Article │ Received 3 December 2024; Accepted 13 May 2025; Published 30 May 2025
https://doi.org/10.55092/let20250003

Risk-based ethics—myth or reality?

Bruno Zeller[1] and Mirella Atherton[2,*]

[1] Sir Zelman Cowen Centre, Victoria University, Melbourne, Australia
[2] School of Law and Justice, University of Newcastle, Newcastle, Australia

* Correspondence author; E-mail: Mirella.Atherton@newcastle.edu.au.

Highlights:

- Digital technology is proposing new solutions but it is also creating some problems.
- This paper analyses current laws by looking back at past legal theories about ethics.
- We argue that modern regulation needs to be guided by a risk-based approach.

Abstract: It is abundantly clear that the digital revolution involves changes in every corner of our lives. It is affecting the economy by increasing efficiency and hence profitability, but these new developments have also affected everyday transactions of the traditional middle class. The changes have given rise to global and multinational shifts which increasingly affect sectors of our domestic economic structure. The technology giants control the digital systems and hence control our personal information, that is the way we live and interact in a social setting. This has changed the very fabric of society. It is important to recognise these changes as the inevitable fact is that the digital revolution is here to stay and indeed it has not run its course yet. New institutional frameworks have emerged and these are untested. We are experiencing changes to our existing social reality but without all the necessary understandings of our new reality. This paper will ask how and importantly whether a risk based ethical construct can protect our personal security and our privacy.

Keywords: digital revolution, ethics, data, security, privacy

1. Introduction

The world is experiencing a new form of complexity driven by the digital ecosystem which combined with increased global conflict has put a sharp focus on the construction of society itself. This paper will argue that the way we interact with each other has fundamentally changed. The driver of these changes is the increasing use and development of digital systems. The issue is that to function in a society, that is, to fulfil all the necessary tasks in our daily life we use the Internet of Things (IoT). An asymmetrical power imbalance exists in relation to the use and control of the IoT and the question is now, "who has the power to raise issues, define problems, or propose and create the solutions to the problems created [1]" by the IoT? This paper will analyse the effect of the IoT on society.

A key problem society is facing is that the digital age has brought about fundamental changes affecting the social fabric that holds us together. Some changes no doubt have brought benefits but others such as surveillance have not. The issue is that risks have emerged and need to be highlighted. Solutions need to be found to eliminate the risks. The tools to do this need to be ethically driven by people to be sustainable. For the purpose of this paper, we define a model of risk-based ethics while considering the EU GDPR and the EU AI Act which are at this time important and pioneering legislation pieces.

Digital technology continues to propose new solutions but it is clear that it is exacerbating some problems and these are being laid bare [2]. Texting and short communications have gained prominence and these are replacing face to face conversations. The direct human connection that we once knew is vanishing. Devices are now babysitters, teachers and surveillance apparatus. How then does a democratic society adapt to these changes? Saul noted that the difficulty in adapting to change is not to be found in internationalism or international commerce, "It is in Globalisation's construct of how the two come about [3]." Already in 1835 Tocqueville asked "can it be believed that the democracy which has overthrown the feudal system and vanquished kings will retreat before tradesmen and capitalists [4]." The rising power today may be "private sector technocrats, money market specialists, the dominant school of economics and, of course, those public commentators [and influencers] who fit the role of adoring courtiers [3]."

Originally the internet was meant to be a "free, open and global" and good for all but it lacked security and privacy [5]. Not surprisingly Zuboff termed the current state of Big Data in the phrase "Surveillance Capitalism". Her observations include that there is a form of concealed control within networks and platforms which out of sight [6]. It is obvious that there is no going back to a time when we knew our neighbours in our community and we had time to think before we made a decision. One of the issues is that not only the technology climate but the political climate and economic climate are changing rapidly. It is not surprising that data security, data privacy and data ethics are becoming urgent principles to manage.

For the purpose of this paper and to analyse the current laws it is important to look to past legal theories about ethics. Rawls defined ethics in the following way:

"The two main concepts of ethics are those of the right and the good; the concept of a morally worthy person is, I believe, derived from them. The structure of an ethical theory is, then, largely determined by how it defines and connects these two basic notions [7]."

