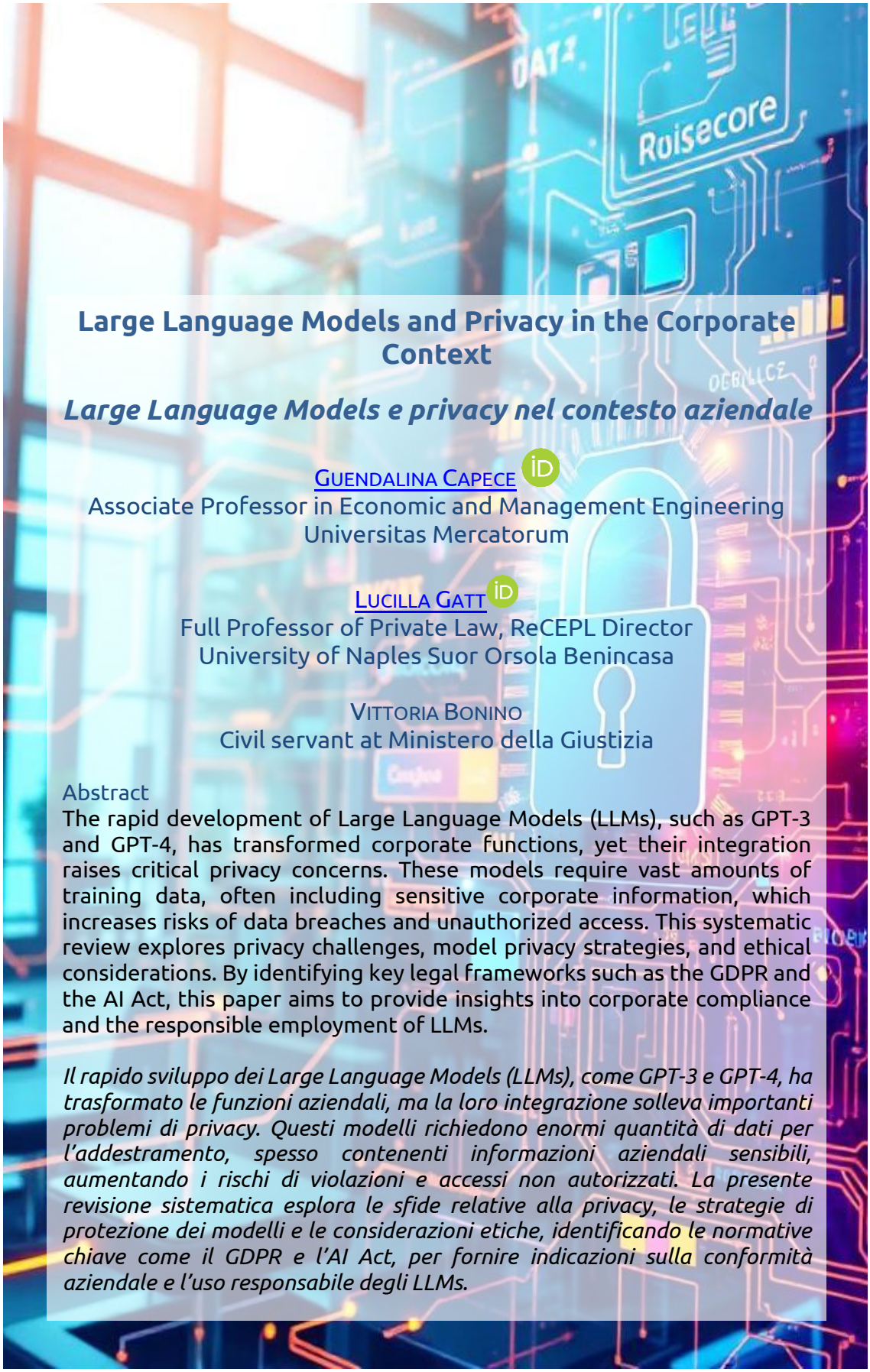
Capece G, Gatt L, Bonino V, 'Large Language Models and Privacy in a Corporate Context' (2025) 1 EJPLT.
DOI: https://doi.org/10.57230/EJPLT251GCLGVB

EJPLT
ISSN 2704-8012



Large Language Models and Privacy in the Corporate Context

Large Language Models e privacy nel contesto aziendale

GUENDALINA CAPECE
Associate Professor in Economic and Management Engineering
Universitas Mercatorum

