DOI: 10.38146/BSZ-AJIA.2026.v74.i1.pp165-182

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

Wasim Khraisha
PhD Student
Károli Gáspár University of the Reformed Church in Hungary,
Doctoral School of Law and Political Sciences
wasimkhraisha@gmail.com

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

The manuscript was submitted in English. Received: 1 February 2025. Revised: 31 March 2025
Accepted: 11 August 2025.

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

Introduction

Nowadays, the Cloud industry has become increasingly important for both corporations and individuals due to the benefits and services it offers. For corporations, the cloud is an essential tool; it enables them to access multiple services such as computing power, storage, and databases on an as-needed basis from well-known cloud services providers like Amazon Web Services, Microsoft Azure, and Alibaba, among others, instead of buying, owning, and maintaining physical data centers and servers (McGillivray, 2022). Cloud computing involves the delivery of computing services over the Internet, including software, databases, servers, storage, and other IT resources delivered on demand via the Internet with pay-as-you-go pricing; this eliminates the need for managing files and services on local storage devices, offering a cost-efficient alternative (Dagostino, 2019). Based on that, cloud technology can be described as a type of computing where individual businesses depend on a third party to manage their data and computer processing via the Internet. Cloud service providers (CSPs) are companies that supply secure, reliable, and scalable computing through shared data centers that users can access remotely (Millard, 2021). Notably, the introduction of cloud technology has substantially forced different institutions to reassess cybersecurity levels, as data and applications are often distributed across both local and remote systems, presenting new challenges and opportunities in data privacy and trust (Lynn et al., 2021). Systems and data can always be accessed online; for example, data accessed via services like Google

Docs on a smartphone may be stored in various global locations. Consequently, ensuring its protection has become increasingly complex compared to when it was merely a matter of preventing unwanted users from accessing a network. (Millard, 2021) Cybersecurity for cloud services has become increasingly critical for two primary reasons:

Firstly, the cloud industry is growing exponentially as a dominant platform for both personal and enterprise-level applications. Innovation has allowed new technologies to outpace the development of industry-wide security standards, shifting more responsibility onto users to assess accessibility-related security risks. Secondly, centralized, multi-tenant storage systems now allow everything from basic infrastructure to individual-level data such as emails and documents, to be located and accessed remotely via web-based connections 24/7. This aggregation of data in the servers of a few major service providers poses risks, as threat actors can target large, multi-enterprise data centers and cause massive data breaches. (Rittinghouse & Ransome, 2010) This paper examines the interplay between legal frameworks and technological advancements in shaping data protection obligations, the allocation of cybersecurity responsibilities between cloud service providers and customers, and the implications for liability in the event of data breaches.

Overview: Cloud Security Risks Landscape and the Role of Legal Safeguards

The transfer of all or part of the data to the cloud results in the customer losing exclusive control over that data, thus creating a need to adopt effective measures to ensure its integrity and confidentiality or to verify that the data processing and retention are carried out appropriately (McGillivray, 2022). Proper isolation of resources, data categorization, and strong security measures are especially critical in shared environments like cloud computing (Eryurek et al., 2021). Crucially, weak security measures in the cloud can expose users to various cybersecurity threats. Some common cloud security threats include cloud-based infrastructure risks, such as outdated, incompatible IT frameworks and third-party data storage service outages, internal threats are often caused by human error, such as the misconfiguration of user access controls, while external threats are almost exclusively caused by hackers, including malware and viruses (Lynn et al., 2021). Malicious actors and hackers frequently infiltrate networks by exploiting weak authentication credentials. Once a hacker gains access, they can extend their reach by exploiting poorly protected cloud interfaces to locate

data across different databases. They may even use cloud servers as repositories for storing and transmitting stolen data (Dagostino, 2019). The storage and access of data by third parties online also introduce additional threats. For instance, if these services are interrupted for any reason, users may lose access to their data. For example, a telephone network outage could prevent timely access to cloud services, or a power outage could affect the data center where the data is stored, potentially resulting in permanent data loss (Rittinghouse & Ransome, 2010). Subsequently, to tackle and mitigate these risks and challenges, several legal requirements are imposed on the cloud actors to follow to ensure cybersecurity for data stored in cloud environments.

