The impact of the CLOUD Regulation on digital information management methods and tools in public procurement

Raffaele Picaro, Carla Pernice, Martino Monaco, Denard Veshi, Alessia Fachechi, Roberta Catalano, Beniamino Di Martino, Luigi Colucci Cante, Mariangela Graziano, Alberto Pavan, Claudio Mirarchi

Abstract This study analyses the impact of the recent Regulation for digital infrastructures and cloud services for the public administration (the so-called CLOUD Regulation), adopted by the National Cybersecurity Agency pursuant to Article 33 septies, paragraph 4, of Legislative Decree no. 18 October 2012, converted by Law no. 221 of 17 December 2012, on the methods and tools of digital information management in the context of public contracts. In particular, there is a need to assess the adequacy of the regulatory framework outlined by the Procurement Code and the voluntary technical standards to guarantee the security standards required by the latter legislative intervention with specific reference to the Data Sharing Environment.

Raffaele Picaro e-mail: raffaele.picaro@unicampania.it, Carla Pernice e-mail: carla.pernice@unicampania.it, Martino Monaco e-mail: martino.monaco@unicampania.it, Alessia Fachechi e-mail: alessia.fachechi@unicampania.it and Roberta Catalano e-mail: roberta.catalano@unicampania.it
Department of Law, University of Campania "L. Vanvitelli", Caserta, Italy

Denard Veshi e-mail: dveshi@beder.edu.al
School of Law at University of Bedër(Tirana, Albania)
Department of Law, University of Campania "L. Vanvitelli", Caserta, Italy

Luigi Colucci Cante e-mail: luigi.coluccicante@unicampania.it, Mariangela Graziano e-mail: mariangela.graziano@unicampania.it and Beniamino Di Martino e-mail: beniamino.dimartino@unicampania.it
Department of Engineering, University of Campania "L. Vanvitelli", Aversa, Italy

Alberto Pavan e-mail: alberto.pavan@polimi.it and Claudio Mirarchi e-mail: claudio.mirarchi@polimi.it
Department of Architecture, Built Environment and Construction Engineering Politecnico di Milano Milano, Italy

1 Introduction to the Digitalization of the Italian Public Procurement.

The profound metamorphosis brought about by the digital transition – which has transformed the world of contracts and payments in the last decades, and is about to revolutionize the justice system – is also preparing to renew the construction sector and, in particular, the public procurement sector, inducing a rethinking of the tools used for the management of buildings and infrastructures. The purely documentary approach to the administration of real estate assets, for a long time, based on the preparation of heterogeneous and difficult-to-reconcile plans and documents [12], has had to give way, also in light of the interventions of the European legislator, to a different organization of the phenomenon, based on the digitalization of construction processes. In this perspective, Art. 22(4) of Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 gives the opportunity of Member States to require, for public contracts and design competitions, the use of specific electronic tools, such as electronic Building Information Modeling (so-called "BIM") [3, 6]. More specifically, BIM can be defined as a method for the design and management of buildings and infrastructures, based on cooperation between the actors involved [14, 4]. Therefore, BIM is not software but a method of building and infrastructure construction that uses all information related to architecture, structure, mechanical engineering, civil engineering, structure, and construction of the life of the building [16]. This paper focuses on the Italian case due to the recent valorization of the use of BIM in public works contracts, as well as the approval of the recent regulation of the National Cybersecurity Agency (ACN) (the so-called CLOUD Regulation) concerning the security of cloud infrastructures used by the public administration. The inadequacy of traditional design and maintenance mechanisms adopted in the building sector has required a thorough review of the current regulatory framework on the matter, which culminated, at an Italian national level, in the adoption of a discipline dedicated explicitly to the topic of Building Information Modeling. BIM was first introduced by Ministerial Decree 560/2017, a secondary legal source, and then, subsequently rewritten by the new Italian Public Procurement Code in March 2023, a primary legal source. The Public Procurement Code intended to maximize the use of electronic modeling tools for construction and infrastructure by implementing an organic arrangement of BIM in the context of public procurement, seeking to fully exploit the potential of this working method to ensure the best outcome of the collective investment. It not only dedicates new and significant provisions to BIM, codified in art. 43 and Annex I.9, by also filling substantial gaps in the previous regulation, but it also attempted to implement its adoption by contracting authorities even beyond the conception phase, enhancing its role to digitalize the entire life cycle of the public contract [13]. The introduction to BIM is part of a broader general project to strengthen the use of new technologies in administrative activities and procedures. This objective is expressly codified in art. 19 of the Italian Public Procurement Code, entitled Digital principles and rights. Based on this background, in June 2024, the ACN published the Regulation for Dig-

