Ethical Dilemmas in Emerging Technologies

Subjects: Engineering, Electrical & Electronic

Contributor: Lubna Luxmi Dhirani , Noorain Mukhtiar , Bhawani Shankar Chowdhry , Thomas Newe

Emerging technologies have featured prominently in the research on technology ethics, which is progressively concentrating on early-stage intervention in technological innovation. Techno Ethics (TE) serves as a multidisciplinary research field that incorporates theories and techniques from various domains including communications systems, sociology, innovation, ethical theories, and principles. Cybercrime is an umbrella term for all illicit activities made possible by access to an IT infrastructure including unauthorized access, unlawful data comparison interception, system disruption, digital identity fraud, etc. The goal of cybersecurity (counterpart to cybercrime) is to assist people in mitigating risks in their systems, networks, and data, ensuring security and privacy. To secure cyberspace, formal and informal resources, including equipment, people, infrastructure, services, policies, training, and technologies are used. As more firms post details to demonstrate their public commitment to ethical ideals while promoting security, discussions regarding ethical standards for emerging technologies are becoming more common.

ethics regulations standards

1. Ethical Concerns in Cloud Computing

Cloud Computing has enabled and provided promising outcomes for the industrial IoT environment. The cloud offers different models (i.e., public, private, hybrid, multi-cloud, federated, etc.) and services (Software as a Service, Platform as a Service, and Infrastructure as a Service) [1]. A cloud Service Level Agreement (SLA) is a legal contract agreed between the cloud tenant and the service provider for delivering the promised services. At any point, if the services are not met, the vendor may be subject to a penalty (the contract could be voided) or renegotiated based on new SLA. However, despite having an Service Level Agreement (SLA) for controlling the Quality of Service (i.e., reliability, availability, etc.) metrics, the biggest ethical and privacy issues arise when services are processed on third-party premises, without the end-user's knowledge/consent. Many terms and linked conditions mentioned in the SLA lead to ambiguity and misleading statements [2].

By 2025, around 85% of the world's industrial data will be processed in the cloud [3][4]. The existing models lack the capacity for such resource demands and would rely on federated and brokerage cloud models. However, the federated models lack in terms of standardization, security, governance, risk and control (GRC), trust, access management, incident response, and business continuity. The NIST Cloud Federation Reference Architecture (NIST SP 500-332) [5] only provides a basic understanding of the roles different cloud actors (vendors, carriers, brokers, users, auditors, etc.) perform, a description of technical and service levels, and guidance to ease the barriers for adoption [6].

In 2021, the IEEE P2302 *"Standards for Cloud Federation"* [7] is working on aligning with NIST 800-332; however, that is an on-going project and presently there is no cloud federation model that would provide interoperability and uniform governance.

Considering these limitations, and taking into account the fact that cloud setups cannot provide end-to-end security or a guaranteed service, is it ethical to process sensitive data on such setups just to save computational costs? Further, if an industry does, the cloud must follow a baseline/minimal security standards and controls to protect the data.

Consider the example of a Genomic datacenter that computes, analyses, and processes DNA structures/patterns and may require huge computing power. At times, the data centers would require sharing the DNA/sensitive information for treatments with other research centers based in different jurisdictions through cloud models. Any breach, or negligence of cloud security standards or policy, would impact all those people receiving treatments, resulting in a breach of the social contract and GDPR as well. In [8], the authors mention ethical challenges related to the privacy and security of genomic data and raises concerns whether the existing compliance and security mechanisms would suffice in securing the data in the transforming nature of emerging technologies. The ethical implications of Cloud Computing are influenced by several technological factors such as: security, privacy, compliance, performance metrics, etc. **Table 1**, provided below highlights the ethical and privacy considerations in a cloud environment.

Table 1. Ethics and privacy in Cloud Computing.