LUCILLA GATT
Full Professor of Private Law, ReCEPL Director
University of Naples Suor Orsola Benincasa

VITTORIA BONINO
Civil servant at Ministero della Giustizia

Abstract
The rapid development of Large Language Models (LLMs), such as GPT-3 and GPT-4, has transformed corporate functions, yet their integration raises critical privacy concerns. These models require vast amounts of training data, often including sensitive corporate information, which increases risks of data breaches and unauthorized access. This systematic review explores privacy challenges, model privacy strategies, and ethical considerations. By identifying key legal frameworks such as the GDPR and the AI Act, this paper aims to provide insights into corporate compliance and the responsible employment of LLMs.

Il rapido sviluppo dei Large Language Models (LLMs), come GPT-3 e GPT-4, ha trasformato le funzioni aziendali, ma la loro integrazione solleva importanti problemi di privacy. Questi modelli richiedono enormi quantità di dati per l'addestramento, spesso contenenti informazioni aziendali sensibili, aumentando i rischi di violazioni e accessi non autorizzati. La presente revisione sistematica esplora le sfide relative alla privacy, le strategie di protezione dei modelli e le considerazioni etiche, identificando le normative chiave come il GDPR e l'AI Act, per fornire indicazioni sulla conformità aziendale e l'uso responsabile degli LLMs.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: LLMs; Privacy; GDPR; AI Act; Corporate Compliance; Data Protection

Summary: 1. Introduction. – 2. Methodology. – 3. Results. – 4. Analysis of the Results. – 4.1 Data Privacy Concerns. – 4.2 Model Privacy Concerns. – 4.3 Ethical Considerations. – 4.4 Regulatory and Compliance Issues. – 4.5 Mitigation Strategies. – 5. Conclusion.

1. Introduction.

The evolution of Large Language Models (LLMs) such as GPT-3 and GPT-4 has had a significant impact on various business functions, ranging from customer service to data analysis. However, the integration of LLMs into corporate environments brings with it important concerns regarding information privacy and the huge amounts of data required to train these models, which frequently tend to include sensitive corporate information, thus increasing the risks of data breaches and unauthorised access, and not to be overlooked are the ethical implications of using LLMs, including bias and transparency issues. This systematic literature review aims to examine the privacy implications of implementing LLMs in business contexts. Data privacy concerns, model privacy strategies as well as ethical considerations will be explored, with the aim of providing a comprehensive overview of the current state of knowledge and identifying areas for future research.

2. Methodology.

In order to conduct a comprehensive literature review on the intersection between Large Language Models (LLMs) and privacy in the business context, a systematic approach was followed. The selection of studies was based on criteria defined with the aim of including only relevant research in the field in question and, more specifically, studies were selected that focus on the use of LLMs and their close correlation with the violation of data protection regulations and legislation both at national and European level without neglecting, however, the corporate context in which these tools are increasingly used and employed not only to improve production activities but also to speed up the decision-making processes of employees in the performance of their duties. Thus, peer-reviewed articles, conference papers and normative documents between 2020 and 2024 were selected, while, on the contrary, non-academic studies, such as blog posts and opinion articles, as well as those not directly addressing privacy issues were excluded.

The search was conducted using numerous databases to collect relevant literature, including *Google Scholar, IEEE Xplore, PubMed, Scopus, Web of Science and legal databases such as Westlaw, LexisNexis, the European Journal of Privacy Law & Technologies archive, DeJure and Wolters Kluwer*. The aim was to select the studies starting with the selection of keywords such as Large Language

Models, LLMs, privacy, data protection, business context, GDPR, General Data Protection Regulation, AI ethics, data security, regulation, EU regulation, AI, AI privacy, AI Act, Data Act and Digital Services Act and, to refine the search and ensure a broader coverage of studies related to the topics under study, Boolean operators (AND, OR, NOT), synonyms and alternative terms were used.

For the proper selection of studies, an initial assessment of the titles and abstracts was carried out by identifying potentially relevant and topic-related articles. Only afterwards, a detailed review of the texts of the individual articles was carried out to assess their eligibility on the basis of the previously selected criteria and to eliminate duplicates and irrelevant content accordingly.

