



Universiteit
Leiden
The Netherlands

From compliance to security, responsibility beyond law

Boeken, J.

Citation

Boeken, J. (2024). From compliance to security, responsibility beyond law. *Computer Law & Security Review*, 52. doi:10.1016/j.clsr.2023.105926

Version: Publisher's Version

License: [Creative Commons CC BY-NC 4.0 license](https://creativecommons.org/licenses/by-nc/4.0/)

Downloaded from: <https://hdl.handle.net/1887/4210348>

Note: To cite this publication please use the final published version (if applicable).



Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

From compliance to security, responsibility beyond law

Jasmijn Boeken^{a,b,*}^a Institute of Security and Global Affairs (ISGA), Leiden University, Turfmarkt 99, The Hague 2511 DP, the Netherlands^b Centre of Expertise Cyber Security, The Hague University of Applied Sciences, Johanna Westerdijkplein 75, The Hague 2521 EN, the Netherlands

ARTICLE INFO

Keywords:

Cybersecurity
Stakeholder theory
Pacing problem
Cybersecurity standards
Legislation
Care ethics

ABSTRACT

In this opinion piece, I advocate for the adoption of a care-based stakeholder approach in cybersecurity for companies. With the ever-increasing digitization of all aspects of life, companies are struggling to keep themselves and their customers secure. This is, at least in part, due to their focus on compliance to standards and regulations, they fall victim to a checkbox-mentality where compliance instead of security is seen as the goal. This strong focus on compliance creates security blind-spots and the negative impact it has on security is strengthened by the “pacing problem” – where technology evolves faster than the law. Thus, leaving a gap where there is a lack of legislation and enforcement for new technologies. In this opinion piece I argue that the responsibility for cybersecurity should be shared by governments and companies. To give companies the tools they need for ethical decision-making and thus truly take responsibility, I suggest combining the ethics of care with stakeholder theory to provide a context-based relational view of companies. With this caring stakeholder model, companies have the tools they need to transition from compliance to security.

1. Introduction

Companies are struggling with the ramifications of increased digitization: cyberattacks are constantly occurring [18]; no company, big or small, is safe [6]; and at the bottom-line, cybercrime is costing society a considerable amount of money [1]. While companies are trying to be secure in the digital domain, it remains a relatively new challenge that demands further research. Current corporate cybersecurity strategies predominantly center around technical risk assessments [56]. With a strong focus on being compliant rather than being secure, companies are striving to abide by the guidelines of cybersecurity standards and legislative frameworks such as NIST, ISO, NIS2 and the GDPR, but consequently suffer from blind spots [22,31,51]. Companies are currently in problem-solving mode [30], focusing on compliance to (legal) frameworks to stay on course. In this opinion piece, I argue that companies need to go beyond the focus on standards and regulations if they want a comprehensive cybersecurity strategy. Moreover, I propose that companies can adopt a caring stakeholder theory to shape their cybersecurity responsibilities.

2. Compliance and security

There exists a prevalent misconception that compliance to standards

and regulation equals strong cybersecurity [29,31,67]. However, attackers don't care whether an organization is fully compliant or not, they will try to find vulnerabilities anyway. In their empirical study of 243 hospitals, Kwon and Johnson [29] reveal that for mature organizations, compliance to regulatory frameworks had no impact on data breach occurrence. Furthermore, they find that: “immature hospitals are motivated by meeting compliance mandates rather than actually protecting information.” ([29], p. 61). Although compliance did improve data security for these immature hospitals, it could hinder them from achieving more comprehensive data protection beyond the minimum requirements. Furthermore, because such standards focus on the existence of certain security processes but do not prescribe the quality, they could lead to a false sense of security [59]. Kwon and Johnson [29] argue that policy makers should move away from providing checkbox requirement lists and instead encourage a more context-driven approach for organizations. The act of ticking off items from a list of requirements may create a false sense of security completion within companies. In reality, cybersecurity is an ongoing and perpetual task. While a lot of work remains to be done to study the effects that security measures have on actual security, there are signs that the focus on compliance to standards and regulations does not always produce the desired result. The limitation of standards and regulations is further emphasized by “the pacing problem”.

