Digital Ethics Lab Yearbook

Carl Öhman
David Watson *Editors*

The 2018 Yearbook of the Digital Ethics Lab

Digital
Ethics
Lab

Springer

Digital Ethics Lab Yearbook

Series Editors
Luciano Floridi, Oxford Internet Institute, Digital Ethics Lab,
University of Oxford, Oxford, UK
The Alan Turing Institute, London, UK
Mariarosaria Taddeo, Oxford Internet Institute, Digital Ethics Lab,
University of Oxford, Oxford, UK
The Alan Turing Institute, London, UK

The Digital Ethics Lab Yearbook is an annual publication covering the ethical challenges posed by digital innovation. It provides an overview of the research from the Digital Ethics Lab at the Oxford Internet Institute. Volumes in the series aim to identify the benefits and enhance the positive opportunities of digital innovation as a force for good, and avoid or mitigate its risks and shortcomings. The volumes build on Oxford's world leading expertise in conceptual design, horizon scanning, foresight analysis, and translational research on ethics, governance, and policy making.

More information about this series at http://www.springer.com/series/16214

Carl Öhman • David Watson
Editors

The 2018 Yearbook of the Digital Ethics Lab

Springer

Editors
Carl Öhman
Oxford Internet Institute, Digital Ethics Lab
University of Oxford
Oxford, UK

David Watson
Oxford Internet Institute, Digital Ethics Lab
University of Oxford
Oxford, UK

ISSN 2524-7719 ISSN 2524-7727 (electronic)
Digital Ethics Lab Yearbook
ISBN 978-3-030-17151-3 ISBN 978-3-030-17152-0 (eBook)
https://doi.org/10.1007/978-3-030-17152-0

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

1 Digital Ethics: Goals and Approach . . . 1
Carl Öhman and David Watson

2 Digital Ethics: Its Nature and Scope . . . 9
Luciano Floridi, Corinne Cath, and Mariarosaria Taddeo

3 Do We Need a Critical Evaluation of the Role of Mathematics in Data Science? . . . 19
Patrick Allo

4 Using Data from Git and GitHub in Ethnographies of Software Development . . . 35
Andrew Turner

5 The Price of Discovery: A Model of Scientific Research Markets . . . 51
David Watson

6 Projecting AI-Crime: A Review of Plausible Threats . . . 65
Thomas King

7 The Challenges of Cyber Deterrence . . . 85
Mariarosaria Taddeo

8 Internet Governance and Human Rights: A Literature Review . . . 105
Corinne Cath

9 Privacy Risks and Responses in the Digital Age . . . 133
Josh Cowls

10 Digitalised Legal Information: Towards a New Publication Model . . . 149
Václav Janeček

11 From Bones to Bytes: A New Chapter in the History of Death . . . 167
Carl Öhman

12 The Green and the Blue: Naïve Ideas to Improve Politics in a Mature Information Society . . . 183
Luciano Floridi

Index . . . 223

Chapter 1
Digital Ethics: Goals and Approach

Carl Öhman and David Watson

1.1 Digital Technologies As a Force of Good

Are digital technologies a force for good? The question is perhaps somewhat simplistic, but has been posed and rephrased since the early development of computers. As noted by Arthur L. Samuel, one of the great pioneers of Artificial Intelligence (AI), “as to the portents for good or evil which are contained in the use of this truly remarkable machine—most, if not all, of men’s inventions are instrumentalities which may be employed by both saints and sinner” (Samuel 1960, p. 742). Indeed, digital technologies have shown a great potential to perpetrate good and evil. From enhancing biomedical research and healthcare (Krutzinna et al. 2018) to improving social interactions (Taddeo and Floridi 2011) and education (Eynon 2013), digital technologies drive major developments of our societies and of individual wellbeing. At the same time, they can enable and exacerbate unfair discrimination (Floridi 2014), undermine fundamental rights (Floridi 2016b; Cath and Floridi 2017; Taub and Fisher 2018), foster mass surveillance (Taddeo 2013), and facilitate cyber warfare (Kello 2017; Taddeo and Floridi 2018) and cyber crime (King et al. 2018). In other words, Samuel was right. As with all technology, the ethical impact of the digital depends on the purposes of its designers and users, the saints and the sinners of Samuel’s paper.