Legal Framework for Cybersecurity in the Cloud: Obligations and Assigning Liabilities

The EU General Data Protection Regulation (GDPR)

The GDPR is an EU regulation (effective from May 2018) that governs data protection and privacy, enhancing individuals' control over their personal data and imposing strict compliance obligations on organizations processing such data (Voigt & von dem Bussche, 2017). It specified significant provisions about security failures, breaches, and the overall safety of a digital environment. The cloud customer -for instance, an institution using cloud services- is the controller since it is the party that determines what, how, and why the data is processed (GDPR 2016, Art 4/7). Therefore, it bears liability in case of any violations, failures, or lack of commitment to the compliance requirements (Millard, 2021). The other party is the processor, which is usually the CSP. Similarly, several security measures are required from the processor to conduct according to the GDPR (Dagostino, 2019). Various duties and policies enhancing data security are imposed on the controllers and processors mainly by the obligation of 'Implementing appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation' (GDPR 2016, Art 32/1). Subsequently, any negligence or failure to consider these precautions may result in liability for the controller, the processor, or both (GDPR 2016, Art 4 & 5).

Data transfer to third countries or international organizations can present significant cybersecurity risks in the cloud. Since cloud services typically involve the transfer, processing, and storage of data across various locations and multiple clouds globally, this data is vulnerable to a range of threats during these

processes. (Lynn et al., 2021) The GDPR provides a practical regulatory framework for such transfer in Articles 44-50. Crucially, the cloud actors have to follow these obligations to contribute to sufficient cybersecurity levels. However, several challenges might arise since the GDPR did not provide a definition of what data transfer means, which could complicate compliance efforts for cloud actors. Additionally, it is not clear if these rules should apply when the processor acts on behalf of a non-EU controller since this is very common in cloud transactions. Moreover, such strict obligations may hinder CSPs' operational efficiency. (Millard, 2021). The last important obligation to point out concerns the cybersecurity breaches or incidents occurring to data in the cloud. The GDPR introduced key provisions related to this obligation. The cloud customer as controller has to notify the supervisory authority about any breach within 72 hours of becoming aware of it and without undue delay. Similarly, the processor or CSP shall also notify the controller about any breach without undue delay from the time of knowing it. (GDPR, Articles 33-34).

The GDPR is seen as a cornerstone of data protection and cybersecurity regulation in the EU. However, researchers who study this have different views on how clear and useful it is for cloud computing. On one side, supporters say that the GDPR gives a strong and flexible framework for keeping data secure in the cloud, where Articles 24, 28, 32, and 82 give a clear split of duties and demands for data controllers and processors. This rule is seen to encourage cloud customers and providers to choose best security practices, conduct risk checks, and make sure they are responsible through contract terms like Data Processing Agreements (DPAs). Also, the addition of breach alerts under Articles 33-34 is thought to be a significant advancement in responding to different risks. (Dagostino, 2019).

Nonetheless, opposing opinions argue that the GDPR's definitions, especially for international data transfers and joint controllers' roles, continue to be vague in cloud-related situations. This has caused issues in the enforcement of compliance and liability assignment. For example, the lack of a definite definition of what exactly is a 'data transfer' under Article 44 makes it difficult to comply with regulatory requirements for cloud providers operating across jurisdictions. This ambiguity, as noted by Millard (2021), also threatens the extraterritorial application of the GDPR by creating uncertainty for non-EU cloud parties, particularly processors acting on behalf of non-EU controllers. (Kuner 2020) Additionally, while the GDPR establishes the principle of accountability, it does not have much useful guidance on how cloud actors are to apply it in multi-tenant clouds. (Carey, 2018) Marriott International, British Airways, and Capital One are real examples of how the provisions of the GDPR, such as

Article 32, call for appropriate measures to protect personal data have been used by regulators. While these cases demonstrate enforceability under the GDPR, they also demonstrate that liability typically rests with the controller, even in complex cloud arrangements. Critics argue that this assignment of liability is not always compatible with the technical reality where CSPs have significant operational control (URL1).