ital Infrastructures and Cloud Services for public administration (so-called CLOUD Regulation) with the goal of protecting e-digitalization from various attracts without losing efficiency. The regulation aims to define, among other things, the methods of classification, migration, and qualification of cloud services used by the public administration. The problem might arise of verifying the applicability of the CLOUD Regulation to construction processes managed with BIM, with specific reference to the Common Data Environment (so-called CDE), which is a BIM instrument based, usually, on cloud technology. With specific reference to qualification processes, the Public Procurement Code does not provide for the CDE any certification of conformity to ISO standards; on the contrary, the CLOUD Regulation identifies, for cloud services used by public administrations, four qualification levels that presuppose specific certifications and, sometimes, self-declarations that attest to conformity to ISO standards. Focusing on the specific object of the paper, it shall be mentioned that currently, the majority of the private operators of cloud service have all the needed certifications established for the first qualification level, which corresponds to the application of "ordinary" data. However, under the CLOUD Regulation, such certifications are insufficient to manage critical or strategic data. Therefore, the applicability of the regulation to the Common Data Environment will prevent public administrations from using cloud services without the corresponding qualification for managing critical or strategic data. Thus, this paper, through an interdisciplinary approach, aims to verify the applicability of the new Italian CLOUD Regulation to the public procurements working on CDE.

2 Digitization and Cybersecurity in the Public Procurements Code.

The objective of the complete digitalization of public procurement procedures, pursued by the Public Procurement Code, raises numerous questions regarding the risk of data breach and, more generally, the IT security of the platforms adopted by public administrations. The topic of IT security, in fact, assumes particular relevance in legislative intentions. Numerous legal and technical standards refer to it. For example:

- art. 19 of the Italian Public Procurement Code, after having stated that the contracting authorities and the granting bodies ensure the digitalization of the life cycle of the contracts, states that the contracting authorities and the granting bodies, as well as the economic operators who participate in the activities and procedures related to life cycle of the contract, adopt technical and organizational measures to protect IT security and the protection of personal data;
- art. 25(3) of the Italian Public Procurement Code provides that the contracting authorities and the granting bodies not equipped with their own digital procurement platform make use of the platforms made available by other contracting authorities or granting bodies, by central purchasing bodies or by aggregators,

by regions or autonomous provinces, which in turn can use a system manager that guarantees the functioning and security of the platform;
- art. 108(4) of the Italian Public Procurement Code establishes that in the case of procurement of IT goods and services for the public administration, the contracting authorities, including the central purchasing bodies, in the evaluation of the qualitative element to identify the best quality/price ratio for the award, shall take into account elements of cybersecurity by attributing specific and peculiar importance according to the context of use to the protection of strategic national interests;
- art. 1(8)(c) Annex I.9 of the Italian Public Procurement Code states that in the event of the assignment of services relating to architecture and engineering, the contracting authorities shall prepare an information specification to be attached to the tender documentation which contains, inter alia, the description of the specifications relating to the CDE and the conditions of ownership, access and validity of the same, also with respect to the protection and security of data and confidentiality, the regulation of copyright and intellectual property;
- art. 12(10) Annex II.14 of the Italian Public Procurement Code stablishes that the accounting of the works is carried out through the use of specific electronic tools, which use platforms, including telematics, interoperable by means of open non-proprietary formats, in order not to limit competition between technology suppliers. Such electronic tools shall guarantee the authenticity and security of the data entered and their origin from the competent subjects.
- Among the technical provisions dedicated to the topic of IT security is the UNI EN ISO 19650 standard since it also enhances the application of a new working culture of security in organizations that handle sensitive information. In addition, also the ISO 27001 standard is fundamental since it contains the requirements for assessing and treating information security risks.

Having clarified this and considering that the following discussion focuses on the security of the CDE, it is appropriate, as a preliminary step, to describe the architectural characteristics and IT components of this new technology, and in particular, the relationship between CLOUD and CDE. Once this relationship is clear, the research question of this paper can be easily answered.

