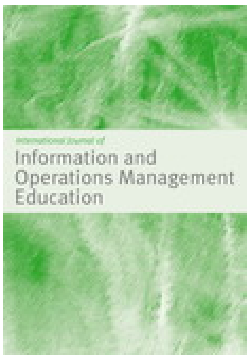
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



**International Journal of Information and Operations Management Education**

ISSN online: 1744-2311 - ISSN print: 1744-2303
https://www.inderscience.com/ijiome

# Ethical pitfalls of technologies enabling disruption and fostering cyber ethical mindset in management curriculum

Soham Sengupta, Asit Bandyopadhayay

**DOI:** 10.1504/IJIOME.2024.10062764

**Article History:**

| | |
|---|---|
| Received: | 02 September 2023 |
| Last revised: | 29 November 2023 |
| Accepted: | 30 November 2023 |
| Published online: | 06 March 2024 |

# Ethical pitfalls of technologies enabling disruption and fostering cyber ethical mindset in management curriculum

Soham Sengupta

Department of Management Information Systems,
University of Memphis,
Memphis, TN 38152, USA
Email: ssngupta@memphis.edu

Asit Bandyopadhayay*

Department of Management and Marketing,
Austin Peay State University,
Clarksville, TN 37044, USA
Email: bandya@apsu.edu
*Corresponding author

**Abstract:** There is a need to emphasise and educate future business leaders on emerging technologies' disruptive and transformative impact on business processes. Allen (2020) suggests the need for a digital mindset and tech literacy in business management education. In our study, we define cyber literacy and cyber ethical mindset emphasising the importance of informing future leaders in business schools about the ethical dilemmas arising while using these emerging technologies. Additionally, we highlight various ethical pitfalls of using technologies enabling disruption (TED). Further, we contribute to the understanding of cyber literacy, cyber ethics and business ethics, how to incorporate cyber ethics into the management curriculum, and why there is a need to integrate cyber ethics into management education.

**Keywords:** cyber ethical mindset; cyber literacy; ethical pitfalls; technologies enabling disruption; TED.

**Reference** to this paper should be made as follows: Sengupta, S. and Bandyopadhayay, A. (2024) 'Ethical pitfalls of technologies enabling disruption and fostering cyber ethical mindset in management curriculum', *Int. J. Information and Operations Management Education*, Vol. 7, No. 3, pp.282–297.

**Biographical notes:** Soham Sengupta is an Assistant Professor of Teaching in the Management Information Systems Department of the University of Memphis. He completed his undergraduate degree in Electrical Engineering from India. He has received his Master's in Electrical Engineering from Michigan Technological University and Master's in Business Administration from the University of Memphis. He completed his PhD in Management Information Systems from the University of Memphis. His research interests are in digital transformation, mobile-based applications, and cyber ethics.

Asit Bandyopadhayay is an Assistant Professor of MIS and Business Analytics in the Department of Management and Marketing, College of Business at Austin Peay State University. He enjoys research on blockchain technology applications, e-commerce, supply chain management, information systems, business analytics and his work has been published in reputed academic journals. His current research interests include blockchain applications in ensuring data privacy; blockchain applications in supply chain management; information literacy and cybersecurity challenges among Gen Z; cybersecurity breaches and privacy policy, generative AI and sustainable supply chain management.

## 1 Introduction

Although Industry 4.0 is still developing, several industrial innovators and technological experts are anticipating the beginning of the 5th industrial revolution (Industry 5.0). The introduction of Industry 5.0 is based on the observation or assumption that Industry 4.0 focuses less on the original principles of social fairness and sustainability but more on digitalisation and artificial intelligence (AI) driven technologies for increasing the efficiency and flexibility of production (Sasikumar et al., 2023). Hence, Industry 5.0 provides a distinct perspective and highlights the importance of research and innovation to support the industry’s long-term service to humanity. Furthermore, while technology-enabled disruption (TED) is associated with Industry 4.0 or the age of augmentation, Industry 5.0 focuses more on the ethical use of those technologies where the human and machine work in symbiosis (Xu et al., 2021), ensuring ethical and sustainable practices.

Even though Industry 5.0 suggests ethical practices while using technologies, management education still does not incorporate handling ethical lapses of technologies in its curriculum. Allen (2020) suggested that management educators need to develop a digital mindset by studying TED, introducing courses or modules within the coursework, and providing assignments based on them that help synthesise those concepts and eventually prepare students for the future workplace. Many universities have started offering such courses by offering degrees, majors, minors, concentrations, certificates, or even revising their curriculum (Kung et al., 2006). However, very few programs discuss these technologies’ ethical pitfalls. Technologies that enable disruption are moving at high speed to market, from their concept to practice. We can see programs are offering courses surrounding disruptive technologies. However, at the same time, they are not talking about the ethical dilemmas associated with them. Take the example of artificial intelligence (AI) tools like machine learning (ML). ML is a field of inquiry devoted to understanding and building methods that ‘learn’ the methods that leverage data to improve performance on some tasks (Mitchell, 1997). Now, for example, using ML, analysts develop predictive modelling that identifies individuals with unpaid debt records. In the future, although an individual with outstanding debt records clears their debt, still that model will consider that individual with negative credit behaviour. ML is perceived to be able to exacerbate the problem by collecting and analysing past data by holding the information forever. Besides credit checks, companies are also using this information in insurance, medical, and loan applications, which can harm and amplify bias for individuals, raising privacy concerns. The concept of 'right to be forgotten' is getting popularised to handle such practices. A requirement of privacy regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) is that individuals whose data is housed by organisations have the right to request for this data to be erased (Bourtoule et al., 2021). The right to be forgotten is necessary for many situations, preventing one from being indexed in search engines for unpaid debts, petty crimes that have been committed in the past, and so on. Responding to such ethical pitfalls, researchers have started talking about machine unlearning (MU) process. MU is a nascent field of artificial intelligence where the goal is to remove all the traces of a selected data point from the predictive model without affecting the model's performance. Therefore, while incorporating TED into the business curriculum, we must be equally careful that our curriculum addresses such ethical pitfalls. As management educators, we are charged with preparing young people for successful careers in business; however, if we do not expose them to the flip side of technology, the purpose of education is incomplete.