Fundamentally, assigning the liabilities of any cybersecurity breaches or incidents might be a critical and challenging issue in the cloud. This must be considered in light of the complexity of cloud operations and the multiple actors that may interact in the cloud ecosystem. The GDPR provided provisions that are useful for assigning liabilities. Initially, the cloud customer who was involved in the processing will be responsible for any damage caused by processing activities conducted in a way contrary to the GDPR rules. The processor will be liable only if it has not complied with the GDPR or if it acted beyond or opposite to the controller's instructions. However, both the controller and processor shall be free of any liability for the damage if they can prove they were not involved in the alleged damage. Additionally, if one controller, processor, or both, or even multiple parties are involved in the same damage that occurred due to illegal data processing, they are to be held all responsible for the whole damage occurred. Also, if one or both of them covered the entire compensation of the damage, they can go back to the other controllers or processors of the expenses proportionally according to each one's responsibility. (GDPR, Article 82).

Overall, while the GDPR has established a foundational legal framework for cloud cybersecurity, the academic discourse underscores the need for further clarity, especially in joint controllership, international data transfers, and processor-controller dynamics. As cloud computing continues to evolve, ongoing legal and policy developments will be crucial in addressing these concerns and refining GDPR's application in the cloud context.

Network and Information Systems Directive (NIS2)

The NIS2 directive is one of the most important EU pieces of legislation dealing with cybersecurity in digital environments. One of its main objectives is to improve cybersecurity levels within the EU. It replaced the previous original NIS directive for the year 2016. The original directive contained many legal gaps and posed several challenges in implementation. That was the reason for the need for an updated version to overcome the increased number of cybersecurity risks and incidents. The NIS2 directive was officially adopted in 2022, enhancing resilience and promoting EU cybersecurity conditions (URL2).

A key legal advancement introduced by this directive that helps improve cybersecurity compliance in the cloud is presenting the CSPs as essential entities and the consequent stricter and more precise security compliance requirements on them. Such measures include risk assessment obligations, incident reporting in proper style, and applying inclusive cybersecurity programs. (Hon, 2018) The NIS2 highlights the importance of supply chain security, a crucial concept in the cloud ecosystem, since data is often processed and stored across multiple servers located in various locations around the world, also cloud services typically operate over intricate networks that involve numerous service providers, infrastructure suppliers, various vendors, and subcontractors to guarantee secure service delivery. (Millard, 2021). Subsequently, any loopholes or vulnerabilities in these networks may cause serious cybersecurity risks and incidents as well as affect and restrict the efficiency and authenticity of CSPs in the market. Therefore, under the NIS2 provisions, they now have to make sure to apply proper risk assessments that promote the accountability and resilience of the entire network of the cloud services. (Hon, 2018) A further crucial advance of the NIS2 is applying stronger compliance requirements for CSPs operating in different jurisdictions. (Vandezande, 2023) Typically, CSPs are international corporations covering various markets in multiple places around the world; thus, offering integrated rules for them to follow may contribute significantly to cost savings and overcome the challenges of implementing accurate measures, helping achieve optimal cybersecurity levels for cloud customers. (NIS2, Articles 5, 7, 18) This directive encouraged collaboration among CSPs and the involved stakeholders in essential domains like incident reporting obligations and information-sharing mechanisms. (NIS2, Articles 21, 23) Such cooperation may help in mitigating the consequences of cybersecurity breaches to maintain service continuity and enhance user confidence in cloud-based systems. (Hon, 2018) The directive requires CSPs as essential entities to inform the competent authorities about serious cybersecurity incidents within 24 hours and to submit a comprehensive report about it in 72 hours, in addition to proper notification for customers about any possible threats and the needed measures to be taken to confront them. *In case of cross-border incidents, the concerned Member State should be informed.* (NIS2, Article 23) Overall, the NIS2 directive is a significant piece of legislation that leads to strengthening the security of the cloud by mitigating the evolving cyber threats in cloud services. (Millard, 2021).