This paper acknowledges and argues that society cannot exist without the assistance of and certainty of the digital ecosystem. This is especially so as digital systems know no borders and can advance risks to society at large. The digital influence on our lives now affects positive and negative perceptions of morally worthy pursuits and hence an ethical grounding is important to the minimise and avoid risks. The balance between maintaining security and maintaining privacy is of particular interest to this article. It is useful to at least attempt to address the "political realities of surveillance [8]", that is, distinguishing between safety and control of a nation. It must be kept in mind that two risk-based models of data regulations can exist. "One concerned with better compliance [of data protection regulations] and one concerned with the determination of which Artificial Intelligence (AI) systems should be regulated [9]." Data protection and security is only regulating one side of the coin, the other side of the coin is the system maintaining privacy and minimising data collection.

With the increasing capability and capacity of AI, framing of legislation to include ethical standards is especially important to protect human rights which in turn protects society at large. Not surprisingly, ethical considerations have taken on a new meaning in the digital age. Hasselbalch recognised that two sociotechnical infrastructures are at work, namely the Big Data and the AI sociotechnical infrastructure. He described a digital "data double" that could potentially be used for purposes of scrutiny and control, sold for profit and targeted by direct acts of digital violence and abuse [1].

Sociotechnical infrastructure, [10] unites people and technology for a common purpose and is a driving factor in our current reality. Instilling a level of personal security and privacy is guided by the practice of cybersecurity [11]. However, the control of cybersecurity and the guiding principles in the exercise of cybersecurity need to be considered. To that end ethical solutions when developing balanced cybersecurity systems have been advocated for [12]. The IoT is such a diverse "beast" that "ethical conduct is pretty much in the eye of the beholder [13]" which is not a reliable or positive situation. Interestingly, Posner in 1993 argued that only practical reasoning can yield ethical certainty, but logic and science cannot do the same [14]. If that is true then perhaps the IoT being based on logic and science is not capable of solving ethical problems?

Existing technological structures can be insufficiently flexible in recognising ethical issues [15]. Simply put new institutional frameworks need to be developed consisting "of standards and laws that directly addressed the ethical and social implications [1]." Many institutions are obliged to address ethical problems in order to survive the ever-inversing competitiveness of a digitally driven economy [16]. For the purpose of this discussion ethics in the broadest sense attempts to answer the question: what is a good life, in other words, what is right or wrong? Ethics is a moral principle and "is often formulated in formal codes or standards to which all members of a profession are held, such as those of medical or legal ethics [17]." Hasselbalch referring to Stoddart suggested that one of the approaches to an ethics process is a "'rights-based' approach, with reference to a body of human rights work that demands the accountability of those with the power to watch [1]." She continued saying that "the foundation of data ethical governance is an awareness of the very conditions of power between different stakeholders [1]."

Technology is increasingly shaping the way humans work and live and seek a good life. A poorly designed system will not advance the welfare of people if it is based on an alternative outcome that the designers want to achieve, be it data mining or the surveillance of the population. These types of systems undermine personal security and privacy of the population [6]. Collection, utilisation and trading of data traverses jurisdictions as well as the legal and ethical frameworks that may exist [18]. The simple fact is that the designers and owners of a system need to recover costs and make a profit. One of the vehicles to make a profit is the harvesting and selling of data generated by everyday people. Herein lies the challenge and where ethics becomes important. There is an ethical obligation to keep personal data safe.

The institutions with the power to preserve personal security and privacy include the law. The law used to keep pace with developments in technology, but the IoT has outpaced the ability of laws to order everyday life in an ethical way. It is difficult to predict the social impact of the IoT and increasingly laws are often outdated and inadequate to guide society and preserve our personal security and privacy. "Another factor driving the recent explosion of interest in ethics is the way in which 21st century technologies are reshaping the global distribution of power, justice, and responsibility [17]." A further point is that vulnerable members of a society need to be protected and this is an issue of justice. "Social

order is not to establish and secure the more attractive prospects of those better off unless doing so is to the advantage of those less fortunate [19].”

Part II of this article will examine whether the European Data Protection Legislation (EU GDPR) [20] and regulation of Artificial Intelligence (AI), vis the EU AI Act are risk based and whether the EU AI Act is inconsistent with the EU GDPR. Part III will examine ethical issues linked to cybersecurity and specifically whether policing can protect data generated by the IoT. Part IV will discuss the ethical challenges in cybersecurity. This will be followed in Part V with a discussion of ethical challenges in personal security and privacy. The conclusions are presented in Part VI.