This article aims to bring attention to the need for ethical considerations to be included in designing a management curriculum focusing on technologies enabling disruption (TED). The goal is to raise awareness of these technologies' potential negative impacts on society and encourage responsible use in the business world without neglecting the ethical implications that may arise with deploying such technologies. We, as management educators, are not fully informed about these situations. Essentially, our lack of preparation and, in some cases, understanding means that our students will be disadvantaged (Allen, 2020). We must prepare our students to be technically competent managers with an ethical mindset. Technically competent means having the digital smarts (Weill et al., 2021) to understand how the technology works and its multiple applications in transforming and disrupting existing societal or business processes. To be managerially competent is to have the critical thinking ability to discern the various ethical challenges and tradeoffs of TEDs and act accordingly for the betterment of society and organisations. Our averment in this article challenges management educators to develop a technically competent and cyber ethical mindset. The objective is not only incorporating TED in the curriculum, but more importantly creating awareness about the ethical pitfalls of these technologies. Management educators must be more intentional in inculcating this mindset, so they are well-prepared to navigate a technology-enabled future effectively.

This paper is organised as follows: Section 1 talks about introduction; Section 2 highlights the concepts of cyber literacy and cyber ethics; Section 3 talks about how cyber ethics is different from business ethics traditionally taught in business schools; Section 4 deliberates why is there a need to teach cyber ethics in management education; Section 5 talks about ethical pitfalls of TEDs, and finally the conclusion is available in Section 6.

## 2 Cyber literacy and cyber ethics

Cyber literacy refers to using, understanding, and navigating technology and the internet safely and responsibly. It encompasses a range of skills, including the ability to use computers and the internet and proficiency in online communication tools, software applications, and digital media. With the ever-increasing importance of technology in our personal and professional lives, cyber literacy has become an essential skill for everyone.

One aspect of cyber literacy is using the internet and technology safely. In addition, it includes understanding the potential risks of using the internet, such as viruses and malware, and taking steps to protect oneself from these threats (Hammond and Cooper, 2015).

Furthermore, using anti-virus software, creating strong passwords, and being wary of suspicious emails or links. It also includes understanding and following online safety protocols, such as being aware of one's personal information and not sharing it with strangers. Another aspect of cyber literacy is using software applications, such as word processing and spreadsheet programs. These skills are essential for completing tasks such as writing a report or analysing data. Cyber literacy also includes using online communication tools, such as social media and messaging apps, to connect with others and share information safely. In addition to these technical skills, cyber literacy encompasses evaluating and using digital media. It includes the ability to critically assess the credibility and reliability of online sources and the ability to safely and responsibly create and share digital content, such as videos and images. Another essential aspect of cyber literacy is understanding the legal and ethical considerations of using technology and the internet. It includes understanding copyright, intellectual property, and data privacy issues. It also includes understanding the potential impact of technology on society and being aware of one's digital footprint. Given the importance of cyber literacy, individuals of all ages must have access to the training and resources they need to develop these skills. It includes providing access to technology and the internet and offering classes and training programs on cyber literacy. Additionally, schools must integrate cyber literacy instruction into their curriculum to ensure that students are prepared for the digital world they will encounter after graduation.

In conclusion, cyber literacy is a critical skill in today's digital world. It encompasses a range of technical skills, such as the ability to use the internet and technology safely and the ability to evaluate and create digital media responsibly. Furthermore, to succeed in both personal and professional life, individuals must be able to navigate the digital world safely and responsibly. Finally, it includes understanding the legal and ethical considerations of using technology and having access to the training and resources needed to develop cyber literacy skills.

Cyber ethics is the behavioural, societal, and environmental implications of TED like artificial intelligence, internet of things, augmented/virtual reality, metaverse, blockchain, automation/robotics, sensor/RFID, etc. (Sousa and Rocha, 2019) Being cyber ethical means anticipating, detecting, analysing, and acting accordingly toward challenging ethical dilemmas posed by TEDs. To become cyber ethical, an individual must possess the technical and managerial competencies required to critically analyse various ethical dimensions of TED. Cyber ethics refers to the principles and values that guide the use of technology and the internet. As technology continues to advance and becomes increasingly integrated into every aspect of our lives, it is essential to consider the ethical implications of its use. It includes issues such as privacy, security, and the impact of technology on society. A critical aspect of cyber ethics is privacy. With the rise of social media and the internet, individuals share more personal information than ever. However, the collection and use of this information by companies and governments can raise serious privacy concerns. For example, companies may use personal data for targeted advertising, or governments may use it for surveillance purposes. Individuals need to be aware of these potential risks and take steps to protect their personal information.

