanizmy kontroli tożsamości i autoryzacji, co minimalizuje ryzyko nieautoryzowanego dostępu do zasobów. Kolejnym kluczowym aspektem jest wybór dostawcy chmurowego zgodnego z RODO. Organizacje muszą dokładnie ocenić polityki bezpieczeństwa i procedury stosowane przez dostawców. Powinny sprawdzić, czy dystrybutor oferuje funkcje, takie jak audyty bezpieczeństwa, regularne testy penetracyjne, a także czy ma wdrożone mechanizmy reagowania na incydenty. Ważne jest także zawarcie umów o przetwarzaniu danych[31], które jasno określają obowiązki i odpowiedzialność obu stron w zakresie ochrony danych. Pierwszym przykładem dostawcy jest Google. Dostosował on swoje usługi i produkty do wymogów RODO, wprowadzając szereg zmian i ulepszeń w zakresie ochrony danych osobowych. Jednym z kluczowych działań było zwiększenie przejrzystości i kontroli nad danymi użytkowników. Dzięki narzędziom, takim jak Google Account, użytkownicy mogą przeglądać, eksportować, a także usuwać swoje dane w prosty i przejrzysty sposób. Kolejnym ważnym krokiem była aktualizacja polityki prywatności. Google zadbało o to, aby jego polityki były bardziej zrozumiałe i przejrzyste

[30] Por. Kanungo S. Data Privacy and Compliance Issues in Cloud Computing: Legal and Regulatory Perspectives, https://www.ijisae.org/index.php/IJISAE/article/view/5710 (dostęp: 10.02.2025).

[31] Od tego momentu będzie używany skrót DPA, Data Processing Agreements.

dla użytkowników. Firma zapewniła, że użytkownicy są informowani o tym, jakie dane są zbierane, w jaki sposób są wykorzystywane oraz jakie mają prawa w związku z tymi danymi. W zakresie bezpieczeństwa danych Google wzmocniło swoje mechanizmy ochrony, aby zapewnić, że dane osobowe są chronione przed nieautoryzowanym dostępem, utratą lub naruszeniem. Firma stosuje zaawansowane technologie szyfrowania oraz regularnie przeprowadza audyty bezpieczeństwa, aby zapewnić najwyższy poziom ochrony danych. Dodatkowo, Google zawiera z klientami umowy DPA, które precyzyjnie określają obowiązki obu stron w zakresie przetwarzania danych osobowych zgodnie z wymogami RODO. Dla administratorów danych Google oferuje specjalne narzędzia i zasoby, które pomagają w zarządzaniu zgodnością z RODO. W ramach usług Google Cloud dostępne są narzędzia do monitorowania i raportowania zgodności z przepisami, co ułatwia administratorom wypełnianie ich obowiązków. Ponadto, Google wprowadziło mechanizmy umożliwiające uzyskanie wyraźnej zgody użytkowników na przetwarzanie ich danych osobowych, zgodnie z wymogami RODO. Użytkownicy mają możliwość wyrażenia lub cofnięcia zgody w dowolnym momencie, dając im większą kontrolę nad swoimi danymi[32].

Microsoft dostosował się do wymogów ogólnego RODO przez wdrożenie kompleksowych rozwiązań organizacyjnych, technologicznych i prawnych. Firma podkreśla, że traktuje ochronę prywatności i bezpieczeństwo danych jako integralną część swoich usług zarówno w produktach dla klientów indywidualnych, jak i przedsiębiorstw. W ramach dostosowania do RODO Microsoft wprowadził mechanizmy umożliwiające przejrzyste zarządzanie danymi, w tym narzędzia do monitorowania, raportowania i usuwania informacji zgodnie z żądaniami użytkowników. Kluczowym elementem strategii Microsoft jest zapewnienie klientom kontroli nad ich danymi. Firma udostępnia funkcje umożliwiające przeglądanie, eksportowanie lub kasowanie danych osobowych. Jest to zgodne z zasadą prawa dostępu, umożliwiającego osobie wgląd w swoje dane i prawem do bycia zapomnianym, pozwalającego na ich usunięcie. Ponadto Microsoft jako procesor danych współpracuje z administratorami poprzez zawieranie umów DPA. W swoich usługach chmurowych, takich jak Azure czy Microsoft 365, firma zapewnia domyślne szyfrowanie danych, audytowanie dostępu oraz mechanizmy bezpiecznego przechowywania informacji. Microsoft oferuje szczegółową dokumentację, wskazówki prawne oraz narzędzia oceny ryzyka, np. Microsoft Compliance Manager. Platforma ta pomaga identyfikować luki w zgodności i monitorować postępy wdrażania zabezpieczeń. Firma regularnie aktualizuje swoje polityki i procedury, uwzględniając zmieniające się interpretacje przepisów oraz orzecznictwo. Dodatkowo Microsoft współpracuje z europejskimi organami nadzoru, zgłaszając incydenty naruszenia ochrony danych w wymaganym czasie i udzielając wsparcia w dochodzeniach. W zakresie transparentności Microsoft publikuje szczegółowe informacje o tym, jakie dane zbiera, w jakim celu oraz na jakiej podstawie prawnej. Użytkownicy mogą zapoznać się z tymi zasadami w Centrum Zaufania Usług Microsoft oraz w dokumentacji prawnej. Firma podkreśla również globalny charakter swoich działań, dostosowując

[32] Por. Google Cloud & the General Data Protection Regulation (GDPR), https://cloud.google.com/privacy/gdpr (dostęp: 15.01.2025).

standardy ochrony danych we wszystkich regionach, w tym poprzez mechanizmy transferu danych poza UE, na przykład klauzule umowne zatwierdzone przez Komisję Europejską[33].

Apple także dostosował swoje praktyki do wymogów RODO. Przede wszystkim firma wzmocniła przejrzystość przetwarzania danych, klarownie informując użytkowników o celach zbierania informacji, okresie ich przechowywania oraz podmiotach, z którymi są udostępniane. Wszystkie te kwestie są szczegółowo opisane w polityce prywatności, dostępnej na stronie Apple, a także w ustawieniach urządzeń i usług, gdzie użytkownicy mogą na bieżąco śledzić i modyfikować swoje preferencje. W zakresie praw osób, których dane dotyczą, Apple umożliwił użytkownikom łatwy dostęp do swoich danych, ich poprawiania, usuwania lub przenoszenia do innych dostawców usług. Narzędzie Privacy Request pozwala na złożenie wniosku o eksport danych lub usunięcie konta, co realizuje wymóg RODO dotyczący prawa do bycia zapomnianym. Dodatkowo, w aplikacjach i systemach operacyjnych, np. iOS czy macOS wprowadzono funkcję Transparentność Śledzenia Aplikacji, która wymaga od developerów uzyskania wyraźnej zgody użytkownika przed śledzeniem jego aktywności w celach reklamowych. Apple wzmocnił również bezpieczeństwo danych, stosując zaawansowane techniki szyfrowania zarówno podczas przechowywania informacji, jak i ich przesyłania. Firma ograniczyła również gromadzenie danych do niezbędnego minimum, stosując zasadę *privacy by design*, np. funkcje, takie jak Private Relay w iCloud+ ukrywają adres IP użytkownika, utrudniając tworzenie profilu na jego podstawie. W przypadku usług opartych na chmurze, Apple zapewnia, że dane użytkowników z UE są przetwarzane w centrach danych spełniających standardy RODO, nawet jeśli znajdują się poza granicami Unii. W relacjach z partnerami biznesowymi i podwykonawcami Apple wymaga podpisania DPA, które gwarantują, że podmioty trzecie przestrzegają równie restrykcyjnych zasad ochrony. Firma regularnie przeprowadza audyty zgodności, a w przypadku naruszeń danych wprowadziła procedury zgłaszania incydentów do organów nadzorczych i poszkodowanych użytkowników w ciągu 72 godzin, co jest bezpośrednią odpowiedzią na wymogi RODO[34].

Ustawa o krajowym systemie cyberbezpieczeństwa stanowi jeden z kluczowych filarów ochrony systemów informatycznych w Polsce, a jej znaczenie w kontekście chmur obliczeniowych jest szczególnie istotne. Prawo to określa podstawowe wymagania techniczne i organizacyjne, które muszą być spełnione przez podmioty świadczące usługi IT, aby zapewnić ciągłość działania systemów, ochronę danych przed nieautoryzowanym dostępem oraz skuteczną reakcję na incydenty cybernetyczne. W sektorze usług chmurowych ustawa nakłada na dostawców obowiązek wdrożenia zaawansowanych środków bezpieczeństwa, mających na celu minimalizację ryzyka utraty danych czy naruszenia poufności informacji. Wymogi te obejmują m.in. stosowanie szyfrowania przesyłanych i przechowywanych danych, wdrożenie systemów monitorowania oraz mechanizmów wczesnego wykrywania zagrożeń, a także regularne testowanie systemów informatycznych pod kątem podatności na

[33] Por. Microsoft Dostępne na: https://learn.microsoft.com/pl-pl/legal/gdpr (dostęp: 13.02.2025).

[34] Por. Apple, https://www.apple.com/pl/legal/privacy/pl/governance/ (dostęp: 6.01.2025).

ataki. Dzięki takim rozwiązaniom możliwe jest nie tylko zabezpieczenie danych przed atakami zewnętrznymi, ale również ograniczenie skutków potencjalnych incydentów. Istotnym elementem regulacji jest również obowiązek współpracy dostawców usług chmurowych z organami odpowiedzialnymi za cyberbezpieczeństwo. Wdrożenie procedur raportowania incydentów oraz udział w krajowych systemach wczesnego ostrzegania umożliwia szybkie reagowanie na zagrożenia oraz koordynację działań naprawczych na poziomie krajowym. Z perspektywy użytkowników usług chmurowych, implementacja ustawy o krajowym systemie cyberbezpieczeństwa przekłada się na wyższy poziom ochrony przechowywanych danych. Użytkownicy mogą oczekiwać, że ich dane będą zabezpieczone zgodnie z najwyższymi standardami bezpieczeństwa, co jest niezbędne w sytuacjach, gdy informacje te mają kluczowe znaczenie w funkcjonowaniu firmy czy instytucji. W przypadku wystąpienia incydentów, mechanizmy przewidziane przez ustawę umożliwiają szybką interwencję oraz podejmowanie działań naprawczych, co może obejmować również procedury odzyskiwania danych lub rekompensatę strat wynikłych z naruszeń bezpieczeństwa[35].

