ARTICLE

Incorporating emerging technologies for enhancing data privacy protection regulations

Bareq Muntadher Abdul Wahhab[1,*], **Safinaz Mohd Hussein**[1] **and Ramalinggam Rajamanickam**[1]

[1] Universiti Kebangsaan Malaysia, 43,600 Bangi, Selangor, Malaysia

Abstract

In the era of ever-evolving technological advancements and growing concerns about data privacy, exploring the crucial intersection between emerging technologies and data privacy protection regulations is crucial. The objective is to understand how cutting-edge technologies, such as artificial intelligence (AI), blockchain, Internet of Things (IoT), and biometric authentication, can be harnessed to strengthen data privacy safeguards in a rapidly changing digital landscape. This study investigates the positive and negative implications for incorporating these technologies into the framework of data privacy regulations, while emphasizing the importance of striking a balance between innovation and the protection of individuals' personal information. The findings suggests that a comprehensive approach to data privacy must integrate these technologies with strong emphasis on privacy by design, policies with consent management, ethical consideration that evidenced transparency and auditability, and education. This study contributes to ongoing discourse on data privacy in a digitalized world and offers insights into the future of data protection in the age of technological innovation.

Keywords: data privacy, regulations, emerging technologies, privacy enhancing technologies, security

Submitted: 11 October, 2024
Accepted: 29 December, 2024
Published: 17 March, 2025

Vol. 2025, **No.** 1, 2025.
https://doi.org/10.71442/mari2025-0006

***Corresponding author:**
✉ Bareq Muntadher Abdul Wahhab
bariq_montder@yahoo.com

Citation
Bareq Muntadher Abdul Wahhab, Safinaz Mohd Hussein and Ramalinggam Rajamanickam (2025). Incorporating emerging technologies for enhancing data privacy protection regulations . Mari Papel Y Corrugado, 2025(1), 44–56.

1 Introduction

In an increasingly digital world, where vast amount of personal and sensitive information are generated, collected [1], and shared [2], the need for robust data privacy protection [3] has never been more pressing. Emerging technologies are not only transforming the way we interact with data but also reshaping the regulatory landscape surrounding data privacy. The challenge at hand is to harness the power of these innovations to strengthen data privacy protection regulations without compromising the fundamental right to privacy.

Data privacy, once a niche concern, has now taken center stage in the global discourse. The rapid digitalization of personal and business activities, coupled with the proliferation of connected devices and the ubiquity of data-driven-decision-making, has raised both the stakes and the complexities of safeguarding individual privacy [4]. The European Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) [5], as well as the OECD 2023 Emerging Privacy Enhancing Technologies [6] represents significant strides in recognizing the importance of data protection. Similarly, other issue specific regulations like the Health Insurance Portability and Accountability Act (HIPAA) and Children's Online Privacy Protection Act (COPPA) in the United States, are regulations safeguarding individual's privacy against violation in the digital age. However, the evolving technological landscape constantly challenges the efficacy of existing

regulations.

This study embarks on a journey to explore the dynamic interplay between emerging technologies and data privacy protection regulations. It investigates how technologies such as artificial intelligence [7], blockchain [8, 9], the Internet of Things (IoT), biometric authentication and identity management can be leveraged to enhance data privacy while ensuring compliance with evolving legal requirements. These technologies offer immense potential, yet they introduce novel challenges and complexities.

The path forward is not without its challenges. Balancing innovation with privacy protection is a delicate equilibrium that requires thorough examination. Ethical considerations [10], the potential for algorithmic bias [11], and the need for user-centric control over data [12] are all facets that demand attention. While these technologies offer the promise of stronger data security, they also pose risks if not implemented thoughtfully. Hence, this study seeks to unravel the complexities and intricacies of incorporating emerging technologies within the framework of data privacy protection regulations. Contributing to the ongoing discourse on data privacy, and to guide organizations and policymakers, as well as governments in shaping a more secure and privacy-conscious digital future. By doing so, the research underscores the importance of safeguarding data privacy rights in an era marked by unparalleled technological progress.

1.1 Research questions

This research seeks to answer the following questions:

1. How can data privacy regulations adapt to the rapid advancements in AI and machine learning?

2. How can IoT devices be secured to protect personal information effectively?

3. How can the risk to individual and organizational data privacy and security be minimized?

2 Review of the literature on emerging technologies for data privacy

Emerging technologies have been well researched. Discussions on data privacy protection is also widespread. Quach and others [13], created a foundation for understanding the digital technology implications for the performance of firms in the context of privacy concerns and legal consequences. They proposed data privacy strategy for user privacy protection behavior and privacy innovation as tools for developers and as responses for firms, to clarify digital technologies and the future of data for firms, users, regulators and developers. Chaudhuri [14], discusses the association of data protection and data privacy concerns with particular reference to IoT services offering as small retail, smart home, smart wearables, smart health devices, smart televisions, and smart toys. He emphasized that IoT businesses must align with the GDPR, to prevent adverse consequences. Shahzad and others [15], assessed urban planning from an environmental point of view. Providing extensive research on the latest technological advancements such as deep learning, machine learning, IoT, mobile computation, big data, blockchain, 6th generation networks, robotics, WiFi-7, heating, ventilation, and air conditioning. As well as digital forensic, industrial control systems, electrical vehicles, flying cars and others. Arguing that these technologies enables future dimensions of smart cities for smart living.

Whaiduzzaman and others [16], reviewed emerging technologies for IoT-Based smart cities. They provided the concepts of smart cities, characteristics and applications within the context of machine learning and blockchain technologies. While Krishnamoorthy and friends [17], discussed the latest paradigm of wireless body area network and its significance to the development of next generation healthcare application using emerging technologies like machine learning, blockchain, cloud computing, IoT, edge/Fog computing, tele-healthcare, big data analytics, software defined networking and others. At the same time emphasizing the need to ensure security and privacy in the future healthcare systems. Thakker and Japee [18], discussed emerging technologies in accounting and finance through a comparative studies, elaborating the implications of emerging technologies for professionals and organizations to adapt to in the field of accounting and finance. Furthermore, Mbunge and others [19], proposed ethical framework for using emerging technologies to contain the Covid-19 pandemic where they proposed ethical practices such as security, privacy, justice, human dignity, autonomy, solidarity, beneficence, and non-maleficence. Similarly, Dhirani and friends [4], reviewed discussions on the ethical dilemmas and privacy issues in emerging technologies.