However, various legal debate surrounds the NIS2 Directive. While widely praised as a necessary upgrade from its predecessor (NIS), legal scholars offer contrasting views on its scope and practical implementation. Some argue that NIS2 brings essential improvements, especially by broadening the scope of

regulated entities and formalizing the role of CSPs as essential entities. These developments are seen as increasing harmonization and resilience in cross-border cybersecurity governance. (Vandezande, 2023)

On the other hand, critics attack the directive's operational complexity, especially regarding the ambiguity in national implementation mechanisms and the capacity of smaller entities to comply. The compliance burden placed on SMEs and decentralized actors may be too high, potentially creating uneven enforcement across Member States. This concern is echoed in practitioner commentaries that warn about fragmented interpretations of key obligations, such as reporting timelines or risk management protocols. (Hon, 2018) Scholars also debate the feasibility of NIS2's supply chain security provisions. While some support these efforts, stating they align with the distributed nature of cloud services (Millard, 2021), others question whether such requirements are realistically enforceable in large-scale cloud ecosystems involving global subcontractors. Critics argue that enforcing deep due diligence in supply chains could pose operational bottlenecks or legal overreach. A good case example to significantly illustrate the practical implications and importance of the NIS2 Directive in improving cybersecurity within cloud computing environments is the 'OVH cloud incident' of 2021, when a major fire destroyed several data centers in Strasbourg, France, resulting in the widespread disruption of cloud services for thousands of customers globally. This event highlighted critical vulnerabilities in cloud supply chain management and resilience planning. Under the NIS2 Directive, OVHcloud, as an essential entity, would have clearer and stricter obligations regarding risk assessment, incident reporting, and resilience measures, potentially reducing the impact and recovery time from such incidents (URL3).

The academic debate offers both support and criticism regarding the implications of the NIS2 directive on the cloud. The directive's intent to promote uniform cybersecurity measures and collaborative governance is widely supported. Yet, ongoing challenges such as the enforceability of cross-border requirements and administrative burdens on SMEs suggest continued refinement in regulatory design and practical application.

Cybersecurity Act and ENISA

In addition to the GDPR and NIS2, the Cybersecurity Act 2019 (CSA) stands as a fundamental piece of legislation establishing a high level of cybersecurity, resilience, and trust within the EU, contributing to the proper functioning of the internal market. (Montagnani & Cavallo, 2018) The CSA in Article 2 defines cybersecurity as '*The activities necessary to protect network and information*

systems, the users of such systems, and other persons affected by cyber threats'. It is to be noted that the act addressed several significant concepts and obligations to be adopted in the digital environments by the service providers, which would lead to best security compliance and enhance trust levels among customers (Millard, 2021). According to the act, the goal is to enrich the digital market through unified cybersecurity standards across the EU internal market. (CSA, Article 1) Imperatively, the establishment of the cybersecurity certification framework is a landmark of the CSA. The framework stipulated mechanisms for the certification schemes, which ratify that ICT '*refers to Information and Communications Technology, which refers broadly to technologies involved in communication, computing, networking, and data management, including hardware, software, internet services, and telecommunications infrastructure',* (Roztocki et al., 2019) products, services, and processes follow particular security requirements aiming to ensure confidentiality, integrity, authenticity, and the availability of the data stored, transferred, or processed through its whole lifecycle in the cloud ecosystem. (CSA, Article 46) These certification schemes have several essential security objectives, mainly to protect the data in the cloud against any accidental or unauthorized activities and to ensure that only authorized actors can access the data (Tsvilii, 2021). To manage and administrate these schemes, the CSA mandates the European Agency for Cybersecurity (ENISA), whose primary role is to recommend collaboration with the national authorities and the European Commission to design and organize them in compliance with the related regulations. (CSA, Article 4).