Dostawcy usług chmurowych są zobowiązani do wdrożenia i utrzymania kompleksowych mechanizmów ochrony systemów informatycznych, które gwarantują wysoki poziom bezpieczeństwa przetwarzanych danych. Konieczne jest stosowanie rozwiązań technicznych oraz organizacyjnych, umożliwiających ciągłe monitorowanie zagrożeń, identyfikację potencjalnego ryzyka oraz podejmowanie szybkich działań naprawczych. Wśród kluczowych wymagań znajduje się wdrożenie systemu zarządzania bezpieczeństwem informacji, który pozwala na bieżącą analizę stanu zabezpieczeń, regularne testowanie systemów oraz aktualizację procedur bezpieczeństwa. Istotnym aspektem obowiązków jest opracowanie i realizacja procedur reagowania na incydenty, co umożliwia szybkie wykrycie i skuteczne usunięcie skutków ewentualnych ataków. Systemy alarmowe, narzędzia monitorujące oraz plany awaryjne stanowią fundament działań, które pozwalają na minimalizowanie skutków zagrożeń oraz przywracanie ciągłości świadczenia usług. Równie ważna jest implementacja mechanizmów ochrony danych, takich jak szyfrowanie, kontrola dostępu i ochrona przed nieautoryzowanym wglądu. Współpraca z organami nadzorczymi oraz terminowe zgłaszanie incydentów to kolejne elementy systemu bezpieczeństwa, które wzmacniają ochronę całej infrastruktury cyfrowej. Dostawcy usług chmurowych muszą udostępniać niezbędne informacje oraz współpracować podczas audytów i kontroli, co umożliwia skuteczną analizę zagrożeń oraz wdrażanie działań naprawczych[36].

Chmury obliczeniowe zmieniły sposób przechowywania i udostępniania danych, wprowadzając nowe wyzwania w zakresie ochrony własności intelektualnej. Umieszczenie pliku na zewnętrznym serwerze, który jest częścią infrastruktury

[35] Por. K. Wiśniewska, Przechowywanie danych w chmurze w perspektywie dyrektywy w sprawie niektórych aspektów umów o dostarczenie treści cyfrowych i usług https://uokik.gov.pl/Download/554 (dostęp: 9.02.2025).

[36] Por. M. Kruk, Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa, https://repozytorium.uni.wroc.pl/Content/122487/PDF/04_Obowiazki_dostawcow_uslug_cyfrowych.pdf (dostęp: 11.02.2025).

dostawcy usług, oznacza jego zapis w postaci cyfrowej, co budzi pytania o to, czy taki zapis należy traktować jako zwielokrotnienie utworu. W praktyce operacja ta nie wymaga uzyskania zgody twórcy, o ile mieści się w granicach dozwolonego użytku, zwłaszcza gdy dotyczy celów prywatnych i nie wiąże się z działalnością komercyjną. Nowoczesne technologie skłaniają do ponownej analizy tradycyjnych koncepcji prawa autorskiego, które muszą być reinterpretowane w kontekście globalnej dystrybucji treści oraz automatycznych operacji wykonywanych przez systemy przechowywania danych. Samo przesłanie pliku do systemu chmurowego może być postrzegane jako utworzenie kopii, co w niektórych sytuacjach może kolidować z wyłącznymi prawami twórców do reprodukcji ich dzieł. Konieczne jest znalezienie równowagi między ochroną praw autorskich a swobodnym dostępem do zasobów cyfrowych, co wymaga elastycznego podejścia do interpretacji przepisów w świetle nowych możliwości technicznych. Równocześnie istotne staje się określenie granic, w których operacje wykonywane automatycznie przez systemy chmurowe mogą być uznane za dozwolony użytek, bez naruszania praw właścicieli utworów[37].

Równolegle z rozwojem usług chmurowych pojawia się kluczowe zagadnienie związane z prawną odpowiedzialnością dostawców tych usług za przechowywane w nich treści. W systemie prawnym Stanów Zjednoczonych istnieje zasada safe harbor związana z Digital Millennium Copyright Act[38], która stanowi ochronę dla dostawców usług internetowych, w tym także chmurowych, przed odpowiedzialnością za naruszenie praw autorskich przez ich użytkowników. Warunkiem tej ochrony jest ich szybka reakcja na zgłoszenia o naruszeniach, polegająca na usunięciu nielegalnych treści. Zasada ta odgrywa istotną rolę w kształtowaniu praktyki korzystania z chmur obliczeniowych, ponieważ daje użytkownikom pewność, że dostawcy usług chmurowych nie ponoszą odpowiedzialności za treści, które są wgrywane na ich serwery przez osoby trzecie. W kontekście prawa autorskiego oznacza to, że operatorzy takich usług nie muszą przeprowadzać skomplikowanej kontroli treści przed ich umieszczeniem. Mimo tej ochrony, dostawcy usług chmurowych mają obowiązek usunięcia treści, które naruszają prawa autorskie po otrzymaniu odpowiedniego zgłoszenia. Ten mechanizm pozwala na politykę czystych rąk dla operatorów, jednocześnie minimalizując ryzyko nielegalnego korzystania z materiałów chronionych prawami autorskimi w Internecie. Kalkulacja ta ma na celu balansowanie odpowiedzialności między twórcami treści a dostawcami technologii, przy jednoczesnym stymulowaniu rozwoju rosnącej gospodarki cyfrowej. Rozwój technologii cyfrowych i globalny zasięg usług internetowych wymagają ponownego przemyślenia pojęć związanych z kopiowaniem oraz zwielokrotnianiem utworu. Automatyczne tworzenie kopii przy przesyłaniu danych do serwerów zewnętrznych nie zawsze musi być traktowane jako naruszenie praw twórców. Istotnym elementem tego zagadnienia jest również kwestia odpowiedzialności prawnej dostawców usług chmurowych za treści umieszczane przez użytkowników. W systemie prawnym,

[37] Por. L. Determann, What Happens in the Cloud: Software as a Service and Copyrights, https://lawcat.berkeley.edu/nanna/record/1126823/files/fulltext.pdf?withWatermark=0&withMetadata=0&registerDownload=1&version=1 (dostęp: 5.02.2025).

[38] Od teraz będzie używany skrót DMCA.

w którym funkcjonuje zasada *safe harbor*, platformy internetowe i chmurowe są chronione przed odpowiedzialnością za naruszenia praw autorskich, o ile podejmują szybkie działania w przypadku zgłoszeń o nielegalnych treściach. Adaptacja przepisów do zmieniającego się środowiska cyfrowego wymaga stałego poszukiwania rozwiązań, które umożliwią skuteczną ochronę własności intelektualnej bez ograniczania innowacyjności i rozwoju technologii. Wprowadzenie jasnych reguł dotyczących odpowiedzialności prawnej oraz granic dozwolonego użytku pozwala na budowanie bezpiecznego środowiska, w którym zarówno twórcy, jak i użytkownicy mogą korzystać z zalet nowoczesnych systemów przechowywania danych. Kluczowe jest zapewnienie, by procedury szybkiego reagowania na naruszenia były skuteczne[39].

Orzecznictwo sądowe, które precyzyjnie określa zakres ochrony praw autorskich, wywiera istotny wpływ na rynek usług cyfrowych, wpływając na strategie biznesowe firm działających w obszarze *cloud computingu*. Dokładne ustalenie granic ochrony własności intelektualnej umożliwia przedsiębiorstwom lepsze zarządzanie ryzykiem prawnym, a jednocześnie kształtuje warunki, w których mogą wprowadzać innowacyjne rozwiązania technologiczne. Z drugiej strony, rygorystyczna interpretacja przepisów dotyczących ochrony praw autorskich może skutkować obciążeniem odpowiedzialnością prawną, co wpływa na ostrożność przy podejmowaniu decyzji inwestycyjnych. Firmy działające w chmurze muszą równoważyć innowacyjność z przestrzeganiem prawa, dostosowując się do zmian regulacyjnych, co sprzyja rozwojowi gospodarki cyfrowej oraz zwiększa innowacyjność i konkurencyjność rynku usług chmurowych w Europie[40].

Różnice w podejściu do regulacji w poszczególnych jurysdykcjach przekładają się na zróżnicowane standardy ochrony własności intelektualnej, co komplikuje funkcjonowanie usług chmurowych na arenie międzynarodowej. Niejednolity system prawny może prowadzić do rozbieżności w interpretacji przepisów dotyczących kopiowania, zwielokrotniania i udostępniania treści, co w rezultacie wpływa na stabilność operacyjną oraz inwestycje w sektorze technologii cyfrowych. Konieczne staje się poszukiwanie rozwiązań umożliwiających ujednolicenie przepisów na poziomie globalnym. Wspólne standardy prawne mogłyby zapewnić większą pewność zarówno dostawcom usług chmurowych, jak i ich użytkownikom, upraszczając transgraniczne operacje oraz ograniczając ryzyko związane z różnicami w lokalnych systemach prawnych. Standaryzacja regulacji w zakresie ochrony praw autorskich sprzyjałaby nie tylko efektywności działania przedsiębiorstw, ale także wspierała innowacje poprzez tworzenie bardziej przewidywalnego środowiska inwestycji w technologie cyfrowe. Harmonizacja przepisów umożliwiłaby sprawniejsze rozwiązywanie sporów prawnych oraz ułatwiłaby przepływ danych między państwami, co jest kluczowe do funkcjonowania globalnych usług chmurowych. Ujednolicone reguły ochrony własności intelektualnej przyczyniłyby się do redukcji kosztów

[39] Por. M.A. Melzer, Copyright Enforcement in the Cloud, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1492&context=iplj (dostęp: 3.02.2025).

[40] Por. J. Lerner, G. Rafert, Lost in the Clouds: The Impact of Copyright Scope on Investment in Cloud Computing Ventures, https://www.hbs.edu/faculty/Pages/item.aspx?num=43482 (dostęp: 2.02.2025).

operacyjnych, eliminując potrzebę dostosowywania się do odmiennych wymogów prawnych w każdym kraju z osobna. Taki system prawny zwiększałby także konkurencyjność rynku, umożliwiając łatwiejszą ekspansję usług na nowe rynki przy jednoczesnym zachowaniu wysokich standardów ochrony praw autorskich. Międzynarodowa współpraca oraz dialog między państwami są kluczowe w osiągnięciu tego celu, ponieważ pozwalają na wypracowanie kompromisowych rozwiązań, które z jednej strony chronią prawa twórców, a z drugiej sprzyjają rozwojowi technologii i swobodnemu przepływowi informacji. W efekcie, stworzenie globalnego, spójnego systemu regulacji mogłoby stanowić fundament stabilnego rozwoju gospodarki cyfrowej, przynosząc korzyści wszystkim uczestnikom rynku, od innowacyjnych startupów po międzynarodowe korporacje[41].

Usługi chmurowe umożliwiają przechowywanie, przetwarzanie i udostępnianie treści cyfrowych na skalę międzynarodową, co wiąże się z występowaniem problemów dotyczących właściwej jurysdykcji oraz stosowania różnych systemów prawnych. Wielość lokalizacji serwerów, zróżnicowane regulacje krajowe oraz brak jednolitej interpretacji przepisów dotyczących praw autorskich sprawiają, że ustalenie, która jurysdykcja powinna rozstrzygać spory związane z naruszeniami własności intelektualnej, staje się wyzwaniem. W takiej sytuacji określenie miejsca, w którym doszło do naruszenia praw autorskich, oraz ustalenie odpowiedzialności za naruszenie staje się skomplikowanym procesem, wymagającym precyzyjnego dopasowania przepisów międzynarodowych do specyfiki cyfrowej dystrybucji treści. Równocześnie, odpowiedzialność dostawców usług chmurowych w zakresie ochrony praw autorskich jest przedmiotem intensywnych analiz. W miarę jak dane i treści są przetwarzane w rozproszonych lokalizacjach, konieczne jest wprowadzenie mechanizmów umożliwiających skuteczne monitorowanie oraz egzekwowanie przepisów o ochronie własności intelektualnej. Kluczową kwestią pozostaje ustalenie, na jakich zasadach można przypisać odpowiedzialność za ewentualne naruszenia prawa autorskiego, w tym czy i w jakim zakresie obowiązki te dotyczą zarówno dostawców usług, jak i użytkowników korzystających z usług chmurowych[42].