* Corresponding author at: Institute of Security and Global Affairs (ISGA), Leiden University, Turfmarkt 99, The Hague 2511 DP, the Netherlands.

E-mail address: j.boeken@fpga.leidenuniv.nl.

<https://doi.org/10.1016/j.clsr.2023.105926>

Available online 22 November 2023

0267-3649/© 2023 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

3. The pacing problem and Collingridge dilemma

The European Union has made diligent efforts to enhance cybersecurity through the development of legal frameworks such as the GDPR, the NIS2 directive and the AI Act. However, crafting legislation in an emerging domain presents persistent challenges [2,4]. For instance, the GDPR has faced criticism for a perceived lack of transparency [54] and its deficiency in functional enforcement mechanisms [44,54]. The inherent challenges in legislating cybersecurity can be, at least in part, attributed to the pacing problem. The pacing problem can be defined as: “the gap between the introduction of a new technology and the establishment of laws, regulations, and oversight mechanisms for shaping its safe development.” ([65], p. 251). While the pace of technological development is fast, the pace of developing regulation and oversight is slow [33]. This slow pace of legislation might be beneficial regarding stability and comprehensiveness of law; however, it also leaves considerable gaps for companies and consumers regarding the requirements of cybersecurity for products and companies’ infrastructure.

The pacing problem can be illustrated with a recent instance involving the EU’s AI Act, which had reached the draft stage when ChatGPT was introduced to the market. This necessitated changes within the AI act, since the initial draft did not consider this type of AI [25,62]. While generative AI systems have since been incorporated into the AI Act, Helberger and Diakopoulos [25] contend that the Act’s high-risk/no-risk framework is ill-suited for regulating this form of AI. This case underscores how technological advancements can outpace legislative developments. The issue of the pacing problem is not limited to the field of cybersecurity alone; it also affects fields like human genome editing [66] and nano technology [61]. In these fields, the pacing problem poses similar challenges and implications.

The pacing problem, although not a new phenomenon, is being exacerbated by the rapidly accelerating pace of technological advancements [23,60,61]. In essence, the time in-between the launch of new technologies and the development of new regulatory frameworks for these technologies is increasing [23]. While the swift progress of technologies is one side of the story, the other side is the legislators. Besides suffering from slow governance processes, even with the help of experts, legislators lack the in-dept knowledge and understanding of technical issues, casting doubt on whether the political level can ever provide adequate cybersecurity guidelines [7].

In addition to the pacing problem, the Collingridge dilemma poses a significant challenge for responsible technological advancements [28]. The dilemma elucidates the difficulties of regulating new technologies and the issues that arise in the different developmental stages of such technologies [40]. During the initial stage of technological development, there is a dearth of information, making it challenging to develop new legislation. At this stage, there is very little information on the risks of these technologies, and this lack of data makes the work for legislators significantly harder [40,43,61]. While there is thus little information on the risks in this initial state of development, EU digital policies like the GDPR, the DSA and the AI Act, adopt a risk-based approach [9]. Nonetheless, the scarcity of information on cyber-risks amplifies the probability of inaccuracies [10]. For instance, Helberger and Diakopoulos [25] contend that a risk-based approach is ill-suited for legislating generative AI because “it is simply impossible to predict if, and if so, what the risks are that we can expect from unleashing extremely powerful AI models on society.” ([25], p. 2). This limitation of risk-based approaches, exacerbates the concern of companies prioritizing technical risk assessments for their cybersecurity [56].

While at the early stage of technological advancements the uncertainties are thus too big to effectively regulate, new difficulties arise when the technology is embedded in society [40]. At this later stage, Collingridge argued, the costs of adapting these technologies to new legislation would be significant, and the development of legislation would be slow and costly [40]. Pearlman et al. [47] offer an illustration of the Collingridge dilemma through their examination of the

Metaverse, a platform that gathers a substantial amount of (sensitive) data. Predicting the full extent of the Metaverse’s impact and the associated security risks remains challenging until widespread adoption occurs. However, enacting legislation to address these issues once widespread adoption has taken place will require costly and complicated adaptations of an existing product [47].