2. EU GDPR and EU AI Act

The EU GDPR is arguably the model on which all other data protection legislations are based and features a risk-based approach [9]. The European Commission subsequently unveiled a new proposal, the Artificial Intelligence Act (AIA) [21]. The AIA or EU AI Act ‘distinguishes between prohibited AI systems, high-risk AI systems, and AI system that interact with natural persons (for which a number of transparency requirements apply [9]).’ The proposal specifically targets AI systems which are deemed to be of a high risk character and question whether AI is beneficial to society. The proposal defines high risk as ‘those concrete situations where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future [20].’ With these developments in mind, Gellert argues that:

“Even though both the GDPR and the proposed AIA rely upon the same moniker, the latter refers to different regulatory models. In the first case, the point is to use risk and risk management tools as a means to better comply. In the second, the point is to determine which AI systems should be regulated [9].”

Gellert came to the conclusion that the AIA and the GPDR appear to use the same risk management system. The key issue therefore in the regulatory intervention is the dependence on decisions by a government or semi government department as to what constitutes a risk. The inherent problem is that depending on the government of a country, a risk and how it can be managed is determined. As AI is a global issue global solutions theoretically ought to be devised and this is arguably difficult if not impossible [21].

At face value this could be detrimental depending what tools are employed to give effect to legislations. “The precautionary principle is at the heart of many instruments of the new legislative framework”, [22] and “extremely important in harnessing the way AI technology is being deployed” into the European Union for example. This principle is universal as it not only applies in common law countries but also in civil law countries. Arguably it could be termed a transnational model which can be applied in cases where unknown events need to be taken into consideration. In addition as we are living in the age of the “risk society [23]”, careful consideration of this principle [24], is important. It is not by accident that the precautionary principle has been discussed in recent years as there is a greater awareness of the limitations and threats of scientific knowledge [25]. This is especially relevant in the application of the IoT and in relation to data protection and importantly answering the question of whether humans control AI or will AI control humans.

The approach in the EU is “to promote Europe’s innovation capacity in the area of AI while supporting the development and uptake of ethical and trustworthy AI across the EU economy. AI should work for people and be a force for good in society”. The main argument for the inclusion of the precautionary principle in decision making is that it encourages enterprises to look at the past mistakes which “helps [to] address the evolving, complex and systemic challenges currently facing it by

facilitating people-centric progress [25].” However of importance is that risk and hence the principle will only be effective if it is applied in an ethical way that is with the interest of profiting all and not only business and commerce.

3. Ethical issues in the practice of cybersecurity

There is no global culture of cybersecurity even among allies. “Between the United States and Europe, walls are going up that are making it more challenging for both the public and private sectors alike to pool their resources and expertise to better confront common challenges [26].” The same can be said about data protection laws. The UK GDPR and Data Protection Act have a focus implementing checks on profiling and automated decision-making systems “to protect vulnerable groups”. India has the Digital Personal Data Protection Act [27], and China has the Personal Information Protection Law. In the US privacy regulation hinges on “political debates and encompass innovation, education, society, corporations, and democracy [28]”. The EU has the strongest digital privacy, security and AI law in the world. The EU GDPR deals with the control and processing of personal data in relation to privacy rights. The EU Artificial Intelligence Act recognises certain types of high-risk AI and together these examples provide bright-line rules. The US and the EU have different approaches and a sound knowledge of the conflict of laws is necessary in order to select a governing law which is best suited to the trading climate of a company.

The practice of cybersecurity is meant to ensure that digital information is kept safe within the relevant computer systems and the attached networks but it is commonly left to the identification of breaches to mitigate risks. What “Cyber security practices essentially protect is the integrity, functionality, and reliability of organizations that rely upon such data and systems [29].” One of the methods to better prepare institutions in developing cybersecurity is horizon scanning. Horizon scanning “attempts to systematically imagine the future in order to better plan a response [30]” and to “evaluate the importance of ‘things to come [31].’’ It is “the systematic outlook to detect early signs of potentially important developments [32].” However increasingly more scandals are discovered around security and surveillance techniques and hence this directly affects personal security and privacy [33].

Surveillance carried out without an ethical framework will always be problematic. Kant’s theories of ethics are among the most significant in history, the Kantian notion of moral responsibility was connected with duty and obligation, “There is nothing it is possible to think of anywhere in the world, or indeed anything at all outside it, that can be held to be good without limitation, excepting only a good will [34].” In the modern world ethical issues are closely linked to personal security and privacy and three important ethical issues linked to cybersecurity are as follows: “harm to privacy, cybersecurity resource allocation and transparency and disclosure [29].” This paper will concentrate on commercial cybersecurity “where issues such as just war theory, state sovereignty and national security are not central [35].”