Another vital aspect of cyber ethics is security. As technology becomes more integrated into our lives, it also becomes a target for cyberattacks. These attacks can have serious consequences, from stealing personal information to disrupting critical infrastructure. Individuals and organisations must protect themselves from these threats using strong passwords and regularly updating software.

Cyber ethics also includes considering the impact of technology on society. As technology advances, it can potentially transform the way we live and work significantly. It has everything from automation replacing jobs to using artificial intelligence in decision making. Therefore, it is essential to consider the potential consequences of these changes and ensure that they are implemented fairly and justly. One of the most crucial aspects of cyber ethics is the responsible usage of technology. While technology has many benefits, it can also be used in harmful ways. For example, the use of social media can lead to the spread of misinformation, and the use of technology can lead to addiction and the erosion of face-to-face communication. Therefore, individuals need to be aware of these potential risks and take steps to use technology responsibly and healthily. Knowing how crucial cyber ethics is, individuals and organisations must be educated about these issues and take steps to ensure that technology is used ethically and responsibly. It includes providing training and resources for individuals and organisations, as well as incorporating cyber ethics into the curriculum of schools and universities. Additionally, technology companies need to consider the ethical implications of their products and take steps to ensure that they are used responsibly.

In conclusion, cyber ethics is critical to responsibly using technology and the internet. It encompasses issues such as privacy, security, and the impact of technology on society. As technology continues to advance and becomes increasingly integrated into every aspect of our lives, it is vital to consider the ethical implications of its use and take steps to ensure that it is used responsibly. It includes educating individuals and organisations about cyber ethics and incorporating it into the curriculum of schools and universities. Additionally, technology companies are responsible for considering their products' ethical implications and taking steps to ensure that they are used responsibly.

## 3 How is cyber ethics different from business ethics traditionally taught in business schools?

Cyber ethics and business ethics are both concerned with the ethical principles and values that guide the use of technology and the internet, but they have some distinct differences. Business ethics is a broader field that deals with the ethical principles and values that guide the actions of organisations and individuals in the business world. Business ethics can include issues such as honesty, fairness, and responsibility. Business ethics also encompasses matters critical to business success, such as corporate social responsibility, labour standards, and environmental protection. On the other hand, cyber ethics is more specific and focused on the ethical principles and values that guide the use of technology and the internet. Cyber ethics can include issues such as online privacy, security, and responsible usage of technology. Cyber ethics also encompasses online reputation management, data privacy, and the ethical implications of artificial intelligence and automation. Another key difference is that, while business ethics can be applied to any organisation and industry, cyber ethics focuses more on the digital world, the internet, and technology-based companies. However, due to the rapid rise of digital transformation across industries, the aptitude for cyber ethics has become imperative for business-digital fit.

Online privacy: privacy in an era of digital ubiquity is a highly sought after commodity. The sensitivity around privacy or the privacy outcry among individuals get more pronounced when one realises how vulnerable one is with the presence of misinformation and disinformation. The Oxford English Dictionary defines misinformation as 'wrong or misleading information' and disinformation as 'the dissemination of deliberately false information'. Stahl (2006) defines misinformation as accidental falsehood and disinformation as deliberate falsehood. Information whose role is to 'in-form' individuals and help them orient themselves to take the appropriate decision has been muddled with the presence of information overload. The information overload has been further fuelled by the advent of mobile devices and the social media applications on them.

Online reputation management: after realising the privacy vulnerability in contemporary times, an individual can work towards managing their identity or reputation in the digital world. To do so, there is a need to adopt logistical tools to bring in behavioural changes to curb the need for instant gratification (Grellhesl and Punyanunt-Carter, 2012; Van Deursen et al., 2015) and approval fuelled by the presence of mobile devices at all times.

Data privacy and security: in this era of digitalisation across organisations and society it is critical to address data privacy and security. The technology (big-tech) companies are generally entrusted with data governance. A big part of the data governance encompasses data stewardship by the organisations. Data stewardship can be defined as a set of procedures to ensure responsible data planning and data management. With the plethora of data brokers and other data intermediaries through the use of third-party cookies makes it hard for the technology companies to have complete control over data privacy. In addition, due to lack of proper data security standards companies often fail to protect consumer information. This opens up the organisation to a host of regulatory issues. To address this issue, one solution can be to change the business model of Facebook and Instagram that provides free services now to a subscription-based model. In a subscription-based model users will pay a monthly subscription fee to maintain their social media presence. In doing so big tech can move from an ad-based business model to a paid service model. This will cut out the third-party intermediaries ensuring data privacy and security to higher standards.

Responsible usage of technology: the onus for the responsible usage of technology is on everybody. The 'everybody' in this context are the individuals, organisations, groups, nation states and global bodies. To become a responsible user of emerging technologies like AI it is imperative to understand the technology from an operational point of view (POV), but more importantly recognise or take part in discussing the pros and cons of the technology across different walks of life. This should be a continuous endeavour of growing into and understanding the different nuances of emerging technologies. This requires having digital savviness as a human attribute to be an effective global citizen.

In summary, while business and cyber ethics share some similarities, they have distinct differences. Business ethics is a broader field that deals with ethical principles and values in the business world. At the same time, cyber ethics is more specific and focused on the ethical principles and values that guide the use of technology and the internet essential to business operations and innovations.

## 4 Why is there a need to teach cyber ethics in management education?

There are several reasons why it is essential to teach cyber ethics in the management curriculum:

1 Technology is increasingly integrated into business: with the rapid advancement of technology, the internet, and digital tools are essential for companies to operate and compete. As a result, management students need to understand the ethical implications of using these tools to make responsible decisions.