While some scholars have proposed to change the governance process of legislating new technologies to be more anticipatory or flexible [23,61], I advocate for a shift of focus towards the companies responsible for developing these new technologies. After all, they are the ones who possess the knowledge that legislators often lack in this rapidly evolving landscape. While conducting risk assessments for new technologies will always remain challenging, the companies at the forefront of technological advancements are better equipped to calculate the risks. Consequently, I argue for holding these companies accountable and urging them to take on the responsibility for cybersecurity that goes beyond mere compliance with existing standards and regulations.

Although some might be understandably skeptical regarding companies taking responsibility, the growing emphasis on socially responsibility is motivating companies to do well by doing good [19]. An alternative incentive for companies to take responsibility and transcend legal requirement is that when they don’t, the government might step in and regulate [5,8,41]. Taking responsibility now means less strict regulations later, and a smoother transition when new legislation does arrive. A good example comes from environmental regulations: “being proactive on environmental issues can lower the costs of complying with present and future environmental regulations.” ([5], p. 489). Therefore, by taking responsibility for ensuring robust cybersecurity for all stakeholders, companies may not only demonstrate their commitment to social welfare but also potentially save costs when new cybersecurity legislation eventually arises. This, however, raises the question for which stakeholders the firm is responsible, and how this responsibility should translate into action.

4. Stakeholder theory

The preceding sections have highlighted the drawbacks of companies fixating solely on compliance by arguing that compliance does not guarantee security, and explaining the pacing problem which underscores how legislation lags behind technological advancements. If companies aspire to take responsibility, they will need an ethical approach for moral decision-making regarding cybersecurity. At the 50th World Economic Forum (WEF) meeting of 2020 in Davos, the stakeholder approach was described as a promising philosophy for organizations to cope with the new challenges of increased digitization [36]. This resulted in the Davos Manifesto 2020, setting ethical guidelines for companies on how to navigate these challenges, including a large focus on stakeholders [57]. Likewise, at the Business Roundtable in that same year, 181 CEOs committed to leading their companies to the benefit of all stakeholders.

The 1984 seminal work of Freeman, *Strategic management: A stakeholder approach*, was written to provide corporations with a new way of approaching strategic management. His main argument is that corporations have more stakeholder groups than just the shareholders, and that these should be considered in companies’ decision-making [14]. The theory prescribes whom the firm should serve and how it should operate [68]. Freeman famously describes stakeholders as “Any group or individual who can affect or is affected by the achievement of the firm’s objectives.” ([14], p. 25). According to Morgan and Gordijn [39] when stakeholder theory is applied to cybersecurity, there are eight legitimate stakeholders: shareholders, employees, the local community, customers, suppliers, competitors, hackers and the general public.

Stakeholder theory is enjoying increased popularity in academia [32]. While there are alternative theories within management science like corporate social responsibility or corporate citizenship, stakeholder theory is distinctive due to its foothold in strategic management. It can

be used as a practical tool to establish a corporate strategy [58]. This practicality is favorable due to the need for guidance companies have regarding their cybersecurity. According to McVea and Freeman [35], the challenges that new technologies have brought to our economy are in need of stakeholder theory for at least two reasons. First, the economy is increasingly dependent on networks of relationships, and thus it becomes ever more important to look further than the boundaries of traditional organizations. Second, increased digitization makes operating complex stakeholder networks easier and more fruitful [35]. For example, due to the increased possibilities of working together online. For the other challenges of our time that also suffer from the pacing problem, like climate change, ethical guidelines are developed, however, for cybersecurity this remains a gap [38].