W kontekście polskiego systemu prawnego, charakter umowy Software as a Service stanowi kluczowy element regulacji stosunków między dostawcą a odbiorcą usług chmurowych. Umowy te, będące specyficzną formą kontraktu, precyzują zasady korzystania z oprogramowania udostępnianego w modelu abonamentowym, gdzie oprogramowanie pozostaje własnością dostawcy, a użytkownik otrzymuje jedynie prawo do korzystania z usługi. Kluczowym aspektem tych umów jest określenie zakresu licencji, która umożliwia dostęp do aplikacji oraz zapewnia ochronę praw autorskich, jednocześnie uwzględniając kwestie związane z modyfikacjami, aktualizacjami oraz ewentualnymi naruszeniami praw własności intelektualnej. Precyzyjne sformułowanie postanowień umownych jest niezbędne, aby w sytuacjach

[41] Por. K. Kariyawasam, C. Talagala, *Cloud Computing and the Future of Copyright Law*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3110398 (dostęp: 4.02.2025).

[42] Por. A. Fortuna, *Jurysdykcja w sprawach z zakresu prawa autorskiego w chmurze obliczeniowej*, https://skubisz.pl/jurysdykcja-w-sprawach-z-zakresu-prawa-autorskiego-w-chmurze-obliczeniowej/ (dostęp: 11.02.2025).

spornych możliwe było jednoznaczne określenie obowiązków stron, a także aby zapewnić ochronę interesów obu stron umowy. W ramach polskiego prawa, umowy typu Software as a Service wymagają uwzględnienia zarówno przepisów dotyczących prawa autorskiego, jak i norm regulujących stosunki kontraktowe w obszarze usług elektronicznych. Umowy te muszą uwzględniać specyfikę funkcjonowania oprogramowania udostępnianego w chmurze, w tym nieustanny charakter świadczenia usługi, który różni się od tradycyjnego modelu sprzedaży oprogramowania jako produktu. Istotne staje się również zabezpieczenie danych przechowywanych w systemach chmurowych, a także określenie warunków odpowiedzialności za ewentualne przestoje lub błędy systemowe, które mogą wpływać na ochronę praw autorskich. W efekcie, umowy w modelu Software as a Service w polskim systemie prawnym stanowią przykład nowoczesnych rozwiązań, które odpowiadają na wyzwania związane z cyfryzacją i globalizacją usług informatycznych. Integracja regulacji dotyczących ochrony praw autorskich z postanowieniami umownymi pozwala na wypracowanie równowagi między interesami stron oraz umożliwia dynamiczne reagowanie na zmieniające się warunki rynkowe. W umowach regulujących świadczenie usług przechowywania danych często znajdują się klauzule, które definiują, w jakim zakresie dostawca ma prawo przetwarzać, modyfikować czy udostępniać treści przechowywane przez użytkownika. Tego rodzaju zapisy mają na celu zapewnienie prawidłowego funkcjonowania systemu, optymalizację wydajności czy utrzymanie bezpieczeństwa infrastruktury. Jednocześnie muszą być formułowane w sposób gwarantujący, że nie dochodzi do naruszenia integralności utworu oraz do ograniczenia osobistych praw twórców, których ochrona stanowi fundament ustawy o prawie autorskim i prawach pokrewnych. Kluczowe znaczenie ma również właściwe wyważenie interesów stron umowy. Z jednej strony, niezbędne jest umożliwienie usługodawcy działania w ramach konserwacji systemu, aktualizacji oprogramowania czy wprowadzania poprawek technicznych. Z drugiej strony, nadmierna ingerencja w treści przechowywane przez użytkowników może prowadzić do ograniczenia praw autorskich i utrudniać egzekwowanie roszczeń w przypadku naruszeń. Umowy zawierane na zasadzie adhezyjnej często przenoszą ryzyko wynikające z ewentualnych sporów o naruszenie praw autorskich na użytkownika, co wymusza szczególną ostrożność przy wyborze materiałów do przechowywania w chmurze. Odpowiedzialność za naruszenia praw autorskich w środowisku chmurowym obejmuje zarówno szkody bezpośrednie, wynikające z nieautoryzowanego kopiowania czy modyfikacji utworów, jak i szkody pośrednie, związane na przykład z utratą reputacji lub konsekwencjami finansowymi wynikającymi z długotrwałych sporów sądowych. Z tego względu klauzule umowne dotyczące praw autorskich powinny być formułowane w sposób precyzyjny i zgodny z obowiązującymi przepisami, aby nie ograniczały nadmiernie możliwości ochrony praw twórców, a jednocześnie umożliwiały sprawne funkcjonowanie usług chmurowych[43].

[43] Por. S. Malkowski, *Charakter prawny umowy Software as a Service w polskim systemie prawnym*, https://repozytorium.uni.wroc.pl/Content/136425/PDF/06_S_Malkowski_Charakter_prawny_umowy_Software_as_a_Seervice_w_polskim_systemie_prawnym.pdf (dostęp: 10.02.2025).

Zmiany na rynku technologii cyfrowych i rosnące znaczenie usług przechowywania danych w chmurze wymagają ciągłej adaptacji przepisów prawnych do nowych realiów. Konieczne jest, aby regulacje prawne nadążały za zmianami technologicznymi, zapewniając równocześnie ochronę praw autorskich oraz wspierając innowacyjność usług chmurowych. Wymaga to współpracy ustawodawcy z dostawcami usług oraz bieżącej weryfikacji umów pod kątem zgodności z międzynarodowymi standardami ochrony własności intelektualnej.

Użytkownicy chmur obliczeniowych w Polsce korzystają z szeregu praw chronionych przez ustawę o prawach konsumentów, która reguluje zasady dotyczące umów zawieranych na odległość oraz poza lokalem przedsiębiorstwa. W kontekście usług chmurowych, często dostarczanych w formie treści cyfrowych, kluczowe znaczenie ma kilka aspektów. Przede wszystkim, konsument ma prawo odstąpić od umowy zawartej na odległość w terminie 14 dni bez podawania przyczyny, a w przypadku umów zawartych podczas nieumówionej wizyty przedsiębiorcy, termin ten wynosi 30 dni. To prawo obejmuje również umowy dotyczące dostarczania treści cyfrowych i usług cyfrowych, co oznacza, że użytkownik może zrezygnować z usługi chmurowej w określonym czasie[44].

Zgodnie z nowelizacją ustawy o prawach konsumenta, która weszła w życie 1 stycznia 2023 r., przedsiębiorcy są zobowiązani do zapewnienia, że dostarczane treści lub usługi cyfrowe są zgodne z umową. Przedsiębiorcy oferujący usługi chmurowe muszą przestrzegać obowiązków informacyjnych wobec konsumentów, co obejmuje dostarczenie jasnych informacji o warunkach umowy, takich jak cena, zakres usług oraz procedury reklamacyjne. Użytkownicy muszą być informowani o wszelkich istotnych aspektach umowy przed jej zawarciem przypadku stwierdzenia niezgodności treści cyfrowej lub usługi cyfrowej z umową, konsument ma prawo zgłosić reklamację. Przedsiębiorca odpowiada za wady ujawnione w ciągu dwóch lat od dostarczenia usługi. W sytuacji, gdy naprawa lub wymiana są niemożliwe lub wymagają nadmiernych kosztów, konsument może żądać obniżenia ceny lub odstąpienia od umowy. Nowe przepisy wprowadzają również obowiązek dostarczania aktualizacji, w tym aktualizacji zabezpieczeń, dla towarów z elementami cyfrowymi, takich jak smartfony czy tablety. Ma to na celu zapewnienie, że produkty te pozostają zgodne z umową przez cały okres ich użytkowania[45].

Nowe regulacje dotyczą nie tylko tradycyjnych form sprzedaży, ale również sytuacji, gdy konsument udostępnia swoje dane osobowe w zamian za dostęp do treści cyfrowych. Jest to istotne w kontekście wielu usług chmurowych, które oferują darmowe wersje w zamian za dane użytkowników. Implementacja dyrektyw unijnych do polskiego prawa konsumenckiego ma na celu zwiększenie ochrony konsumentów w dynamicznie rozwijającym się środowisku cyfrowym. Zmiany te mają szczególne znaczenie dla sektora usług chmurowych, który staje się coraz bardziej powszechny zarówno w życiu prywatnym, jak i w działalności gospodarczej[46].

[44] Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (Dz.U. 2014 poz. 827).

[45] Ustawa z dnia 1 grudnia 2022 r. o zmianie ustawy o prawach konsumenta oraz niektórych innych ustaw (Dz.U. 2022 poz. 2581).

[46] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych.

Dostawcy usług chmurowych mają obowiązek zapewnienia pełnej przejrzystości informacji, co stanowi fundament budowania zaufania pomiędzy usługodawcą a użytkownikiem. W ramach tego zobowiązania prezentowane są szczegółowe opisy charakterystyki oferowanych usług, warunki cenowe i płatności, a także określane są zasady dotyczące okresu obowiązywania umowy oraz procedury jej rozwiązania. Informacje te obejmują także dane kontaktowe oraz klarowne wytyczne dotyczące składania reklamacji, co umożliwia konsumentom szybkie i efektywne reagowanie w sytuacjach problemowych. Obecny rynek chmur obliczeniowych wymaga, aby każdy użytkownik miał dostęp do rzetelnych danych, pozwalających na świadome podejmowanie decyzji. Dlatego informacje o usłudze muszą być nie tylko kompletne, ale również zrozumiałe i łatwo dostępne, co umożliwia porównanie różnych ofert oraz ocenę ich zgodności z indywidualnymi potrzebami[47].

Dostawcy usług chmurowych są zobowiązani do zapewnienia najwyższego poziomu bezpieczeństwa danych konsumentów, co obejmuje zarówno wdrożenie zaawansowanych środków technicznych, jak i kompleksowych procedur organizacyjnych. Kluczowym elementem tego zadania jest zastosowanie mechanizmów zapobiegających utracie danych, takich jak systemy backupu i odzyskiwania po awarii, które pozwalają na szybkie przywrócenie pełnej funkcjonalności usług nawet w przypadku wystąpienia nieprzewidzianych incydentów. Utrzymanie ciągłości działania usług jest realizowane poprzez skrupulatne przestrzeganie warunków umownych, w których określony jest poziom dostępności działań zgodnie z ustalonymi wskaźnikami SLA. Dostawcy są zobowiązani do zapewnienia, że wszystkie umowy oraz warunki świadczenia usług są zgodne z obowiązującym prawem konsumenckim. W praktyce oznacza to, że umowy muszą być sporządzane w sposób przejrzysty i uczciwy, z pełnym poszanowaniem praw konsumentów. Istotnym elementem tych regulacji jest unikanie stosowania nieuczciwych klauzul umownych, które mogłyby naruszać równowagę między stronami i ograniczać możliwości ochrony interesów użytkowników. Prawo do odstąpienia od umowy stanowi kolejny filar ochrony konsumentów w obszarze usług chmurowych. Umowy powinny jasno określać warunki, na jakich użytkownicy mogą zrezygnować z usługi, co daje im poczucie bezpieczeństwa i pewność, że nie zostaną obciążeni niekorzystnymi konsekwencjami w razie zmiany decyzji[48].

