DOI: 10.38146/BSZ-AJIA.2026.v74.i1.pp121-143

Kiberbiztonság a felhőiparban

Jogi kötelezettségek és felelősség az európai szabályozás és a technológiai fejlődés tükrében

Cybersecurity in Cloud Industry: Legal Obligations and Liabilities under European Regulations & Technological Advancements

Khraisha Wasim
Dr., jogász, doktorandusz
Károli Gáspár Református Egyetem,
Állam- és Jogtudományi Doktori Iskola
wasimkhraisha@gmail.com

Absztrakt

Cél: A tanulmány a felhőalapú számítástechnika (cloud computing) alkalmazásával összefüggő kiberbiztonsági sebezhetőségeket, valamint az ezek kezelésére irányuló európai uniós jogi szabályozásokat vizsgálja. Az írás áttekinti a felhőalapú környezetben felmerülő felelősségi és jogi kérdéseket, bemutatja a felhőszolgáltatásban részt vevő szereplők – különösen az adatkezelők és adatfeldolgozók – szerepét, továbbá elemzi, hogy a szerződéses eszközök, így különösen a szolgáltatási szintmegállapodások (Service Level Agreements, SLA) miként járulhatnak hozzá a kiberbiztonsági kockázatok mérsékléséhez. A tanulmány kitér a felhőbiztonságot alakító aktuális technológiai trendekre, így a mesterséges intelligencia és a blokklánc-technológia szerepére.

Módszertan: A kutatás doktrinális jogelemzési módszert alkalmaz, amelynek keretében szisztematikusan elemzi a releváns európai uniós jogszabályokat (különösen az általános adatvédelmi rendeletet – GDPR, a NIS2 irányelvet és a kiberbiztonsági rendeletet), a kapcsolódó szerződéses keretrendszereket, valamint a vonatkozó tudományos szakirodalmat. A források kiválasztása azok szakmai tekintélye, relevanciája és időszerűsége alapján történt, kifejezetten

Magyar nyelvű utánközlés. Jelen cikk angol változata megjelent a Belügyi Szemle 2026. évi 1. számában. DOI link: https://doi.org/10.38146/BSZ-AJIA.2026.v74.i1.pp193-210

a kiberbiztonsági kötelezettségekre, a felelősségi kérdésekre és az olyan feltörekvő technológiákra összpontosítva, mint a mesterséges intelligencia és a blokklánc. Az összehasonlító elemzés és a szintézis révén a tanulmány feltárja a felhőalapú kiberbiztonságot érintő kulcsfontosságú jogértelmezési kérdéseket és technológiai hatásokat.
Megállapítások: A felhőalapú környezetben a kiberbiztonság biztosítása megvalósítható, ugyanakkor rendkívül összetett feladat. A biztonság fenntartása a felhőszolgáltatásban részt vevő felek megosztott felelőssége, miközben számos jogi és gyakorlati kihívás, illetve szabályozási hiányosság továbbra is fennáll. Éppen ezért a technológiai innovációk alkalmazása – az általuk kínált lehetőségek révén – jelentősen hozzájárulhat a felhőbiztonság szintjének növeléséhez. Megfelelő alkalmazás esetén e megoldások összességében erősítik a felhőkörnyezet biztonságát, ami meghatározó jogi és gazdasági következményekkel jár a piaci szereplők számára.
Érték: Az utóbbi években a felhőalapú számítástechnika általános célú technológiává vált, amelynek hatása és elterjedtsége a gazdaság valamennyi ágazatára kiterjed. Ennek fényében a felhőkörnyezet átfogó kiberbiztonsága kiemelt jelentőséggel bír. Bár a jogszabályi keretek és az új technológiák ígéretes lehetőségeket kínálnak a kiberbiztonsági fenyegetések és rosszindulatú magatartások észlelésére és bizonyítására a felhőökoszisztémában, alkalmazásuk új jogi és technikai kérdéseket is felvet. A tanulmány rámutat több kulcsfontosságú felhőbiztonsági követelmény szükségességére, így különösen az előzetes szerződéskötési kockázatértékelésekre, a szabályozás hatékonyságának javítására, valamint megbízható kiberbiztonsági tanúsítási rendszerek kialakítására. Mindez összességében hozzájárul a felhőkörnyezet biztonságának erősítéséhez.

Kulcsszavak: felhőalapú számítástechnika, kiberbiztonság, adatvédelem, GDPR

Abstract

Aim: This article examines the cybersecurity weaknesses associated with cloud computing and the relevant legal regulations within the European Union that address these issues. The topic looks into the responsibilities and legal issues surrounding cloud cybersecurity. It explains the roles of cloud actors, such as controllers and processors, and how contracts – such as Service Level Agreements (SLAs) – can help mitigate cybersecurity threats. Finally, the paper addresses the contemporary trends shaping cloud security, such as artificial intelligence (AI) and blockchain technology.
Methodology: This article utilizes a doctrinal legal analysis method, systematically reviewing relevant European regulations (GDPR, NIS2 Directive,

Cybersecurity Act), contractual frameworks, and academic literature. Sources were selected based on their authority, relevance, and currency, focusing specifically on cybersecurity obligations, liability issues, and emerging technologies like AI and Blockchain. Through comparative analysis and synthesis, the research identifies key legal interpretations and technological impacts on cloud cybersecurity.
Findings: Ensuring cybersecurity in the cloud environment is possible, but it remains a complex task. It is a shared responsibility of the cloud parties. However, many gaps and challenges may still exist. That is why employing technological innovations would enhance the security levels in the cloud thanks to the capabilities they offer. Generally, when applied properly, these measures and techniques would improve the overall security of the cloud environment, leading to crucial legal and economic outcomes for the cloud stakeholders in the market.
Value: Recently, cloud-computing technology has been evolving as a general-purpose technology whose impact and adoption spans all sectors of the economy. Crucially, its overall cybersecurity is a pivotal concern. While regulations and technologies offer exciting potential pathways for detecting and proving cybersecurity threats and malicious behaviors in the cloud ecosystem, their deployment raises new legal and technical concerns. This article calls attention to the need for several cloud security requirements, such as pre-contractual risk assessments, improved regulatory effectiveness, and the establishment of credible cybersecurity certification systems. Ultimately, this contributes to enhancing the overall security of the cloud environment.

Keywords: Cloud Computing, Cybersecurity, Data Protection, GDPR

Bevezetés

Napjainkban a felhőipar – az általa kínált előnyök és szolgáltatások következtében – egyre nagyobb jelentőséggel bír mind a vállalatok, mind az egyének számára. A vállalati szektor számára a felhő alapvető eszközzé vált, mivel lehetővé teszi különféle szolgáltatások – így számítási kapacitás, adattárolás és adatbázisok – igény szerinti elérését olyan ismert felhőszolgáltatóktól, mint az Amazon Web Services, a Microsoft Azure vagy az Alibaba, anélkül, hogy a szervezeteknek saját fizikai adatközpontokat és szervereket kellene vásárolniuk, birtokolniuk és fenntartaniuk (McGillivray, 2022).

A felhőalapú technológia a számítástechnikai szolgáltatások interneten keresztüli nyújtását jelenti, amely magában foglalja a szoftvereket, adatbázisokat, szervereket,

adattárolást és egyéb informatikai erőforrásokat, igény szerinti hozzáféréssel és használatarányos díjazással. Ezáltal megszűnik a fájlok és szolgáltatások helyi adathordozókon történő kezelésének szükségessége, ami költséghatékony alternatívát kínál (Dagostino, 2019). Ennek alapján a felhőtechnológia olyan számítástechnikai modellként írható le, amelyben az egyes vállalkozások harmadik félre bízzák adataik és számítási folyamataik kezelését az interneten keresztül.

A felhőszolgáltatók (Cloud Service Providers – CSP) olyan vállalatok, amelyek biztonságos, megbízható és skálázható számítási kapacitást biztosítanak megosztott adatközpontokon keresztül, amelyekhez a felhasználók távoli hozzáféréssel csatlakozhatnak (Millard, 2021). A felhőtechnológia bevezetése jelentős mértékben arra kényszerítette a különböző intézményeket, hogy újraértékeljék kiberbiztonsági szintjüket, mivel az adatok és alkalmazások gyakran egyidejűleg helyi és távoli rendszerek között oszlanak meg, ami új kihívásokat és lehetőségeket teremt az adatvédelem és a bizalom területén (Lynn, et al., 2021).