However, research is lacking in enhancing data privacy protection using emerging technologies. Which this research aims to highlight. At the same time, this research argues that, despite the hazards associated with emerging technologies, businesses, organizations,

and governments can utilize emerging technologies to enhance data privacy protection by balancing the development and deployment of new technologies that incorporates data privacy regulation requirements in designs and policies. While adhering to ethical issues and compliance with regulations and educating users on the new technologies being developed.

2.1 Research objectives

In the present study, the researchers are interested in exploring how data privacy regulations adapt to the rapid advancements in AI and machine learning. To determine the way IoT devices can be secured to protect personal information effectively. As well as to examine the ways that individual and organizational risk can be minimized through AI. The aim is to examine the role of emerging technologies in data privacy protection. The study aims to add to growing discussions on the impact of emerging technologies on data privacy protection.

3 Methodology

This study utilized the qualitative doctrinal research method to explore the dynamic interplay between emerging technologies and data privacy regulations. Qualitative doctrinal research method is an approach used in analysing legal frameworks and regulations, legal texts, statutes, cases, and legal opinions to interpret the underlying principles and doctrines, such as meanings, implications, and challenges [20]. It involves identifying the legal rules and principles that are relevant to a particular issue and then applying those rules and principles to existing facts depending on the circumstances of each case [21, 22]. When this method is employed as a primary form of qualitative research, it aids in synthesising the various types of documents in legal research [23–26]. This type of research can be used to explore a wide range of topics [27] such as the impact of law on social change, the role of law in social institutions, and the ways in which law is used to regulate social behaviour. Similar to this research, which analyses technological advancements that affect human lives with the law, to ensure users are protected as they navigate social change. A doctrinal research is largely documentary. It is a study that focuses on statutory laws, legal documents and reports and can be used for qualitative research in several ways [28]. Such as identifying the legal rules and principles relevant to a particular social issue, in relation to how the law is used to regulate a particular issue [29], and to analyse the impact of law on social change [28].

Qualitative doctrinal legal research method varies from the doctrinal legal research [30]. The doctrinal legal research lays more emphasis on the rudiments and fundamental in exploring the law as it is [31]. However, this research goes beyond the letters of the law to examining the law from the perspective of social reality [32]. It also seeks to answer broader issues [33–35]. This study qualitatively explored the way in which emerging technologies interact with online privacy regulation protection. It emphasizes the benefit that users can derive from emerging technologies in their everyday interactions, the harm that these emerging technologies poses to users when using them. The need for the development of these technologies to align with existing regulations, in other to safeguard user's privacy and minimize harm. As well as, balance in the development, deployment and usage of these emerging technologies, with particular reference to IoT, Blockchain, AI, and Biometrics data.

4 Results and discussion

The key findings in this study discussed in this section includes:

4.1 Emerging technologies

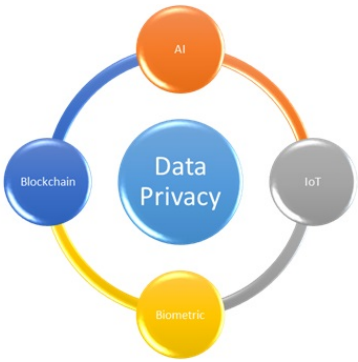

Figure 1. Emerging technologies

Emerging technologies like AI, IoT, Blockchain, and Biometric data as shown in Figure 1 above, have enormous capacities to everyday life. However, their continuous usage raises ethical considerations related to data breaches and intrusion, data security and privacy. These technological innovations have been widespread across disciplines raising ethical considerations relating to cyber security [36] and unauthorized access or intrusion to individual privacy [37]. Resulting in greater risk to computers, personal data and other properties through system disruption, identity fraud, data interruptions, unlawful access and similar acts. Cyber security has become inevitable in this digital age to address the problem and mitigate risks affecting networks, data, systems, and enhancing data privacy protection [37]. IoT for instance is a network of physical

devices that connects and interact in various ways, such as in social life, environmental, medical, and other context of human activities [16]. Such that, its usage is without limits, it has connection and communication abilities when digital devices such as sensors, actuators and mobile phones are linked to the internet [38]. It does not need human interaction to prioritize work, organize itself and interact with things [39]. IoT offers enormous services to users, governments and businesses with its ability to organize volume of data together.

On the other hand, AI refers to the simulation of human intelligence in machines programed to carry out tasks that are required to be undertaken by human intelligence. As a field of computer science AI encompasses broad subfields, including machine learning, computer vision, natural language processing, expert systems, and robotics. AI are designed to interact with their environment, reason, learn from experience, and make decisions or take actions to achieve a given task [18] In other words, AI has the ability of processing large amount of data just like IoT, recognize pattern, understand and interpret human language, and adapt to any given scenario expected of it. Hence, it can be argued that AI is a computer version of human intelligence but upgraded to solve complex problems that would require more than one human mind to execute. With the capabilities of AI and IoT, if both technologies are designed to comply with data privacy regulations, unauthorized access, unlawful intrusion and data breaches would not only be minimized but could be easily detected.

Blockchain's distributed ledger is immutable, meaning that once data is added to the chain, it cannot be altered or deleted. This property ensures the integrity of data records, making it extremely difficult for unauthorized parties to tamper with stored information [40]. Similarly, data stored on a public blockchain is transparent and accessible to all participants, providing a high level of transparency [40]. Data subjects can verify the accuracy and integrity of their own information [41]. Furthermore, blockchain operates on a decentralized network of nodes. This means that no single entity has control over the entire database, reducing the risk of data manipulation or unauthorized access. Blockchain have the capacity to trade data in a tokenized form [42] and their transparency increases the need to make market exchanged data less sensitive [43, 44]. Therefore, data breaches and other violations of privacy protection regulations that have been captured on the blockchain are easily detected, they become solid evidence for further prosecution or any civil action that might arise due to the privacy breach.