Mają oni także obowiązek jasno informować o wtórnym wykorzystaniu danych konsumentów. Powinni oni wyraźnie oddzielać informacje o danych wykorzystywanych wyłącznie do technicznego działania usługi, na przykład przechowywanie plików, uwierzytelnianie, od danych przetwarzanych w celach komercyjnych, takich jak marketing, profilowanie czy sprzedaż danych partnerom. Gdy dostawca opracowuje nowe sposoby wykorzystania treści i informacji transakcyjnych, powinien powiadomić o tym konsumenta i uzyskać jego zgodę przed wdrożeniem nowego wykorzystania[49].

[47] Por. T. Dolny, Consumers in the cloud: EU consumer protection in cloud computing contracts, https://cris.maastrichtuniversity.nl/en/publications/consumers-in-the-cloud-eu-consumer-protection-in-cloud-computing- (dostęp: 13.01.2025).

[48] Por. K. McGillivray, A right too far? Requiring cloud service providers to deliver adequate data security to consumers, https://academic.oup.com/ijlit/article/25/1/1/2525429?login=false (dostęp: 6.02.2025).

[49] Por. C. Reed, Cunningham A., Caveat Consumer? – Consumer Protection and Cloud Com-

Dbałość o pełną transparentność w zakresie informowania o wtórnym wykorzystaniu danych konsumentów jest kluczowa, aby wyraźnie oddzielić wykorzystanie danych niezbędnych do technicznego funkcjonowania usługi od operacji związanych z modelem biznesowym dostawcy. Użytkownik powinien mieć jasność co do tego, które dane są wykorzystywane do zapewnienia ciągłości działania i optymalizacji technicznych, a które mogą być przetwarzane w celach komercyjnych lub rozwojowych, co pozwala na pełną kontrolę nad swoimi informacjami. W sytuacji, gdy pojawiają się nowe sposoby wykorzystania treści oraz informacji transakcyjnych, konieczne jest nie tylko ich wdrożenie, ale również uprzednie poinformowanie konsumentów o planowanych zmianach. Pozyskanie zgody użytkownika na wprowadzenie takich rozwiązań stanowi istotny element ochrony prywatności i budowania zaufania między stronami. Taka procedura umożliwia konsumentom świadome decydowanie o udostępnianiu swoich danych i daje im możliwość wyrażenia sprzeciwu, jeśli proponowane zmiany nie spełniają ich oczekiwań lub naruszają ich prawa[50]. Ma to szczególne znaczenie w kontekście analizy przypadków naruszenia danych w chmurach, ponieważ brak przejrzystości i zgody użytkownika często prowadzi do utraty kontroli nad danymi oraz zwiększa ryzyko incydentów związanych z ich nieuprawnionym wykorzystaniem.

Dostawcy darmowych usług chmurowych mają obowiązek przestrzegania tych samych zasad, co dostawcy tradycyjnych usług płatnych. Choć konsumenci nie płacą bezpośrednio za korzystanie z tych usług, dostawcy zazwyczaj generują dochody poprzez wykorzystanie informacji osobowych użytkowników. Oznacza to, że powinni oni równie odpowiedzialnie podchodzić do kwestii ochrony danych, przejrzystości wytycznych dotyczących prywatności oraz realizacji zobowiązań umownych, jak w przypadku usług, za które konsumenci bezpośrednio płacą. Równocześnie zapewnienie takich samych standardów usługom płatanym i bezpłatnym pozytywnie wpływa na konkurencję na rynku chmurowych technologii. Oferujący darmowe rozwiązania powinni podlegać tym samym zasadom, jakie obowiązują w przypadku usług płatnych, co stanowi gwarancję równego traktowania wszystkich użytkowników. Konsumenci nie ponoszą bezpośrednich kosztów związanych z korzystaniem z bezpłatnych usług, natomiast dostawcy czerpią zyski z przetwarzania i analizy danych osobowych użytkowników. Taki model biznesowy wymaga stosowania jednolitych standardów ochrony konsumentów, aby zagwarantować, że informacje są wykorzystywane w sposób przejrzysty i zgodny z obowiązującymi przepisami[51].

Konsumenci, których dane zostały naruszone w wyniku wycieku z chmury, mogą domagać się przede wszystkim informacji o incydencie. Firmy są zobowiązane do szybkiego i przejrzystego informowania użytkowników o incydentach

puting Part 1 – Issues of Definition in the Cloud, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2202758 (dostęp: 13.01.2025).

[50] Por. K. Kariyawasam, C. Talagala, Contracts for Clouds, Revisited: An Analysis of the Standard Contracts for 40 Cloud Computing Services, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3624712 (dostęp: 11.01.2025).

[51] Por. K. Pande Joshi, L. Elluri, Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing, https://consumerfed.org/pdfs/Cloud-report-2010.pdf (dostęp: 14.01.2025).

naruszenia danych, co jest kluczowe do umożliwienia konsumentom podjęcia odpowiednich działań ochronnych. Ponadto, użytkownicy mają prawo żądać dostępu do swoich danych osobowych oraz informacji o tym, jak są one przetwarzane przez dostawcę usług chmurowych. Mogą również domagać się usunięcia swoich danych, jeśli nie są one już potrzebne, lub jeśli wycofali zgodę na ich przetwarzanie. W przypadku poniesienia strat w wyniku naruszenia danych, konsumenci mogą dochodzić odszkodowania od dostawców usług, którzy nie spełnili wymogów bezpieczeństwa. Wiele przepisów prawnych przewiduje możliwość składania pozwów cywilnych w takich sytuacjach. Firmy powinny także jasno przedstawiać warunki korzystania z ich usług, w tym szczegółowe informacje dotyczące polityki prywatności oraz zabezpieczeń stosowanych do ochrony danych konsumentów[52].

Po incydentach związanych z naruszeniem danych, konsumenci często zmieniają swoje nawyki dotyczące udostępniania informacji oraz stają się bardziej ostrożni w korzystaniu z usług online. Regulacje dotyczące ochrony danych nakładają na dostawców chmur obowiązki związane z bezpieczeństwem danych oraz informowaniem konsumentów o naruszeniach. W Europie RODO wymaga od firm natychmiastowego powiadamiania organu nadzorczego oraz osób dotkniętych naruszeniem w ciągu 72 godzin od jego wystąpienia. W Stanach Zjednoczonych sytuacja jest bardziej skomplikowana, ponieważ przepisy różnią się w zależności od stanu, co może prowadzić do zamieszania zarówno dla konsumentów, jak i dla firm działających w wielu jurysdykcjach[53].

Konsumenci mają szereg praw i możliwości dochodzenia roszczeń w przypadku wycieku danych z chmury. Jednocześnie, firmy korzystające z usług chmurowych muszą być świadome złożoności prawnych i operacyjnych związanych z przechowywaniem danych w różnych jurysdykcjach oraz podejmować proaktywne kroki w celu ochrony danych konsumentów. Konsumenci, którzy otrzymają adekwatne wsparcie po incydencie, są bardziej skłonni kontynuować współpracę z firmą, mimo wcześniejszych problemów. Wybór konkretnej formy rekompensaty może wpłynąć na postrzeganie całej organizacji i jej zdolność do dbania o bezpieczeństwo danych, co przekłada się na długoterminową lojalność oraz pozytywne intencje korzystania z oferowanych usług. Regulacje prawne omówione w tym rozdziale stanowią punkt wyjścia do analizy rzeczywistych incydentów wycieków danych, pozwalając ocenić, w jakim stopniu obowiązujące przepisy były przestrzegane lub naruszone w praktyce.

[52] Por. J. Lerner, G. Rafert, *Are consumers well protected in cloud computing contracts?*, https://www.maastrichtuniversity.nl/blog/2024/03/are-consumers-well-protected-cloud-computing-contracts (dostęp: 9.02.2025).

[53] Por. D. Kolevski, K. Michael, R. Abbas, M. Freeman, Dostępne na: https://par.nsf.gov/servlets/purl/10344523 (dostęp: 12.01.2025).

3. ANALIZA WYBRANYCH INCYDENTÓW NARUSZEŃ DANYCH W CHMURACH

W niniejszym rozdziale przeprowadzono analizę przyczynowo-skutkową, która umożliwia kompleksowe zrozumienie mechanizmów leżących u podstaw incydentów naruszeń bezpieczeństwa danych. Metoda ta została wybrana ze względu na jej zdolność do identyfikacji bezpośrednich przyczyn zdarzeń, jak i długofalowych konsekwencji oraz do wyciągania wniosków, mających na celu zapobieganie podobnym sytuacjom w przyszłości. Pozwala ona na prześledzenie sekwencji zdarzeń od momentu zaistnienia luki w zabezpieczeniach, przez etap eskalacji ataku aż po skutki społeczne, prawne i finansowe. Jest to niezbędne w kontekście oceny wpływu cyberincydentów na organizacje i ich otoczenie.

Metoda ta została wyselekcjonowana jako optymalne podejście ze względu na jej wartość praktyczną i eksplikatywną[54]. W przypadku badania incydentów cyberbezpieczeństwa kluczowe jest nie tylko opisanie faktów, ale także zrozumienie zależności między czynnikami technicznymi, proceduralnymi i ludzkimi, które umożliwiły atak. Wnosi ona do pracy strukturalizację procesu badawczego, umożliwiając weryfikację hipotez dotyczących źródła problemów oraz ocenę skuteczności podjętych działań naprawczych. Ponadto, pozwala na wyodrębnienie uniwersalnych wzorców i rekomendacji dla sektora IT, wykraczających poza analizę pojedynczych przypadków.

Metoda ta została wprowadzona w następujących krokach, odpowiadających strukturze każdego z omówionych przypadków:

- szczegóły incydentu – precyzyjne określenie czasu, podmiotów zaangażowanych oraz kontekstu operacyjnego;
- mechanizm ataku – identyfikacja technik wykorzystanych przez sprawców, źródeł podatności oraz procesu eskalacji naruszenia;
- skala naruszenia – ilościowa i jakościowa ocena zakresu;
- skutki – analiza konsekwencji dla organizacji oraz użytkowników;
- działania naprawcze – ocena reakcji poszkodowanych firm;
- wnioski – synteza lekcji wyciągniętych z incydentu.

Zastosowanie powyższego schematu pozwoliło nie tylko opisać naruszenia, ale też ujawnić systemowe słabości w cyberbezpieczeństwie, takie jak: zaniedbania w aktualizacji haseł, brak szyfrowania danych czy niewystarczające szkolenia pracowników. Metoda ta umożliwiła również wskazanie powtarzalnych czynników ryzyka oraz wypracowanie modelowych rozwiązań, mających na celu minimalizację podobnych zagrożeń w przyszłości. Tym samym, ten opis stanowi nie tylko studium przypadków, ale także praktyczny przewodnik dla organizacji dążących do wzmocnienia swojej odporności na cyberataki.