A rendszerek és az adatok folyamatosan elérhetők az internet révén; például az olyan szolgáltatásokon keresztül, mint a Google Docs, okostelefonon elért adatok a világ különböző pontjain található helyszíneken kerülhetnek tárolásra. Ennek következtében az adatok védelmének biztosítása lényegesen összetettebbé vált, mint amikor pusztán a jogosulatlan hálózati hozzáférés megakadályozásáról volt szó (Millard, 2021).

A felhőszolgáltatások kiberbiztonsága két alapvető okból vált különösen kritikus jelentőségűvé. Egyrészt a felhőipar exponenciális növekedést mutat, és mind a személyes, mind a vállalati szintű alkalmazások domináns platformjává vált. Az innováció lehetővé tette, hogy az új technológiák gyorsabban fejlődjenek, mint az iparági szintű biztonsági szabványok, ami fokozott felelősséget ró a felhasználókra a hozzáféréssel kapcsolatos biztonsági kockázatok értékelése terén. Másrészt a központosított, több bérlőt kiszolgáló adattárolási rendszerek lehetővé teszik, hogy az alapvető infrastruktúrától kezdve az egyéni szintű adatokig – például e-mailekig és dokumentumokig – minden távolról, webalapú kapcsolatokon keresztül, a nap 24 órájában elérhető legyen. Az adatok ilyen mértékű koncentrációja néhány nagy szolgáltató szerverein jelentős kockázatot hordoz, mivel a fenyegetést jelentő szereplők nagyméretű, több vállalat adatait kezelő adatközpontokat célozhatnak meg, ami súlyos adatvédelmi incidensekhez vezethet (Rittinghouse & Ransome, 2010).

A tanulmány azt vizsgálja, miként hatnak egymásra a jogi keretrendszerek és a technológiai fejlődés az adatvédelmi kötelezettségek kialakításában, hogyan oszlanak meg a kiberbiztonsági felelősségek a felhőszolgáltatók és az ügyfelek között, valamint milyen felelősségi következményekkel járhatnak az adatvédelmi incidensek.

Áttekintés: a felhőbiztonsági kockázatok tájképe és a jogi biztosítékok szerepe

Az adatok egészének vagy egy részének felhőbe történő áthelyezése azzal jár, hogy az ügyfél elveszíti kizárólagos ellenőrzését az adatok felett, ami szükségessé teszi hatékony intézkedések alkalmazását azok integritásának és bizalmasságának biztosítása érdekében, illetve annak ellenőrzésére, hogy az adatkezelés és az adattárolás megfelelő módon történik-e (McGillivray, 2022). A megosztott környezetekben – így különösen a felhőalapú számítástechnikában – kiemelt jelentőséggel bír az erőforrások megfelelő elkülönítése, az adatok kategorizálása, valamint az erős biztonsági intézkedések alkalmazása (Eryurek et al., 2021).

A felhőben alkalmazott gyenge biztonsági intézkedések a felhasználókat számos kiberbiztonsági fenyegetésnek tehetik ki. A leggyakoribb kockázatok közé tartoznak a felhőalapú infrastruktúrát érintő veszélyek, mint például az elavult vagy nem kompatibilis informatikai keretrendszerek, illetve a harmadik fél által nyújtott adattárolási szolgáltatások kiesései. A belső fenyegetések gyakran emberi hibából erednek, például a felhasználói hozzáférési jogosultságok helytelen konfigurálásából, míg a külső fenyegetések szinte kizárólag hackerek tevékenységéhez köthetők, ide értve a rosszindulatú szoftvereket és vírusokat is (Lynn et al., 2021).

A rosszindulatú szereplők és hackerek gyakran gyenge hitelesítési adatok kihasználásával jutnak be a hálózatokba. Amint hozzáférést szereznek, a nem megfelelően védett felhőinterfészek révén tovább bővíthetik tevékenységi körüket, és különböző adatbázisokban tárolt adatokat lokalizálhatnak. Előfordulhat továbbá, hogy a felhőszervereket a jogellenesen megszerzett adatok tárolására és továbbítására használják (Dagostino, 2019).

Az adatok harmadik felek általi, online környezetben történő tárolása és elérése további kockázatokat is magában hordoz. Amennyiben ezek a szolgáltatások bármilyen okból megszakadnak, a felhasználók elveszíthetik az adataikhoz való hozzáférést. Például egy távközlési hálózat kiesése akadályozhatja a felhőszolgáltatásokhoz való időben történő hozzáférést, vagy egy áramkimaradás érintheti azt az adatközpontot, ahol az adatok tárolásra kerülnek, ami akár végleges adatvesztéshez is vezethet (Rittinghouse & Ransome, 2010).

E kockázatok és kihívások kezelése és mérséklése érdekében a felhőszolgáltatásban részt vevő szereplőkre számos jogi kötelezettség hárul, amelyek célja a felhőkörnyezetben tárolt adatok kiberbiztonságának biztosítása.

A felhőalapú kiberbiztonság jogi keretei: kötelezettségek és a felelősség megosztása

Az Európai Unió Általános Adatvédelmi Rendelete (GDPR)

Az általános adatvédelmi rendelet (GDPR) az Európai Unió adatvédelmi és magánéletvédelmi szabályozása, amely 2018 májusától alkalmazandó, és célja az egyének személyes adataik feletti ellenőrzésének megerősítése, valamint szigorú megfelelési kötelezettségek előírása a személyes adatokat kezelő szervezetek számára (Voigt & von dem Bussche, 2017). A rendelet jelentős rendelkezéseket tartalmaz a biztonsági hiányosságokkal, adatvédelmi incidensekkel és a digitális környezet általános biztonságával kapcsolatban.

A felhőszolgáltatást igénybe vevő fél – például egy felhőszolgáltatásokat használó intézmény – adatkezelőnek minősül, mivel ő határozza meg az adatkezelés célját, módját és jogalapját (GDPR 4. cikk 7. pont). Ennek megfelelően az adatkezelő felelősséggel tartozik a rendelet megsértéséből, a megfelelési kötelezettségek elmulasztásából vagy nem megfelelő teljesítéséből eredő jogsértésekért (Millard, 2021). A másik szereplő az adatfeldolgozó, amely a felhőkörnyezetben jellemzően a felhőszolgáltató (CSP). Az adatfeldolgozóval szemben szintén több biztonsági kötelezettséget ír elő a GDPR, amelyek célja az adatkezelés jogszerűségének és biztonságának biztosítása (Dagostino, 2019).

Az adatbiztonság erősítését szolgáló kötelezettségek elsősorban abból az alapelvből fakadnak, hogy az adatkezelőknek és adatfeldolgozóknak *„megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk annak biztosítása és igazolása érdekében, hogy az adatkezelés e rendeletnek megfelelően történik”* [GDPR 32. cikk (1) bekezdés]. Következésképpen e követelmények figyelmen kívül hagyása vagy elmulasztása az adatkezelő, az adatfeldolgozó vagy mindkét fél felelősségét megalapozhatja (GDPR 4–5. cikk).

A személyes adatok harmadik országokba vagy nemzetközi szervezetekhez történő továbbítása a felhőkörnyezetben jelentős kiberbiztonsági kockázatokat hordozhat. Mivel a felhőszolgáltatások tipikusan magukban foglalják az adatok több földrajzi helyszínen és több felhőn keresztül történő továbbítását, feldolgozását és tárolását, az adatok e folyamatok során különféle fenyegetéseknek lehetnek kitéve (Lynn et al., 2021). A GDPR a 44–50. cikkeiben gyakorlati szabályozási keretet biztosít az ilyen adattovábbításokra. A felhőszolgáltatásban részt vevő szereplők kötelesek e rendelkezések betartására annak érdekében, hogy megfelelő kiberbiztonsági szintet biztosítsanak. Ugyanakkor számos kihívás merül fel, mivel a GDPR nem határozza meg pontosan az „adattovábbítás” fogalmát, ami megnehezítheti a megfelelést a felhőszereplők számára. További

bizonytalanságot okoz, hogy e szabályok alkalmazandók-e akkor, amikor az adatfeldolgozó nem uniós adatkezelő nevében jár el, ami a felhőalapú tranzakciókban gyakori jelenség. Ezenfelül az ilyen szigorú kötelezettségek akadályozhatják a felhőszolgáltatók működési hatékonyságát is (Millard, 2021).