In addressing concerns, one of the goals of new legislation is protection of sensitive data from theft or misuse. Data is a raw material with a commercial value and hence it is attractive to many types of data harvesters. Even when people disconnect from the IoT they cannot prevent their data from being exposed, this lack of personal security and privacy is simply unethical. However it must also be remembered that companies are subject to government oversight as far as the IoT is concerned. As an example, the Australian government law enforcement and intelligence agencies are “legally allowed to

demand technology manufacturers and providers to make encrypted communications accessible, by forcing developers to create 'back doors'—access points in their products which make it possible for the government agencies to access encrypted messages [33]."

Cybersecurity practices guided by ethical considerations come at a cost to any business. "The cost is great because cybersecurity efforts take up a considerable number of individuals as well as organizational resources like time, money, and expertise [29]." Ethics does not mean good behaviour but conduct in compliance with accepted values and expectations. Ethical compliance can help determine which potential uses of technology are inappropriate, harmful and/or intrusive. Ethical decision-making practices can help to navigate challenging dilemmas and complex value trade-offs, and ultimately decide whether to prioritise transparency or privacy where providing more of one may mean less of the other [36]. It is obvious that not having adequate cyber security in place can be costly. In addition an over complicated system also has cost implications as users will have issues with an overly complicated security system.

Not all risks can be eliminated and hence data breaches can always occur. There is an ethical duty as well as a legal duty to disclose information about a breach to users when a breach has occurred or if a critical vulnerability in the system occurs. It allows customers to make informed decisions and to minimise any perceived risks. Simply put "Cybersecurity professionals and organizations should adopt procedures for rigorously evaluating the compliance of their members with the applicable ethical cyber security obligations [29]." In a changing sociotechnical environment compromises need to be made and "spaces of negotiation" need to be created [1]. Cybersecurity is no different to any other structure or framework and hence is also subject to sound practices. One of the issues in defining and indeed applying cybersecurity ethics is the need to understand the underlying framework. What is required is an ethical control or "set of processes, procedures, cultures and values designed to ensure the highest standard of behaviour [37]."

Formosa *et al* argue that it is "apparent that many frameworks succumb to the problem of principle proliferation, whereby new principles are added in an effort to capture the diversity of moral concerns relevant to a particular domain [35]." They put forth a model which is useful as it includes five specific principles of cybersecurity:

"**Beneficence:** Cybersecurity technologies should be used to benefit humans, promote human well-being, and make our lives better overall. **Non-maleficence:** Cybersecurity technologies should not be used to intentionally harm humans or to make our lives worse overall. **Autonomy:** Cybersecurity technologies should be used in ways that respect human autonomy. Humans should be able to make informed decisions for themselves about how that technology is used in their lives. **Justice:** Cybersecurity technologies should be used to promote fairness, equality, and impartiality. It should not be used to unfairly discriminate, undermine solidarity, or prevent equal access. **Explicability:** Cybersecurity technologies should be used in ways that are intelligible, transparent, and comprehensible, and it should also be clear who is accountable and re- sponsible for its use [35]."

It needs to be remembered that the written word "provides the means of objectifying new experiences allowing their incorporation into the already existing stock of knowledge [38]."

3.1. Security

The IoT "swallows" up a lot of private sensitive data which needs to be protected from unauthorised access. The fact is that only "When we know that our systems and data are secured and accessible, we can interact with, store, and generate data with the confidence that it will be protected [39]." This principal mandates that every system should or even must be in a state to be secure from unauthorised access. The European Commission defines this form of security as "… the safeguards and actions that can be used to protect the cyber domain … Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure, and the confidentiality of the information contained therein [35]."

3.2. Harm to privacy

In Article 12 of the Universal Declaration of Human Rights (UDHR) privacy is a fundamental right [40]. Poor cybersecurity can lead to breaches of security and privacy causing harm to victims. One of the real problems as noted by Vallor is that the "risks of privacy harm created by poor or unethical cybersecurity practices are amplified further by the continued growth of a chaotic global data ecosystem" and that most individuals have "little to no ability to personally curate, delete, correct, or control the storage or release of their private information [41]."

At present there is no international data protection convention and it is fanciful to contemplate that an international data convention could be drafted within the next decade. By that time advancements in technology would have already made a convention redundant. The fact is that even living off the digital grid "cannot prevent sensitive data about [people] from being generated and shared by their friends, family, employers, clients, and service providers [17]." In effect, protecting private information is not only a duty related to cybersecurity but can also be termed a duty related to human rights [17]. A balance needs to be met between protecting sensitive data and basic human rights. Arguably other methods may be less time efficient [42]. "Utilitarianism allows for the possibility of situational ethics, meaning that in some circumstances, one might need to violate a society's or a personal moral code if the outcome is better for a greater number of people [43]."