Title	Overview	Ethical and Privacy Risks
Ethical Considerations in Cloud Computing Systems [3]	Elaborates the relationship between ethics and the Terms and Conditions (T&C) guidelines. It provides a comparison of ethical concerns with cloud-based applications versus regular web-based alternatives.	Privacy, security, compliance, monitoring, QoS metrics issues arising due to lack of pre-defined rules end-user cloud SLAs.
Tenant-Vendor and Third-Party Agreements for the Cloud: Considerations for Security Provision [1]	Discusses data-integrity and security implications in hybrid cloud tenant-vendor-subcontracting scenario, highlights SLA limitations and provides solutions to mitigate these issues.	Highlights data integrity, compliance, GDPR implications and cloud virtualization based risks. These ethical, privacy and vendor lock-in issues are an outcome of ambiguous and inconsistent vendors service level agreements.
Data Privacy and Trust in Cloud Computing [9]	Explores some of the identified obstacles to cloud trust and suggests some potential solutions. Also proposes a high-level framework for examining responsibility (trust repairing) and assurance (trust building) in the cloud and argues for a better integrated multi-stakeholder	Following data risks were demonstrated: relational, performance-based, regulatory and compliance based, technological risks, raising trust based concerns related to cloud deployments.

Title	Overview	Ethical and Privacy Risks
	approach to convince research in this complex environment.	
Hybrid Cloud SLAs for Industry 4.0: Bridging the Gap [2]	Addresses lack of alignment of Cloud Computing in Industry 4.0 and its impact on the industrial environment. It also provides a roadmap for mitigating the gap issues.	Mentions lack of data integrity, compliance, trust-method and standards issues that arise due to unalignment between the industrial and cloud environment. Each industry varies in terms of functionality and operations, in such scenarios generic cloud or security standards may not protect the environment. The only way to resolve these issues is by performing a gap analysis between the cloud and enabling technologies deployed in the industry. Once the gaps/flaws are identified, security controls can be applied to neutralize/mitigate the risks. This approach will also help in building cross platform convergence between the emerging technologies. [10]

curity and vulnerabilities (i.e., (i) Accenture's LockBit ransomware attack happened because of misconfigured cloud servers that led to data breach, compromising 40,000 customer accounts, causing financial and reputational damage (ii) where as Kesaya's lack of security implementations for access control, zero trust, remote policies, and multi-factor authentication controls left the cloud SaaS vulnerable and open to zero-day exploits. The number of managed service providers were affected as an outcome of this ransomware attack, leading to three weeks of operational disruption, and financial and reputational damage. The companies impacted by the breaches are well-known, and the cloud service providers were well-known as well, claiming to have strong security mechanisms; yet, a supply-chain type of cyber attack took place). This supports the legitimacy of claims made in [1][3][9][11][12] regarding privacy and regulatory issues, claiming that they are valid and still persist.

With the increasing adoption of Cloud Computing in different sectors, especially the healthcare industry, it is essential that the appropriate regulatory (GDPR) and security standards controls and kept in place. As cloud is mistaken to be a separate/exclusive entity, the security methods (zero trust, availability, and compliance) used within an industry's private and public cloud may differ, making it easier for cyber criminals to breach the environment. At present, none of the standardization organizations have provided or released an interoperable cloud standards platform; therefore, the only way to mitigate cloud-based risk would be by developing insights, visibility, and control. Ref. [9] provides a roadmap for understanding the differences at the SLA levels and bridging the gaps between the industrial operational environment and the cloud. However, the gap analysis must be extended as new and innovative technologies are additionally deployed for mitigating the ethical, social, and privacy implications.

2. Ethical Dilemmas in Autonomous Vehicles

Fully automated vehicles are already in the development stage and will soon be offered on the market. In recent years, questions related to ethical concerns in autonomous technologies have been increasing. Lawmakers are accustomed to driver assistance, automatic braking, blind spot monitoring, and adaptive cruise control since they regulate traffic safety. These arguments have primarily focused on extreme traffic circumstances portrayed as moral dilemmas, and they are well-documented in the scientific literature, i.e., circumstances where the autonomous vehicle (AV) seems to be required to make challenging ethical choices (e.g., potential hazard situations). Standardization and

legalization are needed to help prevent serious issues between society and technology. Also, policies are needed that can verify and validate the ethical behavior of autonomous systems. Once these principles are put in place, they will help to make the system more transparent, effective, and easy to operate. As autonomous vehicles highly rely on Artificial Intelligence algorithms, they are susceptible to various ethical dilemmas, as shown in **Table 2**.