3 Architectural characteristics and operational modes of information modeling. Focus on the Common Data Environment.

The CDE represents a crucial element in the context of BIM. The CDE is a central hub that allows all project actors to access, share, and update data in a coordinated and secure way [11]. The Italian Public Procurement Code emphasizes the lifecycle management of data in the CDE, underlining the importance of their integrity, traceability and controlled accessibility. Another key element of the regulation is the

promotion of interoperability and portability. In BIM, these features are essential to allow the transfer and use of data between different software platforms, avoiding the risk of vendor lock-in. Most significantly, art. 1 (4) of Annex I.9 of the Italian Public Procurement Code states that Italian public administrations adopt their own CDE by defining its characteristics and performance, ownership of the data, and the methods for processing, sharing, and management. The rule aims to avoid the risk that the owner of the environment may prevent the client from accessing it or even altering its contents [4]. Actually, this problem was also resolved by judges in the case Trant Engineering Limited v. Mott Macdonald Ltd., decided by the Technology and Construction Court of the United Kingdom and Wales in 2017 [10]. Although this rule has its own ratio, it increases doubts about data security since the Public Procurement Code does not include any specific provision rule for the data protection of CDE, although some input for interpretation can be found in Art. 1(8) and Art. 1(12) Annex I.9, when it allows contracting authorities to evaluate, with a view to the recognition of specific rewards, proposals aimed at facilitating the management of the CDE in the context of cybersecurity.

4 Analysis of the CLOUD regulation and coordination with IT security regulations.

The "CLOUD Regulation" rules the adoption and management of digital infrastructures and cloud services within the context of the public administration [15]. This regulation is part of a larger regulatory framework that includes the GDPR (General Data Protection Regulation) and the Italian legislation on administrative digitalization [2]. It aims to ensure high security, interoperability, scalability, and energy savings for all infrastructures part of the public contracts. One of the key features of the law is the categorizing of data into three major categories: i)**Ordinary**, whose compromise does not have significant impacts on critical functions; ii) **Critical**, whose compromise can damage the maintenance of essential functions for society, health and public safety and iii)**Strategic**, whose compromise can put national security at risk. This classification guides infrastructure and service choices, imposing specific requirements to ensure data integrity, confidentiality, and availability. In the context of Building Information Modeling (BIM), a digital methodology for designing and managing construction, the Data Sharing Environment (ACDAT)[1] represents a crucial element. The ACDAT is a central hub that allows all project actors to access, share and update data in a coordinated and secure way. In light of the ACN regulation rules, the ACDAT must be hosted on cloud infrastructures that meet stringent security and compliance requirements. These requirements are determined by the classification of the data managed in the environment. The relationship between ACDAT and the cloud represents a balance between technological innovation and centralised information management. On the one hand, ACDAT is an institutional

[1] https://processinnovation.wordpress.com/wp-content/uploads/2020/02/meridian-acdat.pdf

repository that guarantees the control and security of critical data; on the other hand, the adoption of the cloud offers scalability, accessibility and speed in the management of the same information. Integrating these two realities means being able to take advantage of the flexibility of the cloud without losing the reliability and governance inherent in a centralised system such as ACDAT, thus creating a modern and functional ecosystem. The CLOUD Regulation requires cloud service providers to comply with open standards to ensure data can be easily transferred between different systems without losing information or functionality [1, 7]. The cloud migration criteria further explore the relationship between data and infrastructure. The regulation requires Italian administrations to adopt detailed migration plans that include a risk assessment and a mapping of sensitive data [5]. The CLOUD Regulation will impact the operating methods and structure of the CDE since the CDE generally uses cloud systems [8, 17]. It shall be mentioned that CDE is based on a central repository in which all the documentation produced within the scope of that specific project is managed. More specifically, the platform used for this purpose is based on logging processes capable of recording the operations carried out, as well as on access systems regulated by strict authentication mechanisms and, above all, on the management of workflows through validation systems operating in each design phase, in compliance with the structural requirements established by the technical standard UNI EN ISO 19650. The obligation imposed on contracting authorities to use a 'proprietary' CDE, as established in art. 1(4) of the Annex I.9 of Italian Public Procurement Code, as well as the CLOUD Regulation, should not raise particular doubts regarding its applicability to the cloud platforms adopted by contracting authorities [9]. The cloud infrastructures must guarantee stringent security and compliance requirements in light of the CLOUD Regulation. These requirements are determined by the classification of the data managed in the environment. For example, strategic data related to the design of critical infrastructures shall be managed on systems that guarantee the highest level of protection against cyber threats. Every data operation, such as updating or deleting, must be logged to ensure transparency and accountability. In addition, CDE is expected to integrate advanced authentication systems to limit access to sensitive data only to authorized users, mitigating the risk of unauthorized access or security breaches. According to the CLOUD Regulation, also the authentication method depends on the risk of violation of information flows. For CDE, the approval of the CLOUD Regulation means that the transition to the cloud shall be planned in such a way as to minimize operational disruptions and ensure continuity of information flow during the migration process. Furthermore, the chosen cloud infrastructure must offer scalability capabilities to support the future expansion of BIM data and projects. Art. 17 of the CLOUD Regulation divides the qualification of cloud services for public administrations into 4 levels, assigning to the ACN the task of verifying compliance with the requirements for the qualification requested by the service provider[2]. With specific reference to the required certifications, Annex 4 of CLOUD Regulation establishes that:

[2] https://www.ingenio-web.it/articoli/ambienti-di-condivisione-dei-dati-acdat-o-cde-usi-e-costumi

- the QC1 qualification level, which allows the application of ”ordinary” data, presupposes a self-certification attesting to compliance with the ISO 9001 standard and an ISO/IEC 27001 certification or, alternatively, the Cloud Security Alliance – Star Level 2 certification;
- the QC2 qualification level, which allows the application of ”critical” data, presupposes, in addition to the certifications for QC1, also two self-declarations attesting compliance with the ISO 22301 and ISO 20000 standards respectively;
- the QC3 qualification level, which allows the application of ”strategic” data, presupposes, for the cloud service being qualified, the ISO 22301 certification, the ISO/IEC 20000 certification and the Cloud Security Alliance - Star Level 2 certification;
- the QC4 qualification level, which allows the application of ”strategic” data, presupposes, in addition to the certifications required for QC3, further requirements that concern, among other things, the inclusion of cybersecurity issues in personnel management processes (e.g. screening, deprovisioning) and the encryption mechanism of data managed in the cloud, in the sense that the administration must be able to autonomously manage and access the encryption keys exclusively.

Based on the qualification requirements, the self-declarations and certifications that shall be presented differ. More specifically, the cloud service could be usefully provided by a Software as a Service (SaaS) model in which the supplier takes care of its preparation and maintenance, leaving the public administration the role of the end user of the service. While, in general, a QC1 is sufficient, except that the law – according to the type of object of the public procurement (i.e., building a new airport) – a higher level of qualification is required. Thus, although the Public Procurement Code does not explicitly specify the type of certifications for CDE's management, this has been established by the CLOUD Regulation. In simple words, there is a need for a systematic interpretation of the Italian legal system. Furthermore, there is a need for the CDE to comply with the requirements imposed by the CLOUD Regulation by precluding the parties from downloading the data contained in the CDE onto personal devices. Otherwise, the requirements imposed by the CLOUD Regulation would lose their importance, considering that then the data can be accessed by the personal devices of the parties that do not apply all the standards of security codified in the CLOUD Regulation. The CLOUD Regulation also emphasizes energy savings and the sustainability of digital infrastructures since Annex 2 of CLOUD Regulation identifies, among other things, the minimum energy-saving requirements for cloud service infrastructures for public administration. The use of energy-efficient cloud infrastructures not only reduces operational costs but also contributes to environmental sustainability goals. In the context of BIM, this means that projects can benefit from data management that is not only secure and interoperable but also environmentally sustainable. Figure 1 shows the flow of actions and actors involved in complying with the ACN regulations in the context of a BIM project. This figure tries to visually demonstrate the main operation within BIM in the interplay with CLOUD Regulation. In particular, its main actors have the following duties:

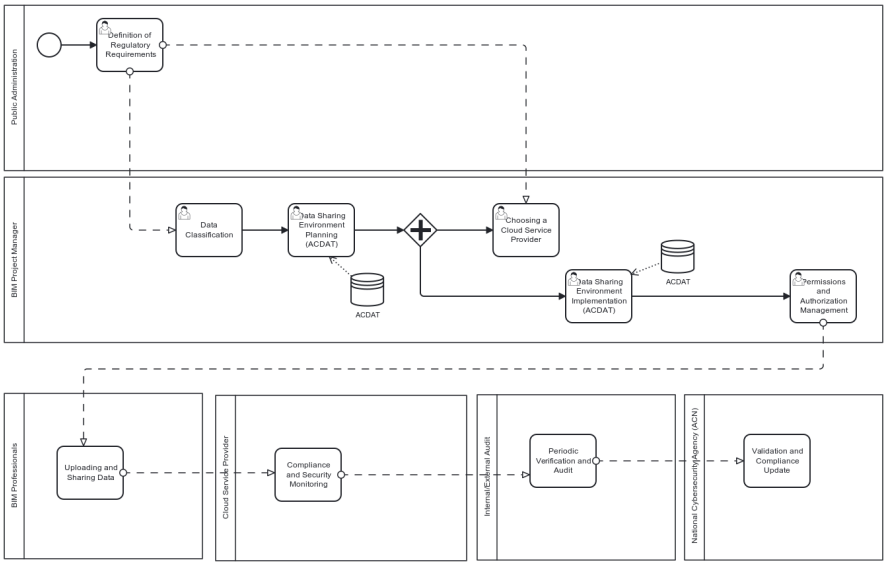

Fig. 1 BPMN of actions and actors involved in complying with the ACN regulations in the context of a BIM project

- **Public Administration**: analyzes CLOUD Regulation and identifies the requirements applicable to the project that includes BIM. This initial phase of the process ensures that regulatory aspects are considered from the beginning, laying the foundations for a well-structured approach that complies with current regulations.
- **BIM Project Manager**: classifies the project data into ordinary, critical, and/or strategic, as established in the CLOUD Regulation, and ensures that each data type is treated with the appropriate level of protection. They then define the CDE architecture, specifying the security, scalability, and interoperability requirements. These actions ensure that the CDE is designed to adequately respond to the needs of the project and security regulations. He then proceeds to select a Cloud Service Provider compliant with the different rules and proceed to configure the Cloud environment, and implement the CDE, following the defined specifications. After implementing the CDE, the BIM Project Manager configures data access following the principle of least privilege, according to which each user must have access only to the information strictly necessary, thus reducing the risks associated with security breaches.
- **BIM Professionals**: use the CDE to upload, update, and share project data, thus ensuring a collaborative workflow and constant updating of information
- **Cloud Service Provider**: constantly monitors the security and integrity of the infrastructure, reporting any incidents. In this way, there is a guarantee that the environment always remains safe throughout the entire life cycle of the project

- **Internal/External Audit**: figures responsible for verifying the compliance and security of the CDE and cloud infrastructures in relation to CLOUD Regulation. Through this periodic control phase, it is possible to identify gaps and continuously improve the system
- **National Agency for Cybersecurity (ACN)**: validates the system's compliance and updates, if necessary, the regulatory requirements. This validation activity ensures that the project remains aligned with regulations and adequately protects data

5 Discussion and conclusion

This paper studied the application of CLOUD Regulation in the case of public procurements, that currently also include BIM. The contribution included an interdisciplinary approach since this topic is per se interdisciplinary. In other words, there is a need to understand the technical and legal perspectives. The research focused on the case of Italy since, in 2023, the Italian lawmaker introduced BIM, starting from 1 January 2025, as a mandatory requirement for all public procurements over 2.000.000 EUR, while the EU only stimulated EU Member States to include the use of specific electronic tools, such as of building information electronic modeling tools or similar (Art. 24(2) Dir. 2014/24/EU). After uncovering the importance of the digitalization of public procurements and the interplay with cybersecurity threats, this paper focused on the CDE by answering the following research question: is the new CLOUD Regulation applied to public procurements that also include BIM? Based on art. 43(3) of the Italian Public Procurement Code, a primary legal source, as well as Chapter V of the CLOUD Regulation, CLOUD Regulation is also applied to public procurements that include BIM. More specifically, depending on the type of data – ordinary, critical, and strategic – there are four different levels of qualifications. While the first two levels of qualifications – QC1 and QC2, which correspond to ordinary and critical data – also include self-declarations, in the case of strategic qualifications – meaning QC3 and QC4 – only certifications are allowed. Additionally, in the case of QC4, there is also the need to demonstrate other requirements such as the inclusion of cybersecurity issues in personnel management processes (e.g. screening, deprovisioning) or the encryption mechanism of data managed in the cloud, in the sense that the administration must be able to autonomously manage and access the encryption keys exclusively. In addition, and more importantly, although operators have these certifications, the ACN needs to qualify them. Nevertheless, as stated in CLOUD Regulation, security protection depends on the project that will be built. For instance, in the case of an airport, the security threshold is much higher than in other cases. Last but not least, to give a compelling application to the requirements for its application, there is a need to prohibit the downloading of data onto personal devices. Otherwise, the data protection of the Italian public administration would lose its effective application.