Kiemelt jelentőségű kötelezettség továbbá a felhőben tárolt adatokat érintő adatvédelmi incidensek kezelése. A GDPR e körben kulcsfontosságú rendelkezéseket vezetett be. Az adatkezelő köteles a tudomásszerzést követően indokolatlan késedelem nélkül, de legkésőbb 72 órán belül értesíteni a felügyeleti hatóságot az adatvédelmi incidensről. Hasonlóképpen az adatfeldolgozó – illetve a felhőszolgáltató – köteles az incidensről indokolatlan késedelem nélkül tájékoztatni az adatkezelőt attól az időponttól kezdve, amikor arról tudomást szerez (GDPR 33–34. cikk).

A GDPR-t az Európai Unió adatvédelmi és kiberbiztonsági szabályozásának egyik alappilléreként tartják számon. Ugyanakkor a szakirodalomban eltérő vélemények fogalmazódnak meg arra vonatkozóan, hogy a rendelet mennyire egyértelmű és mennyire alkalmazható a felhőalapú számítástechnika sajátosságaira. A támogatók szerint a GDPR erős és rugalmas keretet biztosít a felhőkörnyezet adatbiztonságának megőrzésére, különösen a 24., 28., 32. és 82. cikkek révén, amelyek világosan meghatározzák az adatkezelők és adatfeldolgozók kötelezettségeit és felelősségét. E megközelítés ösztönzi a felhőszolgáltatásokat igénybe vevőket és a szolgáltatókat a legjobb biztonsági gyakorlatok alkalmazására, kockázatelemzések elvégzésére, valamint arra, hogy szerződéses eszközök – például adatfeldolgozási megállapodások (Data Processing Agreements, DPA) – útján biztosítsák az elszámoltathatóságot. Az incidensbejelentési kötelezettségek (33–34. cikk) bevezetése szintén jelentős előrelépésnek tekinthető a kockázatokra adott válaszok terén (Dagostino, 2019).

Ezzel szemben a kritikus álláspontok szerint a GDPR egyes fogalmi meghatározásai – különösen a nemzetközi adattovábbítás és a közös adatkezelők szerepe – továbbra is homályosak a felhőalapú környezetben. Ez nehézségeket okoz a megfelelés kikényszerítésében és a felelősség pontos meghatározásában. Például a 44. cikk szerinti „adattovábbítás" fogalmának hiányos meghatározása megnehezíti a több joghatóságban működő felhőszolgáltatók számára a szabályozási követelmények teljesítését. Millard (2021) szerint ez a bizonytalanság az extraterritoriális alkalmazást is veszélyezteti, mivel kiszámíthatatlanságot teremt a nem uniós felhőszereplők – különösen a nem uniós adatkezelők nevében eljáró adatfeldolgozók – számára (Kuner, 2020). Továbbá bár a GDPR rögzíti az elszámoltathatóság elvét, kevés gyakorlati útmutatást ad arra vonatkozóan, hogy a felhőszereplők miként alkalmazzák azt több bérlős felhőkörnyezetben (Carey, 2018).

A Marriott International, a British Airways és a Capital One ügyei valós példákként szolgálnak arra, miként alkalmazzák a hatóságok a GDPR egyes rendelkezéseit – különösen a 32. cikket – a személyes adatok megfelelő védelmének megkövetelése érdekében. Bár e döntések a rendelet érvényesíthetőségét igazolják, egyúttal azt is mutatják, hogy a felelősség jellemzően az adatkezelőt terheli, még összetett felhőalapú konstrukciók esetén is. A kritikusok szerint ez a felelősségi allokáció nem minden esetben áll összhangban azzal a technikai valósággal, amelyben a felhőszolgáltatók jelentős operatív ellenőrzéssel rendelkeznek (URL1).

Összességében a kiberbiztonsági incidensekért fennálló felelősség meghatározása a felhőkörnyezetben kiemelten összetett és problémás kérdés, tekintettel a felhőműködés komplexitására és az ökoszisztémában részt vevő számos szereplőre. A GDPR ugyanakkor hasznos rendelkezéseket tartalmaz a felelősség megállapítására. Alapvetően az adatkezelő felelős minden olyan kárért, amely a GDPR-ral ellentétes adatkezelési műveletek következtében keletkezik. Az adatfeldolgozó kizárólag akkor vonható felelősségre, ha nem tartotta be a rendelet rá vonatkozó kötelezettségeit, vagy az adatkezelő utasításait túllépve, illetve azokkal ellentétesen járt el. Mind az adatkezelő, mind az adatfeldolgozó mentesül a felelősség alól, ha bizonyítani tudja, hogy a kárt okozó eseményben nem vett részt. Amennyiben ugyanazon jogellenes adatkezelés több adatkezelő vagy adatfeldolgozó – vagy mindkettő – közreműködésével okoz kárt, valamennyi érintett fél egyetemlegesen felel a teljes kárért. Az a fél, amely a kártérítés egészét vagy egy részét megfizette, jogosult a többi érintett adatkezelővel vagy adatfeldolgozóval szemben regressz igényt érvényesíteni a felelősségük arányában (GDPR 82. cikk).

Mindazonáltal, bár a GDPR megalapozta a felhőalapú kiberbiztonság jogi keretrendszerét, a tudományos diskurzus rámutat arra, hogy további pontosításra van szükség, különösen a közös adatkezelés, a nemzetközi adattovábbítás és az adatkezelő–adatfeldolgozó viszony tekintetében. A felhőalapú számítástechnika folyamatos fejlődésével elengedhetetlenek lesznek a további jogalkotási és szakpolitikai fejlemények e kérdések kezeléséhez, és a GDPR felhőkörnyezetben történő alkalmazásának finomításához.

A hálózati és információs rendszerek biztonságáról szóló irányelv (NIS2)

A NIS2 irányelv az Európai Unió egyik legjelentősebb jogszabálya a digitális környezetek kiberbiztonságának szabályozása terén. Elsődleges célja az uniós kiberbiztonsági szint emelése. Az irányelv a 2016-ban elfogadott eredeti NIS irányelvet váltotta fel, amely számos joghézagot tartalmazott, és jelentős végrehajtási nehézségeket okozott. E hiányosságok, valamint a kiberbiztonsági

kockázatok és incidensek számának növekedése indokolttá tették egy korszerűsített szabályozás megalkotását. A NIS2 irányelvet hivatalosan 2022-ben fogadták el, célja az ellenálló képesség növelése és az uniós kiberbiztonsági feltételek megerősítése (URL2).

Az irányelv egyik legfontosabb jogi újítása, amely közvetlenül hozzájárul a felhőkörnyezetben történő megfelelés javításához, hogy a felhőszolgáltatókat (CSP-ket) „lényeges szervezetekként" határozza meg, és ennek megfelelően szigorúbb, részletesebb biztonsági kötelezettségeket ír elő számukra. E kötelezettségek közé tartozik a kockázatértékelési kötelezettség, az incidensek megfelelő formában történő jelentése, valamint átfogó kiberbiztonsági programok alkalmazása (Hon, 2018).

A NIS2 különös hangsúlyt fektet az ellátási lánc biztonságára, amely a felhőökoszisztémában kiemelt jelentőségű, mivel az adatfeldolgozás és adattárolás gyakran több, földrajzilag eltérő helyen található szerveren történik. A felhőszolgáltatások jellemzően összetett hálózatokon működnek, amelyek számos szolgáltatót, infrastruktúra-beszállítót, különböző értékesítőket és alvállalkozókat foglalnak magukban a biztonságos szolgáltatásnyújtás érdekében (Millard, 2021). Következésképpen e hálózatok bármely gyenge pontja vagy sebezhetősége súlyos kiberbiztonsági kockázatokhoz és incidensekhez vezethet, valamint hátrányosan befolyásolhatja a felhőszolgáltatók piaci hatékonyságát és megbízhatóságát. A NIS2 rendelkezései értelmében a felhőszolgáltatók kötelesek olyan megfelelő kockázatértékeléseket alkalmazni, amelyek elősegítik a teljes felhőszolgáltatási hálózat elszámoltathatóságát és ellenálló képességét (Hon, 2018).