To organize the extensive research on the theory, Donaldson and Preston [11] have divided it into descriptive, instrumental, and normative research. Whereas descriptive work deals with question of how companies currently do things [21,48]; instrumental work studies the effects of stakeholder management on corporate goals like profit [34,37,45,46,52,53,64]; and normative work deals with the question of what a corporation ought to do [15,16,49,63,68]. This opinion piece is situated in the normative domain of stakeholder theory, while not losing sights of the others because what is now normative theory might one day become the topic of a descriptive or instrumental research.

According to Freeman [13], stakeholder theory should always be combined with a normative core, this will help determine who the legitimate stakeholders are and what a companies' behavior should look like. Whether this normative core is based on Rawlsian theory [49], Kantian theory [63], libertarian theory [16], or ethics of care [68], can vary. While the ethical cores all have some distinct benefits, what the first three have in common is that they propose some type of universal principles. For this opinion piece, stakeholder theory will be used in combination with a normative core of ethics of care, which is divergent due to its ability to focus on specific context.

5. Care ethics as the normative core

As discussed in the previous section, the ethics of care can be used as a normative core for stakeholder theory. Originating from feminist theory, Gilligan's [20] book *In a Different Voice*, became the leading work in care ethics. The five key features of care ethics are: (1) recognizing care as a moral value, (2) emphasizing the value of emotions, (3) considering context, (4) reevaluating the boundaries between the public and the private spheres, and (5) adopting a relational view of the person [20,26,51]. For instance, applying care ethics principles to cybersecurity implies that stakeholder relationships should extend beyond mere compliance with laws and regulations [24,42]. Simply adhering to a cyber risk management framework may prove insufficient. Furthermore, the effect of emotions on (security) behavior needs to be considered within the companies' cybersecurity strategy [3,27,50,55]. An illustrative case highlighting the importance of emotions is provided by Lundgren and Bergström [31], who shed light on the role of security-related stress during the initial stages of corporate cyber risk management implementation. According to their research, this stress is partly attributed to the implementation of generic standards, such as the ISO/IEC 2700 series, which prove challenging to tailor to company-specific needs. This is where implementing care ethics can yield a noticeable impact. By recognizing the role of emotions on individuals' problem-solving approaches, including their response to cybersecurity challenges, we can enhance the safeguard of our digital environment.

Combining the ethics of care with stakeholder theory as a framework for cybersecurity has already been proposed by Morgan and Gordijn [39]. Building upon Engster's [12] care-based stakeholder theory, they assess the responsibilities of businesses towards their stakeholders in the case of a ransomware attack. Engster defines stakeholders as "any groups or individuals whose ability to care for themselves or others is

directly dependent upon a firm's actions or decisions." ([39], p. 101), and argues that employees and shareholders are the most important groups. Morgan and Gordijn [39] identify eight legitimate stakeholders in the case of a ransomware attack: shareholders, employees, the local community, customers, suppliers, competitors, hackers, and the general public. They further assess what the risks and benefits of these stakeholders are, and whether paying or not paying the ransom would be in their best interest. This study provides us with a great example of how a caring stakeholder approach can be employed to assess cybersecurity incidents. However, it also leaves opportunities for improvement by considering a broader perspective than Engster's relatively narrow definition of stakeholders [39]. Furthermore, while the case of ransomware attacks provides a great example, companies are in need of guidelines for their overall cybersecurity strategy.

An interesting angle of using the ethics of care is to introduce the obligation of care. Noddings [42] identifies two criteria that must be met for an obligation of care to arise: (1) the existence or the potential existence of a relationship, and (2) the potential for growth within this relationship. Given that companies are comprised of webs of relationships, often including a potential for growth, it may be argued that companies bear the obligation to care for their stakeholders. This obligation to care must then also be applied to the cybersecurity of companies, necessitating them to take responsibility for, for example, their supply chain's security. To gain a deeper insight, further research should explore how such an obligation to care for stakeholders influences the cybersecurity strategy of companies.