Notably, some concerns were raised over the voluntary nature of these certification schemes, whereas without mandatory enforcement, the CSA risks creating a two-tier system where only well-resourced CSPs pursue certification, leaving SMEs vulnerable and less compliant. These concerns highlight a need for regulatory balance between flexibility and obligation in certification implementation. The paragraph also addresses the CSA's reliance on ENISA for certification oversight. While some experts commend ENISA's technical competence and independent role in guiding certification efforts, others question whether ENISA has sufficient enforcement capabilities or resources to oversee certification at the scale needed across the EU (Montagnani & Cavallo, 2018).

A further example that aligns with the CSA's certification goals is the Gaia-X initiative. It emphasizes European control over data infrastructure and integrates principles of data sovereignty and standardized security protocols. Scholars frequently cite Gaia-X as a model for operationalizing CSA ideals. However, critics caution that without legal enforceability, initiatives like Gaia-X may suffer from limited market adoption. (URL4) As well, the 2022 Vodafone Portugal

cyberattack serves as a cautionary case, underlining why standardization and certification are vital. While the CSA aims to mitigate such risks, some experts argue that certification alone is insufficient without clear incident response mechanisms and accountability structures (URL5).

The CSA's creation of the European Cybersecurity Certification Scheme for Cloud Services (EUCS) is seen as a transformative step. Scholars argue that EUCS promotes a harmonized standard of cybersecurity certification, which is essential in a fragmented regulatory landscape. Additionally, the fact that major cloud providers like Microsoft Azure, Google Cloud, and Amazon Web Services (AWS) align their practices with EUCS illustrates strong industry support for uniform standards (Tsvilii, 2021). A good case illustrating this alignment is AWS's acquisition of ISO certifications, such as ISO 27001, ISO 27017, and ISO 27018, highlighting adherence to security principles echoed by the CSA (AWS, 2023). These certifications serve as proxies for the forthcoming EUCS and demonstrate how voluntary schemes can foster trust, transparency, and robust cybersecurity practices for digital environments like the cloud industry (URL6).

Cybersecurity Failures in the Cloud: The Role of Contractual Agreements

Contracts and agreements are necessary tools in demonstrating and assigning liabilities of cybersecurity breaches in the cloud. The relationship between the cloud provider and their customers could be structured on various sources such as the Cloud Service Agreements (CSAs), the SLAs (Service Level Agreements), and the Shared Responsibility Model. (Radu, 2015) These agreements mainly specify the mutual rights, duties, and responsibilities of the parties in the cloud transactions, and the allocation of risks as they help to divide risks between the parties by their level of control depending on the cloud service deployment model used (SAAS, PAAS, or IAAS)(URL7) these are the main types of cloud computing. Each offers different levels of control and flexibility. SaaS (Software as a Service) allows the use of software applications online so no need to install them on your computer. Examples are Google Workspace and Microsoft 365, which provide productivity tools over the web. PaaS (Platform as a Service) gives a platform in the cloud for developers. They can create, test, and deploy applications without handling infrastructure. For instance, Google App Engine offers these developer-friendly services. IaaS (Infrastructure as a Service) provides virtual computing resources like servers and storage over the internet. Users have the most control over these IT resources.