A NIS2 további jelentős előrelépése, hogy megerősített megfelelési követelményeket vezet be a több joghatóságban működő felhőszolgáltatók számára (Vandezande, 2023). Tekintettel arra, hogy a CSP-k jellemzően globális vállalatok, amelyek számos piacon és földrajzi térségben nyújtanak szolgáltatásokat, az egységes szabályok alkalmazása jelentős költségmegtakarítást eredményezhet, valamint hozzájárulhat a megfelelő intézkedések végrehajtásával kapcsolatos nehézségek leküzdéséhez, elősegítve az optimális kiberbiztonsági szint elérését a felhőfelhasználók számára (NIS2 5., 7. és 18. cikk).

Az irányelv továbbá ösztönzi a felhőszolgáltatók és az érintett érdekelt felek közötti együttműködést olyan kulcsfontosságú területeken, mint az incidensbejelentési kötelezettségek és az információmegosztási mechanizmusok (NIS2 21. és 23. cikk). Az ilyen együttműködés elősegítheti a kiberbiztonsági incidensek következményeinek mérséklését, a szolgáltatásfolytonosság fenntartását, valamint a felhasználói bizalom erősítését a felhőalapú rendszerek iránt (Hon, 2018).

A NIS2 előírja, hogy a lényeges szervezetnek minősülő felhőszolgáltatók kötelesek a súlyos kiberbiztonsági incidensekről 24 órán belül értesíteni az illetékes

hatóságokat, továbbá 72 órán belül részletes jelentést benyújtani. Emellett megfelelő módon tájékoztatniuk kell ügyfeleiket az esetleges fenyegetésekről és az azok kezeléséhez szükséges intézkedésekről. Határokon átnyúló incidensek esetén az érintett tagállamokat is értesíteni kell (NIS2 23. cikk). Összességében a NIS2 irányelv olyan meghatározó jogszabály, amely jelentősen hozzájárul a felhőszolgáltatások biztonságának megerősítéséhez az egyre összetettebb kiberfenyegetések kezelése révén (Millard, 2021).

Ugyanakkor a NIS2 irányelv jelentős jogtudományi viták tárgya. Bár széles körben szükséges és indokolt előrelépésként értékelik az eredeti NIS irányelvhez képest, a jogtudósok eltérően ítélik meg annak hatókörét és gyakorlati alkalmazhatóságát. Egyes álláspontok szerint a NIS2 lényeges javulást hoz, különösen a szabályozott szervezetek körének bővítése és a felhőszolgáltatók lényeges szervezetként való formális elismerése révén, ami fokozza a határokon átnyúló kiberbiztonsági kormányzás harmonizációját és ellenálló képességét (Vandezande, 2023).

Ezzel szemben a kritikusok az irányelv működési komplexitását hangsúlyozzák, különösen a nemzeti végrehajtási mechanizmusok bizonytalanságát és a kisebb szereplők megfelelési képességének korlátait illetően. A kis- és középvállalkozásokra, valamint a decentralizált szereplőkre háruló megfelelési teher aránytalanul magas lehet, ami egyenlőtlen végrehajtást eredményezhet a tagállamok között. Ezt a gyakorlati szakirodalom is megerősíti, amely figyelmeztet a kulcsfontosságú kötelezettségek – például a bejelentési határidők vagy a kockázatkezelési protokollok – töredezett értelmezésére (Hon, 2018).

A tudományos vita kiterjed a NIS2 ellátási láncra vonatkozó biztonsági követelményeinek megvalósíthatóságára is. Míg egyes szerzők szerint e rendelkezések összhangban állnak a felhőszolgáltatások megosztott jellegével (Millard, 2021), mások megkérdőjelezik azok tényleges érvényesíthetőségét a globális alvállalkozókat is magában foglaló nagyléptékű felhőökoszisztémákban. A kritikusok szerint a mélyreható ellátásilánc-átvilágítás kikényszerítése szűk működési keresztmetszetekhez vagy túlzott jogi beavatkozáshoz vezethet.

A NIS2 irányelv gyakorlati jelentőségét jól szemlélteti a 2021-es „OVH felhőincidens”, amikor egy súlyos tűzeset több adatközpontot megsemmisített Strasbourgban, ami világszerte több ezer ügyfél számára okozott szolgáltatáskimaradást. Az esemény rávilágított a felhőellátási lánc kezelésének és az ellenálló képesség tervezésének kritikus hiányosságaira. A NIS2 hatálya alatt az OVHcloud mint lényeges szervezet egyértelműbb és szigorúbb kötelezettségekkel rendelkezett volna a kockázatértékelés, az incidensjelentés és az ellenállóképességi intézkedések terén, ami potenciálisan csökkenthette volna az esemény hatását és a helyreállítási időt (URL3).

Összességében az akadémiai diskurzus egyaránt tartalmaz támogató és kritikus álláspontokat a NIS2 irányelv felhőkörnyezetre gyakorolt hatásáról. Bár az irányelv egységes kiberbiztonsági intézkedések és együttműködésen alapuló kormányzás kialakítására irányuló céljai széles körű támogatást élveznek, a határokon átnyúló végrehajthatóság és az adminisztratív terhek továbbra is olyan kihívások, amelyek a szabályozás további finomítását teszik szükségessé.

A kiberbiztonsági rendelet (Cybersecurity Act) és az ENISA szerepe

A GDPR és a NIS2 mellett a 2019-ben elfogadott kiberbiztonsági rendelet (Cybersecurity Act – CSA) az uniós jog egyik alapvető pillére a magas szintű kiberbiztonság, ellenálló képesség és bizalom megteremtése érdekében, elősegítve ezzel a belső piac megfelelő működését (Montagnani & Cavallo, 2018). A rendelet a 2. cikkben a kiberbiztonságot úgy határozza meg, mint *„a hálózati és információs rendszerek, e rendszerek felhasználói, valamint a kiberfenyegetések által érintett egyéb személyek védelméhez szükséges tevékenységek összességét."*

A CSA számos olyan lényeges fogalmat és kötelezettséget vezetett be, amelyeket a digitális környezetben működő szolgáltatóknak alkalmazniuk kell, és amelyek elősegítik a legjobb biztonsági gyakorlatok érvényesülését, valamint erősítik az ügyfelek bizalmát (Millard, 2021). A rendelet célja az egységes kiberbiztonsági standardok kialakítása az uniós belső piacon a digitális gazdaság megerősítése érdekében (CSA 1. cikk).

A CSA egyik legjelentősebb újítása az uniós kiberbiztonsági tanúsítási keretrendszer létrehozása. E keretrendszer olyan tanúsítási rendszereket határoz meg, amelyek igazolják, hogy az információs és kommunikációs technológiák (IKT) termékei, szolgáltatásai és folyamatai meghatározott biztonsági követelményeknek felelnek meg. Az IKT fogalma széles értelemben magában foglalja a kommunikációs, számítástechnikai, hálózati és adatkezelési technológiákat, ideértve a hardvert, a szoftvert, az internetes szolgáltatásokat és a távközlési infrastruktúrát (Roztocki et al., 2019). A tanúsítás célja az adatok bizalmasságának, sértetlenségének, hitelességének és rendelkezésre állásának biztosítása az adatok teljes életciklusa során a felhőökoszisztémában (CSA 46. cikk).

E tanúsítási rendszerek elsődleges biztonsági céljai közé tartozik az adatok védelme minden véletlen vagy jogosulatlan tevékenységgel szemben, valamint annak biztosítása, hogy kizárólag felhatalmazott szereplők férhessenek hozzá az adatokhoz (Tsvilii, 2021). A tanúsítási rendszerek kidolgozásának és irányításának koordinálására a CSA az Európai Unió Kiberbiztonsági Ügynökségét (ENISA) jelöli ki, amelynek feladata az együttműködés elősegítése a nemzeti

hatóságokkal és az Európai Bizottsággal a vonatkozó uniós szabályokkal összhangban álló tanúsítási rendszerek kialakítása érdekében (CSA 4. cikk).

Ugyanakkor aggályok merültek fel a tanúsítási rendszerek önkéntes jellegével kapcsolatban. Kötelező alkalmazás hiányában fennáll annak kockázata, hogy a CSA egy kétszintű rendszert hoz létre, amelyben kizárólag a jelentős erőforrásokkal rendelkező felhőszolgáltatók törekednek tanúsítás megszerzésére, miközben a kis- és középvállalkozások kiszolgáltatottabbá válnak, és kevésbé megfelelők maradnak. Ez a kritika rámutat a rugalmasság és a kötelező jelleg közötti megfelelő szabályozási egyensúly szükségességére.