2 Cyber-attacks are a growing concern: cybersecurity threats are becoming increasingly prevalent, and businesses need to be able to protect themselves from them. As future managers, students must understand the ethical considerations of safeguarding company and customer data.

3 Data privacy is a primary concern: the collection and use of personal data by businesses has become a significant concern for individuals and governments. Therefore, business/management students need to understand the ethical implications of collecting and using personal data and the laws and regulations governing data privacy.

4 Artificial intelligence and automation: artificial intelligence (AI) and automation are changing how businesses operate and can change the workforce significantly. As future managers, students need to understand the ethical implications of using these technologies, such as the potential consequences of replacing human jobs with machines.

5 The impact of technology on society: the use of technology can significantly impact society, and management students need to understand the ethical implications of these impacts to make responsible decisions.

In summary, the management curriculum needs to include cyber ethics education to ensure that future managers are prepared to navigate the ethical challenges of the digital world.

## 5 Ethical pitfalls of technologies enabling disruption

**Table 1** Various ethical pitfalls of TED to foster cyber ethical mindset

| *Technology* | *Ethical pitfalls* |
|---|---|
| 3-D printing | • It can replicate objects relatively easily, raising challenges to intellectual property rights and piracy (Depoorter, 2013).<br>• Hard to ensure the quality (Wu and Chen, 2018) and reliability of the 3D printed parts.<br>• 3D printed parts or devices can create safety and liability issues in fire and explosion hazards for critical systems like aerospace or healthcare. |

**Table 1** Various ethical pitfalls of TED to foster cyber ethical mindset (continued)

| *Technology* | *Ethical pitfalls* |
|---|---|
| | • Materials used for 3D printing can create non-recyclable and toxic waste creating environmental concerns. For example, polylactic acid (PLA) is used as printing material.<br>• It can be used to print illegal and dangerous items like illicit drugs, weapons, and counterfeit items, creating destructive societal implications (Daly et al., 2021).<br>• Due to the cost and skillset necessary for 3D printing, one can raise questions on who can benefit from the technology in society due to inequity and lack of access.<br>• 3D scanning and printing is used from detailed and accurate models of real-world objects, raising privacy concerns about the use and storage of the model data. |
| Artificial intelligence (AI)/machine learning | • AI algorithms can perpetuate and amplify existing biases (Ntoutsi et al., 2020; Srinivasan and Chander, 2021) in the training dataset leading to discriminatory outcomes (e.g., COMPAS). In addition, the lack of transparency and explainability in complex AI systems makes it challenging to ensure accountability and trust in healthcare, finance, criminal justice, etc.<br>• From a safety perspective, AI systems can create hazards and risks in self-driving cars, financial trading, and military plans.<br>• AI systems' autonomy and reinforced nature can make it unpredictable and difficult for humans to control.<br>• Efficient AI systems (Cristofaro et al., 2021) can automate many tasks leading to job displacement and economic disruption.<br>• AI systems collect and process large amounts of data raising privacy concerns due to the storage of data about personal information.<br>• Lack of regulation in a fast-changing landscape like AI technology can create ethical lapses in human-computer interaction. |
| Augmented reality (AR) and virtual reality (VR) | • AR technology requires collecting vast amounts of sensitive personal data like facial characteristics (Cowan et al., 2021) and biometric features, which can bring privacy (Roesner et al., 2014; Harborth and Pape, 2021) concerns if not handled properly.<br>• Lack of transparency and existing biases in real-time AR systems design can increase unnecessary complexity and discriminatory outcomes.<br>• It will be hard to ensure the safety and liability of AR/VR headsets (Rauschnabel et al., 2018) when individuals are not supposed to, like driving or operating heavy machinery.<br>• Excessive usage of AR/VR technology can hinder social interactions among human beings (O'Shea and Hurriyet, 2018) and cognitive stunt growth, particularly among adolescents and emerging adults. |

**Table 1** Various ethical pitfalls of TED to foster cyber ethical mindset (continued)

| *Technology* | *Ethical pitfalls* |
|---|---|
| | • Reality distortion is another ethical pitfall of technology where it will be hard to discern between the virtual and real-world, leading to confusion, disorientation, and reduced ability to operate in the real world.<br>• Malicious actors can misuse this technology by spreading misinformation and disinformation and facilitating cybercrime. |
| Automation/robotics | • Automation makes tasks more automated, making people overly dependent on technology (Alvim and Alturas, 2021) and reducing their ability to function without it.<br>• Due to a lack of human oversight, it might be hard to anticipate automated systems leading to unintended and harmful consequences in specific contexts where lack of accountability becomes a glaring challenge.<br>• Job displacement (Pham et al., 2018) is another ethical pitfall, as low-skilled workers can be replaced by automation leading to inequality and social disruption. |
| Big data/analytics | • In analytics, security and privacy (Puaschunder, 2019) are of prime importance, as in the event of data breaches, personal data is potentially misused for malicious or unauthorised purposes (Richterich, 2018).<br>• Lack of transparency in complex data analytics systems (Firth et al., 2021) can be challenging to ensure bias-free data-driven decision-making.<br>• Due to a lack of regulation and standardisation, it is easier to manipulate data by selectively presenting information, distorting or hiding specific facts, or creating fake data, which can lead to societal or personal harm. |
| Blockchain technology | • There are privacy concerns as transactions made on blockchain are public (Zhang et al., 2019) and can be viewed by anyone, which can potentially have privacy concerns.<br>• Smart contracts are self-executing contracts with the terms of the agreements written directly into lines of code (Unsworth, 2019). Therefore, any bugs in those lines of code can perpetuate and amplify the error.<br>• Lack of regulation is a concern as industries like healthcare and finance require oversight and compliance.<br>• Blockchain technology facilitates criminal activities like money laundering and illicit transactions (Raza and Raza, 2021) due to anonymity and pseudonymity.<br>• Lack of governance mechanism can be challenging to bring about proper changes and updates to the technology affecting the network's stakeholders.<br>• Due to the decentralised nature of blockchain (Bandyopadhayay et al., 2023), it is difficult to hold anyone accountable for issues like security breaches or malfunctions. |