6. Conclusion

In this opinion piece I argue that a narrow focus on standards and regulatory frameworks is not the solution for companies struggling with cybersecurity. This is because, on the one hand, a focus on compliance gives companies a checkbox mindset where they lose sight of actual security. And on the other hand, because the checkboxes we use are inherently outdated compared to new technologies due to the pacing problem. While the EU is making great efforts on the front of legislation, legislating such a new field remains difficult. I suggest moving our focus from governments to companies regarding the responsibility of cybersecurity. Where governments may lack the knowledge and skills on new technological developments, companies that develop these technologies should carry a larger responsibility to keep the digital domain safe. Whereas the World Economic Forum suggested that a stakeholder theory of the firm could be a viable approach to address cybersecurity challenges, work remains to be done regarding the practical application of the theory. I suggest combining stakeholder theory with the ethics of care for a context-based relational view of cybersecurity. Adopting an ethics-based approach to cybersecurity can provide companies with a framework that extends beyond conventional reliance on risk assessments, encouraging them to incorporate their core values into their decision-making processes. To evolve from mere compliance to robust security, it is essential to redistribute some of the responsibility from governments to companies. This does not entail a reduction in regulatory oversight; rather, it calls for additional responsibility.

A potential challenge associated with this approach is the extent to which companies will willingly embrace cybersecurity measures when not compelled to do so. However, as previously elucidated, there exist other incentives, such as a commitment to ethical conduct and the desire to preempt future regulatory measures, which may motivate companies to adopt a caring stakeholder approach to cybersecurity. Moreover, the caring stakeholder approach should avoid adapting a checklist-style method but instead draw inspiration from methodologies like Value Sensitive Design [17]. Although the caring stakeholder approach requires further research and refinement for full development, its emphasis on relational and context-based strategies seems promising for the vastly changing field of cybersecurity. By empowering companies with a care-based stakeholder theory, we can create a more resilient

cybersecurity landscape.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author(s) used OpenAI in order to improve readability. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