Table 2. Ethical dilemmas in Autonomous vehicles.

Title	Overview	Ethical Concerns
The Future of Transportation: Ethical, Legal, Social and Economic Impacts of Self-driving Vehicles in the Year 2025 [13]	Summarises the numerous ethical, legal, societal, and economic effects that may arise while implementing self-driving vehicles by 2025, including concerns about individuality, confidentiality, accountability, privacy, and data security.	Security and damage prevention, autonomy, responsibility, rights, data privacy insurance, and discrimination.
Ethical issues in focus by the autonomous vehicles industry [14]	Reviews AVs ethical stories published in scientific papers and business reports by organizations holding California AV testing permits.	Raises concerns over cybersecurity, safety, accountability, human carelessness, and control concerns.
Self-Driving Vehicles—an Ethical Overview [15]	Offers a thorough discussion on the ethical concerns that realistic self-driving car technologies offer. Highlights strong arguments in favor of and against driverless cars and safety necessities for the road traffic system.	Responsibility, public attitudes, safety, control, information, and social Justice
The Future of Automated Vehicles in Canada [16]	Outlines the Transportation and Road Safety Ministries report on adoption of AV on public roads having short, medium, and long-term policy ramifications. Also identifies possibilities, limitations, and strategies for fostering collaboration both domestically and abroad.	The following issues were mentioned: road safety, standards and rules cannot be created separately, innovation needs to be encouraged, privacy issues, education and awareness, technological expertise, traffic laws and requirement of updated traffic rules.
Cybersecurity Challenges in the uptake of Artificial Intelligence in Autonomous Driving [17]	Discusses the key ideas underlying the cybersecurity of AI for autonomous vehicles.	The following issues were summarized: lack of knowledge and data validation techniques for the AI system, encryption and authentication issues, and flaws in security design.

The recent Autonomous Vehicles cyber-attacks (i.e., Yandex taxi hack [18], Tesla Model Y [19]) raise similar ethical, privacy, security, and regulatory concerns to those mentioned in [13][14][15][16][17]. At present, one of the biggest concerns is related to the AI-based decision making software used in self-driving vehicles. For example, if the Autonomous Vehicle predicts a collision endangering pedestrians, the AI-based self-learning software (using Big Data and Machine Learning algorithms for predictive analysis in cloud), quickly reroutes and tries to find an alternate path with lesser casualties [20][21]. If this choice is given to the AI software, it may take the path with the least possible casualties (that is single pedestrian), saving the rest of the crowd. Such an approach is called utilitarian ethics. Utilitarian decision making is widely known to be used in warfare situations, where the path for the least

fatalities/casualties is optimised. Morally and ethically, it would be impossible for humans to make such a choice: a loss of life is a loss, there is no comparison between a single fatality or multiple. From this perspective, there must be a standardized, compliant, and legal system developed before such autonomous vehicles and devices are implemented in real-time scenarios.