Pierwszym przykładem jest Snowflake, wiodąca platforma do przechowywania i analizy danych w chmurze, która padła ofiarą poważnego wycieku danych. Atak rozpoczął się w połowie kwietnia 2024 r., kiedy grupa cyberprzestępcza UNC5537,

[54] Synonim.net, Synonimy, https://synonim.net/synonim/eksplikatywny (dostęp: 15.05.2025).

znana również jako ShinyHunters, rozpoczęła kampanię ataków na konta klientów Snowflake. Atakujący wykorzystali skradzione dane logowania, które były dostępne na forach cyberprzestępczych, aby uzyskać nieautoryzowany dostęp do środowisk Snowflake należących do różnych organizacji[55].

ShinyHunters wykorzystali kilka kluczowych mechanizmów, aby przeprowadzić atak, jak:

- Wykorzystanie skradzionych danych logowania – grupa UNC5537 zakupiła dane logowania na forach cyberprzestępczych, które były wcześniej skradzione za pomocą złośliwego oprogramowania typu infostealer[56]. Te dane logowania, często niezaktualizowane od lat, pozwoliły na dostęp do kont Snowflake.
- Brak uwierzytelniania wieloskładnikowego[57] – większość skompromitowanych kont nie miała włączonej MFA, co umożliwiło atakującym dostęp do kont tylko za pomocą ważnych nazw użytkowników i haseł.
- Wykorzystanie słabych punktów w API – atakujący wykorzystali luki w zabezpieczeniach Snowflake, aby ominąć standardowe protokoły uwierzytelniania i uzyskać dostęp do wrażliwych danych[58].

Skala naruszenia była znacząca, wpływając na około 165 organizacji, w tym takie firmy jak: Santander Group, Ticketmaster i Advance Auto Parts. Atakujący uzyskali dostęp do milionów rekordów klientów, w tym danych osobowych, finansowych i potencjalnie własności intelektualnej, takie jak poufne informacje, patenty czy innowacje. Atakującym udało się przejąć ogromne zbiory danych, obejmujące m.in. informacje o ponad 30 milionach kont bankowych, 28 milionach kart kredytowych oraz poufne dane personalne pracowników. Incydent związany z naruszeniem bezpieczeństwa w Snowflake doprowadził do licznych spraw sądowych, zaostrzenia nadzoru ze strony organów regulacyjnych oraz głośnych apeli o wzmocnienie standardów ochrony danych w rozwiązaniach chmurowych. Choć platforma została przywrócona do pełnej funkcjonalności, skutkiem wycieku były przejściowe utrudnienia w działaniu przedsiębiorstw korzystających z usług Snowflake[59].

Po wykryciu wycieku danych platforma podjęła szereg istotnych działań naprawczych. Przede wszystkim niezwłocznie załatano lukę w systemie, wprowadzając niezbędne aktualizacje zabezpieczeń w interfejsach API, co skutecznie zablokowało możliwość kolejnych nieuprawnionych dostępów. Równolegle firma uruchomiła specjalny program wsparcia poszkodowanych klientów, oferując im szczegółowe instrukcje dotyczące ochrony danych oraz metod wykrywania potencjalnych naruszeń. Dodatkowo znacznie wzmocniono politykę bezpieczeństwa przez wdrożenie

[55] Por. StrongDM Team, Snowflake Data Breach – What Happened & How to Prevent It, strongdm.com/what-is/snowflake-data-breach (dostęp: 25.03.2025).

[56] Oprogramowanie, które kradnie informacje z urządzenia.

[57] Od tego momentu będzie używany skrót MFA.

[58] Por. D. Green, Snowflake Retro: Analyzing the Breach, pushsecurity.com/blog/snowflake-retro (dostęp: 25.03.2025).

[59] Por. StrongDM Team, Snowflake Data Breach – What Happened & How to Prevent It, strongdm.com/what-is/snowflake-data-breach (dostęp: 25.03.2025).

zaostrzonych procedur uwierzytelniania oraz systematycznych przeglądów systemów pod kątem potencjalnych zagrożeń[60].

Incydent związany z wyciekiem danych w Snowflake wyraźnie pokazał, że zapewnienie bezpieczeństwa w środowisku chmurowym to wspólne zadanie zarówno dostawców usług, jak i ich klientów, którzy powinni ściśle monitorować dostęp do swoich zasobów. Okazało się, że brak stosowania MFA znacząco ułatwił atak, co dobitnie potwierdza konieczność jego wdrażania jako podstawowego zabezpieczenia. Problemem okazało się także przechowywanie niezabezpieczonych danych uwierzytelniających na prywatnych urządzeniach pracowników czy w systemach do zarządzania projektami. W takich przypadkach szyfrowanie wrażliwych informacji staje się absolutną koniecznością. Kluczową lekcją z tej sytuacji jest również potrzeba regularnego szkolenia personelu w zakresie zasad cyberbezpieczeństwa, szczególnie dotyczących właściwego przechowywania i ochrony danych[61].

Drugim przykładem jest Toyota Financial Services[62], która w 2023 r. doświadczyła dwóch poważnych incydentów związanych z wyciekiem danych. Pierwszy incydent wynikał z nieprawidłowej konfiguracji chmurowej bazy danych, co przez niemal dekadę, od listopada 2013 do kwietnia 2023 r., umożliwiało nieuprawniony dostęp do danych lokalizacji pojazdów należących do 2,15 miliona klientów. Drugie, znacznie poważniejsze naruszenie, było skutkiem ataku ransomware[63] przeprowadzonego przez grupę Medusa, która zaatakowała europejskie i afrykańskie oddziały koncernu, uzyskując dostęp do poufnych informacji osobowych i finansowych. W grudniu 2023 r. TFS poinformowała klientów o zakresie wycieku, który obejmował pełne nazwiska, adresy, dane kontaktowe, informacje o umowach leasingowych oraz numery kont bankowych. Grupa hakerska Medusa przeprowadziła atak ransomware na TFS, wykorzystując lukę w oprogramowaniu Citrix Gateway, znaną jako Citrix Bleed, do wniknięcia do wewnętrznej sieci przedsiębiorstwa. Po skutecznym włamaniu cyberprzestępcy zażądali od Toyoty okupu w wysokości 8 milionów dolarów, grożąc upublicznieniem przejętych informacji w przypadku odmowy zapłaty. W celu udowodnienia skuteczności ataku, opublikowali wyciek próbki danych zawierającej wrażliwe dokumenty finansowe, faktury, zahasłowane dane logowań, skany dokumentów tożsamości oraz inne poufne materiały[64].

Wyciek danych poważnie odbił się na Toyocie, narażając klientów na utratę prywatności, potencjalne oszustwa związane z tożsamością oraz znacząco szkodząc wizerunkowi marki. Koncern stanął przed koniecznością poniesienia znacznych kosztów likwidacji skutków incydentów, obejmujących zarówno odszkodowania

[60] Por. B. Gebremeskel, Understanding the Snowflake Data Breach: What Happened and What Is Affected, teckpath.com/understanding-the-snowflake-data-breach-what-happened-and-what-is-affected (dostęp: 25.03.2025).

[61] Por. Understanding the Snowflake Data Breach and Its Implications,kosmos.com/authentication/understanding-the-snowflake-data-breach-and-its-implications (dostęp: 3.04.2025).

[62] Od teraz będzie używany skrót TFS.

[63] Ransomware to rodzaj złośliwego oprogramowania, które blokuje dostęp do systemu lub szyfruje pliki i żąda okupu w zamian za przywrócenie dostępu.

[64] Por. S. Gatlan, Toyota Confirms Third-Party Data Breach Impacting Customers, bleepingcomputer.com/news/security/toyota-confirms-third-party-data-breach-impacting-customers (dostęp: 3.04.2025).

dla klientów, jak i modernizację systemów zabezpieczeń. W reakcji na te zdarzenia Toyota wprowadziła nowe rozwiązania – zautomatyzowany system ciągłego nadzoru nad konfiguracją środowisk chmurowych i baz danych, mający zapobiegać podobnym incydentom w przyszłości. Jednocześnie firma zapewniła kompleksowe wsparcie poszkodowanym, w tym indywidualną pomoc w przypadku wystąpienia problemów związanych z wyciekiem[65].

W marcu 2022 r. zespół ds. cyberbezpieczeństwa Safety Detectives odkrył, że duża liczba wrażliwych danych należących do tureckich linii lotniczych Pegasus Airlines była odbezpieczona online. Dane te były przechowywane w niezabezpieczonym kubełku AWS S3 – kontenerze w chmurze Amazon Web Services, służącym do przechowywania i organizowania danych w postaci plików z możliwością zarządzania dostępem i uprawnieniami[66].

Zawierał on informacje związane z systemem Electronic Flight Bag[67], używanym przez pilotów do zarządzania procesami w locie. W kubełku znajdowały się dane lotnicze, wykresy lotów, materiały nawigacyjne, dane osobowe załogi oraz kod źródłowy oprogramowania. Wyciek danych Pegasus Airlines był wynikiem błędu konfiguracji kubełka AWS S3, który pozostawiono bez ochrony hasłem. Zawierał on dane EFB, które były do wglądu dla każdego, kto miał dostęp do Internetu. Znajdowały się tam również pliki z hasłami w tekście jawnym oraz kluczami tajnymi, które mogły być wykorzystane do manipulowania wrażliwymi plikami[68].

Wyciek danych mógł wpłynąć na bezpieczeństwo pasażerów i załogi Pegasus Airlines oraz innych linii lotniczych korzystających z oprogramowania Pegasus EFB. Ujawnienie tożsamości załogi naruszało tureckie prawo o ochronie danych osobowych, co mogło skutkować karą finansową do 183 000 dolarów. Ponadto, dostęp do kodów źródłowych i kluczy tajnych mógł umożliwić atakującemu manipulowanie danymi lotniczymi, co stwarzało potencjalne zagrożenie bezpieczeństwa lotów[69].

Po odkryciu wycieku, Safety Detectives skontaktowało się z Pegasus Airlines, informując o problemie. Linia lotnicza szybko zabezpieczyła kubełek AWS S3, optymalizując jego ustawienia bezpieczeństwa. Ponadto, turecki organ ochrony danych osobowych KVKK[70] potwierdził wyciek i rozpoczął dochodzenie w tej sprawie[71].

Incydent z wyciekiem danych Pegasus Airlines ukazuje, że właściwe zarządzanie i prawidłowa konfiguracja usług chmurowych, takich jak AWS S3, mają kluczowe

---

[65] Por. P. Paganini, ZeroSevenGroup – Toyota Data Breach, securityaffairs.com/167274/data-breach/zerosevengroup-toyota-data-breach.html (dostęp: 7.04.2025).

[66] Por., S. Mathew, AWS Overview, listopad 2014, https://www.sysfore.com/Assets/PDF/aws-overview.pdf (dostęp: 24.04.2025).