Design plays a central role with respect to the ethical impact of technology. Indeed, technological artefacts tend to enable dual uses. However, it is important to stress that, in many cases, artefacts have an “oriented” dual use, which is informed by their design (see Chap. 12 on this concept). They can be used for good or evil,

C. Öhman (✉) · D. Watson
Oxford Internet Institute, Digital Ethics Lab, University of Oxford, Oxford, UK
e-mail: carl.ohman@oii.ox.ac.uk

C. Öhman, D. Watson (eds.), *The 2018 Yearbook of the Digital Ethics Lab*,
Digital Ethics Lab Yearbook, https://doi.org/10.1007/978-3-030-17152-0_1

but seldom can they be used equally well for either. A bayonet may be used for some good, perhaps, but it is really meant to kill a human being. The same holds true for a Swiss army knife: it may have evil applications, but it is designed to provide a set of handy tools. This also applies to digital technologies.

At the same time, the ethical impact of the digital transcends its design and uses. This is because digital technologies transform the reality in which we live by creating a new environment, new forms of (artificial) agency, and new affordances for our interactions with them. Floridi refers to this as to the *cleaving power* of the digital: “the digital ‘cuts and pastes’ reality, in the sense that it couples, decouples, or recouples features of the world—and therefore our corresponding assumptions about them—which we never thought could be anything but indivisible and unchangeable” (Floridi 2017, p. 123). This the case, for example, of ‘real and physical’ or ‘warfare and violence’. Reality in the information age is no longer coupled to tangibility as much as it is to *interactability* (Taddeo 2012; Floridi 2013). Think of the way in which Alice and her grandfather Bob enjoy their music: Bob may still own a collection of his favourite vinyls, while Alice simply logs into her favourite streaming service (she does not even own the files on her computers). E-books, movies, pictures are all good examples of the decoupling of real and physical in the digital age. Cyber warfare is another compelling case of cleaving power of the digital. For it separates conflict waging from violence (cyber warfare may not cause any casualties or destroy any physical object) (Taddeo and Floridi 2014), agency from responsibility (cyber warfare can be waged by autonomous weapons that are not morally responsible for their actions) (Floridi 2012, 2016c), and undermines state monopoly of political power (grass-roots movements, terrorists, and private companies may all challenge state power in cyberspace) (Nye 2010; Taddeo 2017).

As digital technologies become widely disseminated and their cleaving power reshapes reality and social dynamics, it is crucial to identify the right direction in which to steer this power. To do so, we need to understand what principles should guide the development of current and future information societies, as well as what policies we should enact to ensure that those principles are respected, so that we harness the value of digital innovation to design open, tolerant, equitable, and just information societies. These are ethical questions. Digital ethics is the branch of ethics that addresses them.

Digital ethics “studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing, and use), algorithms (including AI, artificial agents, machine learning, and robots), and corresponding practices (including responsible innovation, programming, hacking, and professional codes), in order to formulate and support morally good solutions (e.g., right conducts or right values)” (Floridi and Taddeo 2016, p. 3).

While they are distinct lines of research, the ethics of data, algorithms, and practices are obviously entangled. One may consider them as three axes defining a conceptual space within which ethical problems may be located. As stressed in Chap. 2, most of the ethical problems posed by digital innovation do not lie on just a single axis. For example, analyses focusing on privacy will also address issues concerning consent and professional responsibilities. Likewise, ethical auditing of algorithms often implies analyses of the responsibilities of their designers, developers, users, and adopters. "Digital ethics addresses the whole conceptual space and hence all three axes together, albeit with different priorities and focus. And for this reason, it needs to be developed as a macroethics, that is, as an overall 'geometry' of the ethical space that avoids narrow, *ad hoc* approaches, but rather addresses the diverse set of ethical implications of digital transformation within a consistent, holistic, and inclusive framework" (Floridi and Taddeo 2016, p. 4).

As a macroethics, digital ethics can provide the necessary guidelines to leverage the transformative power of digital innovation as a force of good. It does so by identifying socially preferable solutions and by assessing trade-offs between conflicting values to inform policy decisions. Digital ethics translates theoretical analyses and principles concerning fundamental ethical issues—like autonomy, human dignity, freedom, tolerance, and justice—into viable guidelines to shape the design and use of digital technologies. The key word here is "translational". Much like translational medicine builds on research advances in biology to develop new therapies and medical procedures, *translational* ethics goes from the whiteboard of academia to the desk of policy making, using theoretical analyses to shape regulatory and governance approaches to digital innovation.