A graph in [13] presents the automotive industry's awareness about the ethical concerns regarding self-driving vehicles. Reports from 66 companies based in California were evaluated in the research conducted by [13]. It is interesting to note that the majority of companies focused on: (i) safety and cybersecurity; (ii) sustainability; (iii) human oversight, control, and auditing; (iv) public awareness; (v) privacy; (vi) accountability; (vii) transparency; (viii) ethical design; (viii) legislative frameworks; (ix) dual use problem and military certification. However, none of them addressed the ethical issues related to fairness, non-discrimination, justice, and hidden costs. This form of negligence is in breach of data protection, privacy, and legislative regulations. Also, none of the companies [13] invested in responsible research funding for an emerging technology, which is susceptible to high-risk impact scenarios. Consider if such an AV became involved in an incident or accident, and went unprosecuted due to lack of fairness of data [22], judiciary regulations, and laws in this domain. This may potentially lead to major unrests and promote crimes. Ref. [23] presents an intriguing question related to robot ethics, that is, whether social robots should have certain rights or not. Although the research provides sets of modalities related to robot rights, it mentions that, at this point in time, robots do not possess the necessary capabilities or properties to be considered full moral and legal beings [24][25]. Referring back to cyber attacks mentioned in [18][19], where the hackers took over the command and control, and exploited software vulnerabilities, of Autonomous Vehicles, leading to hours of traffic jam, presents the level of escalated cyber risks autonomous devices are susceptible to and the impact they may have. The authors agree with the recommendations of [24][25] in terms of autonomous decision making: such devices must only be enabled once the potential risks have been realised, controlled, and mitigated. They should also be bound around standardised regulatory and ethical guidelines/bindings.

3. Understanding Ethical Artificial Intelligence (AI)

Artificial Intelligence (AI)-based technologies have accomplished incredible things such as machine vision, medical diagnosis, and Autonomous Vehicles. They hold immense potential for improving societal progress, economic expansion, and human welfare and security [26]. Despite this, industries, societies, and communities face serious hazards because of the low degree of interpretability, data inaccuracies, data protection, privacy laws, and ethical issues with AI-based technologies. One of the biggest challenges in this domain is developing AI that is compliant with moral and ethical requirements. To deal with this, industries must look at both dimensions (AI Ethics and ways to develop Ethical AI). AI Ethics refers to the study of the moral principles, regulations, standards, and laws that apply to AI, following the fundamental principles related to: transparency, respect for human values, fairness, safety, accountability, and privacy [26][27]. These principles are similar to the ones the European GDPR [27] provides. The EU AI Act, passed in 2022, aims to develop a legal framework for AI to promote trust and mitigate potential harm that the technology may cause. However, the Members of the European Parliament have addressed their concerns associated with fundamental rights assessment for high-risk users this year. As per the AI Act, a detailed plan for risk impact assessment related to various threat scenarios, potential breaches (i.e., compliance, AI-cybersecurity, etc.)

must be provided [28]. As the AI Act is still a work in progress, it is essential to understand the principles on which AI ethics is based and how Ethical AI could be developed.

3.1. Transparency

AI-based algorithms and techniques must be transparently designed, with a thorough description as well as a valid justification for being developed, as they play a crucial role in tracking the results and ensuring their accordance with human morals so that one can unambiguously comprehend, perceive, and recognize the designs decision-making mechanism. Twitter serves as an eye-opener here, in 2021 the company faced huge criticism for using AI algorithms to assess racial and gender bias [29]. Twitter is now making amends to mitigate the damages caused by the algorithm and implement the six fundamental attributes of AI Ethics. Considering an industrial/Cyber-Physical System (CPS) environment, transparency is essential for both humans and universal machines.

3.2. Respect for Human Values

AI inventions are obliged to uphold human values and positively affect the progress of individuals and industries, as well to assure to protect sensitivity toward cultural diversities and beliefs.

3.3. Fairness

Fostering an inclusive environment free from discrimination against employees based on their gender, colour, caste, or religion is essential (including team members from various cultural backgrounds helps to reduce prejudice and advance inclusivity). In the past, AI algorithms have been criticized for profiling healthcare data, employees' resumes, etc. Considering this from a GDPR perspective, fair use of data in the European jurisdiction is mandatory. Since the fairness aspect maps across AI fairness and GDPR fair use of data, they must be aligned.

3.4. Safety

Safety relates to both the security of user information and the welfare of individuals. It is essential to recognize hazards and focus on solutions to eliminate such issues. The users' ownership over the data must be protected and preserved by using security techniques such as encryption and giving users control over what data are used and in what context. This also aligns with the scope of GDPR.

3.5. Accountability

Decision-making procedures should be auditable, particularly when AI is handling private or sensitive information such as copyright law, or identifying biometrics information or personal health records.