Biometric authentication is a critical tool for ensuring information system security. It has been advanced to steadily integrate a variety of AI technologies to achieve greater diversity and accuracy [45]. There are two categories of biometric authentication: physical biometric which uses voice, iris, and fingerprint scanners to rely on individuality of specific physical characteristics authentication, and behavioral biometrics [46]. Behavioral biometrics like physical biometrics works under the premise that human behavior is distinct to be utilized for authentication. Besides traditional passwords, image recognition, such as fingerprint and face recognition, and human behavior, such as keystroke dynamics as well as mouse movements, are used in different authentication methods [17, 47–49]. However, designing and developing a scalable and widespread communication paradigm would assist in addressing the challenges of obfuscated harmful ULRs, malware distribution, account hijacking, phishing and impersonation [50] associated with biometric authentication risks. Once these information are stored on the system, the violator can be easily detected through any of his/her physical characteristics. This provides greater safeguards for businesses, organizations and governments, because each of these technologies would perform at least one function that strengthen data privacy protection in an inter-related and interconnected manner. Making data privacy protection regulations more effective in application than when it is enforced without the use of these technologies.

4.2 Data privacy regulations

The main data protection regulations that are interconnected with emerging technologies analyzed in this study include the European GDPR which has gained wide popularity across the globe, the Californian CCPA with its wide presence in the USA, the OECD 2023 regulation on emerging technologies, the COPPA and HIPAA of the USA. The GDPR is a key legal instrument that protects individual's privacy rights in the EU, providing a comprehensive legal framework for the collection, processing, and storage of personal data Article 4 [51]. It is EU's lone legal framework on privacy that has inspired and influenced the development of other privacy regulations across the globe [52]. In a way that privacy and data protection has become a major concern and even corporations in the United States have had to comply with its provisions especially those carrying out services that

affect EU nationals [53]. The GDPR improves personal data protection [54], emphasizing individual rights, set new standards for data protection and privacy, data protection principles, and accountability for organizations. The GDPR grants individuals control over their data, imposes obligations on businesses, and introduces strict penalties for non-compliance [55]. Enforcing these standards and detection of violation by organizations and businesses becomes easier with the use of emerging technologies. The CCPA has a more restricted coverage, with greater influence among other US states. The CCPA was enacted by the US Legislative Council in California, to protect consumer data and identify those subject to the law, such as businesses and service providers or third parties who are neither business entities, nor persons to whom personal information is disclosed to, pursuant to a written contract prohibiting them from sale and use other than as specified in the contract terms (Cal. Civ. Code § 1798.140(w)). The CCPA gives California residents the right to know what personal information businesses are collecting about them, the right to request that their personal information be deleted, and the right to opt-out of the sale of their personal information. It also requires businesses to disclose certain information about their data collection and sharing practices. Emerging technologies help to control, manage and ensure compliance, as well as detect likelihood or actual breaches to the CCPA.

The HIPAA is a federal legislation in the United States, enacted by the department of health and human services (HHS). This legislation protects medical information in the USA [56]. The law covers any medical entities dealing with medical information. HIPAA has five sections, including health insurance of workers and their families, fraud and abuse related to health care and medical liability, pre-tax medical spending accounts, group health plans, and life insurance policies for treating foreign patients. The law mandates the issuance of notice to patients prior to the use and disclosures of protected health information (PHI) made by the relevant entities according to the law. These notices must be made available to customers when requested, and these rights must be published on the website of the institutions outlining their activities or advantages. Patients may also request a copy of their protected health information, as well as the right to inquire about specific disclosures of their PHI, such as the dates, recipients, and reasons for the disclosures (I45 CFR §164.528). Regulating entities are required to take efforts to protect the security of electronic health information (I45 CFR § 164.302). In the case of a breach, the patient must be notified within 60days of commission of the breach (I45 CFR 164.402), which can only be more effective where AI and IoT are employed to manage these complex details and quickly receive information and send feedbacks without delay.

In addition, COPPA was enacted in 1998 (15 U.S.C. §§ 6501–6506) to protect children's online privacy and any implementing rules issued by the federal territory (16 C.F.R. part. 312) of the US. Limiting how children's personal data is collected and used in the cyberspace (15 U.S.C. §§ 6501–6506). The law contains six sections, including definitions (Section 601 of COPPA), regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet (Section 601 of COPPA), safe harbors (Section 603 of COPPA), State actions (Section 604 of COPPA) administration and applicability (Section 605 of COPPA), and review (Section 605 of COPPA). When an operator has full awareness that it is gathering personal information from juveniles, the obligations of COPPA apply. These obligations are related to data processing, use, collection, disclosures policy, and security measures. Operators who fall within the scope of this policy are subjected to these obligations. Parental consent is required for the processing of personal information of children under 13years of age (15 U.S.C. § 6502(a)–(b)). Which must be obtained before any data processing must be clear and substantiated (15 U.S.C. § 6502(b)(1)(A)(ii); 16 C.F.R. § 312.5(a)(1)). Operators have the obligation to provide parents with clear and concise information on how they handle their children's personal information (15 U.S.C. § 6502(b)(1)(A)(i); 16 C.F.R. §§ 312.4(a), (c)). They must also, include in their home page on their Website, a link to online notifications of their privacy policies (16 C.F.R § 312.4(d)). The collected information can only be shared with third parties when, confidentiality is protected, there is security, and integrity of the shared information. Meaning effective safeguards must be provided by third parties and operators (16 C.F.R § 312.8). The rules on the storage and deletion of data must be complied with. The right of children is better safeguarded and protected from unauthorized access when emerging technologies are deployed to enforce or ensure compliance with COPPA, while at the same time helping to minimize associated risk to children's privacy.

Furthermore, the OECD guidelines on emerging privacy enhancing technologies current regulatory

and policy approaches makes provision requiring organizations, institutions, developers and policy makers to incorporate privacy enhancing technologies in technologies that provides the protection of confidentiality of personal data [6]. When collecting, processing, analyzing and sharing data. These privacy enhancing technologies must be incorporated in designs and defaults. Requiring de-identification, digital security and accountability and/or regulatory mandate, for the purpose of protection and security of personal data [57]. The privacy enhancing techniques identified by the OECD guidelines are grouped into four Article 3.1 [6]: data obfuscation (consisting of anonymization/pseudonimisation, synthetic data, differential privacy and zero-knowledge proofs), encrypted data processing such as homomorphic encryption, multi-party computation and private set interaction, and trusted execution environments, federated and distributed analytics like federated learning and distributed analytics, data accountability tools such as accountable systems, threshold secret sharing and personal data stores or personal information management systems.