- Anderson R, Barton C, Böhme R, Clayton R, Van Eeten MJ, Levi M, Moore T, Savage S. Measuring the cost of cybercrime. The economics of information security and privacy. Springer; 2013. p. 265–300.
- Backman S. Risk vs. threat-based cybersecurity: the case of the EU. *Eur. Secur.* 2023;32:85–103.
- Barrett LF. How emotions are made: the secret life of the brain. Pan Macmillan; 2017.
- Bechara FR, Schuch SB. Cybersecurity and global regulatory challenges. *J Finance Crime* 2021;28:359–74.
- Berman SL, Wicks AC, Kotha S, Jones TM. Does stakeholder orientation matter? The relationship between stakeholder management models and firm financial performance. *Acad Manag J* 1999;42:488–506.
- Buil-Gil D, Lord N, Barrett E. The dynamics of business, cybersecurity and cyber-victimization: foregrounding the internal guardian in prevention. *Vict Offenders* 2021;16:286–315.
- Carrapico H, Farrand B. Dialogue, partnership and empowerment for network and information security: the changing role of the private sector from objects of regulation to regulation shapers. *Crime Law Soc Chang* 2017;67:245–63.
- Davis K. Can business afford to ignore social responsibilities? *Calif Manag Rev* 1960;2:70–6.
- De Gregorio G, Dunn P. The European risk-based approaches: connecting constitutional dots in the digital age. *Common Mark Law Rev* 2022;59.
- de Jong E. Own the unknown: an anticipatory approach to prepare society for the quantum age. *Digit Soc* 2022;1:15.
- Donaldson T, Preston LE. The stakeholder theory of the corporation: concepts, evidence, and implications. *Acad Manag Rev* 1995;20:65–91.
- Engster D. Care ethics and stakeholder theory. *Appl Care Ethics Bus* 2011;93–110.
- Freeman RE. The politics of stakeholder theory: some future directions. *Bus Ethics Q* 1994:409–21.
- Freeman RE. Strategic management: a stakeholder approach. Cambridge University Press; 1984. <https://doi.org/10.1017/CBO9781139192675>.
- Freeman R.E., Harrison, J.S., Wicks, A.C., Parmar, B.L., De Colle, S., 2010. Stakeholder theory: the state of the art.
- Freeman RE, Phillips RA. Stakeholder theory: a libertarian defense. *Bus Ethics Q* 2002;12:331–49.
- Friedman B, Kahn PH, Borning A, Huldgren A. Value sensitive design and information systems. *Early Engagem New Technol Open Lab* 2013;55–95.
- Ganin AA, Quach P, Panwar M, Collier ZA, Keisler JM, Marchese D, Linkov I. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Anal* 2020;40:183–99. <https://doi.org/10.1111/risa.12891>.
- Gelles D, Yaffe-Bellany D. Shareholder value is no longer everything, top CEOs say. *N Y Times* 2019;19.
- Gilligan C. In a different voice: psychological theory and women's development. Harvard University Press; 1993.
- Greenley GE, Foxall GR. Consumer and nonconsumer stakeholder orientation in UK companies. *J Bus Res* 1996;35:105–16.
- Groves C. Future ethics: risk, care and non-reciprocal responsibility. *J Glob Ethics* 2009;5:17–31.
- Hagemann R, Huddleston Skees J, Thierer A. Soft law for hard problems: the governance of emerging technologies in an uncertain future. *Colo Tech LJ* 2018;17:37.
- Hardwig J. Should women think in terms of rights? *Ethics* 1984;94:441–55.
- Helberger N, Diakopoulos N. ChatGPT and the AI Act. *Internet Policy Rev* 2023;12.
- Held V. The ethics of care: personal, political, and global. Oxford University Press on Demand; 2006.
- Kahneman D. Thinking, fast and slow. Macmillan; 2011.
- Kudina O, Verbeek PP. Ethics from within: google Glass, the Collingridge dilemma, and the mediated value of privacy. *Sci Technol Hum Values* 2019;44:291–314.
- Kwon J, Johnson ME. Health-care security strategies for data protection and regulatory compliance. *J Manag Inf Syst* 2013;30:41–66.
- Liedtka JM. Feminist morality and competitive reality: a role for an ethic of care? *Bus Ethics Q* 1996:179–200.
- Lundgren M, Bergström E. Security-related stress: a perspective on information security risk management. In: Proceedings of the international conference on cyber security and protection of digital services (cyber security). IEEE; 2019. p. 1–8.
- Mahajan R, Lim WM, Sareen M, Kumar S, Panwar R. Stakeholder theory. *J Bus Res* 2023;166:114104.
- Marchant GE. Addressing the pacing problem, in: the growing gap between emerging technologies and legal-ethical oversight. Springer; 2011. p. 199–205.
- Margolis JD, Walsh JP. Misery loves companies: rethinking social initiatives by business. *Adm Sci Q* 2003;48:268–305.
- McVea JF, Freeman RE. A names-and-faces approach to stakeholder management: how focusing on stakeholders as individuals can bring ethics and entrepreneurial strategy together. *J Manag Inq* 2005;14:57–69.