3. Results.

A PRISMA guideline system was used as shown in Figure 1. Based on this methodology, in the first phase, 800 records were identified from multiple databases, including legal archives as indicated above. After the removal of duplicates (n = 117) and records marked as ineligible by automated tools (n = 20) and records removed for other reasons (n = 89), 574 unique records remained. consequently, through an initial screening based on titles and abstracts, 527 studies were selected on the basis of a careful assessment of the relationship of keywords, titles and abstracts.

To this end, a detailed analysis of the full texts was conducted, resulting in an evaluation of 444 records, of which 403 studies were excluded for various reasons: insufficient relevance to the topic (n = 138), exclusive focus on technical aspects without in-depth analysis on privacy (n = 56), non-business contexts (n = 75), lack of correlation with LLMs and privacy (n = 33) or irrelevant publication date (n = 101). With reference to the period of analysis used and with reference to the North American and European studies, it can be seen that the largest number of articles was produced in the last two years.

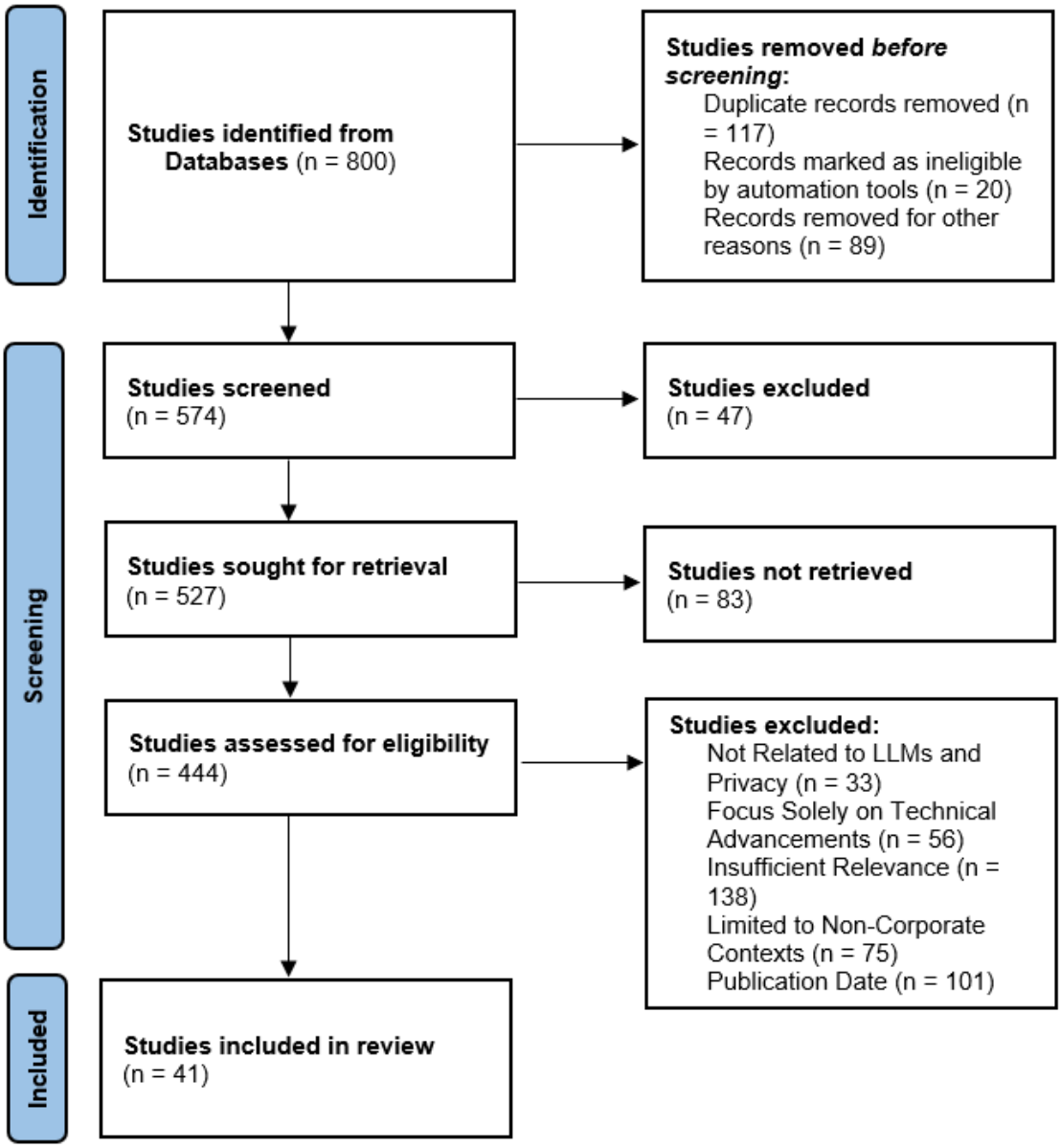


Fig 1: PRISMA flow diagram for new systematic reviews which includes searches of databases