3.3. Harm to property

Harm to privacy can also cause harm to property via extortion. The threat of publishing stolen sensitive data on the dark web often results in the paying of ransom. The theft of intellectual property, bank account numbers can also cause damage to corporate or individual property. Even though property has only a material value, extortion is nevertheless an unethical act [42]. It follows therefore that the harm to property is often the result of the harm to privacy and hence "professionals tasked with cybersecurity have a default ethical obligation to protect their organization's networks, or those of their clients, from any and all property-targeting intrusions and attacks [17]." Sufficient resource allocation to the secure maintenance of any system is an ethical issue and cannot be compromised.

3.4. Transparency and disclosure

Besides the ethical duty to keep data secure, there is also an ethical duty to provide transparency in disclosing data breaches and allowing those affected by data breaches to make decisions and choices.

Informed decisions like "informed consent does not ever decrease risk to users; it only alleviates researchers from some responsibility for that risk and may even increase risk to users by removing any traces of plausible deniability [17]." In 2022 Medibank revealed a cyber-attack that hacked customer data of approximately 4 million people in Australia, this had devastating effects on vulnerable consumers who were suffering multiple disadvantages.

The point is that a duty to disclose in a timely fashion helps to manage risk. Each situation may require different decisions because the collection and storage of data has become essential to the functioning of markets [44]. In the meantime individuals are becoming more aware of data security breaches [45]. Latitude Financial was subject to a cyber-attack in 2023 that resulted in the theft of personal information of around 14 million people in Australia and New Zealand. Aside from the lack of legislation, there are significant concerns and emerging challenges where individuals know less and less about their personal information and how it is collected, stored, and used. Both transparency and disclosure requires well-reasoned ethical judgements to minimise risks and procedures on what to do. The next part will discuss the ethical challenges for the future.

4. Ethical challenges for the future

It must be stressed that even if an ethical practice is legal, a legal practice may not be ethical in some views. It is therefore important that evaluation of risks cannot only be made to be legally compliant but must also be ethically compliant as it will affect not only harm to individuals but can also generate reputational damage to a company. Macnish and van der Ham [46], used an interesting case study to highlight the issues and problems which can and should be avoided using a sound level of ethical control. In brief, a private security research group MedSec, purchased and attempted to hack St. Jude pacemakers and heart monitors designed for home use. MedSec claimed that they discovered vulnerability in the devices. Instead of advising St. Jude they teamed up with an investment firm to short the shares of St. Jude. MedSec then made some of the information public with the result that there was a drop in St. Jude's shares.

The subsequent research by independent companies was mixed with some supporting that the items were not vulnerable whereas others found the opposite to be true. MedSec's motivations were brought into question by their decision to profit from shorting the stock instead of making their findings available to St. Jude. The main issue was that there was a slow response. As Spring noted, "We've all seen how consumer products are often designed and built in insecure ways, and let's face it, there has been virtually no improvement unless there's a major financial or reputational impact in doing so [15]." In the business sector there appears to be no oversight or reporting nor any policy governing behaviour because of the conflict between consent, transparency, disclosure and making money.

It should also be noted that security can influence privacy, and that privacy can influence security. The question is where is the boundary between protecting individual privacy and security of many? The social dimension or social values determine the boundaries between security and privacy. One of the problems is that devices are subject to diverse users and owners who challenge the balance because they have different interests. The owners of the devices including technology giants are driven by profits whereas the users are looking for security of the data they entrust to the owners.

An action plan can be devised reflecting what can be done rather that what is most likely to be done [47]. Resources are scarce and we need to question have "we adequately considered the risks of

'collateral damage' to innocent parties, or reputational damage to ourselves and our organization, if our response steps over the ethical line [17]?"

To start with it is useful to be reminded what ethics means, "moral principles; maxims, precepts or observations concerning these [17]." Ethics includes cooperation, productivity and respect to others. Ethical challenges can emerge at many points in the chain of usage of a system such as what is the vulnerability to a breach and how is the system protecting privacy but also monitoring possible misuses of the system. The issue is how are competing issues resolved between all stakeholders. Important factor include how is data stored and encrypted as well as how long should sensitive data be stored and how is the full life cycle of data determined.