Figure 2. Data privacy protection regulations

These regulations as captured in Figure 2 above, provides protection for users in various forms. It reveals the importance of privacy and personal data protection [57] in the collection, processing, analyzing and sharing of user data by organizations and businesses across the globe. The protection of privacy data is so germane that, developers are expected to incorporate privacy enhancing tools in the development of new technologies before deployment in compliance with the OECD 2023. Once these new technologies are deployed, organizations, institutions, businesses and governments using them must equally make policies that ensures proper security of the data collected and provide safeguards for the data.

4.3 Benefits of emerging technologies to data privacy protection

Emerging technologies have countless benefits to everyday human life and especially to its users. See Figure 3 below.

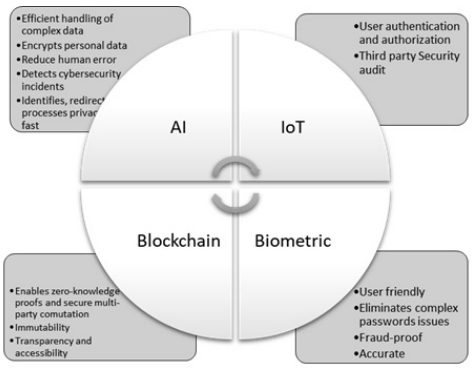

Figure 3. Benefits of emerging technologies to privacy protection

IoT application is enabled using various infrastructures and functional components like sensors that capture predefined contextual data, gateway devices that gather data from the source sensor, centralized data storage that can be found in cloud, analytical processing functions, application programming interface, command and control functions, and wired or wireless network communications [14]. As such, in terms of privacy protection, each of these device processes is susceptible to data breach [4, 58]. IoT data privacy involves the following a) identity privacy, because it is owned by an individual or organization; b) location privacy, it can be used to track location of the user; c) search query privacy, personality traits can be inferred by tracking the search history of users; d) digital footprint privacy which can leave a trail of data on the internet; e) personal behavior privacy, the ability to gather personal behavior without consent using different parameters; and f) personal health data, gather health data of users without prior consent [14]. Personal information can be protected through securing IoT devices to prevent unauthorized access, data breaches, and privacy violations when PETs like encryption and anonymity are used to safeguard data privacy [59].

Similarly, AI is recently influences decision-makers in companies, through innovating partial or full automation of business processes, by enabling a more efficient green-driven marketing efforts. AI can be relied upon to power strategy, internal upgrade and client-value management improvement [60]. When AI is integrated in sustainability strategies, it helps to solve complex and interrelated challenges faced by companies

to handle enormous data. As well as tackle complex environmental, social, and economic challenges [61] faced by organizations, businesses, and governments. When data is stored on the blockchain, users have greater control over their personal information. They can grant or revoke access to their data, ensure that it is only shared with authorized parties [62]. They have greater ownership of their data and can easily transfer it between services or platforms, enhancing data portability and control. Smart contracts, which are self-executing contracts with predefined rules, can be used to manage consent [63]. Data subjects can set conditions for data access and sharing [64], and blockchain enforces these rule automatically. Also, blockchains use advanced cryptographic techniques to secure data, which if utilized in data privacy protection regulation, can enhance compliance. This provides an added layer of protection against unauthorized access and data breaches.

Biometric authentication and identity management have significant implications for data privacy, both positive and negative. These technologies offer improved security and user convenience, but they also raise privacy concerns. Biometric authentication is user-friendly, as it eliminates the need to remember and input complex passwords. This convenience can encourage users to adopt stronger security measures [45]. Users often rely on weak passwords or reuse them across multiple accounts due to the challenges of managing numerous credentials. Biometric reduce the need for passwords and reduces password fatigue. It can be used as part of a multi-factor authentication system, where biometrics act as one of the authentication factors, enhancing overall security [65]. It ensures that data is accessed only by authorized users, which minimizes data privacy breaches.

4.4 Implications of emerging technologies to individual privacy

While emerging technologies can enhance data privacy protection, it can also cause serious harm to individual privacy. Some harm can be temporary and reversible, other harm caused by emerging technologies are irreversible. See Figure 4 below. IoT devices are vulnerable to various security threats. Some researchers have found that IoT is used to leak sensitive information sent to cloud unencrypted [66]. Cloud in most cases stand as an intermediary to two IoT devices communicating. It usually acts without limitation and consent of the owner [67]. But there are strategies and best practices to enhance their security and safeguard personal data. One of the most common security vulnerabilities in IoT devices is the use of default usernames and passwords, as well as smartwatches, head-mounted devices, and other smart wares mostly paired with smartphone apps to operate in sync [14].

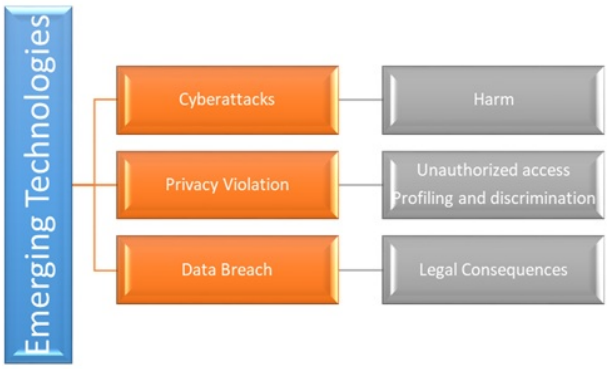

Figure 4. Balancing emerging technologies with data privacy protection

Here, blockchain technology offers significant advantages in preserving data integrity and protecting data subject rights, it is not without challenges [68]. Some concerns includes scalability issues for a data-intensive production environment [69], energy consumption and the need for interoptability between different blockchain and legal systems [70]. Despite these challenges, blockchain remains a powerful weapon for data privacy and integrity protection, particularly in applications where transparency, control, and immutability are paramount.

Biometric authentication comes with some negative implications. For instance biometric data, such as fingerprints and facial images, are highly personal and can be misused if not properly protected. Unauthorized access to biometric data can have severe privacy consequences. Storing biometric data on centralized servers can make it a target for cybercriminals [65]. If biometric data is compromised in a data breach, it can have long-lasting consequences for individuals. Unlike passwords, which can be changed if compromised, biometric data is difficult to revoke or change. Hence, if compromised, it poses a severe long-term risk to an individual's privacy [45]. Similarly, biometric systems may not be entirely accurate and can sometimes exhibit bias, particularly in facial recognition systems. This can result in incorrect authentication decisions and privacy infringements. Biometric data may be collected and used without clear and informed consent, leading to potential privacy violations [45]. Additionally, biometric surveillance, especially in public

spaces, raises concerns about individual privacy and surveillance states. The theft of biometric data, combined with personal information, can result in identity theft and fraudulent activities.