Examples include Amazon and Microsoft Azure Virtual Machines. These models make up the backbone of cloud services, each meeting different user needs from those simply using the software to developers and IT professionals managing complex systems. (Geradin et al., 2022) The SLAs could be a significant instrument for determining and assigning liabilities of cybersecurity incidents between the parties involved in a cloud services agreement, especially when integrating security management as an indicator of tackling cybersecurity failures. (Millard, 2021) 'A service-level agreement (SLA) defines the level of service expected by a customer from a supplier, laying out metrics by which that service is measured, and the remedies or penalties, if any, should service levels not be achieved. Usually, SLAs are between companies and external suppliers. Still, they may also be between two departments within a company'. (URL8). The SLAs usually contain service metrics that manage incident-related issues like the initial response time until the final resolution. Additionally, it specifies the penalties imposed on vendors in case of non-compliance. (URL9). It should be structured on clear terms of liabilities and indemnities of the vendors for any data breaches or confidentiality violations. Moreover, it is essential to highlight guarantees of secure data migration and deletion to avoid exposure risks. Such legal clauses of secure data management would contribute to minimizing and controlling threats and the side effects of unauthorized access or data loss, which is an important factor for cybersecurity compliance in the cloud. (URL10). Most importantly, an indemnification clause is a pivotal contractual provision where the service provider agrees to compensate the customer for any costs arising from third-party legal claims due to the provider's breach of its warranties. This may include covering litigation expenses, while Standard SLAs often exclude such clauses; it is advisable to have legal counsel draft one. However, the CSP may require additional negotiations to agree on its inclusion. (URL11). The shared responsibility model is another common style followed in cloud transactions to demonstrate mutual responsibilities, where cybersecurity measures are not only on the side of the CSPs, the cloud customers are also obliged to take several steps and bear an amount of liability arising from any cybersecurity incidents, or breaches that occur to data in the cloud. (URL12). The shared responsibility model is a framework stipulating the mutual responsibilities of security aspects in the cloud between the providers and the customers. (URL13). Usually, cybersecurity responsibilities are divided by the customer's responsibility, which always includes the device security, accounts, and identity management. Provider Responsibility: Includes physical hosts, networks, and data centers (URL14). Cloud services contracts are vital tools for assigning liability and distributing different responsibilities in the cloud ecosystem.

They help to boost accountability by adhering to security requirements such as data encryption and incident reporting measures, leading to the best results of cybersecurity practices among cloud transactions. Considering the complexity and dynamic risks connected with various layers and parties in the cloud ecosystem, it is mandatory to conduct well-structured cloud service agreements to enhance cybersecurity resilience and ensure fair division of liabilities for cybersecurity failures in the cloud (Millard, 2021).

Impact of Evolving Technologies on Cloud Cybersecurity

AI: Opportunities, Capabilities, and Compliance Challenges

Despite the importance and the crucial role of cybersecurity obligations specified in multiple regulations -as described in this article- the application of technological innovation as a tool for enhancing cloud security defenses is now in rapid growth. (URL15) That is understandable when evaluating the benefits of AI, like the ability to screen out massive amounts of data, spot and tackle threats, and make real-time judgments. (URL16). Several functions of AI may benefit security in cloud environments, for instance, threat detection where machine-learning models are applied to spot deviations or risks. Additionally, deep learning techniques could be employed in the cloud, such as CNNs and RNNs, which are vital for processing big amounts of data and detecting risk patterns. Moreover, AI provides exceptional advancements in terms of incident response, as it can tackle and assess the severity of the attack and act accordingly in a way that is more efficient and saves time and effort. (URL17). AI in the cloud could also be used to analyze trends in the cloud ecosystem, such as user behavior, network traffic, and resource utilization, and indicate any future possibilities of threats or gaps in the cloud infrastructure that would lead to mitigating risks and associated impacts of any cybersecurity risks. (URL18). Generally, AI-based solutions and systems indicate a promising future for better cloud cybersecurity. However, several challenges exist, such as privacy concerns, since AI usually deals with huge amounts of data that would create tension between ensuring the best data security and adhering to data protection regulations such as the GDPR. Additionally, integration with legal systems is another issue, enterprises would face difficulties in applying technological innovation systems such as AI with their current old infrastructure, forcing them to upgrade to bridge the gap, which as a result imposes more costs and efforts, especially for evolving companies. Last but not least, adopting AI security solutions requires IT professionals and

experts in this field to be correctly applied for the best outcomes, which would put more pressure and costs, especially for small companies (URL19).