A rendelet ENISA-ra támaszkodó végrehajtási modellje szintén vitákat váltott ki. Míg egyes szakértők elismerik az ügynökség magas szintű technikai szakértelmét és független szerepét a tanúsítási folyamat irányításában, mások kétségbe vonják, hogy az ENISA rendelkezik-e elegendő végrehajtási jogosítvánnyal és erőforrással az uniós szintű tanúsítás hatékony felügyeletéhez (Montagnani & Cavallo, 2018).

A CSA tanúsítási célkitűzéseivel összhangban álló kezdeményezés a Gaia-X projekt, amely az európai adatinfrastruktúra feletti ellenőrzés megerősítését, valamint az adatszuverenitás és a szabványosított biztonsági protokollok elvének érvényesítését hangsúlyozza. A szakirodalom gyakran hivatkozik a Gaia-X-re mint a CSA elveinek gyakorlati megvalósítását elősegítő modellre. Ugyanakkor kritikus hangok szerint jogilag kikényszeríthető kötelezettségek hiányában az ilyen kezdeményezések piaci elfogadottsága korlátozott maradhat (URL4).

Hasonló tanulságokkal szolgál a 2022-es Vodafone Portugal elleni kibertámadás is, amely rávilágított arra, hogy a szabványosítás és a tanúsítás miért kulcsfontosságú. Bár a CSA célja az ilyen kockázatok mérséklése, egyes szakértők szerint a tanúsítás önmagában nem elegendő világos incidenskezelési mechanizmusok és egyértelmű elszámoltathatósági struktúrák nélkül (URL5).

A CSA által létrehozott Európai Kiberbiztonsági Tanúsítási Rendszer a Felhőszolgáltatásokra (EUCS) átalakító jelentőségű lépésnek tekinthető. A szakirodalom szerint az EUCS harmonizált kiberbiztonsági tanúsítási szintet biztosít, amely különösen fontos a széttagolt szabályozási környezetben. Emellett az a tény, hogy olyan meghatározó felhőszolgáltatók, mint a Microsoft Azure, a Google Cloud és az Amazon Web Services (AWS) gyakorlataikat az EUCS követelményeihez igazítják, erős iparági támogatottságot jelez az egységes szabványok iránt (Tsvilii, 2021).

Ezt jól példázza az AWS által megszerzett ISO-tanúsítványok – így az ISO 27001, az ISO 27017 és az ISO 27018 –, amelyek a CSA-ban is megjelenő biztonsági elveknek való megfelelést tükrözik (AWS, 2023). Ezek a tanúsítások a jövőbeni EUCS-rendszer előképeiként szolgálnak, és szemléltetik, miként

járulhatnak hozzá az önkéntes tanúsítási rendszerek a bizalom, az átláthatóság és a magas szintű kiberbiztonsági gyakorlatok megerősítéséhez a digitális környezetekben, így különösen a felhőiparban (URL6).

Kiberbiztonsági hiányosságok a felhőben: a szerződéses megállapodások szerepe

A felhőkörnyezetben a szerződések és megállapodások elengedhetetlen eszközök a kiberbiztonsági incidensekért fennálló felelősség igazolására és allokálására. A felhőszolgáltató és az ügyfelei közötti jogviszony többféle dokumentumon alapulhat, így különösen felhőszolgáltatási szerződéseken (Cloud Service Agreements – CSA), szolgáltatási szintmegállapodásokon (Service Level Agreements – SLA), valamint a megosztott felelősségi modellen (Shared Responsibility Model) (Radu, 2016). E megállapodások alapvetően a felek kölcsönös jogait, kötelezettségeit és felelősségi körét rögzítik a felhőszolgáltatási tranzakciókban, továbbá a kockázatok megosztását is szolgálják: a kockázatokat a felek között a kontroll mértékéhez igazodva osztják meg, összhangban az alkalmazott szolgáltatási modellel (SaaS, PaaS vagy IaaS) (URL7).

A felhőalapú számítástechnika három alapvető szolgáltatási modellje eltérő kontroll- és rugalmassági szinteket biztosít. A SaaS (Software as a Service – szoftver mint szolgáltatás) lehetővé teszi, hogy a felhasználó online, helyi telepítés nélkül használjon szoftveralkalmazásokat; tipikus példák a Google Workspace és a Microsoft 365, amelyek webes hozzáféréssel biztosítanak produktivitási eszközöket. A PaaS (Platform as a Service – platform mint szolgáltatás) felhőalapú fejlesztői környezetet nyújt, amelyben az alkalmazások létrehozása, tesztelése és telepítése infrastruktúra-kezelés nélkül végezhető; erre példa a Google App Engine. Az IaaS (Infrastructure as a Service – infrastruktúra mint szolgáltatás) virtuális informatikai erőforrásokat, így szervereket és tárhelyet biztosít interneten keresztül, amely felett a felhasználó rendelkezik a legnagyobb kontrollal; ide sorolhatók például az Amazon és a Microsoft Azure virtuálisgép-szolgáltatásai. E modellek alkotják a felhőszolgáltatások gerincét, és eltérő felhasználói igényeket elégítenek ki az egyszerű szoftverhasználattól a fejlesztői, illetve összetett IT-rendszereket üzemeltető igényekig (Geradin et al., 2022).

A felhőszolgáltatási szerződésekben az SLA-k fontos eszközként szolgálhatnak a kiberbiztonsági incidensekből eredő felelősség megállapításában és megosztásában, különösen akkor, ha a biztonságmenedzsmentet kifejezett indikátorként integrálják a kiberbiztonsági hiányosságok kezelésére (Millard, 2021). Az SLA meghatározza, hogy az ügyfél milyen szolgáltatási szintet vár

el a szolgáltatótól, rögzíti a teljesítménymutatókat, amelyek alapján a szolgáltatást mérni lehet, továbbá (adott esetben) a jogkövetkezményeket vagy szankciókat arra az esetre, ha a szolgáltatási szintek nem teljesülnek. Az SLA-k jellemzően vállalatok és külső beszállítók között jönnek létre, de előfordulhatnak szervezeten belüli egységek között is (URL8).

Az SLA-k rendszerint olyan szolgáltatási metrikákat tartalmaznak, amelyek az incidensekkel kapcsolatos kérdéseket kezelik – például az első reagálási időtől a végső megoldásig terjedő határidőket –, továbbá rögzítik a szolgáltatóval szemben alkalmazandó szankciókat nemteljesítés esetére (URL9). Indokolt, hogy adatvédelmi incidensek vagy titoktartási kötelezettség megsértése esetén az SLA-k egyértelmű rendelkezéseket tartalmazzanak a szolgáltató felelősségéről és kártalanítási (indemnity) kötelezettségéről. Emellett különösen fontosak a biztonságos adatmigrációra és adattörlésre vonatkozó garanciák, amelyek az adatok „kitettségi" kockázatának csökkentését szolgálják. Az ilyen, biztonságos adatkezelést előíró szerződéses klauzulák hozzájárulhatnak a jogosulatlan hozzáférés vagy adatvesztés kockázatának és következményeinek kontrollálásához, ami a felhőben való megfelelés egyik kulcstényezője (URL10).

Kiemelendő az úgynevezett kártalanítási klauzula (indemnification clause) szerepe: e rendelkezés alapján a szolgáltató vállalja, hogy megtéríti az ügyfél azon költségeit, amelyek harmadik felek jogi igényeiből (például peres eljárásokból) erednek, amennyiben a szolgáltató megsérti a saját szavatossági vagy jótállási nyilatkozatait. Ez magában foglalhatja a peres költségek viselését is. A standard SLA-k gyakran kizárják vagy korlátozzák az ilyen rendelkezéseket, ezért célszerű, hogy az ügyfél jogi tanácsadó bevonásával alakítsa ki a megfelelő klauzulát. A felhőszolgáltató azonban jellemzően további tárgyalásokat igényelhet az ilyen feltételek elfogadása érdekében (URL11).