4.5 Balancing data privacy protection and emerging technologies

To balance data privacy and emerging technologies, there is a need for developers to incorporate privacy enhancing technologies in new technologies before deployment as shown in Figure 4. The impacts of emerging technologies on data privacy protection has increased security risks to users' privacy protection. Practitioners and corporations have increased system security as a reaction to these continuous risk [71]. The sale of data and replication of data is not sufficiently safeguarded by the use of confidentiality alone. But requires data to be modified or managed to enhance privacy which must be incorporated into the designs of new technologies. Therefore, institutions and organizations must utilize and employ privacy enhancing technologies or techniques [72], as well as incorporating the requirement for consent, as part of its policies. Such as syntactic anonymizations [73], homomorphic encryptions [74], trusted execution environments [71]. Pseudonymization [75]. zero-knowledge proofs [76], and security multiparty computation [77] amongst others.

Ethical guidelines and stands should also be developed and enforced in emerging technologies. These guidelines should address issues such as unauthorized access, identity theft, intrusion, algorithmic bias, discrimination, and fairness, ensuring that built systems respect privacy and human rights. Furthermore, it is important to promote the principle of "privacy by design", which encourages organizations to build privacy protections into their new technologies from outset. Privacy should not be an afterthought but an integral part of system development. Also, data minimization practices should be encouraged. Organizations, businesses and governments should collect and use only the data that is strictly necessary for the intended purpose, reducing the risk of privacy violations.

There is a need to change IoT credentials to unique, strong passwords during setup as a measure. Similarly, firmware and software should be updated. As such manufacturers should release updates to patch security vulnerabilities, and enable automatic updates when available. IoT devices should be isolated on a separate network from critical systems and personal devices. This helps to limit the potential damage when an IoT device is compromised. Data transmitted by IoT devices should be encrypted using strong encryption protocols, both in transit and at rest [14]. This includes data stored on the device and data sent to the cloud or other servers. Secure Wi-Fi network with strong encryption (WPA3) and a strong, unique password. Unnecessary network services should be disabled and a separate network for IoT devices should be utilized. Strong access control should be implemented, including secure user authentication and authorization mechanisms. Only authorized users should have access to device settings and data. While at the same time conducting regular vulnerability assessments to identify security weaknesses in IoT devices and addressing it without delay. Firewalls and intrusion detection systems should be deployed to monitor network traffic and protect against unauthorized access and suspicious activity. Secure boot processes and trusted execution environments should be used to ensure the integrity of IoT device software and firmware. Sensitive data stored on the device should be encrypted, and anonymize data [14] when possible to minimize the risk of exposing personal information.

Additionally, manufacturers of IoT should clearly provide privacy policies that outline how data is collected, used, and protected. These policies should be communicated in clear terms through the controller to users and the same procedure should be followed in principle in compliance with Article 13(1c) and 13(1f) of the GDPR. Since IoT services might store personal data across geographical boundaries in the cloud for easy accessibility and data redundancy, users must be informed about the appropriateness and suitability of the established safeguard for such process, and a copy of the data should be made available to the user [14]. Users should be informed about their rights and how to exercise them in compliance with Article 15 of the GDPR. Users should be able to request information regarding the purpose of processing, category of data, and the receipt of their personal data. Device authentication should be implemented to verify the identity of devices connecting to the network and prevent unauthorized access. Physical access to IoT deices should be protected or secured. Limit exposure to potential attackers by placing devices in secure locations and using tamper-evident or tamper-resistant packaging. Also, there is a need for data privacy regulations to keep pace with rapid advancement in AI and machine learning.

Techniques like zero-knowledge proofs and secure

multi-party computation enable privacy-preserving solutions on the blockchain. These methods allow data to be used for specific purposes without revealing sensitive information. Blockchain can be designed to comply with data protection regulations such as the GDPR and CCPA when users are allowed to exercise their rights, like the right to be forgotten or the right to access their data. Additionally, blockchain can be used for data verification and authentication. This is particularly valuable in supply chain management, where the authenticity and integrity of products and transactions can be verified on the blockchain. It also provides a transparent and auditable trial of data transactions. This trial can be used to hold organizations and individuals accountable for their actions related to data handling.

Similarly, there is a need to ensure strong encryption and secure storage of biometric data. Privacy considerations should be incorporated into designs and development of new technologies from the outset. The development of these technologies should be done ethically and responsibly, including ethical implications of algorithms ad machine learning models among others. While ensuring that clear and easily understandable privacy policies, are outlined to enable informed decisions by users. Implement user consent mechanisms for data collection, as well as before collecting and processing user data. This is because Article 7 of the GDPR, provides for consent to be obtained on request by controller before the processing of user data. This provision stresses the fact that the consented user data must be necessary for the performance of the contract before collection. Service providers' should ensure that the collected data is necessary before collection for data minimization in compliance with the data privacy regulation. Only strictly necessary data should be collected to reduce the risk of data breaches and violations. Users should have the right to know what data is being collected and the purpose of collection [14] as well as have a right to revoke consent at any time (Article 17(1) and recital 65 of the GDPR 2018). Often referred to as the right to erasure under the GDPR after a lawful processing (Article 17(1d) of the GDPR 2018) such that where the processing is unlawful, the user has the right to restrict the processing of collected data (Article 18(1b) of the GDPR 2018). The users can exercise the right to object to the processing of their personal data and profiling (Recital 71 of the GDPR 2018) for any purpose (Article 21 and recital 21 of the GDPR 2018) and automated decision-making without their explicit consent obtained, especially where it directly affects them (Article 22 of the GDPR 2018). This can help promote competition among organizations and businesses and give users more control over their personal data.

Transparency should be encouraged, users should be informed about the factors and data used in making decisions that affect them, especially in applications like credit scoring, hiring, and automated decision-making in the case of AI [7]. Data portability should be encouraged to allow individuals to transfer their data while maintaining privacy and control over their information. Auditing and accountability should be implemented as a mechanism, as part of organizational policy to ensure they comply with data privacy regulations. Organizations, businesses and institutions should be held accountable for any violations of these regulations. Governments should enforce strong security measures for handling data, including encryption, access controls, and secure storage. Specify data retention and deletion policies that ensure these technologies do not retain data longer than necessary. Data should be securely disposed of when it is no longer needed in compliance with the GDPR and the CCPA.