3.6. Privacy

Protecting user privacy while using AI techniques must be kept as the highest priority. The user's permission must be obtained to utilize and preserve their information. The strictest security measures must be followed to prevent the disclosure of sensitive data.

Lessons must be learnt from Google's project Nightingale and Ascension [30] lawsuits which were an outcome of gathering personal data and raised privacy concerns in terms of data sharing and the use of AI. There are various dilemmas when it comes to the applicability of AI. As an example, AI's implementation in self-driving vehicles has raised huge ethical concerns because, when its designed software was based on a utilitarian approach, in a crash type of situation it would opt for the option with the least casualties; however, when it was programmed based on the social contract theory, the autonomous vehicle could not make a decision as it kept looking for pre-set conditions in loops which ultimately resulted in an accident, as it did not move itself away from the hazard situation [20]. This is one of the biggest challenges, to enable AI to think similarly to humans and have the same ethical and moral conduct; however, with the growing autonomous and self-driving industry there is no going back. Therefore, the only means to control ethical issues related to AI would be to fully develop the standards and regulations. As the authors mentioned earlier, risk impact assessment is merely a means for damage control (analyzing the impact of a breach or vulnerability if exploited). As well, for the cybersecurity threat landscape [31], where the threat actors are constantly evolving, regulating AI—where number of implications are yet to be realized, only best practices and following existing standards and policies can mitigate risks associated to AI deployments in the Industrial environment.

Table 3 elaborates ethical guidelines and existing directives for AI. The authors suggest that a gap analysis of the similarities between them could assist in bridging the compliance/regulatory gaps in the Industrial environment.

Table 3. Ethical Issues and Directives for AI.

Title	Overview	Ethical Guidelines and Directives
Ethics guidelines for trustworthy AI—Publications Office of the EU [32]	Proposes a hierarchy of ethical standards for reliable AI and provides a framework that includes a systematic approach for resilient AI, ethical AI, and legal AI. It also focuses on respect for individual freedom, avoiding violence, justice, and explicability that serve as the foundation of the paradigm.	Provides policies on human intervention and control, technological reliability and security, management of data and privacy, equal protection, transparency, individual and community safety, and liability.
IEEE [33]	Addresses both arguments in favor of the beneficial consequences as well as cautions regarding potential privacy violation, prejudice, skill loss, economic repercussions, protection of vital infrastructure, and everlasting impacts on society.	Individual rights, security, data accountability, efficiency, compliance, awareness of abuse, and competency.
Artificial Intelligence Policy: A Primer and Roadmap [34]	Provides a conceptual framework based on AI policy, intended to assist decision-makers, investors, academics, and students in comprehending the current policy landscape surrounding AI and the issues it poses.	Fairness and Justice, use of force, security and authentication, sovereignty and concealment, taxes, and labor mobility.
AI-based applications and algorithms used in an Industrial IoT (IIoT) environment [35][36] demonstrated that none of the applications and algorithms had data privacy controls in place leading to ethical and legal issues.		

Title	Overview	Ethical Guidelines and Directives
Smart Helmet 5.0 for Industrial IoTs using AI [35]	Presents a comparative analysis of the latest AI-based supervised learning approaches and proposes the use of a Deep Convolutional Neural Network (ConvNet/CNN) to identify potential professional threats.	Threat identification was performed using an AI algorithm but the Smart Helmet 5.0 did not provide data privacy
Industrial IoT and unsupervised deep learning enabled real-time occupational safety monitoring in cold storage warehouses [36]	Proposes a structure for a smart system using the IIoT and digital twin (DT) systems, to implement real-time workplace safety surveillance in the warehouse and guarantee synchronized cyber-physical areas for data provenance and accessibility.	The implementation involved surveillance and lacked securing data privacy in the workplace.

[28][37][38] [32][33][34] [34][35][36]

rming the have nent.