A megosztott felelősségi modell a felhőtranzakciók másik gyakori keretrendszere a kölcsönös felelősségek rögzítésére. Eszerint a kiberbiztonsági intézkedésekért viselt felelősség nem kizárólag a felhőszolgáltatót terheli: a felhőszolgáltatást igénybe vevő félnek is több lépést kell megtennie, és a felhőben tárolt adatokat érintő incidensek, illetve adatvédelmi jogsértések esetén a felelősség egy része őt is terhelheti (URL12). A megosztott felelősségi modell olyan keretrendszer, amely meghatározza a biztonság különböző aspektusaihoz kapcsolódó kölcsönös felelősségi köröket a szolgáltatók és az ügyfelek között (URL13). A gyakorlatban a kiberbiztonsági felelősségek rendszerint úgy oszlanak meg, hogy az ügyfél felelősségi körébe tartozik többek között a végpontok (eszközök) biztonsága, a felhasználói fiókok kezelése, valamint az identitás- és hozzáférésmenedzsment; míg a szolgáltató felelőssége jellemzően a fizikai infrastruktúrára, a hálózatra és az adatközpontokra terjed ki (URL14).

Összességében a felhőszolgáltatási szerződések meghatározó eszközök a felelősség allokálásában és a különböző feladat- és kockázati körök elhatárolásában a felhőökoszisztémában. Elősegítik az elszámoltathatóságot olyan biztonsági követelmények szerződéses rögzítésével, mint az adattitkosítás vagy az incidensjelentési eljárások, ami a felhőtranzakciók során a kiberbiztonsági gyakorlatok javulásához vezethet. Tekintettel a felhőökoszisztéma rétegeinek és szereplőinek összetettségére, valamint a dinamikusan változó kockázatokra, nélkülözhetetlen megfelelően strukturált felhőszolgáltatási megállapodások alkalmazása a kiberbiztonsági ellenálló képesség növeléséhez és a kiberbiztonsági hibákból eredő felelősség méltányos megosztásához (Millard, 2021).

A fejlődő technológiák hatása a felhőkörnyezet kiberbiztonságára

Mesterséges intelligencia: lehetőségek, képességek és megfelelési kihívások

Bár – amint azt a tanulmány bemutatta – a kiberbiztonsági kötelezettségek több uniós szabályozásban is részletesen megjelennek, a technológiai innováció felhőbiztonsági alkalmazása napjainkban gyors ütemben terjed (URL15). Ez érthető a mesterséges intelligencia (MI) előnyeinek fényében, mivel az képes nagy mennyiségű adat elemzésére, fenyegetések azonosítására és kezelésére, valamint valós idejű döntések támogatására (URL16).

A mesterséges intelligencia több funkciója közvetlenül javíthatja a felhőkörnyezetek biztonságát. Ilyen például a fenyegetésészlelés, amely során gépi tanulási modellek alkalmazhatók az anomáliák és kockázatok azonosítására. A felhőben deep learning technikák is alkalmazhatók – például konvolúciós neurális hálózatok (CNN) és rekurzív neurális hálózatok (RNN) –, amelyek különösen alkalmasak nagy adatmennyiségek feldolgozására és kockázati mintázatok felismerésére. Emellett az MI kiemelkedő előnyöket kínál az incidenskezelés terén is: képes a támadás súlyosságának értékelésére és az ennek megfelelő, gyorsabb és erőforrás-hatékonyabb reagálás támogatására (URL17).

Az MI a felhőökoszisztémában trendek elemzésére is használható – például a felhasználói viselkedés, a hálózati forgalom és az erőforrás-kihasználtság vizsgálatára –, és előre jelezheti a lehetséges fenyegetéseket vagy az infrastruktúra sérülékeny pontjait, ami hozzájárulhat a kockázatok és azok várható hatásainak mérsékléséhez (URL18). Összességében az MI-alapú megoldások ígéretes irányt jelentenek a felhő kiberbiztonságának erősítésében.

Mindazonáltal több kihívás is fennáll. Ilyenek elsősorban az adatvédelmi aggályok, mivel az MI rendszerint nagy mennyiségű adatot kezel, ami feszültséget

teremthet az adatbiztonság maximalizálása és az olyan adatvédelmi jogszabályoknak való megfelelés között, mint a GDPR. További probléma a meglévő (gyakran elavult) infrastruktúrával való integráció: a vállalatok számára nehézséget okozhat MI-alapú rendszerek bevezetése a régi rendszerek mellé, ami korszerűsítést tehet szükségessé, jelentős költségek és erőforrás-ráfordítás mellett – különösen a fejlődő vállalkozások esetében. Végül a mesterséges intelligenciára épülő biztonsági megoldások alkalmazása megfelelő szaktudást igényel, és az informatikai szakemberek iránti szükséglet további költségterhet jelenthet, különösen kisebb vállalkozások számára (URL19).

Blokklánc: a bizalom erősítése és a jogi–technikai korlátok kezelése

A blokklánc-technológia felhőalapú számítástechnikában történő alkalmazása jelentős mértékben átalakíthatja a kiberbiztonságot, mivel képes kezelni a hagyományos felhőinfrastruktúrák több strukturális gyengeségét. A blokklánc decentralizált és megváltoztathatatlan (immutábilis) jellege biztonságos és átlátható adattranzakciókat tesz lehetővé, és jelentősen javítja az adatintegritást, valamint az incidensekkel szembeni ellenálló képességet. A központosított adatbázisokkal szemben – amelyek egyetlen hibapontja (single point of failure) kompromittálható – a blokklánc titkosított információt oszt el számos csomópont (node) között, ami a jogosulatlan hozzáférést lényegesen megnehezíti. Emellett a blokklánc ellenőrizhető tranzakciós nyilvántartást biztosító képessége erősítheti a felhasználók és a felhőszolgáltatók közötti bizalmat azáltal, hogy átláthatóságot nyújt az adattárolással és adatfeldolgozással kapcsolatban. A blokklánc ezért a biztonságosabb digitális környezet kialakítását támogató technológiaként jelentős szerepet tölthet be a növekvő kiberfenyegetések mellett is (URL20).

A blokklánc kiberbiztonsági előnyei a felhőben többek között az integrált kriptográfiai eljárásokból és a központi hatóság hiányából fakadnak. Megbízható eszközt nyújt az adatintegritás biztosítására, valamint a jogosulatlan módosításokkal szembeni védelemre. A jogosulatlan változtatások kockázata jelentősen csökken azáltal, hogy a módosításokhoz konszenzusmechanizmusok – például Proof of Work vagy Proof of Stake – szükségesek, és ezzel párhuzamosan megbízható auditnyomvonal (audit trail) keletkezik. A blokklánc továbbá erősítheti az identitás- és hozzáférésmenedzsmentet is a decentralizált adattárolás révén, csökkentve a jogellenes hozzáférések és személyazonosság-lopások valószínűségét. Elosztott struktúrája ellenállóbbá teheti a rendszert bizonyos fenyegetésekkel – például elosztott szolgáltatásmegtagadásos (DDoS) támadásokkal – szemben, mivel a hálózat működőképessége részben akkor is fennmaradhat,

ha egyes csomópontok kompromittálódnak, ami hasznos eszközzé teszi a blokkláncot a felhőkiberbiztonságban (URL21).

A blokklánc felhőkörnyezetben történő alkalmazása ugyanakkor számos kihívással jár. Előfordulhat, hogy egyedi fejlesztések vagy testreszabott funkciók új sebezhetőségeket eredményeznek; továbbá bár a blokklánc decentralizáció és kriptográfia révén jelentős biztonsági előnyöket kínál, nem mentes saját korlátaitól. A lánc adatállományának növekedése kedvezőtlenül befolyásolhatja a teljesítményt és a skálázhatóságot, különösen gyors tranzakciókat igénylő felhasználási esetekben. Szolgáltatási és üzemeltetési aggályok is visszatarthatják a piaci szereplőket, mivel a szolgáltatóknak stabil szolgáltatások és megfelelő szerződéses garanciák révén kell bizalmat építeniük. Végül a blokklánc több joghatóságot érintő és decentralizált jellege miatt a releváns és alkalmazandó jog kiválasztása is kritikus kérdéssé válhat. E problémák kezelése nélkülözhetetlen ahhoz, hogy a blokklánc-technológia előnyei teljes mértékben kiaknázhatók legyenek a felhőtranzakciókban (URL22).