Blockchain: Strengthening Trust and Confronting Legal-Technical Barriers

The application of Blockchain technology within cloud computing can revolutionize cybersecurity by tackling significant weaknesses found in conventional cloud infrastructures. The decentralized and immutable characteristics of Blockchain guarantee secure and transparent data transactions, greatly improving data integrity and resilience against breaches. In contrast to centralized databases, which a single point of failure can compromise, Blockchain disperses encrypted information across numerous nodes, rendering unauthorized access nearly unattainable. Furthermore, Blockchain's capacity to deliver a verifiable record of transactions fosters trust between users and cloud service providers by providing full transparency regarding data storage and processing. Considering the facilities it provides for more secure digital environments, Blockchain is an excellent technology that significantly enables companies to create safe, effective, and trustworthy systems even when cyber threats are growing significantly (URL20). Blockchain has advantages connected to cybersecurity in terms of its implementation in cloud computing due to the integrated cryptographic procedures and the lack of a central authority. It establishes a reliable means of ensuring data integrity and safeguarding against alterations. In addition, the risks of unauthorized changes are significantly lowered by requiring agreement on changes using consensus mechanisms such as Proof of Work or Proof of Stake, and there is a reliable audit trail. Moreover, Blockchain strengthens identity and access management using data decentralization that lowers the likelihood of breaches and identity theft occurring. Its distributed structure also provides resistance against certain threats such as DDoS (distributed denial of service) attacks, suggesting network reliability even when some nodes are taken over, making it a useful tool for cloud cybersecurity (URL21). However, the adoption of Blockchain technology in the cloud faces numerous challenges. There is the possibility that custom features can create weaknesses, and while Blockchain technology brings remarkable security utilizing both decentralization and cryptography, it does have its weaknesses. The growing volume of the database may heavily impact performance and scalability, especially for users that need swift transactions. Service and operation concerns hinder many from attempting to use this solution, with vendors required to establish strong trust through solid services and contracts. Lastly, due to the multi-jurisdictional and decentralized nature of Blockchain, the selection of relevant or applicable regulations

could be a critical issue. It is crucial to address and handle these problems and challenges to fully utilize the benefits of Blockchain technology in cloud transactions (URL22).

Conclusion

Cloud technology has changed the way we manage data and deliver services, but it has also brought complex cybersecurity and legal challenges. This article looked at the relationship between regulatory frameworks (GDPR, NIS2 Directive, Cybersecurity Act) and emerging technologies (AI and Blockchain) in cloud cybersecurity. Through doctrinal analysis, several key findings have emerged.

Firstly, cybersecurity in the cloud is a shared responsibility. Both cloud service providers and customers must work together to meet legal obligations and implement robust technical controls. Although European regulations provide a good foundation, practical application still has its challenges. Uncertainties around cross-border data transfers, joint controllership, and liability between controllers and processors, especially in multi-jurisdictional scenarios, remain unresolved. Contractual instruments, especially Service Level Agreements (SLAs) and Shared Responsibility Models, have emerged as key tools to define obligations and liability. However, most SLAs lack the necessary depth in cybersecurity-specific terms and, therefore, create legal uncertainty and increased risk for both parties. Furthermore, the integration of emerging technologies like AI and Blockchain brings opportunities to improve threat detection, incident response, and data integrity. But it also brings new legal and operational challenges, including compliance with data protection regulations, interoperability issues, and increased costs, especially for smaller companies. Cybersecurity certification frameworks introduced by the Cybersecurity Act offer a way to improve trust and standardization across the EU. However, the voluntary nature of these schemes may lead to unequal adoption, especially among small providers, and create compliance gaps in the market. Real-world incidents like the OVHcloud fire and the Vodafone Portugal cyberattack show the importance of supply chain security, resilience planning, and clear incident reporting protocols.