[67] Od tego momentu będzie używany skrót EFB.

[68] Por. Pegasus Airlines Breach Exposes 6.5 TB of Data, bankinfosecurity.com/pegasus-airlines-breach-exposes-65-tb-data-a-19173 (dostęp: 7.04.2025).

[69] Por. 6.5TB Data of Turkey-Based Pegasus Airlines Got Exposed Online, izoologic.com/region/middle-east/6-5tb-data-of-turkey-based-pegasus-airlines-got-exposed-online (dostęp: 11.04.2025).

[70] Por. Kişisel Verileri Koruma Kurumu – Turecka ustawa o ochronie danych osobowych z dnia 24 marca 2016 r. nr 6698 (Resmî Gazete z dnia 7 kwietnia 2016 r., poz. 29677).

[71] Por. Pegasus Airlines Breach Exposes 6.5 TB of Data, bankinfosecurity.com/pegasus-airlines-breach-exposes-65-tb-data-a-19173 (dostęp: 11.04.2025).

znaczenie dla bezpieczeństwa informacji. Przede wszystkim niezbędne jest regularne monitorowanie i audytowanie konfiguracji bezpieczeństwa w środowiskach chmurowych, co pozwala na wczesne wykrycie potencjalnych zagrożeń. Równie ważne jest wprowadzenie przejrzystych polityk bezpieczeństwa dotyczących zarówno zarządzania danymi, jak i kontroli dostępu do nich. Koniecznością stało się także systematyczne szkolenie pracowników z zakresu bezpieczeństwa informacji, ze szczególnym uwzględnieniem specyfiki pracy z danymi w chmurze. Warto również wdrożyć specjalistyczne narzędzia umożliwiające monitorowanie aktywności użytkowników w systemach o krytycznym znaczeniu dla organizacji. Ostatnim, ale nie mniej ważnym, elementem jest zapewnienie odpowiedniego zabezpieczenia dostępu do wrażliwych danych, co obejmuje stosowanie silnych haseł i właściwe zarządzanie kluczami tajnymi[72].

W październiku 2021 r., Twitch, popularna platforma do streamowania gier, padła ofiarą znaczącego wycieku danych. Incydent ten został spowodowany przez zmianę konfiguracji serwera, która umożliwiła nieautoryzowany dostęp do danych przez podmiot nieuprawniony. W wyniku tego wycieku, na forum 4chan zostało opublikowane ponad 100GB danych, w tym wewnętrzny kod źródłowy Twitcha, dokumenty wewnętrzne, a także informacje o wypłatach dla najlepszych streamerów. Choć dokładne metody ani narzędzia wykorzystane przez cyberprzestępców nie zostały ujawnione, wiadomo że wykorzystali oni lukę zabezpieczeń do penetracji wewnętrznych repozytoriów kodu Git oraz innych poufnych zasobów platformy[73].

Wyciek danych dotknął około 10 milionów osób, w tym streamerów, użytkowników i pracowników Twitcha. Wśród ujawnionych danych znalazły się adresy e-mail, informacje zdrowotne, pracodawcy, lokalizacje geograficzne, stanowiska pracy, imiona i nazwiska, numery telefonów oraz profile w mediach społecznościowych. Ponadto, wyciek ujawnił dane dotyczące wypłat dla top streamerów, co wywołało duże zainteresowanie i dyskusje w społeczności na temat ich wynagrodzenia i przyszłości kariery. Ponadto, ujawnienie wewnętrznego kodu źródłowego i dokumentów mogło potencjalnie umożliwić atakującemu odkrycie luk w zabezpieczeniach, co mogło prowadzić do dalszych ataków[74].

Twitch podjął natychmiastowe kroki w celu naprawienia konfiguracji serwera, która umożliwiła wyciek, oraz zabezpieczenia swoich systemów. Firma zresetowała wszystkie klucze streamowania jako środek ostrożności i skontaktowała się bezpośrednio z użytkownikami, których dane zostały naruszone. Twitch przeprowadził również dokładny przegląd ujawnionych informacji, aby zrozumieć zakres naruszenia i podjąć odpowiednie działania naprawcze. Platforma powinna zastosować zasadę minimalnych uprawnień, udostępniając wrażliwe dane wyłącznie osobom

[72] Por. GDPR Tech, The Future of Unstructured Data: Lessons from the Pegasus Airlines Data Breach, gdprtech.com/en/the-future-of-unstructured-data-lessons-from-the-pegasus-airlines-data-breach (dostęp: 14.04.2025).

[73] Por. Twitch Live Streaming Data Breach 2021, mitnicksecurity.com/blog/twitch-live-streaming-data-breach-2021 (dostęp 14.04.2025).

[74] Por. D. Molloy, T. Tidy, Twitch: Data Breach Reveals Pay for Top Streamers, bbc.com/news/technology-58817658 (dostęp: 14.04.2025).

absolutnie niezbędnym do wykonywania swoich obowiązków. Równie ważne okazuje się systematyczne przeprowadzanie audytów bezpieczeństwa, które poprzez regularną weryfikację konfiguracji serwerów i systemów mogłyby zapobiec podobnym incydentom. Istotna jest szybkość reakcji zarówno w zakresie działań naprawczych, jak i przejrzystej komunikacji z użytkownikami, która pozwala ograniczyć negatywne skutki wycieku. Ważna jest także edukacja użytkowników, zwiększająca ich świadomość zagrożeń związanych z platformami streamingowymi oraz podstawowych metod ochrony danych osobowych[75].

W 2020 r. Capital One, jedna z największych instytucji finansowych w USA, padła ofiarą poważnego wycieku danych. Incydent ten został odkryty, kiedy stwierdzono, że osoba z zewnątrz uzyskała nieautoryzowany dostęp do danych osobowych klientów kart kredytowych oraz osób, które ubiegały się o produkty kredytowe Capital One[76].

Atak na Capital One został przeprowadzony przez Paige Thompson, byłą pracownicę AWS, która wykorzystała swoją wiedzę i dostęp do infrastruktury AWS. Thompson wykorzystała lukę w konfiguracji zapory sieciowej Capital One, która była podatna na atak typu Server-Side Request Forgery. Dzięki tej luce, Thompson mogła uzyskać dostęp do metadanych AWS, co pozwoliło jej na kradzież danych z prywatnego bucketu S3, gdzie przechowywane były informacje klientów[77].

Wyciek danych dotknął ponad 106 milionów klientów w USA i Kanadzie. Wśród danych, które zostały skradzione, znalazły się imiona, adresy, daty urodzenia, numery ubezpieczenia społecznego, numery kont bankowych, dane dotyczące aplikacji kredytowych z lat 2005–2019, w tym wyniki kredytowe, limity kredytowe, salda, historie płatności oraz fragmenty historii transakcji z lat 2016–2018[78].

Wyciek danych Capital One miał poważne konsekwencje finansowe i reputacyjne. Bank zgodził się zapłacić 80 milionów dolarów kary nałożonej przez Office of the Comptroller of the Currency za brak skutecznych procesów oceny ryzyka przed migracją do chmury publicznej oraz za opóźnienia w naprawie tych niedoskonałości. Ponadto, Capital One zgodził się na ugodę w wysokości 190 milionów dolarów w związku z pozwem zbiorowym dotyczącym wycieku danych. Po odkryciu wycieku, Capital One podjęło natychmiastowe kroki w celu minimalizacji dalszych szkód. Bank poinformował władze federalne, współpracował z FBI w celu identyfikacji sprawcy, zaoferował klientom bezpłatne monitorowanie kredytów oraz wdrożył szereg środków mających na celu wzmocnienie swojej postawy w zakresie cyberbezpieczeństwa. Wśród tych działań znalazły się: zaostrzenie kontroli dostępu,

[75] Por. D. Sason, Lessons From the Twitch Data Leak, varonis.com/blog/lessons-from-the-twitch-data-leak (dostęp 18.04.2025).

[76] Por. Capital One, Facts About the 2020 Cyber Incident, capitalone.com/digital/facts2020 (dostęp: 21.04.2025).

[77] Por. Insider Lab, Capital One Data Breach: How SSRF Vulnerability Exposed 100 Million Customer Records, insidersecurity.co/capitalone-data-breach-how-ssrf-vulnerability-exposed-100-million-customer-records (dostęp 18.04.2025).

[78] Por. D. Ennis, Fed Ends Capital One Breach Action, cybersecuritydive.com/news/fed-ends-capital-one-breach-action/686970 (dostęp: 4.05.2025).

wprowadzenie bardziej zaawansowanych protokołów szyfrowania, regularne audyty bezpieczeństwa, testy penetracyjne[79].

Wyciek danych Capital One jest przykładem, jak ważne jest odpowiednie zarządzanie konfiguracją zabezpieczeń, stosowanie zasady najmniejszych uprawnień oraz monitorowanie logów. Pokazuje również, że nawet najbardziej zaawansowane technologicznie organizacje mogą paść ofiarą ataków, jeśli nie będą odpowiednio chronić swoich zasobów w chmurze. Wnioski z tego incydentu podkreślają konieczność ciągłego monitorowania i audytowania konfiguracji systemów, posiadania planu reagowania na incydenty oraz edukacji pracowników w zakresie najlepszych praktyk cyberbezpieczeństwa.

Na przełomie 2020 i 2021 r. doszło do jednego z najbardziej medialnych i problematycznych wycieków danych w świecie platform cyfrowych – OnlyFans, serwisu umożliwiającego twórcom zarabianie pieniędzy na treściach za pośrednictwem subskrypcji. Do sieci trafiło ponad 1,6 terabajta prywatnych materiałów. Wśród ujawnionych danych znalazły się zdjęcia, filmy i inne pliki publikowane przez użytkowników, z których wiele oznaczono jako premium, czyli dostępne wyłącznie dla płacących subskrybentów. Dotyczyło to zarówno anonimowych twórców, jak i znanych osób publicznych, w tym celebrytów takich jak Bella Thorne oraz Cardi B[80].

Treści te pojawiły się na Darknecie[81] oraz w chmurach publicznych, między innymi na Google Drive. Pomimo iż w wycieku znaleziony został ich materiał, to ani Cardi B, ani Bella Thorne nie wypowiedziały się publicznie w tej sprawie. Nie zamieściły oświadczeń na Instagramie, Twitterze czy w innych kanałach[82]. Moim zdaniem kwestie prawne i wizerunkowe związane z wyciekiem były rozwiązane wewnętrznie, aby uniknąć większego nagłośnienia.

OnlyFans oficjalnie zaprzeczył, że doszło do włamania do infrastruktury platformy, a więc nie był to klasyczny atak hakerski z przełamaniem zabezpieczeń systemowych. Dane zostały pozyskane przez subskrybentów z legalnym dostępem do płatnych treści. Pobierali oni pliki hurtowo, korzystając z dostępnych okresów próbnych, promocji, lub nawet darmowych subskrypcji oferowanych tymczasowo przez twórców. Część danych mogła również zostać pobrana przez boty, korzystające z niedoskonałych zabezpieczeń linków do zewnętrznych serwerów hostujących treści multimedialne. W efekcie doszło do masowego zgromadzenia i rozpowszechnienia materiałów. Skala naruszenia była ogromna, zarówno pod względem objętości danych jak i znaczenia ujawnionych treści. Wśród materiałów znalazły się galerie zdjęć

[79] Por. How Did Capital One Respond to Their Major Cyber Incident?, sprintzeal.com/blog/capital-one-cyber-incident (dostęp: 4.05.2025).