Összegzés

A felhőtechnológia alapvetően átalakította az adatkezelés és a szolgáltatásnyújtás módját, ugyanakkor összetett kiberbiztonsági és jogi kihívásokat is eredményezett. A tanulmány a felhőalapú kiberbiztonság összefüggésében vizsgálta a szabályozási keretrendszerek – így a GDPR, a NIS2 irányelv és a kiberbiztonsági rendelet – valamint a feltörekvő technológiák, nevezetesen a mesterséges intelligencia és a blokklánc közötti kapcsolatot. A doktrinális jogelemzés alapján több kulcsfontosságú megállapítás fogalmazható meg.

Elsőként megállapítható, hogy a felhőkörnyezet kiberbiztonsága megosztott felelősség. Mind a felhőszolgáltatóknak, mind a felhőszolgáltatásokat igénybe vevő ügyfeleknek együtt kell működniük a jogszabályi kötelezettségek teljesítése és a megfelelő technikai védelmi intézkedések bevezetése érdekében. Bár az európai uniós szabályozás szilárd alapot biztosít, annak gyakorlati alkalmazása továbbra is számos kihívással jár. Különösen fennmaradnak a bizonytalanságok a határokon átnyúló adattovábbítás, a közös adatkezelés, valamint az adatkezelők és adatfeldolgozók közötti felelősség megosztása tekintetében, különösen több joghatóságot érintő helyzetekben.

A szerződéses eszközök – különösen a szolgáltatási szintmegállapodások (SLA-k) és a megosztott felelősségi modellek – kulcsszerepet játszanak a kötelezettségek és a felelősség meghatározásában. Ugyanakkor a gyakorlatban alkalmazott SLA-k többsége nem tartalmaz kellően részletes, kifejezetten

kiberbiztonságra vonatkozó rendelkezéseket, ami jogbizonytalanságot és fokozott kockázatot teremt mindkét fél számára. Emellett a mesterséges intelligencia és a blokklánc-technológia integrációja lehetőséget kínál a fenyegetések észlelésének, az incidenskezelésnek és az adatintegritás biztosításának javítására, ugyanakkor új jogi és működési kihívásokat is felvet. Ezek közé tartozik az adatvédelmi jogszabályoknak való megfelelés, az interoperabilitási problémák, valamint a megnövekedett költségek, amelyek különösen a kisebb vállalkozások számára jelentenek jelentős terhet.

A kiberbiztonsági rendelet által bevezetett tanúsítási keretrendszerek alkalmas eszközt kínálnak a bizalom erősítésére és a szabványosítás előmozdítására az Európai Unión belül. Ugyanakkor e rendszerek önkéntes jellege egyenlőtlen alkalmazáshoz vezethet, különösen a kisebb szolgáltatók körében, ami megfelelési hiányosságokat eredményezhet a piacon. A valós események – így az OVHcloud adatközponti tűzesete vagy a Vodafone Portugal elleni kibertámadás – egyértelműen rámutatnak az ellátási lánc biztonságának, az ellenálló képesség tervezésének és az egyértelmű incidensbejelentési protokollok fontosságára.

A fenti megállapítások alapján a jövőbeli kutatásoknak indokolt a szerződéses normák uniós szintű standardizálására összpontosítaniuk annak érdekében, hogy a felhőszolgáltatások kiberbiztonsága egységesebb keretek között valósuljon meg. Emellett szükséges a nemzetközi adattovábbításra vonatkozó kötelezettségek, valamint a nem uniós adatfeldolgozók GDPR szerinti felelősségének pontosítása. Empirikus kutatásokra van szükség a kiberbiztonsági tanúsítási rendszerek – különösen az európai felhőszolgáltatásokra vonatkozó kiberbiztonsági tanúsítási rendszer (EUCS) – hatékonyságának értékeléséhez. Végül a jogi keretrendszerek további fejlődése elengedhetetlen a mesterséges intelligencia és a blokklánc alkalmazásából fakadó kérdések kezeléséhez, különös tekintettel az elszámoltathatóságra, az átláthatóságra és a felelősség kérdésére az egyre automatizáltabb vagy decentralizált rendszerekben.

Összegzésként megállapítható, hogy a biztonságos felhőkörnyezet megteremtése összehangolt szabályozási megközelítéseket, erős szerződéses kormányzást és felelős innovációt igényel. A szabályozó hatóságoknak, a szolgáltatóknak, a jogászoknak és a technológiai szakembereknek egyaránt együtt kell működniük annak érdekében, hogy a jogi és szakpolitikai keretek hatékonyan alkalmazkodjanak a digitális világ kihívásaihoz.

Felhasznált irodalom

Carey, P. (2018). *Data protection: A practical guide to UK and EU law* [Adatvédelem: Gyakorlati útmutató az Egyesült Királyság és az Európai Unió jogához] (5th ed.). Oxford University Press.

Dagostino, G. (2019). *Data security in cloud computing* [Adatbiztonság a felhőalapú számítástechnikában] (1st ed.). Momentum Press.

Eryurek, E., Vladimirov, A., Kalyanasundaram, S., & Gupta, P. (2021). *Data governance: The definitive guide* [Adatkormányzás: Az átfogó kézikönyv]. O'Reilly Media.

Geradin, D., Bania, K., Katsifis, D., & Circiumaru, A. (2022). *The regulation of cloud computing: Getting it right* [A felhőalapú számítástechnika szabályozása: A megfelelő megközelítés]. SSRN. https://doi.org/10.2139/ssrn.4285731

Hon, W. K. (2018). *Cloud service providers under the NIS Directive: The UK's implementation (with GDPR comparisons)* [Felhőszolgáltatók a NIS irányelv alatt: Az Egyesült Királyság végrehajtása (GDPR-összehasonlítással)]. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3200149

Lynn, T., Mooney, J. G., van der Werff, L., & Fox, G. (szerk.). (2021). *Data privacy and trust in cloud computing: Building trust in the cloud through assurance and accountability* [Adatvédelem és bizalom a felhőalapú számítástechnikában: Bizalomépítés a felhőben a biztosítékok és elszámoltathatóság révén]. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-54660-1

McGillivray, K. (2022). *Government cloud procurement* [Állami felhőbeszerzés]. Cambridge University Press.

Millard, C. (2021). *Cloud computing law* [A felhőalapú számítástechnika joga]. Oxford University Press.

Montagnani, M. L., & Cavallo, M. A. (2018). *Cybersecurity and liability in a big data world* [Kiberbiztonság és felelősség a big data világában]. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3220475

Radu, B. (2015). Key aspects of cloud-computing services-related contracts [A felhőalapú szolgáltatásokhoz kapcsolódó szerződések kulcskérdései]. *National Strategies Observer*, *1*(2). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2787620

Rittinghouse, J. W., & Ransome, J. F. (2010). *Cloud computing implementation, management, and security* [Felhőalapú számítástechnika: megvalósítás, menedzsment és biztonság]. CRC Press.

Roztocki, N., Soja, P., & Weistroffer, H. R. (2019). The role of information and communication technologies in socioeconomic development: Towards a multidimensional framework [Az információs és kommunikációs technológiák szerepe a társadalmi-gazdasági fejlődésben: egy multidimenzionális keret felé]. *Information Technology for Development*, *25*(2), 171–183. https://doi.org/10.1080/02681102.2019.1596654

Tsvilii, O. (2021). Cybersecurity regulation: Cybersecurity certification of operational technologies [Kiberbiztonsági szabályozás: az operatív technológiák kiberbiztonsági tanúsítása]. *Technology Audit and Production Reserves*, *1*(2(57)), 54–60. https://doi.org/10.15587/2706-5448.2021.225271

Vandezande, N. (2023). *Cybersecurity in the EU: How the NIS2 Directive stacks up against its predecessor* [Kiberbiztonság az Európai Unióban: a NIS2 irányelv összevetése elődjével]. SSRN. https://doi.org/10.2139/ssrn.4383118

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide* [Az Európai Unió általános adatvédelmi rendelete (GDPR): gyakorlati útmutató]. Springer.