Security of users could be guaranteed, and harm avoided by obliging users to verify their identity such as a passport or driver's licence. However, such steps may be problematic as it could result in breach of privacy. It is obvious that any ethical policy must find the middle ground that is how to minimise any adverse effects by looking at all of the factors. Arguably the problem in any ethical definition or policy is where is the acceptable middle ground and how is the risk distributed between the user and operator of the system. Not surprisingly Manish and van der Ham argue that the current methods of ethical oversight are inadequate as they "fail in two areas" namely university-based developments and the broader community of practising cybersecurity experts [48]. They go on to argue that "there needs to be a greater appreciation of the risks of cybersecurity development in ethical review committees and clear codes of conduct for the professional community which cover both development and practice [15]."

An ethical framework on which cybersecurity can rely on, that is also academically sound is lacking. Perhaps theory and practice can learn sufficiently from each other to arrive at a sound ethical cybersecurity model? The issue at hand is whether there is enough flexibility in drawing the line between privacy and security to reach an ethically sound solution. Arguably currently there are no widely used governance structures in place. Perhaps ethical governance protocols in the academic sector can be adapted to also be a useful policy in the private sector?

5. Discussion

As noted, the Big Data and AI sociotechnical infrastructures are embedded in society with the obligation to act ethically within relevant risk factors. The point this paper is making is that there are several interlocking systems at play, each one requiring an ethical approach. At the top are the technology inventions and manufacturing systems ranging from simple consumer items to hidden complicated multifaced systems. At the bottom we have the users of the system who may be consumers or businesses. It is the consumer or end user which expects that the innovation produces an ethically evaluated product. Each level in the chain generates its own risk which needs to be minimised considering "cross risk evaluations" at play. By using digital assets the consumer must understand that there is a risk in relation to preserving security or privacy.

In current times "judicial risk assessment systems" look for patterns in the background of the defendants and then inform the judge about who is most likely to commit a crime in the future [15]. Human involvement has found its way into legislation and the EU GDPR, Article 22 [1], prohibits decisions which are only made by AI if it significantly affects an individual. The question is how is 'significantly' interpreted considering that judges tend to look at past decisions. The point to make is that a risk factor has been determined by AI and it is now left to human ethical considerations. The

difficulty is that we assume that human capacity such as education and ethnic-cultural variations play only a minimal part in a balanced human decision that is made. We propose that it is much more than that. It is not surprising that theories and methodologies are being developed to train models to act ethically.

In the EU a resolution was accepted in 2017 with recommendations for Civil Law Rules on Robotics where the question of legal liability for harmful actions was raised [49]. What can be said is that there is at least a debate about the distribution of morals between robots and humans. As Pasquale noted, we need a general framework for defending human experience in the age of AI [1]. The danger obviously is that ethics or decisions emanating from robots can influence societal transformation. O'Neil discovered a Big Data system used by the US educational and public employment system where teachers were fired on rigid machine-based performance assessment without considering the social context and human factors [50]. The economic reality means that a balance is require that "has politics, it has cultures [and] meaning that is not neutral or natural [51]."

6. Conclusion

This paper has demonstrated that ethics in our digital age need special attention. Globalisation, internationalisation and a borderless economy has meant that ethical considerations are not uniform even among the most highly educated people or the most highly developed nations. It is in effect impossible to reach a global consensus on how digital systems need to be controlled, let alone ethically controlled. Today the EU GDPR stands out as a benchmark for data security and privacy protection and the EU AI Act has recognised that "the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences [1]." The conclusion therefore is that any regulation in the modern era needs to be guided by humans and based on a risk-based approach [21]. Ethical behaviour and ethical principles that guide human conduct can be copied and implemented by innovative technology but this does not mean that technology can make decisions that will be correct every time.

Acknowledgments

The authors are firstly grateful for the helpful comments from the anonymous reviewers and for advice and guidance from our colleagues at our respective universities.

Authors' contribution

Conceptualization, Prof Bruno Zeller; writing—original draft preparation, Prof Bruno Zeller; writing—review and editing, Dr Mirella Atherton. All authors have read and agreed to the published version of the manuscript.

Conflicts of interests

The authors declare no conflict of interest.

References

[1] Hasselbalch G. *Data ethics of power*, 1st ed. Cheltenham: Edward Elgar Publishing, 2021. pp. 15,31,33,36,39,46,73,78,90.

[2] Meng R. Who rules the world. Available: https://www.frankfurter-hefte.de/aktuelle-ausgabe/ (accessed on 25 October 2024).