[80] Por. L. Abrams, Adult content from hundreds of OnlyFans creators leaked online, https://www.bleepingcomputer.com/news/security/adult-content-from-hundreds-of-onlyfans-creators-leaked-online/ (dostęp: 9.06.2025).

[81] Darknet to część Internetu, która nie jest indeksowana przez standardowe wyszukiwarki i wymaga specjalnego oprogramowania, jak Tor, aby uzyskać do niej dostęp. Służy często do anonimowej komunikacji oraz ukrytej wymiany informacji, najczęściej nielegalnych.

[82] Por. L. Abrams, Adult content from hundreds of OnlyFans creators leaked online, https://www.bleepingcomputer.com/news/security/adult-content-from-hundreds-of-onlyfans-creators-leaked-online/ (dostęp: 9.06.2025).

i nagrań o charakterze osobistym, często intymnym, których autorzy nie przewidywali publikacji poza platformą. Dla wielu twórców oznaczało to nie tylko naruszenie prywatności, ale też utratę kontroli nad swoją marką osobistą i źródłem dochodu[83].

Wielu twórców zgłaszało, że po wycieku doświadczyło fali hejtu oraz utraty poczucia bezpieczeństwa. Utrudniona została także ich dalsza działalność zawodowa, głównie ze względu na spadek zysków. U niektórych poszkodowanych pojawiły się również obawy o możliwość poniesienia konsekwencji rodzinnych, zawodowych lub społecznych w związku z rozpowszechnieniem treści wcześniej ukrywanych przed otoczeniem. OnlyFans, pod presją opinii publicznej i mediów, zapowiedział wzmocnienie środków bezpieczeństwa. Zmiany miały obejmować ograniczenie możliwości pobierania materiałów, wprowadzenie znaków wodnych pozwalających identyfikować źródło przecieku, rozbudowanie systemów wykrywania podejrzanej aktywności oraz współpracę z firmami specjalizującymi się w antypiractwie cyfrowym. Podjęto także próbę monitorowania forów i serwisów przechowujących nielegalne kopie treści, jednak efektywność tych działań została powszechnie zakwestionowana. Wielu twórców oskarżało platformę o spóźnioną, niewystarczającą i reaktywną postawę, która nie zapewniła im realnego wsparcia prawnego ani technicznego[84].

Incydent ten jest przykładem rosnących zagrożeń dla twórców działających w modelu subskrypcyjnym. Zbyt słabe mechanizmy kontroli kopiowania oraz nieuwzględnianie scenariuszy nadużyć przez subskrybentów powodują, że treści premium mogą łatwo wyciec poza zamknięty system. Nawet jeśli infrastruktura systemowa pozostaje nietknięta, słabości wynikające z interakcji z użytkownikami mogą doprowadzić do równie poważnych naruszeń. Potrzebne są nie tylko skuteczne narzędzia techniczne ograniczające kopiowanie, ale także jasne procedury reagowania na wtórne wycieki, wsparcie prawne ofiar oraz edukacja cyfrowa twórców na temat zagrożeń związanych z dystrybucją wrażliwych treści. Tylko w ten sposób możliwe jest odbudowanie zaufania do platform i zapewnienie realnej ochrony użytkowników w przestrzeni cyfrowej.

Kolejnym bardzo medialnym wyciekiem danych w 2023 r. był z Real Estate Wealth Network[85], nowojorskiej platformy edukacyjnej działającej w branży nieruchomości. Był efektem nieodpowiedniej konfiguracji oraz zabezpieczenia bazy danych.

Wywołało to ogromne zainteresowanie mediów i podkreśliło skalę oraz powagę wycieku. Mimo to, żadne z nich nie wydało oficjalnego oświadczenia w tej sprawie ani nie skomentowało incydentu w swoich kanałach społecznościowych lub publicznych wypowiedziach. W tym przypadku doszło do wycieku spowodowanego błędami w konfiguracji zabezpieczeń. REWN nie zabezpieczyło bazy żadnym

[83] Por. J. Kastrenakes, M. Farokhmanesh, OnlyFans says it wasn't hacked after hundreds of performers videos leak online, https://www.theverge.com/2020/2/27/21156445/onlyfans-leak-not-hacked-photos-videos (dostęp: 8.06.2025).

[84] Por. L. Abrams, Adult content from hundreds of OnlyFans creators leaked online, https://www.bleepingcomputer.com/news/security/adult-content-from-hundreds-of-onlyfans-creators-leaked-online/ (dostęp: 9.06.2025).

[85] Od tego momentu będzie używany skrót REWN.

mechanizmem uwierzytelniania, co oznaczało, że każdy użytkownik mający adres URL miał nieograniczony dostęp do danych. Dodatkowo, brak szyfrowania danych przechowywanych w formie jawnej ułatwiał ich kopiowanie i analizę. Natomiast brak systemu monitorowania dostępu uniemożliwiał określenie, jak długo baza była dostępna i czy doszło do nieautoryzowanego pobrania danych. Była ona o wielkości 1,16 terabajta zawierała ponad 1,5 miliarda rekordów, co czyni tę ekspozycję jednym z największych wycieków danych w ostatnich latach. Zakres danych obejmował szczegółowe informacje od kwietnia do października 2023 r., w tym dane osobowe, finansowe, podatkowe, hipoteczne oraz logi systemowe. Ilość i rodzaj ujawnionych danych umożliwiał łatwe powiązanie ich z konkretnymi osobami, w tym milionami użytkowników platformy oraz znanymi postaciami ze świata polityki i rozrywki. Dokładna liczba osób poszkodowanych jest trudna do ustalenia, zwłaszcza że nie wiadomo, przez jaki czas baza była dostępna i czy dane zostały pobrane lub wykorzystane przez nieuprawnione podmioty[86].

Doszło do naruszenia prywatności i narażenia na ryzyko osób fizycznych ujawnione dane osobowe mogły zostać wykorzystane do stalkingu, nękania czy innych form naruszeń prywatności, zwłaszcza w przypadku, wymienionych wyżej osób publicznych. Istniało również wysokie ryzyko wykorzystania danych do oszustw, wyłudzeń kredytów hipotecznych, kradzieży tożsamości oraz ataków socjotechnicznych, które mogły skutkować dodatkowymi stratami dla poszkodowanych. Dla samej firmy REWN incydent oznaczał poważne straty reputacyjne i potencjalne konsekwencje prawne, w tym możliwe kary nałożone zgodnie z przepisami RODO czy amerykańskimi regulacjami, takimi jak CCPA. Media i eksperci mocno krytykowali firmę za brak podstawowych zabezpieczeń, co dodatkowo pogłębiało kryzys wizerunkowy. Po otrzymaniu zgłoszenia od Jeremiaha Fowlera, REWN podjęło natychmiastowe działania. Zablokowano publiczny dostęp do bazy i potwierdzono jej autentyczność, co świadczyło o odpowiedzialności i przejrzystości firmy. Publicznie podziękowano badaczowi, podkreślając znaczenie współpracy z niezależnymi ekspertami ds. bezpieczeństwa. Zapowiedziano także przeprowadzenie szczegółowego audytu kryminalistycznego, mającego na celu ocenę czasu ekspozycji danych oraz potencjalnych szkód. Mimo to, brak jest informacji o zakończeniu audytu oraz dalszych krokach, takich jak powiadomienie osób dotkniętych wyciekiem czy współpraca z organami nadzoru[87].

Incydent wskazuje na konieczność wdrożenia automatycznych systemów monitoringu, szyfrowania danych oraz regularnych testów penetracyjnych i szkoleń personelu. Przypadek z Real Estate Wealth Network to dobitny przykład, jak podstawowe błędy w zabezpieczeniach mogą prowadzić na masową skalę do katastrofalnych skutków bezpieczeństwa danych. Pokazuje, że nawet brak hasła lub

[86] Por. J. Fowler, 1.5 billion records leaked in Real Estate Wealth Network Data breach. Security Info Watch, https://www.securityinfowatch.com/cybersecurity/article/53081265/15-billion-records-leaked-in-real-estate-wealth-network-data-breach (dostęp: 9.06.2025).

[87] Por. M. Baram, *Essential steps for protection in the aftermath of recent data breaches. Craincurrency*, https://www.craincurrency.com/family-office-management/essential-steps-protection-aftermath-recent-data-breaches (dostęp: 9.06.2025).

szyfrowania może wystarczyć, by miliony rekordów znalazły się w rękach nieuprawnionych osób.

Przeprowadzona analiza pokazała, że chmura obliczeniowa ma duży potencjał w zakresie zapewniania bezpieczeństwa danych, jednak jego skuteczne wykorzystanie zależy od wielu czynników. Najczęściej wyciekały dane osobowe, informacje finansowe, poufne dane firmowe oraz wizerunkowe, co niosło za sobą poważne konsekwencje prawne, związane z naruszeniem RODO. Utrata zaufania klientów była dla wielu organizacji równie dotkliwa jak same straty materialne. W odpowiedzi na rosnące zagrożenia firmy zaczęły coraz więcej inwestować w rozwiązania zabezpieczające.

Analiza naruszeń danych w latach 2020–2024 ujawnia, że najczęstszymi przyczynami incydentów są błędy konfiguracyjne, brak uwierzytelniania wieloskładnikowego oraz luki w infrastrukturze chmurowej. W wielu sytuacjach przyczyną problemów były również zaniedbania ze strony użytkowników końcowych, np. niewłaściwe zarządzanie hasłami czy ignorowanie procedur.

Przytoczone w artykule incydenty pokazują, że zarówno problemy techniczne, jak i błędy ludzkie mogą prowadzić do poważniejszych konsekwencji. Dowodzą, że zaawansowane technologie to za mało. Skuteczna ochrona danych wymaga przeprowadzania audytów, wdrażania szyfrowania, stosowania MFA oraz zasady minimalnych uprawnień. Ważnym elementem zarządzania ryzykiem jest również szybka reakcja na incydenty oraz jasna komunikacja z osobami poszkodowanymi.

BIBLIOGRAFIA

Źródła

Strony internetowe

Amazon Web Services, About AWS, https://aws.amazon.com/about-aws/ (dostęp: 24.11.2024).

Apple, https://www.apple.com/pl/legal/privacy/pl/governance/ (dostęp: 6.01.025).

Apple, iCloud Overview, https://www.apple.com/icloud/ (dostęp: 24.11.2024).

Apple Support, Security and Privacy of Apple iCloud, 16 września 2024, https://support.apple.com/en-us/102651 (dostęp: 24.11.2024).

Capital One data breach overview, https://www.capitalone.com/facts2024 (dostęp: 18.04.2025).

Data breach notification, notification.gov.pl (dostęp: 7.04.2025).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80).

Google Support, Google Drive overview, https://support.google.com/drive/answer/10375054 (dostęp: 24.11.2024).