**Table 1** Various ethical pitfalls of TED to foster cyber ethical mindset (continued)

| *Technology* | *Ethical pitfalls* |
|---|---|
| Brain-computer interface (BCI) | • BCI systems collect and process sensitive personal information like neural activity raising privacy and security concerns about this information. From a privacy perspective, BCI data on an individual can be used to monitor or manipulate an individual's thoughts and emotions (Steinert and Friedrich, 2020). From a safety perspective, BCI systems can create hazards and risks due to unwanted neural stimulation (Klein et al., 2016) or interference with normal brain function.<br>• Manipulation through the BCI system also infringes on an individual's agency, autonomy (Burwell et al., 2017), and self-determination. |
| Chatbots | • Chatbots are designed to mimic human-like behaviour and emotions encapsulating anthropomorphism (Blut et al., 2021), blurring the real and virtual domains, which can be confusing or misleading.<br>• Due to the reinforced nature of the chatbots, they can become better with time, making humans depend on or feel more comfortable using chatbots, which negatively impacts human-human interactions and social skills.<br>• Chatbots aggravate job loss, especially for customer representatives in the manufacturing and service sectors.<br>• Initially, chatbots may have limited capabilities making it hard to understand complex or nuanced conversations, which can be frustrating and generate user mistrust (Cheng et al., 2022). |
| Cloud computing | • Data ownership (Khan and Hamlen, 2012; de Bruin and Floridi, 2017) is an ethical issue regarding liability as the user does not fully own the data, and the cloud provider can have access and control over the data. It also creates a loss of control and flexibility for organisations.<br>• Cloud computing activities cross national borders, making it difficult to regulate and enforce data privacy and security (Chen and Zhao, 2012), and ownership laws.<br>• Cloud providers with large data centres consume a lot of energy, which could negatively affect the environment if mismanaged. |
| Cybersecurity | • Cybersecurity measures can be used for unwanted surveillance leading to violation of civil liberties and human rights.<br>• Hacking in the context of cyber warfare, cyber espionage, and corporate espionage leads to identifying vulnerabilities (Firth et al., 2021) or gathering intelligence that can inflict damage on the target leading to violation of laws and ethical principles.<br>• The lack of consensus on international norms and laws in cyberspace makes it difficult to establish and enforce ethical principles in the field. |
| Drones (unmanned aircraft systems) | • Drones equipped with cameras and other sensors can be used to make illegal surveillance (West and Bowman, 2016) on individuals and groups, raising concerns about invasion of privacy (Altawy and Youssef, 2016). |

**Table 1** Various ethical pitfalls of TED to foster cyber ethical mindset (continued)

| *Technology* | *Ethical pitfalls* |
|---|---|
| | • Targeted killings and other military/hostile actions using drones generate collateral damage in the form of unintended civilian deaths and injuries, which raises ethical questions about using lethal force, proportionality, and protecting civilians or non-combatants. |
| Internet of things (IoT) | • IoT devices collect and transmit large amounts of personal data (Marjani et al., 2017), leading to questions about protecting the privacy of individuals and ensuring there is no data abuse.<br>• The interconnectedness of IoT devices makes them vulnerable to hacking and cyberattacks (Kimani et al., 2019), leading to questions about personal and national security protection.<br>• Many IoT devices are not transparent about collecting, processing, and sharing data, which raises ethical concerns about informed consent and trust.<br>• As IoT devices become more integrated into our lives (Kazi et al., 2023), they can create dependency and become challenging to opt out of using. |
| Nanotechnology | • The nano-sized and highly reactive particles can unintentionally impact human health and the environment (Sajid et al., 2015). In addition, the uncertainty around the long-term impacts of this technology on humans and non-human organisms is a risk factor.<br>• The development and application of nanotechnology have the potential to create both benefits and drawbacks for society, raising questions about how to ensure that its benefits are widely shared and its risks are mitigated.<br>• Using nanotechnology in products and devices, such as sensors and tracking devices, raises concerns about protecting personal privacy and security.<br>• Some concerns advances in nanotechnology could be used to create new types of weapons (Altmann, 2004).<br>• The small size and unique properties of nanomaterials may make it difficult for regulators and consumers to identify and evaluate potential risks, which raise ethical concerns about transparency and accountability.<br>• There is an ongoing debate about how to regulate the development and application of nanotechnology and how to balance the benefits of nanotechnology with the need to protect public health and safety, human rights, and the environment (Coles and Frewer, 2013). |
| Quantum computing | • Quantum computers can break traditional encryption methods (Buchanan and Woodward, 2017), raising concerns about protecting sensitive information and the potential for cyberattacks.<br>• Quantum computing may give rise to autonomous systems with advanced decision-making capabilities (Biagini et al., 2020), which raises questions about accountability and control. |