- Mhlanga D, Moloi T. The stakeholder theory in the fourth industrial revolution. *Int J Econ Financ* 2020;12:352–68.
- Moon J. Corporate social responsibility: a very short introduction. USA: Oxford University Press; 2014.
- Morgan, G., 2021. Ethical Issues in cybersecurity: employing red teams, responding to ransomware attacks and attempting botnet takedowns.
- Morgan G, Gordijn B. A care-based stakeholder approach to ethics of cybersecurity in business. *Ethics Cybersecur* 2020;119.
- Moses LB. How to think about law, regulation and technology: problems with 'technology' as a regulatory target. *Law Innov Technol* 2013;5:1–20.
- Munilla L, Miles M. The corporate social responsibility continuum as a component of stakeholder theory. *Bus Soc Rev* 2005;110:371–87.
- Noddings N. Caring: a relational approach to ethics and moral education. University of California Press; 2013.
- Nogel M, Kovács G, Wersényi G. The regulation of digital reality in nutshell. In: Proceedings of the 12th IEEE international conference on cognitive infocommunications (CogInfoCom); 2021. p. 1–7.
- NOYB, 2023. 5 Years of the GDPR: national authorities let down European legislator.
- Orlitzky M, Benjamin JD. Corporate social performance and firm risk: a meta-analytic review. *Bus Soc* 2001;40:369–96.
- Orlitzky M, Schmidt FL, Rynes SL. Corporate social and financial performance: a meta-analysis. *Organ Stud* 2003;24:403–41.
- Pearlman K, Initiative X, Visser S, Magnano M, Cameron R. Securing the metaverse-virtual worlds need REAL governance. *Simul Interoperability Stand Organ* 2021.
- Pedersen ER. Making corporate social responsibility (CSR) operable: how companies translate stakeholder dialogue into practice. *Bus Soc Rev* 2006;111:137–63.
- Phillips RA. Stakeholder theory and a principle of fairness. *Bus Ethics Q* 1997;7:51–66.
- Plot FA. Paying attention to attention: care and humanism. *Bus Soc Rev* 2009.
- Preston CJ, Wickson F. Broadening the lens for the governance of emerging technologies: care ethics and agricultural biotechnology. *Technol Soc* 2016;45:48–57.
- Preston LE, Sapienza HJ. Stakeholder management and corporate performance. *J Behav Econ* 1990;19:361–75.
- Ruf BM, Muralidhar K, Brown RM, Janney JJ, Paul K. An empirical investigation of the relationship between change in corporate social performance and financial performance: a stakeholder theory perspective. *J Bus Ethics* 2001;32:143–56.
- Ruohonen J, Hjerpe K. The GDPR enforcement fines at glance. *Inf Syst* 2022;106:101876.
- Sapolsky, R.M., 2017. Behave: the biology of humans at our best and worst. Penguin.
- Schinagl S, Shahim A. What do we know about information security governance? "From the basement to the boardroom": towards digital security governance. *Inf Comput Secur* 2020.
- Schwab, K., 2020. Davos manifesto 2020: the universal purpose of a company in the fourth industrial revolution. URL <https://www.weforum.org/agenda/2019/12/davos-manifesto-2020-the-universal-purpose-of-a-company-in-the-fourth-industrial-revolution/> (accessed 10.1.23).
- Schwartz MS, Carroll AB. Integrating and unifying competing and complementary frameworks: the search for a common core in the business and society field. *Bus Soc* 2008;47:148–86.
- Siponen M. Information security standards focus on the existence of process, not its content. *Commun ACM* 2006;49:97–100.
- Thierer A. The pacing problem and the future of technology regulation. *Mercent Cent* Accessed 2018;8.
- Trump BD, Keisler JM, Galaiti SE, Palma-Oliveira JM, Linkov I. Safety-by-design as a governance problem. *Nano Today* 2020;35:100989.
- Volpicelli, G., 2023. ChatGPT broke the EU plan to regulate AI. Politico.
- Vos JF. Corporate social responsibility and the identification of stakeholders. *Corp Soc Responsib Environ Manag* 2003;10:141–52.
- Waddock SA, Graves SB. The corporate social performance–financial performance link. *Strateg Manag J* 1997;18:303–19.
- Wallach W. A dangerous master: how to keep technology from slipping beyond our control. Basic Books; 2015.

- [66] Wang L, Shang L, Zhang W. Human genome editing after the “CRISPR babies”: the double-pacing problem and collaborative governance. *J Biosaf Biosecur* 2023.
- [67] Webb J, Ahmad A, Maynard S, Shanks G. Foundations for an intelligence-driven information security risk-management system. *J Inf Technol Theory Appl JITTA* 2016;17:3.
- [68] Wicks AC, Gilbert DR, Freeman RE. A feminist reinterpretation of the stakeholder concept. *Bus Ethics Q* 1994;475–97.