Kaspersky Security Bulletin 2024, kaspersky.com/security-bulletin-2024 (dostęp: 19.02.2025).

Kişisel Verileri Koruma Kurumu – Turecka ustawa o ochronie danych osobowych z dnia 24 marca 2016 r. nr 6698 (Resmî Gazete z dnia 7 kwietnia 2016 r., poz. 29677).

Microsoft Azure Overview, https://azure.microsoft.com/en-us/overview/ (dostęp: 24.11.2024).

Microsoft Security Blog, https://techcommunity.microsoft.com/t5/security-compliance-and-identity/bg-/SecurityCompliance (dostęp: 10.02.2025).

Norton Security Blog, https://us.norton.com/internetsecurity-how-to-cloud-computing-security.html (dostęp: 9.02.2025).
Salesforce, What is cloud computing?,https://www.salesforce.com/uk/learning-centre/cloud-computing/ (dostęp: 19.11.2024).
SecurityWeek, https://www.securityweek.com/data-breaches/ (dostęp: 18.04.2025).
ServiceNow Cloud Services, https://www.servicenow.com/products/cloud-computing.html (dostęp: 24.11.2024).
Salesforce, What is cloud computing?, https://www.salesforce.com/uk/learning-centre/cloud-computing (dostęp: 19.11.2024)
Symantec Cloud Security, https://www.symantec.com/security-center/cloud-security (dostęp: 9.02.2025).
Traktat ustanawiający Europejską Wspólnotę Gospodarczą (Dz. U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.).
Trend Micro Cloud Security Report, https://www.trendmicro.com/cloud-security-report-2024 (dostęp: 15.01.2025).
Ustawa z dnia 1 grudnia 2022 r. o zmianie ustawy o prawach konsumenta oraz niektórych innych ustaw (Dz.U. 2022 poz. 2581).
Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (Dz.U. 2014 poz. 827).

Literatura i opracowania

Amini, M., Safavi, N. S., Dashti Khavidaki, S. M., Abdollahzadegan, A., Type of Cloud Computing Public and Private That Transform The Organization More Effectively, https://shorturl.at/wdDYT (dostęp: 19.11.2024).
Baram, M., Essential steps for protection in the aftermath of recent data breaches, Craincurrency, https://www.craincurrency.com/family-office-management/essential-steps-protection-aftermath-recent-data-breaches (dostęp: 9.06.2025).
Cambronero M. E., Martínez M. A., Llana, L., Rodríguez, R. J., Russo A., Dostępne na: https://pmc.ncbi.nlm.nih.gov/articles/PMC11041943/ (dostęp: 7.01.2025).
Centralny Ośrodek Informatyki – POPC Wsparcie, Co to jest chmura obliczeniowa? Portal Gov.pl., https://www.gov.pl/web/popcwsparcie/co-to-jest-chmura-obliczeniowa (dostęp: 20.11.2024).
Determann L., What Happens in the Cloud: Software as a Service and Copyrights, https://lawcat.berkeley.edu/nanna/record/1126823/files/fulltext.pdf?withWatermark=0&withMetadata=0&registerDownload=1&version=1 (dostęp: 5.02.2025).
Dolny T., Consumers in the cloud: EU consumer protection in cloud computing contracts, https://cris.maastrichtuniversity.nl/en/publications/consumers-in-the-cloud-eu-consumer-protection-in-cloud-computing- (dostęp: 13.01.2025).
EY Polska, Co to jest chmura obliczeniowa? Definicja, przykłady, zalety, https://www.ey.com/pl_pl/insights/digital-first/co-to-jest-chmura-obliczeniowa (dostęp: 21.11.2024).
Fowler, J., 1.5 billion records leaked in Real Estate Wealth Network Data breach. Security Info Watch, https://www.securityinfowatch.com/cybersecurity/article/53081265/15-billion-records-leaked-in-real-estate-wealth-network-data-breach (dostęp: 9.06.2025).
Fowler, J., 1.5 billion records leaked in Real Estate Wealth Network Data breach. vpnMentor, https://www.vpnmentor.com/news/report realestatewealthnetwork-breach/ (dostęp: 9.06.2025).
Gatlan S., Toyota Confirms Third-Party Data Breach Impacting Customers, bleepingcomputer.com/news/security/toyota-confirms-third-party-data-breach-impacting-customers (dostęp: 3.04.2025).
Gebremeskel B., Understanding the Snowflake Data Breach: What Happened and What Is Affected, teckpath.com/understanding-the-snowflake-data-breach-what-happened-and-what-is-affected (dostęp: 25.03.2025).
Google Cloud & the General Data Protection Regulation (GDPR), https://cloud.google.com/privacy/gdpr (dostęp: 15.01.2025).
Google Support, About Google Drive, https://support.google.com/drive/answer/10375054?hl=en (dostęp: 24.11.2024).
Green D., Snowflake Retro: Analyzing the Breach, pushsecurity.com/blog/snowflake-retro (dostęp: 25.03.2025).

Kanungo S., Data Privacy and Compliance Issues in Cloud Computing: Legal and Regulatory Perspectives, https://www.ijisae.org/index.php/IJISAE/article/view/5710 (dostęp: 10.02.2025).

Kariyawasam K., Talagala C., Cloud Computing and the Future of Copyright Law, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3110398 (dostęp: 4.02.2025).

Kastrenakes J., Farokhmanesh M., OnlyFans says it wasn't hacked after hundreds of performers videos leak online, https://www.theverge.com/2020/2/27/21156445/onlyfans-leak-not-hacked-photos-videos (dostęp: 8.06.2025).

Kolevski D., Michael K., Abbas R., Freeman M., Dostęp:ne na: https://par.nsf.gov/servlets/purl/10344523 (dostęp: 12.01.2025).

Lerner J., Rafert G., Are consumers well protected in cloud computing contracts?, https://www.maastrichtuniversity.nl/blog/2024/03/are-consumers-well-protected-cloud-computing-contracts (dostęp: 9.02.2025).

Lerner J., Rafert G., Lost in the Clouds: The Impact of Copyright Scope on Investment in Cloud Computing Ventures, https://www.hbs.edu/faculty/Pages/item.aspx?num=43482 (dostęp: 2.02.2025).

Malkowski, S., Charakter prawny umowy Software as a Service w polskim systemie prawnym, https://repozytorium.uni.wroc.pl/Content/136425/PDF/06_S_Malkowski_Charakter_prawny_umowy_Software_as_a_Seervice_w_polskim_systemie_prawnym.pdf (dostęp: 10.02.2025).

Mathew, S., AWS Overview, listopad 2014, https://www.sysfore.com/Assets/PDF/aws-overview.pdf (dostęp: 24.11.2024).

McGillivray K., A right too far? Requiring cloud service providers to deliver adequate data security to consumers, https://academic.oup.com/ijlit/article/25/1/1/2525429?login=false (dostęp: 6.02.2025).

Melzer M. A., Copyright Enforcement in the Cloud, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1492&context=iplj (dostęp: 3.02.2025).

Molloy D., Tidy T., Twitch: Data Breach Reveals Pay for Top Streamers, bbc.com/news/technology-58817658 (dostęp: 14.04.2025).

Paganini P., ZeroSevenGroup – Toyota Data Breach, securityaffairs.com/167274/data-breach/zerosevengroup-toyota-data-breach.html (dostęp: 7.04.2025).

Pande Joshi K., Elluri L., Consumer Protection in Cloud Computing Services: Recommendations for Best Practices from a Consumer Federation of America Retreat on Cloud Computing, https://consumerfed.org/pdfs/Cloud-report-2010.pdf (dostęp: 14.01.2025).

Pegasus Airlines Breach Exposes 6.5 TB of Data, bankinfosecurity.com/pegasus-airlines-breach-exposes-65-tb-data-a-19173 (dostęp: 7.04.2025).

StrongDM Team, Snowflake Data Breach – What Happened & How to Prevent It, strongdm.com/what-is/snowflake-data-breach (dostęp: 25.03.2025).

Sason D., Lessons From the Twitch Data Leak, varonis.com/blog/lessons-from-the-twitch-data-leak (dostęp: 18.04.2025).

Szpor G., *Internet Cloud Computing, Przetwarzanie w chmurach*.

Twitch Live Streaming Data Breach 2021, mitnicksecurity.com/blog/twitch-live-streaming-data-breach-2021 (dostęp: 14.04.2025).

Literatura pomocnicza

Fortuna A., Jurysdykcja w sprawach z zakresu prawa autorskiego w chmurze obliczeniowej, https://skubisz.pl/jurysdykcja-w-sprawach-z-zakresu-prawa-autorskiego-w-chmurze-obliczeniowej/ (dostęp: 11.02.2025).

Kariyawasam K., Talagala C., Contracts for Clouds, Revisited: An Analysis of the Standard Contracts for 40 Cloud Computing Services, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3624712 (dostęp: 11.01.2025).

Krasuski A., *Chmura obliczeniowa. Prawne aspekty zastosowania*, Wolters Kluwer, Warszawa 2017.

Kruk M., Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa, https://repozytrium.uni.wroc.pl/Content/122487/PDF/04_Obowiazki_dostawcow_uslug_cyfrowych.pdf (dostęp: 11.02.2025).

Insider Lab, Capital One Data Breach: How SSRF Vulnerability Exposed 100 Million Customer Records, insidersecurity.co/capitalone-data-breach-how-ssrf-vulnerability-exposed-100-million-customer-records (dostęp: 18.04.2025).

Understanding the Snowflake Data Breach and Its Implications, kosmos.com/authentication/understanding-the-snowflake-data-breach-and-its-implications (dostęp: 3.04.2025).

Wiśniewska K., Przechowywanie danych w chmurze w perspektywie dyrektywy w sprawie niektórych aspektów umów o dostarczenie treści cyfrowych i usług, https://uokik.gov.pl/Download/554 (dostęp: 9.02.2025).

CLOUD DATA BREACH ANALYSIS BASED ON SELECTED INCIDENTS FROM 2020 TO 2024

Summary

This article addresses data security issues in the cloud computing environment, with particular emphasis on legal aspects and examples of data breach incidents from 2020 to 2024. The aim of the paper is to highlight the main threats arising from cloud computing, assess the effectiveness of current legal regulations, and analyze the practices employed by cloud service providers and users regarding information protection. The publication discusses, among other things, basic concepts related to cloud computing, its history, evolution, and typologies; cloud service implementation models; and the technical architecture of cloud systems. Furthermore, it analyzes the legal provisions applicable to cloud computing, discussing key regulations such as the GDPR, the Act on the National Cybersecurity System, and copyright issues. The conclusions from the analysis confirm that the effectiveness of data protection in the cloud depends not only on the technologies used but also on the level of user awareness, correct service configuration, and compliance with applicable regulations. Data protection in cloud computing requires an integrated approach that combines legal, technical, and organizational aspects.

Key words: cloud, data, security, protection, services, GDPR

Nota o Autorce

Emilia RYBICKA – absolwentka studiów licencjackich na kierunku dziennikarstwo i komunikacja społeczna na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie.
Kontakt email: erybicka03@gmail.com