[3] Saul JR. *The Collapse of globalism and the reinvention of the world*, 1st ed. Toronto: Viking Canada, 2005. p. 35.

[4] De Tocqueville A. *Democracy in America*, 1st ed. New York: Vintage Books, 1945. p. 6.

[5] Timmers P. Ethics of AI and cybersecurity when sovereignty is at stake. *Mines Mach.* 2019, 29(4):635–645.

[6] Zuboff S. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, 1st ed. New York: PublicAffairs, 2019. pp. 127,203–213.

[7] Rawls J. *A theory of justice*, Rev. ed. Cambridge: Harvard University Press, 1999. p. 21.

[8] Bauman Z, Lyon D. *Liquid surveillance: a conversation*, 1st ed. Cambridge: Polity Press, 2013. p. 20.

[9] Gellert R. The role of the risk-based approach in the General Data Protection Regulation and in the European Commission's proposed Artificial Intelligence Act: business as usual? *J. Ethics Legal Technol.* 2021, 3(2):15,16,27.

[10] Le Coze JC, Antonsen S. *Safety in the digital age: sociotechnical perspectives on algorithms and machine learning*, 1st ed. Cham: Springer Nature Switzerland, 2023. p. 137.

[11] Florackis C, Louca C, Michaely R, Weber M, Goldstein I. Cybersecurity risk. *Rev. Financ. Stud.* 2023, 36(1):351–407.

[12] Priyadarshini I, Cotton C. *Cybersecurity: ethics, legal, risks, and policies*, 1st ed. Palm Bay: Apple Academic Press, 2022.

[13] Shoemaker D, Kohnke A, Laidlaw G. Ethics and cybersecurity are not mutually exclusive. *EDPACS* 2019, 60(1):1–10.

[14] Posner R. *The problem of jurisprudence*, 1st ed. Cambridge: Harvard University Press, 1993. p. 76.

[15] Macnish K, Van der Ham J. Ethics in cybersecurity research and practice. *Technol. Soc.* 2020, 63:101382,101387.

[16] Australian Government. Financial sector (collection of data) (reporting standard) determination No. 5 of 2024. 2024. Available: https://www.legislation.gov.au/F2024L00434/asmade/text (accessed on 17 October 2024).

[17] Vallor S. An introduction to cybersecurity ethics. 2018, pp. 2,3,8–10,15–16. Available: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf (accessed on 25 October 2024).

[18] Andrew J, Baker M. The general data protection regulation in the age of surveillance capitalism. *J. Bus. Ethics* 168,3:565–578.

[19] Williams AD. The revisionist difference principle. *Can. J. Philos.* 1995, 25(2):257–281.

[20] European Union. 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 Data Protection Regulation) (Text with EEA relevance). Available: https://eur-lex.europa.eu/search.html?scope=EURLEX&text=GDPR&lang=en&type=quick&qid=1748482409106 (accessed on 25 October 2024).

[21] European Commission. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Act. 2021, pp. 1–26. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (accessed on 2 October 2024).

[22] Federal Reserve Bank of San Francisco. What is the economic function of a bank? 2001. Available: https://www.frbsf.org/education/publications/doctor-econ/2001/july/bank-economic-function (accessed on 20 October 2024).

[23] Hess A. *Ulrich Beck: pioneer in cosmopolitan sociology and risk society*, 1st ed. Cham: Springer International Publishing, 2014. pp. 1–193.

[24] Bernard R. *Precautionary principle, pluralism and deliberation: science and ethics*, 1st ed. London: ISTE Ltd & Hoboken: John Wiley & Sons, 2016. pp. 1–298.

[25] Bourguignon D. The precautionary principle: definitions, applications and governance. 2015, pp. 1–12. Available: https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/573876/EPRS_IDA%282015%29573876_EN.pdf (accessed on 28 October 2024).

[26] Shackelford SJ. Seeking a safe harbour in a widening sea: unpacking the schrems saga and what it means for the transatlantic relations and global cybersecurity. *Wm. & Mary Bill Rts. J.* 2021, 30:320.

[27] PwC India. A comparison of cybersecurity regulations: India. 2022. https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html (accessed on 5 November 2024).

[28] Abilock R, Abilock D. I agree, but do I know? Privacy and student data. *Knowl. Quest* 2016, 44(4):10–21.

[29] Swiss Cyber Institute. A holistic approach to ethical issues in cyber security. 2021. Available: https://swisscyberinstitute.com/blog/a-holistic-approach-to-ethical-issues-in-cyber-security (accessed on 22 October 2024).