Given these findings, future research should focus on standardizing contractual norms across the EU to harmonize cybersecurity in cloud services. It should also clarify international data transfer obligations and the responsibilities of non-EU processors under the GDPR. Empirical studies are needed to evaluate the effectiveness of cybersecurity certification schemes, especially the European Cybersecurity Certification Scheme for Cloud Services (EUCS). Finally,

legal frameworks must evolve to address AI and Blockchain with special attention to accountability, transparency, and liability in increasingly automated or decentralized systems. In the end, a secure cloud will need coordinated regulatory approaches, strong contractual governance, and responsible innovation. Regulators, providers, lawyers, and technologists will need to work together to adapt the legal and policy frameworks to the digital world.

References

Carey, P. (2018). *Data protection: A practical guide to UK and EU law* (5th ed.). Oxford University Press.

Dagostino, G. (2019). *Data security in cloud computing* (1st ed.). Momentum Press.

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

Geradin, D., Bania, K., Katsifis, D., & Circiumaru, A. (2022). *The regulation of cloud computing: Getting it right*. 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)*. 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.* Palgrave Macmillan. https://doi.org/10.1007/978-3-030-54660-1

McGillivray, K. (2022). *Government cloud procurement*. Cambridge University Press.

Millard, C. (2021). *Cloud computing law*. Oxford University Press.

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

Radu, B. (2015). Key aspects of cloud-computing services-related contracts. *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*. CRC Press.

Roztocki, N., Soja, P., & Weistroffer, H. R. (2019). The role of information and communication technologies in socioeconomic development: Towards a multidimensional framework. *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. 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*. 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*. Springer.

Online links in the article

URL1: *News analysis on how the UK Information Commissioner's Office adjusted its GDPR enforcement strategy by reducing fines imposed on major companies.* 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.* 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.* https://journal.uptimeinstitute.com/tag/fire-suppression/

URL4: *Policy brief analyzing Europe's strategic challenges and policy options in achieving cloud sovereignty.* 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.* 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.* 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.* 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.* 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.* 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.* 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.* https://www.cio.com/article/274740/outsourcing-sla-definitions-and-solutions.html

URL12: *Industry article clarifying the shared responsibility model in cloud computing environments.* 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.* https://www.wiz.io/academy/shared-responsibility-model
URL14: *Microsoft documentation describing shared responsibility for security and compliance in cloud services.* 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.* 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.* https://ijisae.org/index.php/IJISAE/article/view/6709/5576
URL17: *Research article exploring AI-driven solutions for improving cloud security mechanisms.* 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.* 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.* 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.* 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.* 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.* https://www.diplomacy.edu/wp-content/uploads/2021/06/111220181248_Boujemi.pdf

Laws and regulations

Cybersecurity Act and ENISA (CSA)
Network and Information Systems Directive (NIS2)
The General Data Protection Regulation (GDPR)

Reference of the article according to APA regulation

Khraisha, W. (2026). Cybersecurity in Cloud Industry: Legal Obligations and Liabilities under European Regulations & Technological Advancements. *Belügyi Szemle*, *74*(1), 165–182. https://doi.org/10.38146/BSZ-AJIA.2026.v74.i1.pp165-182

Statements

Conflict of interest

The author has declared no conflict of interest.

Funding

The author did not receive any financial support for researching, writing, and/or publishing this article.

Ethics

No dataset is associated with this article.

Corresponding author

The corresponding author of this article is Wasim Khraisha, who can be contacted at wasimkhraisha@gmail.com.