4. Analysis of the Results.

4.1 Data Privacy Concerns.

The protection of data privacy particularly in the implementation of Large Data Models (LLMs) in corporate organisations entails a number of critical issues highlighted in recent literature outlining the complications and vulnerabilities associated with data breaches involving LLMs that produce significant risks in the implementation of such technologies in corporate

contexts.[1] Some authors[2] point out that a concrete risk is unauthorised access to sensitive corporate data used to train LLMs and if not adequately protected, such data could be exposed or misused with potential legal and reputational risks for the company. There is therefore a need to mitigate these risks through the implementation of appropriate security measures, including advanced security measures such as encryption, secure data storage systems and stringent access controls to limit or totally eliminate the danger of data leakage.

According to Authors[3] , corporate organisations should invest in monitoring and detection systems proactively in order to achieve a faster level of detection of such breaches and, in addition, regular audits and compliance checks may be essential to ensure that data protection protocols are aligned with industry standards and current regulatory requirements.

Going further, unauthorised access poses a critical threat in LLMs in corporate environments and, in particular, in large ones where data leakage or misuse can occur more easily due to the presence of a larger number of operators in the technology systems. The involvement of different operators amplifies the possibility of data leakage, particularly sensitive data, as well as illicit access to data used to train LLMs by compromising confidentiality and integrity. [4] Consequently, among the various tools placed in support of organisations is the implementation of systems aimed at catching suspicious activities at an early stage by protecting access to training data and developing increasingly comprehensive security protocols to help companies reduce and mitigate the risk of legal access while also protecting sensitive data through the ethical and legal use of LLMs technologies during their operations. [5] Organisations, in these terms, should also take care to outline and establish clear policies for the collection, storage and application of sensitive data for the training of such technologies as well as develop compliance controls to verify adherence to certain protocols and thereby mitigate the risks of unauthorised exposure or misuse of data.[6]

4.2 Model Privacy Concerns.

Inversion attacks represent one of the most serious threats to data privacy in the development of large language models, as they can compromise sensitive information used in their training. In fact, such attacks aim to extract

[1] L Gatt, IA Caggiano, MC Gaeta, AA Mollo, 'BCI devices and their legal compliance: A prototype tool for its evaluation and measurement' (2022) Proc IEEE Int Conf MetroXRAINE 551- 556.

[2] E Troisi, 'Automated Decision Making and right to explanation. The right of access as ex post information' (2022) 1 Eur J Privacy L & Tech 186.

[3] A Lombardi, 'Data protection regulation and artificial intelligence regulation: relationships, similarities and differences between GDPR and AI Act' (2023) 2 Eur J Privacy L & Tech 242.

[4] SS Yilmaz, HD Seval, 'Mind Over Matter: Examining the Implications of Machine Brain Interfaces on Privacy and Data Protection under the GDPR' (2022) 347 Eur J Privacy L & Tech 349-350.

[5] R Caso, 'Law, policy and economics of technological innovation: 1940, 1980, 2020' (2023) 2 Eur J Privacy L & Tech, 58-59.

[6] Gatt et al, 'BCI devices and their capacity to express human will having legal value' (2022) 1, Eur J Privacy L & Tech 291-292.

sensitive information by exploiting the vulnerable parts of such models[7] by being able to reconstruct parts of the original training data, putting the confidentiality of corporate information at risk.[8]

The use of differential privacy is an effective strategy that could be used to protect both corporate and personal data as it prevents attackers from isolating specific information within a dataset and thus reducing the risk of exposure.[9] In a study on data protection[10] demonstrated the effectiveness of differential privacy by making it a benchmark for training compliance with stringent data protection regulations. The crucial breakthrough of this type of implementation lies in giving stakeholders greater trust while promoting the responsible and safe use of advanced machine learning technologies in business contexts.[11]