The macroethical and translational approach of digital ethics underpins the vision and work of the Digital Ethics Lab (the DELab). The DELab is a multidisciplinary research environment, which draws on a multitude of academic traditions, including (but not limited to) anthropology, science and technology studies, economics, formal logic, and computer science. Although they may differ in scope and methods, these research areas bring new and important insights that help to identify the ethical problems that arise in our information society and develop the macroethical approach necessary to solve them. At the same time, the DELab has, since the very beginning, established collaborations with a variety of non-academic partners, whose expertise and remits facilitate the translation of ethical analyses into effective guidelines for shaping digital innovation.

1.2 The 2018 Yearbook

The macroethical and translational approach of digital ethics also informs this volume, which collects contributions from the members of the DELab. The goal is to provide an overview of the lines of research undertaken by the DELab and to illustrate the depth and scope of its output. The following 11 chapters of this collection cover a wide range of topics in digital ethics. They highlight the inherently multidisciplinary nature of the subject, which cannot be separated from the epistemological foundations of the technologies themselves or the political implications of the requisite reforms. This is emphasised by Cath, Floridi & Taddeo in the second chapter. The authors provide a helpful overview of the landscape of digital ethics, outlining the major areas of debate, and differentiating the field from related ethical inquiries.

The next three chapters all concern epistemological questions. The third chapter, written by Allo, puts the complex interplay between epistemology and ethics on full display. Allo argues that data science has uncritically imported a collection of so-called "epistemic virtues" from mathematics and statistics, which hinders any meaningful debate around the social structures they inscribe through emerging technologies. In Chap. 4, Turner urges us to take a closer look at how digital technologies evolve in real time, examining the version control platforms Git and GitHub (GitHub 2018). As large scale, collaborative projects are increasingly forged through decentralised networks, Turner argues, researchers in science and technology studies should extend their traditional focus on laboratory studies to online platforms that offer similar, arguably richer resources for investigating the progress of a project. Of course, the largest and best funded scientific projects of our time are major national and international initiatives, like the Large Hadron Collider at CERN. These massive undertakings are the subject of Watson's chapter (Chap. 5), where he draws on classical microeconomic theory to point out potential inefficiencies in contemporary science funding.

How we understand these epistemological and technical questions matters greatly for how we choose to respond to issues that arise from technological innovation. This is illustrated by Chaps. 6, 7, 8, 9 and 10. In Chap. 6, King identifies emerging challenges surrounding AI crime. King analyses the unique and realistic threats posed by AI crime and assesses existing and feasible solutions to mitigate them. Taddeo in turn extends the analysis to cyber-warfare (Chap. 7), arguing that we must "recognise the limits of approaching cyber deterrence by analogy with kinetic conflicts" and move beyond them. In Chap. 8, Cath focuses on the unintended or secondary consequences of technical systems. She points out that the governance and design of such systems are inherently political, advocating for an approach founded on human rights. In pursuing this argument, she identifies a number of biases and gaps in current literature that could be resolved through increasing dialogue and a broader scope.

In Chap. 9, Cowls examines the question of a more specific right, namely that of online privacy. To understand and identify the complex nature of privacy violations, Cowls proposes a framework that applies to three stages of the "information life cycle": collection, analysis, and deployment. He further argues that threats arising at each stage can be considered both on a macro and a micro level, each of which requires its own specific regulatory response strategy. As implied by this chapter, the transition from information society to a *mature* information society (Floridi 2016a) requires massive amounts of new regulation, i.e. legal information. The management and distribution of this information is the topic of Janeček's chapter (Chap. 10). In contrast to the other contributors of the book, Janeček has an explicitly legal, yet also more holistic focus. By first giving a historical overview of the role of ICTs in disseminating legal information, he shows that the information revolution calls for a revision of the current publication and communication model and stresses the importance of designing a system that reaches and communicates well with its ultimate addressees—the citizens who will obey the laws.