Also, it is important to promote education and training programs for organizations and individuals to increase awareness of data privacy issues and best practices in developing and utilizing emerging technologies. Users of IoT should be educated about the importance of IoT security and best practices. They should be encourages to regularly review and update their devices' security settings. They should ensure to use secure communication protocols, such as HTTPS and MQTT-TLS, so that data transmitted between devices and servers is encrypted and protected. Third-party security audits or certifications for IoT devices should be considered, to validate their security and privacy practices. Data retention policies should be defined and enforced to ensure that IoT devices do not retain personal data longer than necessary. Cross-border data flows should be addressed, to ensure that data privacy regulations are effective even when data is transferred internationally, harmonize regulations to maintain privacy standards across borders, and collaborate with international organizations and other countries to establish global standards for data privacy. So that consistent regulations across jurisdictions can be enabled. Independent oversight bodies or authorities should be established to monitor and enforce data privacy regulations and ensure compliance with ethical and legal standards.

Regularly update and patch emerging technologies like IoT, blockchain technologies, and biometric systems to address vulnerabilities. Use PETs like tokenization or secure enclaves for biometric authentication. As well as implement techniques such as data anonymization and pseudonymization to protect individual identities while enabling data analysis (Article 25(2) and Article 42 of the GDPR 2018). Establish clear policies for data retention and deletion. Conduct thorough risk assessments and privacy impact assessments through implementing appropriate technical and organizational measures (Article 25(1) and recital 78 of the GDPR 2018) in compliance with the GDPR and the CCPA.

5 Conclusion

The interaction of emerging technologies and data privacy protection regulations presents a landscape of immense opportunities and challenges. The journey towards enhancing data privacy in an age of technological innovation is a complex and ever-evolving one. There is a need to strike a balance between harnessing the potential of emerging technologies and safeguarding individuals' fundamental right to data privacy. This study, delved into the transformative power of technologies such as AI, blockchain, IoT, and biometric authentication in reshaping the data privacy paradigm. These innovations have the potential to reinforce data protection, streamline user control over personal information, and ensure the integrity of data transactions. From AI-driven privacy-preserving techniques to the decentralization and transparency of blockchain, these technologies offer promising avenues for stronger privacy regulations.

However, vigilance is germane to addressing the complexities and challenges introduced by these technologies. The ethical use of AI, the mitigation of algorithmic bias, and the safeguarding of individual privacy in a world of IoT-connected devices are issues that demand strict attention. The potential for misuse, data breaches, and unauthorized surveillance stresses the need for robust security measures and clear regulatory guidelines that keep pace with advancement in technologies and incorporating them. Therefore, in this evolving landscape, a few fundamental principles must guide the approach to enhancing data privacy protection regulations. Technologies should be developed with privacy considerations as their core through privacy by design. Individuals must be informed about how their data is collected, used, and protection to achieve transparency and informed consent principle, and data minimization which ensures that only necessary data are collected and retained. The responsible and ethical use of technologies is imperative. Therefore, collaboration between governments, regulatory bodies, the private sector, and technology developers is essential in establishing clear and effective privacy regulations and standards.

In conclusion, it is argued that incorporating emerging technologies for enhancing data privacy protection regulations is a complex but vital struggle. To strike the right balance between innovation and safeguarding individual privacy rights, the study recommends as a guide to:

- Embrace privacy by design: ensure that emerging technologies are developed with privacy considerations embedded from the outset. Privacy should be an integral part of the design process, not as an afterthought.
- Provide clear and easily understandable privacy policies: ensure that individuals are well-informed about how their data is collected, used, and protected. Obtain informed consent for data processing.
- Collaborate for robust Regulations: foster collaboration between governments, regulatory bodies, industry leaders, and technology developers to establish clear and effective privacy regulations and standards that adapt to the rapidly changing technological landscape. Similarly, regulatory frameworks should be adaptable and capable of evolving alongside emerging technologies. They should be designed to address both current and future technological advancements challenge.
- Ethical Implementation: embrace ethical practices in the development and deployment of emerging technologies. Prioritize transparency, accountability, and fairness to minimize the risk of unintended consequences and potential harm to individuals. Implement robust cybersecurity measures, such as encryption, intrusion detection systems, and security updates, to protect data from unauthorized access and breaches.
- Data Minimization and Purpose Limitation: collect only the data that is strictly necessary for the intended purpose, and ensure that data is not repurposed for other uses without explicit consent. Implement strict data minimization and purpose limitations practices.

- User-centric control: empower individuals with control over their personal data. Give them the ability to access, correct, or delete their information, and allow them to set preferences for data sharing and processing.

References

[1] Stucke, M. E., & Ezrachi, A. (2018). Alexa et al., what are you doing with my data?. *Critical Analysis L., 5*, 148–169.

[2] Varian, H. R. (2014). Beyond big data. *Business Economics, 49*(1), 27-31.

[3] Di Lella, L. A. (2023). Accept All Cookies: Opting-in to a Comprehensive Federal Data Privacy Framework and Opting-out of a Disparate State Regulatory Regime. *Villanova Law Rev., 68*(3), 511–521.

[4] Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors, 23*(3), 1151.

[5] Zanfir-Fortuna, G. & Bae, M. (2018). "CCPA, face to face with the GDPR: An in depth comparative analysis," *Future of Privacy Forum.* https://fpf.org/blog/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/

[6] OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", *OECD Digital Economy Papers, No. 351*, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en.

[7] Al-Najjar, S. F. M. (2024). "Criminal responsibilities arising from artificial intelligence crimes," *Imam Ja'afar Al-Sadiq University Journal of Legal Studies, 4*(7), 80–111. https://ijsu.researchcommons.org/cgi/viewcontent.cgi?article=1094&context=ijsu

[8] Zhao, Y., & Chen, H. (2024). Enhancing access to digital justice: digital governance of dispute resolution and dispute prevention in online commercial activities. *Journal of International Dispute Settlement, 15*(2), 273-304.

[9] Szabo, J., Bernard, C., & Philip, L. (2024). Legal implications and challenges of blockchain technology and smart contracts. *Computer, 12*(2), 6-10.

[10] Kendal, E. (2022). Ethical, legal and social implications of emerging technology (ELSIET) symposium. *Journal of Bioethical Inquiry, 19*(3), 363-370.