The three frameworks [22][29][30] developed by different professional standards/regulatory bodies have few attributes in common; however, a complete mapping or interoperability between the ethical frameworks was not provided. This becomes a potential issue when industries tend to implement a standardized approach. Another issue arises when industries have different manufacturing regions/setups across the world (Europe, USA, and China) and are subject to different jurisdictions, data regulations, and compliance. In circumstances where a production environment deploys different AI regulatory frameworks, it will make the dissemination of information across the digital factory, supply chain, and data classification a complex process. Industry 5.0 is value driven and its vision may only be achieved by mapping synergies across the ethical, technical, innovative, and sustainable domains. The guidelines provided by the EU in [28][37][38] have been the first ones to take initiative in shaping European Digital Strategy, developing standardized regulatory and legal frameworks for AI and mitigating the potential risks. Aligning the AI deployments with the provided Act and security controls [31] is the only regulated way for now, imbibed with the AI ethical principles (i.e., privacy, accountability, fairness of data, transparency), that contribute and map with GDPR principles as well. However, as discussed earlier, it is important to note that AI depends on various technologies (i.e., Big Data, Machine Learning, etc.). If any of these technologies have security gaps, it may lead to potential breaches in the AI domain as well; therefore, the adapting industries must make sure that their ethical and legal framework is compliant and reflects across the interconnected emerging technologies.

References

1. Dhirani, L.L.; Newe, T.; Nizamani, S. Tenant–vendor and third-party agreements for the cloud: Considerations for security provision. Int. J. Softw. Eng. Its Appl. 2016, 10, 449–460.
2. Dhirani, L.L.; Newe, T. Hybrid Cloud SLAs for Industry 4.0: Bridging the Gap. Ann. Emerg. Technol. Comput. 2020, 4, 41–60.
3. Faragardi, H.R. Ethical Considerations in Cloud Computing Systems. Proceedings 2017, 1, 166.
4. Vigliarolo, B. 85% of Organizations Will Be ‘Cloud-First’ by 2025, Says Gartner. 2021. Available online: https://www.techrepublic.com/article/85-of-organizations-will-be-cloud-first-by-2025-says-gartner (accessed on 30 November 2022).

5. Lee, C.A.; Bohn, R.B.; Michel, M. The NIST Cloud Federation Reference Architecture. 2020. Available online: https://doi.org/10.6028/NIST.SP.500-332 (accessed on 9 January 2023).
6. NIST SP 500-332. The NIST Cloud Federation Reference Architecture. Available online: https://keyvoms.org/f/on-the-publication-of-nist-sp-500-332 (accessed on 9 January 2023).
7. Bohn, R.; Michel, M. Standards for Cloud Federation. Available online: https://ieeecs-media.computer.org/media/membership/StandardsCloudFed_RBMM_03162021.pdf (accessed on 9 January 2023).
8. Wan, Z.; Hazel, J.W.; Clayton, E.W.; Vorobeychik, Y.; Kantarcioglu, M.; Malin, B.A. Sociotechnical safeguards for genomic data privacy. Nat. Rev. Genet. 2022, 23, 429–445.
9. Lynn, T.; Mooney, J.G.; van der Werff, L.; Fox, G. Data Privacy and Trust in Cloud Computing; Palgrave Macmillan: London, UK, 2021.
10. Top 5 Cloud Security Breaches and Lessons. Available online: https://www.cybertalk.org/2022/04/26/top-5-cloud-security-breaches-and-lessons (accessed on 10 January 2023).
11. Foltz, A.C. Stuxnet Schmitt Analysis, and the Cyber Use-of-Force. JFQ 2012, 67, 40–48. Available online: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf (accessed on 9 December 2022).
12. (ISC)² Code of Ethics. Available online: https://www.isc2.org/Ethics (accessed on 4 January 2023).
13. Ryan, M. The Future of Transportation: Ethical, Legal, Social and Economic Impacts of Self-driving Vehicles in the Year 2025. Sci. Eng. Ethics 2020, 26, 1185–1208.
14. Martinho, A.; Herber, N.; Kroesen, M.; Chorus, C. Ethical issues in focus by the autonomous vehicles industry. Transp. Rev. 2021, 41, 556–577.
15. Hansson, S.O.; Belin, M.Å.; Lundgren, B. Self-Driving Vehicles—An Ethical Overview. Philos. Technol. 2021, 34, 1383–1408.
16. The Future of Automated Vehicles in Canada. Available online: https://comt.ca/Reports/The%20Future%20of%20Automated%20Vehicles%20in%20Canada%202018.pdf (accessed on 30 November 2022).
17. European Union Agency for Network and Information Security. Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving. Available online: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-drivin (accessed on 20 November 2022).
18. Hackers Created an Enormous Traffic Jam in Moscow. Available online: https://cybernews.com/cyber-war/hackers-created-an-enormous-traffic-jam-in-moscow (accessed on 20 November 2022).