Though diverse in scope, these five policy-oriented chapters all illustrate the importance of expert knowledge in the project of designing new reforms and political systems for the digital age. Yet, this task also requires a deep self-understanding in terms of who we are as individuals and as a species. This is the topic of Chaps. 11 and 12.

The information revolution inevitably disrupts some of the most fundamental elements of human existence. For example, Öhman (Chap. 11) argues that the advent of the internet marks a historical shift in how we understand the concepts of life and death. This in turn calls for careful ethical analysis of the macroscopic, microscopic, and conceptual consequences of such a shift. How are we to deal with the informational remains that we leave behind on the web when passing? And what does the prospect of a "digital afterlife" tell us about human existence? Questions of a similar gravity are discussed in the closing chapter, where Floridi presents some "naïve" ideas to help facilitate the formation of a new "human social project" (Chap. 12). He argues that in order to make room for a new, healthier politics, the "Ur philosophy" of the Aristotelian and Newtonian worldview must be abandoned. Instead he proposes that we adopt a "relationist" understanding of the world as the basis of political discourse. In contrast to the rather dark picture painted by many of the chapters, this final chapter shows that there is still room for optimism in digital ethics. The challenges arising from the advent of information society surely seem massive, but so too are human creativity and innovation.

1.3 Conclusion

So, are digital technologies a force for good? Certainly, the cleaving power of the digital offers a wealth of new opportunities and affordances to improve individual wellbeing and foster the development of our societies (Cath et al. 2017). However, these opportunities are coupled with serious ethical risks that can hinder the potential for good of digital technologies. It is crucial to identify and mitigate these risks. The present volume provides the first steps in this direction. Its contributions analyse the opportunities and the ethical challenges posed by digital innovation, delineate new approaches to solve them, and offer concrete guidance to harness the potential for good of digital technologies.

The questions raised here have ancient—perhaps even timeless—roots. While the phenomena they address are inherently new, they are unpacked by examining the fundamental concepts—good and evil, justice and truth—that undergird them all. Indeed, every epoch has its great challenges, and the role of philosophy must be to redefine the meaning of these concepts in light of the particular challenges it faces. This is true also for the digital age. While this book treats important and novel subjects, we know that we have only started redefining and re-implementing fundamental ethical concepts. We look forward to continuing on this journey.

Acknowledgments Before leaving the reader to the chapters in this volume, we wish to thank our colleagues and members of the Digital Ethics Lab at the University of Oxford. Our gratitude goes beyond their contributions to this volume and extends to the many insightful discussions, the cheerful lab meetings, and overall, the enthusiastic and bright research environment in which we can develop our work together. We are also deeply grateful to Springer Nature for publishing the yearbook, and in particular to Ties Nijssen for his interest in the Digital Ethics Lab and support during the process that led to the publication of this volume.

References

Cath, C., and L. Floridi. 2017. The design of the internet's architecture by the Internet Engineering Task Force (IETF) and human rights. *Science and Engineering Ethics* 23 (2): 449–468. https://doi.org/10.1007/s11948-016-9793-y.

Cath, C., S. Wachter, M. Taddeo, and L. Floridi. 2017. Artificial intelligence and the "Good Society": The US, EU, and UK approach. *Science and Engineering Ethics*, March. https://doi.org/10.1007/s11948-017-9901-7.

Eynon, R. 2013. The rise of big data: What does it mean for education, technology, and media research? *Learning, Media and Technology* 38 (3): 237–240. https://doi.org/10.1080/17439884.2013.771783.

Floridi, L. 2012. Distributed morality in an information society. *Science and Engineering Ethics* 19 (3): 727–743. https://doi.org/10.1007/s11948-012-9413-4.

———. 2013. *Ethics of information*. Oxford/New York: Oxford University Press.

———. 2014. Open data, data protection, and group privacy. *Philosophy & Technology* 27 (1): 1–3. https://doi.org/10.1007/s13347-014-0157-8.

———. 2016a. Mature information societies—a matter of expectations. *Philosophy & Technology* 29 (1): 1–4. https://doi.org/10.1007/s13347-016-0214-6.

———. 2016b. On human dignity as a foundation for the right to privacy. *Philosophy & Technology* 29 (4): 307–312. https://doi.org/10.1007/s13347-016-0220-8.