[11] Gianpero, P., & Jaimie, S. (2019). Google and project Maven (A): Big tech, government and the AI arms race. Harvard Bus. Publ. Available: https://hbsp.hardard.edu/product/IN1459-PDF-ENG

[12] Lichter, A., Löffler, M., & Siegloch, S. (2021). The long-term costs of government surveillance: Insights from Stasi spying in East Germany. *Journal of the European Economic Association, 19*(2), 741-789.

[13] Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*(6), 1299-1323.

[14] Chaudhuri, A. (2016). Internet of things data protection and privacy in the era of the General Data Protection Regulation. *Journal of Data Protection & Privacy, 1*(1), 64-75.

[15] Javed, A. R., Shahzad, F., ur Rehman, S., Zikria, Y. B., Razzak, I., Jalil, Z., & Xu, G. (2022). Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects. *Cities, 129*, 103794.

[16] Whaiduzzaman, M., Barros, A., Chanda, M., Barman, S., Sultana, T., Rahman, M. S., ... & Fidge, C. (2022). A review of emerging technologies for IoT-based smart cities. *Sensors, 22*(23), 9271.

[17] Krishnamoorthy, S., Dua, A., & Gupta, S. (2023). Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing, 14*(1), 361-407.

[18] Thakker, P., & Japee, G. (2023). Emerging technologies in accountancy and finance: A comprehensive review. *European Economic Letters (EEL), 13*(3), 993-1011.

[19] Mbunge, E., Fashoto, S. G., Akinnuwesi, B., Metfula, A., Simelane, S., & Ndumiso, N. (2021). Ethics for integrating emerging technologies to contain COVID-19 in Zimbabwe. *Human Behavior and Emerging Technologies, 3*(5), 876-890.

[20] Linos, K., & Carlson, M. (2017). Qualitative methods for law review writing. Univ. *Chicago Law. Rev., 84*, 213-238.

[21] Alkhafagy, T., Nazem, S. N., Farhan, A. F., Salman, S. D., Khudadad, A. M., Nsaif, A. D., ... & Abdelhassan, M. I. (2023). Cybercrime and Inheritance Legislation in Iraq: Extension of Perspectives on Inheritance Legislation within Iraq. *International Journal of Cyber Criminology, 17*(2), 63-76.

[22] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard business review, 95*(1), 118-127.

[23] Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report, 13*(4), 544-559.

[24] Malinovsky, A., Osina, D., & Trikoz, E. (2020). Legal instruments for stimulating environmentally friendly behavior: successful practices in Russia and abroad. In *E3S Web of Conferences* (Vol. 164, p. 11039). EDP Sciences.

[25] Kaka, G. E., Said, M. H. M., & Ismail, S. M. (2021, July). Breaking the Barriers of Inequality: A Road Map to Advancing Gender Equality in Sustainable Development Goal. In 27nd *International Sustainable Development Research Society Conference, Mid Sweden University* (pp. 13-15).

[26] Kaka, G. E. (2015). Women, Knowledge and

Legal Reality: The Dichotomy between the Public and Private Domain. *Journal of Public Policy & Governance, 2*(1), 30-39.

[27] Terkildsen, T., & Petersen, S. (2015). The future of qualitative research in psychology—A students' perspective. *Integrative Psychological and Behavioral Science, 49*, 202-206.

[28] Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: doctrinal legal research. *Deakin Law Review, 17*(1), 83-119.

[29] Lung, S. (2008). The Problem Method: No Simple Solution. *Willamette L. Rev., 45*, 723.

[30] Karadimitriou, N., & Pagonis, T. (2019). Planning reform and development rights in Greece: Institutional persistence and elite rule in the face of the crisis. *European Planning Studies, 27*(6), 1217-1234.

[31] Verma, S. K., & Wani, M. A. (2001). Legal research and methodology. (No Title).

[32] Dobinson, I., & Johns, F. (2017). Legal research as qualitative research. *Research Methods for Law*, 18-47.

[33] Warburton, W., Whittaker, E., & Papic, M. (2018). Homelessness pathways for Australian single mothers and their children: An exploratory study. *Societies, 8*(1), 16.

[34] Tulga, A. Y. (2022). Hard and soft terrorism concepts: the case of ISIS. *Pakistan Journal of Terrorism Research, 3*(2), 109-132.

[35] Singh, R., Bajpai, G. S., & Singh, M. (2008). Research methodology: Qualitatiev andQuantitative methods in research. *Production for Courseware,* 1-12.

[36] Brey, P. (2017). Ethics of Emerging Technologies. In S. O. Hansson (Ed.), *Methods for the Ethics of Technology.* Rowman and Littlefield International. 1–17, https://www.4tu.nl/ethics/downloads/default/files/brey-2017-ethics-emerging-tech.pdf

[37] Pawlicka, A., Choraś, M., Kozik, R., & Pawlicki, M. (2023). First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions. Personal and Ubiquitous Computing,27, 1-10.

[38] Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-Khah, M., & Siano, P. (2016, June). Iot-based smart cities: A survey. In *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)* (pp. 1-6). IEEE.

[39] Datta, S. K., Da Costa, R. P. F., Bonnet, C., & Härri, J. (2016, June). oneM2M architecture based IoT framework for mobile crowd sensing in smart cities. In *2016 European Conference on Networks and Communications (EuCNC)* (pp. 168-173). IEEE.

[40] Lohmer, J., Ribeiro da Silva, E., & Lasch, R. (2022). Blockchain technology in operations & supply chain management: a content analysis. *Sustainability, 14*(10), 6192.

[41] Vu, N., Ghadge, A., & Bourlakis, M. (2023). Blockchain adoption in food supply chains: A review and implementation framework. *Production Planning & Control, 34*(6), 506-523.

[42] Sunyaev, A., Kannengießer, N., Beck, R., Treiblmaier, H., Lacity, M., Kranz, J., ... & Luckow, A. (2021). Token economy. *Business & Information Systems Engineering, 63*(4), 457-478.

[43] Cheng, H., Xie, Z., Wu, L., Yu, Z., & Li, R. (2019). Data prediction model in wireless sensor networks based on bidirectional LSTM. *EURASIP Journal on Wireless Communications and Networking, 2019*(1), 203.

[44] Cheng, R., Zhang, F., Kos, J., He, W., Hynes, N., Johnson, N., ... & Song, D. (2019, June). Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 185-200). IEEE.