**Table 1** Various ethical pitfalls of TED to foster cyber ethical mindset (continued)

| *Technology* | *Ethical pitfalls* |
|---|---|
| | • The development of quantum computing may bring new challenges to regulation, the legal system, and the economy.<br>• Quantum computing could be used to enhance human abilities beyond natural limits (Brooks, 2019), which could pose ethical questions about fairness, ethics, and human nature. |
| Renewable energy (clean energy) | • The potential for renewable energy projects to displace or harm low-income and marginalised communities is an ethical concern (Sovacool et al., 2016). It can occur if the land is taken without proper compensation or consultation with the affected community.<br>• Another ethical concern is that the materials required for renewable energy technology, such as rare earth metals and lithium for battery storage, can lead to the exploitation of vulnerable populations and ecosystems (Kramarz et al., 2021; Church and Crawford, 2020) in the countries where they are extracted and manufactured.<br>• Biomass energy, a form of renewable energy, may also raise ethical concerns if it relies on the clear-cutting of forests or the cultivation of crops for fuel at the expense of preserving natural habitats or food security for local communities.<br>• The benefits of renewable energy are not always evenly distributed, and the negative consequences of fossil fuel extraction and burning may disproportionately impact low-income communities or communities of colour. Still, they may not have the same access to the benefits of renewable energy. |
| Sixth generation wireless (6G) | • With the potential for even faster speeds and greater data transfer capabilities, 6G wireless communication could enable more data collection and surveillance than previous generations of wireless technology (Chowdhury et al., 2020). It could lead to a more significant invasion of privacy, as individuals' data could be accessed and used without their knowledge or consent.<br>• There may be concerns about unequal access to 6G technology, particularly in low-income or rural areas where installing and maintaining the necessary infrastructure may be more challenging. In addition, it could exacerbate existing digital divides and further marginalise certain groups of people.<br>• 6G technology could enable new forms of human enhancement, such as augmenting human cognition or physical abilities, using implantable devices connected to the 6G network (Dao, 2023). However, this could raise ethical concerns around the fairness and safety of such enhancements and their potential impact on the definition of what it means to be human.<br>• 6G technology will likely be subject to international regulation and policies, with differing standards and laws among different countries. It could lead to ethical dilemmas related to the potential for additional standards and rules and how that may affect the rollout of 6G and international communication and cooperation ability. |

**Table 1** Various ethical pitfalls of TED to foster cyber ethical mindset (continued)

| *Technology* | *Ethical pitfalls* |
|---|---|
| | • Some studies have suggested that exposure to electromagnetic radiation (EMR) emitted by wireless networks may cause adverse health effects. Therefore, even though the levels of EMR emitted by 6G networks are expected to be lower than those of 5G, it is essential to address any concerns and take necessary measures to mitigate potential health risks related to the 6G networks. |

## 6 Conclusions

While many business schools across the globe are offering certificate programs in analytics, machine learning, AI, information assurance/cybersecurity, etc., almost none offer graduate and undergraduate courses in cyber ethics. Besides some top-tier universities like Princeton having centres of excellence on information technology policy (CITP), there is a lack of a well-designed curriculum in business or management schools highlighting ethics on the design, development, and application of TED. The lack of a cyber ethics curriculum in higher education motivates us to highlight the need and the value of incorporating cyber ethics in management education. In this age of rapid technology-enabled industrialisation and associated disruptions, future business leaders must be aware of the ethical pitfalls/challenges associated with the TED mentioned in Table 1. A further study on this subject matter will be to design, develop and implement a cyber ethics curriculum for business graduates and undergraduates. In that endeavor we are currently working on a multiuser perspective on the ethical pitfalls of technologies enabling disruption (TED). We are using interview methodology to collect the data and perform content analysis to discern the various themes surrounding the ethical pitfalls of TEDs. The need to have a similar curriculum for the K-12 population is also essential, given how adolescents and emerging adults are so invested and savvy in these future technologies. Therefore, it is of vital importance to critically analyse, attend and discuss cyber ethics in workshops and conferences to equip ourselves and future generations with the knowhow and capability to better navigate in a technology-enabled future.

## References

Allen, S.J. (2020) 'On the cutting edge or the chopping block? Fostering a digital mindset and tech literacy in business management education', *Journal of Management Education*, Vol. 44, No. 3, pp.362–393.

Altawy, R. and Youssef, A.M. (2016) 'Security, privacy, and safety aspects of civilian drones: a survey', *ACM Transactions on Cyber-Physical Systems*, Vol. 1, No. 2, pp.1–25.

Altmann, J. (2004) 'Military uses of nanotechnology: perspectives and concerns', *Security Dialogue*, Vol. 35, No. 1, pp.61–79.

Alvim, D. and Alturas, B. (2021) 'Impact on organisations of changes in information systems: the case of two Lisbon universities', *International Journal of Information and Operations Management Education*, Vol. 7, No. 2, pp.137–160.

Bandyopadhayay, A., Mitra, R. and Bandyopadhayay, S. (2023) 'Blockchain based real-time contact tracing – a secure way to mitigate highly infectious diseases', *The Journal of Applied Business and Economics*, Vol. 25, No. 2, pp.37–50.

Biagini, V., Subasic, M., Oudalov, A. and Kreusel, J. (2020) 'The autonomous grid: automation, intelligence and the future of power systems', *Energy Research & Social Science*, Vol. 65, p.101460, DOI: https://doi.org/10.1016/j.erss.2020.101460.