[30] Delaney K. A practical guide: introduction to horizon scanning in the public sector. 2014. pp. 1–62. Available: https://www.researchgate.net/publication/264534064_INNOVATION_TOOL_KIT_-_Horizon_Scanning (accessed on 6 November 2024).

[31] Cuhls K. Horizon scanning in foresight–why horizon scanning is only a part of the game. *Futures Foresight Sci.* 2020, 2(1):2.

[32] Publications Office of the EU. Models of horizon scanning: how to integrate horizon scanning into european research and innovation policies. 2016. Available: https://op.europa.eu/en/publication-detail/-/publication/88ea0daa-0c3c-11e6-ba9a-01aa75ed71a1 (accessed on 25 October 2024).

[33] Pawlicka A, Choraś M, Kozik R, Pawlicki M. First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions. *Pers. Ubiquitous Comput.* 2023:1–10,173–202.

[34] Kant I. *Groundwork for the metaphysics of morals: with an updated translation, introduction, and notes*, Reprint ed. New Haven: Yale University Press, 2018. p. 393.

[35] Formosa P, Wilson M, Richards D. A principlist framework for cybersecurity ethics. *Comput. Secur.* 2021, 109:102382,102385–102387.

[36] Sheth R. Steering the right course for AI. 2018. Available: https://cloud.google.com/blog/products/ai-machine-learning/steering-the-right-course-for-ai (accessed on 10 October 2024).

[37] Winfield AFT, Jirotka M. Ethical governance is essential to building trust in robotics and artificial intelligence systems. *Philos. Trans. R. Soc. A* 2018, 376(2133):20180085.

[38] Pawlicka A, Pawlicki M, Kozik R, Choraś RS. A systematic review of recommender systems and their applications in cybersecurity. *Sensors* 2021, 21(15):5248.

[39] Berger P, Luckmann T. *The social construction of reality*, 1st ed. Garden City: Doubleday & Company, 1966. p. 86.

[40] European Data Protection Supervisor. 2013 Annual report––a single set of rules for all: EU data p rotection reform can support businesses and protect citizens. 2013. Available: https://www.edps.eu ropa.eu/data-protection/our-work/publications/annual-reports/2013-single-set-rules-all-eu-data-pr otection_en (accessed on 17 October 2024).

[41] United Nations. Universal declaration of human rights. 1948. pp. 1–8. Available: https://www.un.org/e n/about-us/universal-declaration-of-human-rights (accessed on 21 December 2024).

[42] Rajamäki J, Hämäläinen H. Ethics of cybersecurity and biomedical ethics: case shapes. *Inf. Secur.: Int. J.* 2021, 50(1):106–107.

[43] Christen M, Loi M. Ethical frameworks for cybersecurity. In *The Ethics of Cybersecurity*, 1st ed. Cham: Springer Nature, 2020. pp. 73–93.

[44] Narayanan A, Zevenbergen B. No encore for encore? Ethical questions for web-based censorship measurement. 2015, pp. 1–23. Available: https://bdes.datasociety.net/council-output/case-study-no-encore-for-encore (accessed on 25 October 2024).

[45] Wagner DN. Economic patterns in a world with artificial intelligence. *Evol. Inst. Econ. Rev*. 2020, 17(1):111.

[46] Boyd T. CEOs pour money into cybersecurity protection. 2023. Available: https://www.afr.com/tech nology/ceos-pouring-money-into-cybersecurity-protection-20230103-p5ca3w (accessed on 11 April 2024).

[47] Spring T. Researchers: MedSec, muddy waters set bad precedent with St. Jude medical short. 2016. https://threatpost.com/researchers-medsec-muddy-waters-set-bad-precedent-with-st-jude-medical-short/120266/ (accessed on 20 December 2024).

[48] Oxford English Dictionary. Available: https://www.oed.com/search/dictionary/?scope=Entries&q=ethics (accessed on 18 October 2024).

[49] European Data Protection Supervisor. 2016. Available: https://www.edps.europa.eu/general-data-protection-regulation_en (accessed on 12 March 2025).

[50] Pasquale F. *New laws of robotics: defending human expertise in the age of AI*, 1st ed. Cambridge: Harvard University Press, 2020. p. 330.

[51] Bridgewater R, O'Neil C. *Weapons of math destruction, how big data increases inequality and threatens democracy*, 1st ed. New York: Penguin Random House, 2016. p. 5.