19. New Attack Can Unlock and Start a Tesla Model Y in Seconds, Say Researchers. Available online: https://www.theverge.com/2022/9/12/23348765/tesla-model-y-unlock-drive-car-thief-nfc-relay-attack (accessed on 20 November 2022).
20. Dilmegani, C. Top 9 Ethical Dilemmas of AI and How to Navigate Them. Available online: https://research.aimultiple.com/ai-ethics (accessed on 12 December 2022).
21. Bonnefon, J.F.; Shariff, A.; Rahwan, I. The social dilemma of autonomous vehicles. Science 2016, 352, 1573–1576.
22. GDPR Article 32. Available online: https://gdpr-info.eu/art-32-gdpr (accessed on 4 January 2023).
23. Gunkel, D.J. The other question: Can and should robots have rights. Ethics Inf. Technol. 2017, 20, 87–99.
24. IEEE Spectrum. Available online: https://spectrum.ieee.org/automation/robotics (accessed on 3 January 2023).
25. Darling, K. Extending legal protection to social robots: The effects of anthropomorphism, empathy, and violent behaviour toward robotic objects. In Robot Law; Calo, R., Froomkin, A.M., Kerr, I., Eds.; Edward Elgar: Northampton, MA, USA, 2016; pp. 213–231.
26. Siau, K.; Wang, W. Artificial intelligence (AI) Ethics: Ethics of AI and ethical AI. J. Database Manag. 2020, 31, 74–87.
27. GDPR. Complete Guide to GDPR Compliance. Available online: https://gdpr.eu (accessed on 12 December 2022).
28. Cyber Resilience Act. Available online: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (accessed on 3 January 2023).
29. BBC News. Twitter Finds Racial Bias in Image-Cropping AI. Available online: https://www.bbc.com/news/technology-57192898 (accessed on 20 September 2022).
30. WSJ. Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans. Available online: https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790 (accessed on 5 November 2022).
31. Dhirani, L.L.; Armstrong, E.; Newe, T. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. Sensors 2021, 21, 3901.
32. Publications Office of the EU. Ethics Guidelines for Trustworthy AI. 2019. Available online: https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf (accessed on 1 December 2022).
33. IEEE. Ethically Aligned Design. Available online: https://ethicsinaction.ieee.org (accessed on 12 December 2022).
34. Calo, R. Artificial Intelligence Policy: A Primer and Roadmap. UCDL Rev. 2017, 51, 399–435.

35. Campero-Jurado, I.; Márquez-Sánchez, S.; Quintanar-Gómez, J.; Rodríguez, S.; Corchado, J.M. Smart Helmet 5.0 for Industrial Internet of Things Using Artificial Intelligence. Sensors 2020, 20, 6241.
36. Zhan, X.; Wu, W.; Shen, L.; Liao, W.; Zhao, Z.; Xia, J. Industrial internet of things and unsupervised deep learning enabled real-time occupational safety monitoring in cold storage warehouse. Saf. Sci. 2022, 152, 105766.
37. A European Approach to Artificial Intelligence. Available online: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (accessed on 3 January 2023).
38. EU Digital Markets Act and Digital Service Acts Explained. Available online: https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained (accessed on 3 January 2023).