Blut, M., Wang, C., Wünderlich, N.V. and Brock, C. (2021) 'Understanding anthropomorphism in service provision: a meta-analysis of physical robots, chatbots, and other AI', *Journal of the Academy of Marketing Science*, Vol. 49, pp.632–658, DOI: https://doi.org/10.1007/s11747-020-00762-y.

Bourtoule, L., Chandrasekaran, V., Choquette-Choo, C.A., Jia, H., Travers, A., Zhang, B., … and Papernot, N. (2021) 'Machine unlearning', *2021 IEEE Symposium on Security and Privacy (SP)*, May, IEEE, pp.141–159.

Brooks, M. (2019) 'Beyond quantum supremacy: the hunt for useful quantum computers', *Nature*, Vol. 574, No. 7776, pp.19–22.

Buchanan, W. and Woodward, A. (2017) 'Will quantum computers be the end of public key encryption?', *Journal of Cyber Security Technology*, Vol. 1, No. 1, pp.1–22.

Burwell, S., Sample, M. and Racine, E. (2017) 'Ethical aspects of brain computer interfaces: a scoping review', *BMC Medical Ethics*, Vol. 18, No. 1, pp.1–11.

Chen, D. and Zhao, H. (2012) 'Data security and privacy protection issues in cloud computing', *2012 International Conference on Computer Science and Electronics Engineering*, March, IEEE, Vol. 1, pp.647–651.

Cheng, X., Zhang, X., Cohen, J. and Mou, J. (2022) 'Human vs. AI: understanding the impact of anthropomorphism on consumer response to chatbots from the perspective of trust and relationship norms', *Information Processing & Management*, Vol. 59, No. 3, p.102940.

Chowdhury, M.Z., Shahjalal, M., Ahmed, S. and Jang, Y.M. (2020) '6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions', *IEEE Open Journal of the Communications Society*, Vol. 1, pp.957–975.

Church, C. and Crawford, A. (2020) 'Minerals and the metals for the energy transition: exploring the conflict implications for mineral-rich, fragile states', *The Geopolitics of the Global Energy Transition*, pp.279–304.

Coles, D. and Frewer, L.J. (2013) 'Nanotechnology applied to European food production – a review of ethical and regulatory issues', *Trends in Food Science & Technology*, Vol. 34, No. 1, pp.32–43.

Cowan, K., Javornik, A. and Jiang, P. (2021) 'Privacy concerns when using augmented reality face filters? Explaining why and when use avoidance occurs', *Psychology & Marketing*, Vol. 38, No. 10, pp.1799–1813.

Cristofaro, M., Giardino, P.L. and Leoni, L. (2021) 'Strengths, weaknesses, opportunities, and threats of online teaching during the COVID-19 pandemic: results of a Delphi survey', *International Journal of Information and Operations Management Education*, Vol. 7, No. 2, pp.93–112.

Daly, A., Mann, M., Squires, P. and Walters, R. (2021) '3D printing, policing and crime', *Policing and society*, Vol. 31, No. 1, pp.37–51.

Dao, N.N. (2023) 'Internet of wearable things: Advancements and benefits from 6G technologies', *Future Generation Computer Systems*, Vol. 138, pp.172–184.

de Bruin, B. and Floridi, L. (2017) 'The ethics of cloud computing', *Science and Engineering Ethics*, Vol. 23, pp.21–39.

Depoorter, B. (2013) 'Intellectual property infringements & 3D printing: decentralized piracy', *Hastings LJ*, Vol. 65, p.1483.

Firth, D.R., Triche, J. and Lucus, D.J. (2021) 'A framework for teaching an undergraduate data analytics class', *International Journal of Information and Operations Management Education*, Vol. 7, No. 1, pp.27–44.

Grellhesl, M. and Punyanunt-Carter, N.M. (2012) 'Using the uses and gratifications theory to understand gratifications sought through text messaging practices of male and female undergraduate students', *Computers in Human Behavior*, Vol. 28, No. 6, pp.2175–2181.

Hammond, S.P. and Cooper, N.J. (2015) 'Embracing powerlessness in pursuit of digital resilience: managing cyber-literacy in professional talk', *Youth & Society*, Vol. 47, No. 6, pp.769–788.

Harborth, D. and Pape, S. (2021) 'Investigating privacy concerns related to mobile augmented reality apps – a vignette based online experiment', *Computers in Human Behavior*, Vol. 122, p.106833.

Kazi, A.S., Shinde, N.R., Mujumdar, S.S., Kulkarni, T.G. and Potdar, P.R. (2023) 'IoT enabled smart window for controlling brightness: a perspective of heat transfer rate', *Int. J. Industrial and Systems Engineering*, Vol. 44, No. 2, pp.220–257.

Khan, S.M. and Hamlen, K.W. (2012) 'AnonymousCloud: a data ownership privacy provider framework in cloud computing', *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, June, IEEE, pp.170–176.

Kimani, K., Oduol, V. and Langat, K. (2019) 'Cyber security challenges for IoT-based smart grid networks', *International Journal of Critical Infrastructure Protection*, Vol. 25, pp.36–49.

Klein, E., Goering, S., Gagne, J., Shea, C.V., Franklin, R., Zorowitz, S., … and Widge, A.S. (2016) 'Brain-computer interface-based control of closed-loop brain stimulation: attitudes and ethical considerations', *Brain-Computer Interfaces*, Vol. 3, No. 3, pp.140–148.