4.3 Ethical Considerations.

The adoption of Large Language Models in the business context has also had repercussions in the ethical sphere with regard to bias, transparency and accountability in the use of data. Biases in training data outline an influence in the behaviour of LLMs generating, in most cases, discriminatory outcomes in business processes as well. Recent research has shown how biases in datasets considerably widen inequalities and negatively delineate business decisions. In order to avoid the emergence of biases, proactive measures such as, for example, the curation of diverse datasets, algorithmic audits and continuous monitoring are required to mitigate discriminatory impacts.[12]

Transparency plays a crucial role. Transparent practices can ensure accountability and build trust among practitioners as well as limit concerns about opacity and potential inappropriate use of LLMs' outputs in business environments.[13] However, knowledge of the training process through outputs as well as the decision-making process can be very complex.[14] In fact, assigning responsibility for the outcomes generated by LLMs makes it difficult to determine who is responsible for errors, biases or highly discriminatory

[7] A Di Cerbo, 'La tutela dell' identità nell' ambiente digitale alla luce delle norme europee' (2024) 2 Eur J Privacy L & Tech, Eur J Privacy L & Tech 255-257.

[8] MG Caraceni, 'Digital surveillance technologies. Ethical, anthropological and political issues' (2022) 1 Eur J Privacy L & Tech, Eur J Privacy L & Tech 347.

[9] A Winograd, 'Loose-lipped large language models spill your secrets: The privacy implications of large language models' (2022) 36 Harv JL & Tech, 615-656.

[10] MAK Raiaan et al, 'A review on large Language Models: Architectures, applications, taxonomies, open issues and challenges' (2024) IEEE Access 26839-26874, doi: 10.1109/ACCESS.2024.3365742.

[11] Y Yao et al, 'A survey on large language model (LLM) security and privacy: The good, the bad, and the ugly' (2024) High-Confidence Comput 100211, https://doi.org/10.1016/j.hcc.2024.100211.

[12] S S Yilmaz and Seval, 'Mind Over Matter' (n 4) 347.

[13] U Pagallo, J Ciani, 'Anatomy of Web Data Scraping: Ethics, Standards, and the Troubles of the Law' (2023) Standards 15-17.

[14] S Guida, 'New machine behavior's evolutionary approaches between AI learning, control and ethics promoting cooperative Human-Machine Intelligence' (2022) 1 Eur J Privacy L & Tech 329.

consequences. The solution may lie in the integration of frameworks assigning the degree of responsibility, not only among developers, but also between users and regulators to ensure greater protection in the development of LLMs.[15]

4.4 Regulatory and Compliance Issues.

Currently, the regulation of the use of data in Large Language Models (LLMs) is mainly based on the General Data Protection Regulation (GDPR), as the main European privacy and security regulatory reference. The latter outlines specific requirements for the processing and protection of personal data as it can directly influence how LLMs secure sensitive information.[16]

In recent years, the regulation of AI has found an initial shape in various regulatory sources such as the IA Act and the Digital Services Act (DSA) developed at European level with the aim of controlling the activity of these technologies by structuring a different degree of risk of different intelligences. The AI Act and the DSA were introduced to establish a clear regulatory framework with a preventive security attitude that regulates both artificial intelligence technologies and digital platforms. Consequently, through a preliminary analysis assessing the context of reference, the AI Act sought to regulate the use of AI technologies, including LLMs, establishing the necessary and very stinging requirements for transparency, accountability and human oversight, thus shaping the needs in the various sectors.[17] [18] However, existing regulations remain deficient if overly stringent to address the new challenges posed by LLMs, fuelling insecurities regarding algorithmic accountability, cross-border data flow and the appropriateness of today's rapidly evolving technologies. For example, the GDPR imposes restrictions on the transfer of data out of the EU, but does not explicitly address how LLMs process cross-border information, creating regulatory and legal grey areas.[19] The hope is to address these gaps through legislative updates and collaborative efforts between different industry players to develop comprehensive guidelines that increasingly align with technological advances and ethical considerations surrounding the use and development of such technologies.[20] [21]

Despite the uncertain framework in which both operators and users, including companies, move, the latter could work to limit the damage by

[15] M G Caraceni, 'Digital surveillance technologies' (n 8) 142.