A cikkben szereplő online hivatkozások

URL1: *News analysis on how the UK Information Commissioner's Office adjusted its GDPR enforcement strategy by reducing fines imposed on major companies.* [Hírelemzés arról, miként módosította az Egyesült Királyság adatvédelmi hatósága a GDPR-érvényesítési gyakorlatát a nagyvállalatokra kiszabott bírságok csökkentésével.] https://ion-analytics-acuris-law-report-group-cslr-staging.staging.services.acuris.com/8063891/ico-hones-gdpr-enforcement-approach-with-reduced-fines-for-british-airways-marriott-and-ticketmaster.thtml

URL2: *European Parliamentary Research Service briefing on the NIS2 Directive and its role in strengthening cybersecurity across the European Union.* [Az Európai Parlament Kutatószolgálatának háttéranyaga a NIS2 irányelvről és annak szerepéről az uniós kiberbiztonság megerősítésében.] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

URL3: *Professional commentary examining lessons learned from the OVHcloud data center fire, with a focus on resilience and fire suppression.* [Szakmai elemzés az OVHcloud adatközponti tűzeset tanulságairól, különös tekintettel az ellenálló képességre és a tűzoltási megoldásokra.] https://journal.uptimeinstitute.com/tag/fire-suppression/

URL4: *Policy brief analyzing Europe's strategic challenges and policy options in achieving cloud sovereignty.* [Szakpolitikai elemzés Európa felhőszuverenitással kapcsolatos stratégiai kihívásairól és szakpolitikai lehetőségeiről.] https://www.clingendael.org/sites/default/files/2024-02/Policy_brief_Cloud_sovereignty.pdf

URL5: *Cybersecurity awareness article analyzing the Vodafone cyber incident as part of the "Behind the Hack" series.* [Kiberbiztonsági ismeretterjesztő cikk a Vodafone elleni kibertámadás elemzéséről a „Behind the Hack" sorozat részeként.] https://ninjio.com/2022/03/behind-the-hack-vodafone/

URL6: *Official Amazon Web Services documentation detailing certifications, compliance programs, and attestations applicable to AWS services.* [Az Amazon Web Services hivatalos dokumentációja az AWS-szolgáltatásokhoz kapcsolódó tanúsítványokról, megfelelőségi programokról és igazolásokról.] https://docs.aws.amazon.com/whitepapers/latest/gxp-systems-on-aws/aws-certifications-and-attestations.html

URL7: *UNCITRAL secretariat notes outlining key legal and liability issues related to cloud computing contracts.* [Az UNCITRAL titkárságának feljegyzései a felhőszolgáltatási szerződésekkel kapcsolatos főbb jogi és felelősségi kérdésekről.] https://uncitral.un.org/en/cloud/liability

URL8: *Overview of service-level agreements, including definitions, best practices, and practical guidance for outsourcing and IT services.* [Áttekintés a szolgáltatási szintmegállapodásokról, fogalmi meghatározásokkal, bevált gyakorlatokkal és gyakorlati útmutatással a kiszervezés és az IT-szolgáltatások területén.] https://www.cio.com/article/274740/outsourcing-sla-definitions-and-solutions.html

URL9: *Academic paper discussing security service level agreements as a framework for quantifiable enterprise security.* [Tudományos tanulmány a biztonsági szolgáltatási szintmegállapodásokról mint a vállalati biztonság mérhető keretrendszeréről.] https://www.nspw.org/papers/1999/nspw1999-henning.pdf

URL10: *Legal guidance on negotiating cloud services agreements, focusing on contractual risk allocation and compliance considerations.* [Jogi útmutató a felhőszolgáltatási szerződések tárgyalásához, különös tekintettel a szerződéses kockázatmegosztásra és a megfelelési szempontokra.] https://parrbrown.com/negotiating-a-cloud-services-agreement/

URL11: *Overview of service-level agreements, including definitions, best practices, and practical guidance for outsourcing and IT services.* [Áttekintés a szolgáltatási szintmegállapodásokról, fogalmi meghatározásokkal, bevált gyakorlatokkal és gyakorlati útmutatással a kiszervezés és az IT-szolgáltatások területén.] https://www.cio.com/article/274740/outsourcing-sla-definitions-and-solutions.html

URL12: *Industry article clarifying the shared responsibility model in cloud computing environments.* [Iparági cikk a felhőalapú környezetekben alkalmazott megosztott felelősségi modell értelmezéséről.] https://www.informationweek.com/it-infrastructure/clearing-the-clouds-around-the-shared-responsibility-model

URL13: *Educational resource explaining the shared responsibility model and its implications for cloud security.* [Oktatási anyag a megosztott felelősségi modellről és annak felhőbiztonsági következményeiről.] https://www.wiz.io/academy/shared-responsibility-model

URL14: *Microsoft documentation describing shared responsibility for security and compliance in cloud services.* [A Microsoft dokumentációja a felhőszolgáltatások biztonsági és megfelelési felelősségének megosztásáról.] https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

URL15: *Industry article examining emerging technologies in cloud security and their role in mitigating cyber threats.* [Iparági elemzés a felhőbiztonság területén megjelenő új technológiákról és azok szerepéről a kiberfenyegetések mérséklésében.] https://informationsecuritybuzz.com/emerging-technologies-in-cloud-security/

URL16: *Academic article analyzing the role of artificial intelligence in enhancing cloud security within the Indian IT industry.* [Tudományos tanulmány a mesterséges intelligencia szerepéről a felhőbiztonság erősítésében az indiai IT-iparban.] https://ijisae.org/index.php/IJISAE/article/view/6709/5576

URL17: *Research article exploring AI-driven solutions for improving cloud security mechanisms.* [Kutatási cikk az MI-alapú megoldásokról a felhőbiztonsági mechanizmusok fejlesztésére.] https://ijisae.org/index.php/IJISAE/article/download/6653/5513/11833

URL18: *Research study on the integration of artificial intelligence and machine learning for advanced cloud threat detection and prevention.* [Kutatási tanulmány a mesterséges intelligencia és a gépi tanulás integrációjáról a fejlett felhőalapú fenyegetésészlelés és -megelőzés érdekében.] https://www.researchgate.net/publication/383095008_ai-powered_cloud_security_a_study_on_the_integration_of_artificial_intelligence_and_machine_learning_for_improved_threat_detection_and_prevention

URL19: *Scholarly article discussing the application of AI techniques to enhance data security in cloud environments, including challenges and future prospects.* [Tudományos cikk az MI-technikák alkalmazásáról a felhőkörnyezetek adatbiztonságának növelése érdekében, bemutatva a kihívásokat és a jövőbeli kilátásokat.] https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/2262/833

URL20: *Exploratory article examining the impact of blockchain technology on cloud computing architectures and services.* [Elemző cikk a blokklánc-technológia hatásáról a felhőalapú számítástechnikai architektúrákra és szolgáltatásokra.] https://medium.com/zee-palm/understanding-the-impact-of-blockchain-technology-on-cloud-computing-ec231aa46d8d

URL21: *Analytical article discussing how decentralization through blockchain can enhance cybersecurity.* [Elemző cikk arról, miként járulhat hozzá a blokklánc-alapú decentralizáció a kiberbiztonság erősítéséhez.] https://cybermagazine.com/articles/blockchain-what-decentralisation-can-bring-to-cybersecurity

URL22: *Policy paper analyzing regulatory and governance challenges related to the deployment of blockchain technologies.* [Szakpolitikai tanulmány a blokklánc-technológiák bevezetésével összefüggő szabályozási és kormányzási kihívásokról.] https://www.diplomacy.edu/wp-content/uploads/2021/06/111220181248_Boujemi.pdf

Alkalmazott jogszabályok

Általános adatvédelmi rendelet (General Data Protection Regulation – GDPR)

A hálózati és információs rendszerek biztonságáról szóló irányelv (Network and Information Systems Directive – NIS2)

Kiberbiztonsági rendelet és az Európai Unió Kiberbiztonsági Ügynöksége (Cybersecurity Act and ENISA – CSA)

A cikk APA szabály szerinti hivatkozása

Khraisha W. (2026). Kiberbiztonság a felhőiparban. Jogi kötelezettségek és felelősség az európai szabályozás és a technológiai fejlődés tükrében. *Belügyi Szemle*, *74*(1), 121–143. https://doi.org/10.38146/BSZ-AJIA.2026.v74.i1.pp121-143

Nyilatkozatok

Összeférhetetlenség

A szerző nem jelentett összeférhetetlenséget.

Finanszírozás

A szerző nem kapott pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Levelező szerző

A cikk levelező szerzője Khraisha Wasim, aki a wasimkhraisha@gmail.com e-mail címen érhető el.