Kramarz, T., Park, S. and Johnson, C. (2021) 'Governing the dark side of renewable energy: a typology of global displacements', *Energy Research & Social Science*, Vol. 74, p.101902.

Kung, M., Yang, S.C. and Zhang, Y. (2006) 'The changing information systems (IS) curriculum: a survey of undergraduate programs in the United States', *Journal of Education for Business*, Vol. 81, No. 6, pp.291–300.

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I.A.T., Siddiqa, A. and Yaqoob, I. (2017) 'Big IoT data analytics: architecture, opportunities, and open research challenges', *IEEE Access*, Vol. 5, pp.5247–5261.

Mitchell, M.T. (1997) *Machine Learning*, McGraw-Hill.

Ntoutsi, E., Fafalios, P., Gadiraju, U., Iosifidis, V., Nejdl, W., Vidal, M.E., … and Staab, S. (2020) 'Bias in data-driven artificial intelligence systems – an introductory survey', *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, Vol. 10, No. 3, p.e1356.

O'Shea, M. and Hurriyet, H. (2018) 'Continuous innovation: interrogating the intersections and gaps between theory and practice for enhanced undergraduate learning and teaching in operations management', *International Journal of Information and Operations Management Education*, Vol. 6, Nos. 3–4, pp.272–289.

Pham, Q.C., Madhavan, R., Righetti, L., Smart, W. and Chatila, R. (2018) 'The impact of robotics and automation on working conditions and employment', *IEEE Robotics & Automation Magazine*, Vol. 25, No. 2, pp.126–128.

Puaschunder, J.M. (2019) 'Big data ethics', *Journal of Applied Research in the Digital Economy*, Vol. 1, pp.55–75.

Rauschnabel, P.A., He, J. and Ro, Y.K. (2018) 'Antecedents to the adoption of augmented reality smart glasses: a closer look at privacy risks', *Journal of Business Research*, Vol. 92, pp.374–384.

Raza, H. and Raza, M.R. (2021) 'A study of blockchain technology, bitcoin and other cryptocurrencies as means of money laundering, frauds and scams', *Global Media and Social Sciences Research Journal (GMSSRJ)*, Vol. 2, No. 1, pp.73–84.

Richterich, A. (2018) *The Big Data Agenda: Data Ethics and Critical Data Studies*, p.154, University of Westminster Press.

Roesner, F., Kohno, T. and Molnar, D. (2014) 'Security and privacy for augmented reality systems', *Communications of the ACM*, Vol. 57, No. 4, pp.88–96.

Sajid, M., Ilyas, M., Basheer, C., Tariq, M., Daud, M., Baig, N. and Shehzad, F. (2015) 'Impact of nanoparticles on human and environment: review of toxicity factors, exposures, control strategies, and future prospects', *Environmental Science and Pollution Research*, Vol. 22, pp.4122–4143.

Sasikumar, A., Vairavasundaram, S., Kotecha, K., Indragandhi, V., Ravi, L., Selvachandran, G. and Abraham, A. (2023) 'Blockchain-based trust mechanism for digital twin empowered industrial internet of things', *Future Generation Computer Systems*, Vol. 141, pp.16–27.

Sousa, M.J. and Rocha, Á. (2019) 'Skills for disruptive digital business', *Journal of Business Research*, Vol. 94, pp.257–263.

Sovacool, B.K., Heffron, R.J., McCauley, D. and Goldthau, A. (2016) 'Energy decisions reframed as justice and ethical concerns', *Nature Energy*, Vol. 1, No. 5, pp.1–6.

Srinivasan, R. and Chander, A. (2021) 'Biases in AI systems', *Communications of the ACM*, Vol. 64, No. 8, pp.44–49.

Stahl, B.C. (2006) 'On the difference or equality of information, misinformation, and disinformation: a critical research perspective', *Informing Science*, Vol. 9, p.83.

Steinert, S. and Friedrich, O. (2020) 'Wired emotions: ethical issues of affective brain-computer interfaces', *Science and Engineering Ethics*, Vol. 26, pp.351–367.

Unsworth, R. (2019) 'Smart contract this! An assessment of the contractual landscape and the Herculean challenges it currently presents for 'self-executing' contracts', *Legal Tech, Smart Contracts and Blockchain*, pp.17–61.

Van Deursen, A.J., Bolle, C.L., Hegner, S.M. and Kommers, P.A. (2015) 'Modeling habitual and addictive smartphone behavior: the role of smartphone usage types, emotional intelligence, social stress, self-regulation, age, and gender', *Computers in Human Behavior*, Vol. 45, No. 4, pp.411–420.

Weill, P., Woerner, S.L. and Shah, A.M. (2021) 'Does your C-Suite have enough digital smarts?', *MIT Sloan Management Review*.

West, J.P. and Bowman, J.S. (2016) 'The domestic use of drones: an ethical analysis of surveillance issues', *Public Administration Review*, Vol. 76, No. 4, pp.649–659.

Wu, H.C. and Chen, T.C.T. (2018) 'Quality control issues in 3D-printing manufacturing: a review', *Rapid Prototyping Journal*, Vol. 24, No. 3, pp.607–614.

Xu, X., Lu, Y., Vogel-Heuser, B. and Wang, L. (2021) 'Industry 4.0 and Industry 5.0 – inception, conception and perception', *Journal of Manufacturing Systems*, Vol. 61, pp.530–535.

Zhang, R., Xue, R. and Liu, L. (2019) 'Security and privacy on blockchain', *ACM Computing Surveys (CSUR)*, Vol. 52, No. 3, pp.1–34.