———. 2016c. Faultless responsibility: On the nature and allocation of moral responsibility for distributed moral actions. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374 (2083): 20160112. https://doi.org/10.1098/rsta.2016.0112.

———. 2017. Digital's cleaving power and its consequences. *Philosophy & Technology* 30 (2): 123–129. https://doi.org/10.1007/s13347-017-0259-1.

Floridi, L., and M. Taddeo. 2016. What is data ethics? *Philsophical Transaction of the Royal Society A* 20160360: 1–4.

Github. 2018. https://github.com/. Accessed 23 Apr 2019.

Kello, L. 2017. *The virtual weapon and international order*. New Haven: Yale University Press.

King, T., N. Aggarwal, M. Taddeo, and L. Floridi. 2018. *Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions,* SSRN scholarly paper ID 3183238. Rochester: Social Science Research Network. https://papers.ssrn.com/abstract=3183238.

Krutzinna, J., M. Taddeo, and L. Floridi. 2018. *Enabling posthumous medical data donation: A plea for the ethical utilisation of personal health data,* SSRN scholarly paper ID 3177989. Rochester: Social Science Research Network. https://papers.ssrn.com/abstract=3177989.

Nye, J. 2010. *Cyber power*. Boston: Harvard Kennedy School, Belfer Center for Science and International Affairs. http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.

Samuel, A.L. 1960. Some moral and technical consequences of automation—A refutation. *Science* 132 (3429): 741–742. https://doi.org/10.1126/science.132.3429.741.

Taddeo, M. 2012. Information warfare: A philosophical perspective. *Philosophy and Technology* 25 (1): 105–120.

———. 2013. Cyber security and individual rights, striking the right balance. *Philosophy & Technology* 26 (4): 353–356. https://doi.org/10.1007/s13347-013-0140-9.

———. 2017. Cyber conflicts and political power in information societies. *Minds and Machines* 27 (2): 265–268. https://doi.org/10.1007/s11023-017-9436-3.

Taddeo, M., and L. Floridi. 2011. The case for E-trust. *Ethics and Information Technology* 13 (1): 1–3. https://doi.org/10.1007/s10676-010-9263-1.

———. 2014. The ethics of information warfare—An overview. In *The ethics of information warfare*, Law, governance and technology series. New York: Springer.

———. 2018. Regulate artificial intelligence to avert cyber arms race. *Nature* 556 (7701): 296–298. https://doi.org/10.1038/d41586-018-04602-6.

Taub, A., and M. Fisher. 2018. Where countries are tinderboxes and Facebook is a match. *The New York Times*, 21 April 2018, sec. Asia Pacific. https://www.nytimes.com/2018/04/21/world/asia/facebook-sri-lanka-riots.html.

Chapter 2
Digital Ethics: Its Nature and Scope

Luciano Floridi, Corinne Cath, and Mariarosaria Taddeo

2.1 Digital Ethics As a Macroethics

The digital revolution provides huge opportunities to improve private and public life, and our environments, from health care to smart cities and global warming. Unfortunately, such opportunities come with significant ethical challenges. In particular, the extensive use of increasingly more data—often personal, if not sensitive (Big Data)—the growing reliance on algorithms to analyse them in order to shape choices and to make decisions (including machine learning, AI, and robotics), and the gradual reduction of human involvement or oversight over many automatic processes, pose pressing questions about fairness, responsibility, and respect of human rights.

These ethical challenges can be addressed successfully by fostering the development and application of digital innovations, while ensuring the respect of human rights and the values shaping open, pluralistic, and tolerant information societies. Striking such a balance is neither obvious nor simple. On the one hand, overlooking ethical issues may prompt negative impact and social rejection. This was the case, for example, with the NHS care.data programme, a failed project in England to extract data from GP surgeries into a central database. On the other hand, overemphasizing the protection of individual or collective rights in the wrong contexts may lead to regulations that are too rigid, and this may harm the chances to harness the social value of digital innovation. The LIBE amendments, initially proposed to the European Data Protection Regulation, offer a good example, as they would have made data-based medical

L. Floridi (✉) · C. Cath · M. Taddeo
Oxford Internet Institute, Digital Ethics Lab, University of Oxford, Oxford, UK

The Alan Turing Institute, London, UK
e-mail: luciano.floridi@oii.ox.ac.uk

C. Öhman, D. Watson (eds.), *The 2018 Yearbook of the Digital Ethics Lab*,
Digital Ethics Lab Yearbook, https://doi.org/10.1007/978-3-030-17152-0_2

research more difficult.[1] *Social preferability* must be the guiding principle to strike a robust ethical balance for any digital project with impact on human life.