[45] Annadurai, C., Nelson, I., Devi, K. N., Manikandan, R., Jhanjhi, N. Z., Masud, M., & Sheikh, A. (2022). Biometric authentication-based intrusion detection using artificial intelligence internet of things in smart city. *Energies, 15*(19), 7430.

[46] Gayathri, M., & Malathy, C. (2022). A deep learning framework for intrusion detection and multimodal biometric image authentication. *Journal of Mobile Multimedia*, 393-420.

[47] Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management, 8*(2), 100063.

[48] Dai, D., & Boroomand, S. (2022). A review of artificial intelligence to enhance the security of big data systems: state-of-art, methodologies, applications, and challenges. *Archives of Computational Methods in Engineering, 29*(2), 1291-1309.

[49] Gupta, R., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Machine learning models for secure data analytics: A taxonomy and threat model. *Computer Communications, 153*, 406-440.

[50] Taiwo, O., Ezugwu, A. E., Oyelade, O. N., & Almutairi, M. S. (2022). Enhanced intelligent smart home control and security system based on deep learning model. *Wireless Communications and Mobile Computing, 2022*(1), 9307961.

[51] GDPR, (2018). "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da." *Official Journal of The European Union, EU*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[52] Schwartz, P. M. (2019). Global data privacy: The EU way. *NYU Law Review, 94*, 771.

[53] Rustad, M. L., & Koenig, T. H. (2019). Towards a

global data privacy standard. *Florida Law Review, 71*, 365.

[54] Puljak, L., Mladinić, A., & Koporc, Z. (2023). Workload and procedures used by European data protection authorities related to personal data protection: a cross-sectional study. *BMC Research Notes, 16*(1), 41.

[55] Pendaroska, L. (2022). International transfer of personal data between the EU and countries outside the EU. *Iustinianus Primus Law Review, 13*, 1.

[56] Act, A. (1996). Health insurance portability and accountability act of 1996. *Public Law, 104*, 191.

[57] Radi, S. M. (2022). The right to the protection of personal data under the Constitution of the Republic of Iraq for the year 2005. *Imam Ja'afar Al-Sadiq University Journal of Legal Studies, 1*(4), 147-171.

[58] Osman, A. (2023). The right to be forgotten: an Islamic perspective. *Human Rights Review, 24*(1), 53-73.

[59] Asrow, K., & Samonas, S. (2021). Privacy Enhancing Technologies: Categories, Use Cases, and Considerations. *Fintech Edge, June*, 1.

[60] Jankovic, S. D., & Curovic, D. M. (2023). Strategic integration of artificial intelligence for sustainable businesses: implications for data management and human user engagement in the digital era. *Sustainability, 15*(21), 15208.

[61] IBM. (2023). "Global AI adoption index 2020," International Business Machine (IBM). https://www.ibm.com/watson/resource/ai-adoption (accessed Dec. 17, 2023).

[62] Roeck, D., Sternberg, H., & Hofmann, E. (2020). Distributed ledger technology in supply chains: a transaction cost perspective. *International Journal of Production Research, 58*(7), 2124-2141.

[63] De Giovanni, P. (2020). Blockchain and smart contracts in supply chain management: A game theoretic model. *International Journal of Production Economics, 228*, 107855.

[64] Al-Farsi, S., Rathore, M. M., & Bakiras, S. (2021). Security of blockchain-based supply chain management systems: challenges and opportunities. *Applied Sciences, 11*(12), 5585.

[65] Ahamed, F., Farid, F., Suleiman, B., Jan, Z., Wahsheh, L. A., & Shahrestani, S. (2022). An intelligent multimodal biometric authentication model for personalised healthcare services. *Future Internet, 14*(8), 222.

[66] Europa, (2023). A European approach to Artificial intelligence, Digital Strategy, 2023. https://digital-strategy.ec.europa.eu/en.policies/european-approach-artificial-intelligence

[67] Car, P., & De Luca, S. (2022). *EU Cyber Resilience Act*. EPRS, European Parliament.

[68] Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: implications for operations and supply chain management. *Supply Chain Management: An International Journal, 24*(4), 469-483.

[69] Li, J., Maiti, A., Springer, M., & Gray, T. (2020). Blockchain for supply chain quality management: challenges and opportunities in context of open manufacturing and industrial internet of things. *International Journal of Computer Integrated Manufacturing, 33*(12), 1321-1355.

[70] U. Arvind, A. J. Oluwasunkanmi, K. A. Kumar, and G.-R. J. Arturo, "A review of challenges and opportunities of blockchain adoption for operational excellence in the UK automotive industry," J. Glob. Strateg. Sources, vol. 12, pp. 7–60, 2020, doi: http://dx.doi.org/10.1108/JGOSS-05-2020-0024.

[71] Garrido, G. M., Sedlmeir, J., Uludağ, Ö., Alaoui, I. S., Luckow, A., & Matthes, F. (2022). Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. *Journal of Network and Computer Applications, 207*, 103465.

[72] Trask, A., Bluemke, E., Collins, T., Drexler, B. G. E., Cuervas-Mons, C. G., Gabriel, I., ... & Isaac, W. (2020). Beyond privacy trade-offs with structured transparency. *arXiv preprint arXiv:2012.08347*.

[73] Samarati, P., & Sweeney, L. (1998). Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. *Epic*, 1-19. https://dataprivacylab.org/dataprivacy/projects/kanonymity/paper3.pdf

[74] Will, M. A., & Ko, R. K. (2015). *A Guide to Homomorphic Encryption*. The cloud security ecosystem: technical, legal, business and management issues. Edited by Ryan Ko and Kim-Kwang Raymond Choo. Waltham, MA USA: Elsevier, 101-127.

[75] Niu, C., Zheng, Z., Wu, F., Gao, X., & Chen, G. (2018). Achieving data truthfulness and privacy preservation in data markets. *IEEE Transactions on Knowledge and Data Engineering, 31*(1), 105-119.

[76] Zhang, Y. (2020, November). Zero-knowledge proofs for machine learning. In *Proceedings of the 2020 Workshop on Privacy-Preserving Machine Learning in Practice* (pp. 7-7).

[77] Zhou, L., Wang, L., Sun, Y., & Ai, T. (2018). AntNest: Fully non-interactive secure multi-party computation. *IEEE Access, 6*, 75639-75649.