Acknowledgements The work described in this paper has been supported by the research project SERICS (PE00000014), under the MUR NRRP funded by the EU - NextGenerationEU.

This preprint has not any post-submission improvements or corrections. The Version of Record of this contribution is published in Advanced Information Networking and Applications, and is available online at https://doi.org/10.1007/978-3-031-87778-0_21

References

1. Mazhar Ali, Samee U Khan, and Athanasios V Vasilakos. Security in cloud computing: Opportunities and challenges. *Information sciences*, 305:357–383, 2015.
2. Mohamed Almorsy, John Grundy, and Ingo Müller. An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*, 2016.
3. Luigi Colucci Cante, Beniamino Di Martino, and Mariangela Graziano. Artificial intelligence in architecture, engineering and construction sector and building information modeling: A review of methodologies, applications and future perspectives. In *International Conference on Complex, Intelligent, and Software Intensive Systems*, pages 363–372. Springer, 2024.
4. Beniamino Di Martino, Mariangela Graziano, and Luigi Colucci Cante. Semantic, business process and natural language processing for ebuilding. In *International Conference on Complex, Intelligent, and Software Intensive Systems*, pages 373–382. Springer, 2024.
5. Venkatachalam Venkat Ganapathy and Sreedevi Sampath. Regulatory and security compliance for software in cloud ecosystems–a systematic literature review. *Sreedevi, Regulatory and Security Compliance for Software In Cloud Ecosystems–a Systematic Literature Review*.
6. Mariangela Graziano, Beniamino Di Martino, and Luigi Colucci Cante. Semantic and inference-based techniques for iot-enabled discovery of escape routes in building information modeling. In *International Conference on Complex, Intelligent, and Software Intensive Systems*, pages 383–392. Springer, 2024.
7. Ibrahim Abaker Targio Hashem, Ibrar Yaqoob, Nor Badrul Anuar, Salimah Mokhtar, Abdullah Gani, and Samee Ullah Khan. The rise of "big data" on cloud computing: Review and open research issues. *Information systems*, 47:98–115, 2015.
8. Meiko Jensen, Jörg Schwenk, Nils Gruschka, and Luigi Lo Iacono. On technical security issues in cloud computing. In *2009 IEEE international conference on cloud computing*, pages 109–116. Ieee, 2009.
9. Indra Macrì. Strategie e modelli operativi per la sicurezza delle pubbliche amministrazioni al tempo del pnrr. *Rivista italiana di informatica e diritto*, 6(2):93–113, 2024.
10. Alberto Pavan et al. Common data environment (cde). an efficient and effective use in italian standard uni 11337: 2017. In *Re-shaping the construction industry*, pages 73–92. Maggioli, 2017.
11. R Picaro, C Pernice, et al. Legal bim e transizione digitale nel codice dei contratti pubblici. 2024.
12. Raffaele Picaro et al. *Il Building Information Modeling. Referente di obblighi e responsabilità.* ESI, 2019.
13. Raffaele Picaro et al. Il building information modeling e la gestione digitale del ciclo di vita del contratto pubblico nel d. lgs. n. 36/2023. *NUOVE AUTONOMIE*, (1):5–53, 2024.
14. Rafael Sacks, Charles Eastman, Ghang Lee, and Paul Teicholz. *BIM handbook: A guide to building information modeling for owners, designers, engineers, contractors, and facility managers*. John Wiley & Sons, 2018.
15. KV Sreevidya. Cloud computing technology and legal challenges. *International Journal of Advanced Research, Ideas, and Innovations in Technology.(4)*, 4:519–525, 2018.

16. Carlo Venditti, Raffaele Picaro, Denard Veshi, et al. Building information modeling in italy: An interdisciplinary approach. *RIVISTA GIURIDICA DI URBANISTICA*, (3):539–565, 2023.
17. Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation computer systems*, 28(3):583–592, 2012.