[16] P Konstantina, 'The implications of the General Data Protection Regulation (GDPR) on cross-border data transfer of the companies' (2021) [master's Thesis] Int Hellenic Univ, https://repository.ihu.edu.gr//xmlui/handle/11544/29826.

[17] A Lombardi, 'Data protection regulation and artificial intelligence regulation' (n 3) 215.

[18] A Tartaro, 'Regulating by standards: current progress and main challenges in the standardisation of Artificial Intelligence in support of the AI Act' (2023) Eur J Privacy L & Tech 147.

[19] M Mylrea, N Robinson, 'Artificial Intelligence (AI) trust framework and maturity model: applying an entropy lens to improve security, privacy, and ethical AI' (2023) 25(10) Entropy 1.24, https://doi.org/10.3390/e25101429.

[20] SF Dicorato, M De Pamphilis, 'Stretching the Rules: How Racing Design May Drive the Evolution of the Technological and Legal Environment' (2022) Eur J Privacy L & Tech 169.

[21] R Caso, 'Law, policy and economics of technological innovation' (n 5) 1940.

providing for privacy impact assessments (PIAs) and data anonymisation techniques as well as the integration of privacy by design principles in AI development processes.[22] [23]

4.5 Mitigation Strategies.

The need for the development of advanced technologies therefore arises in order to strengthen the protection of data privacy and models in LLMs' business applications. Methods such as homomorphic encryption, secure multiparty computing and federated learning allow sensitive data to be processed without compromising confidentiality.[24] Authors[25] point out that these techniques allow LLMs to work on encrypted data, reducing the risk of unauthorised access and data leakage.[26] [27] Indeed, more recent research has been concerned with outlining the interactions of LLMSs in cybersecurity by outlining how big data analytics systems improve the ability to detect cyber threats through advanced anomaly detection techniques applied to network logs and attack patterns.[28]

Among the various strategies to limit the outflow of data, companies should focus on establishing strict data governance, perform regular audits and implement stringent access controls.[29] Furthermore, the need to integrate ethical guidelines into AI development cycles should not be overlooked and fostering a culture of responsible data management among employees is crucial to creating a privacy-conscious corporate environment.[30]

5. Conclusion.

The integration of Large Language Models (LLMs) into businesses is transforming operational and decision-making processes, offering advanced tools for data analysis and business automation. It should not be underestimated, however, that their use raises crucial issues of data protection

[22] S Guida, 'Enisa' s last technical analysis of data pseudonymization advanced measures in data protection and privacy' (2021) Eur J Privacy L & Tech 262.
[23] M G Caraceni, 'Digital surveillance technologies' (n 8) 142.
[24] S F Dicorato and M De Pamphilis, 'Stretching the Rules' (n 21) 169.
[25] A Lombardi, 'Data protection regulation and artificial intelligence regulation' (n 3) 215.
[26] M Hassanin, N Moustafa, 'A Comprehensive Overview of Large Language Models (LLMs) for Cyber Defences: Opportunities and Directions' (2024) Cryptography and Security (cs.CR) 1, https://doi.org/10.48550/arXiv.2405.14487.
[27] S Wairimu et al, 'On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies: A Systematic Literature Review' (2024) IEEE Access 1-26, doi:10.1109/ACCESS.2024.3360864.
[28] N Sharma, EA Oriaku, N Oriaku, 'Cost and effects of data breaches, precautions, and disclosure laws' (2020) 8(1) Int J Emerg Trends Soc Sci 33, doi:10.20448/2001.81.33.41.
[29] A Del Forno, 'Artificial Intelligence in Business Processes Management' (2022) Eur J Privacy L & Tech 119.
[30] R Caso, 'Law, policy and economics of technological innovation' (n 5) 1940.

and ethical responsibility, particularly with regard to the management of sensitive information and the transparency of algorithms. In order to mitigate these risks, it is crucial to adopt advanced data protection strategies, such as differential encryption and anonymisation, as well as to define clear ethical guidelines for the responsible use of LLM. In this way, adequate data protection not only reduces the risk of breaches and information leaks, but also ensures the reliability of LLMs, preventing distortions in models and ensuring greater transparency in decision-making processes. The hope is that future research will focus on the development of more robust regulatory standards and the evolution of ethical practices that allow for the safe and responsible use of LLMs in companies, contributing to a more secure and compliant digital ecosystem with data protection regulations.