The demanding task of digital ethics is navigating between social rejection and legal prohibition in order to reach solutions that maximise the ethical value of digital innovation to benefit our societies, all of us, and our environments. To achieve this, digital ethics builds on the foundation provided by Computer and Information Ethics, which has focused, for the past 30 years, on the challenges posed by information and communication technologies (Floridi 2013; Bynum 2015). This valuable legacy grafts digital ethics onto the great tradition of ethics more generally. At the same time, digital ethics refines the approach endorsed in Computer and Information Ethics, by changing the Levels of Abstraction (LoA) of ethical enquiries from an information-centric (LoA_I) to a digital-centric one (LoA_D).

The method of abstraction is a common methodology in Computer Science (Hoare 1972) and in Philosophy and Ethics of Information (Floridi 2008, 2011). It specifies the different perspective from which a system can be analysed, by focusing on different aspects, called observables. The choice of the observables depends on the purpose of the analysis and determines the choice of LoA. Any given system can be analysed at different LoAs. For example, an engineer interested in maximising the aerodynamics of a car may focus upon the shape of its parts, their weight, and the materials. A customer interested in the aesthetics of the same car may focus on its colour and the overall look, while disregarding the engineer’s observables.

Ethical analyses are developed at a variety of LoAs. The shift from Information (LoA_I) to Digital (LoA_D) is the latest in a series of changes that characterise the evolution of Computer and Information Ethics. Research in this field first endorsed a human-centric LoA (Parker 1968), which addressed the ethical problems posed by the dissemination of computers in terms of professional responsibilities of both their designers and users. The LoA then shifted to a computer-centric one (LoA_C) in the mid 1980s (Moor 1985), and changed again at the beginning of the second millennium to LoA_I (Floridi 2006).

These changes responded to rapid, widespread, and profound technological transformations. And they had important conceptual implications. For example, LoA_C highlighted the nature of computers as universal and malleable tools, making it easier to understand the impact that computers could have on shaping social dynamics and on the design of the environment surrounding us (Moor 1985). Later on, LoA_I shifted the focus from the technological means (the hardware: computers, mobile phones, etc.) to the content (information) that can be created, recorded, processed, and shared through such means. In doing so, LoA_I emphasised the different moral dimensions of information—i.e., information as the source, the result, or the

[1] European Parliament, Committee on Civil Liberties, Justice and Home Affairs. (2012). On the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012-2012/0011(COD)). Amendments 27, 327, 328, and 334–3367 proposed in the Albrecht’s Draft Report, Retrieved from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

target of moral actions—and led to the design of a macro-ethical approach, able to address the whole cycle of information creation, sharing, storage, protection, usage, and possible destruction (Floridi 2006, 2013).

We have come to understand that it is not a specific technology (now including online platforms, cloud computing, Internet of Things, AI, and so forth), but the whole ecosystem created and manipulated by any digital technology that must be the new focus of our ethical strategies. The shift from *information* ethics to *digital* ethics highlights the need to concentrate not only on what is being handled as the true invariant of our concerns but also on the general environment (infosphere), the technologies and sciences involved, the corresponding practices and structures (e.g. in business and governance), and the overall impact of the digital world broadly construed. It is not the hardware that causes ethical problems, it is what the hardware does with the software, the data, the agents, their behaviours, and the relevant environments that prompts new ethical problems. Thus, labels such as "robo-ethics" or "machine ethics" miss the point. We need a digital ethics that provides a holistic approach to the whole universe of moral issues caused by digital innovation.

$\mathrm{LoA_D}$ brings into focus the different moral dimensions of the whole spectrum of digital realities. In doing so, it highlights that ethical problems—such as anonymity, privacy, responsibility, transparency, and trust—concern a variety of digital phenomena, and hence they are better understood at that level. So, digital ethics is best understood as the branch of ethics that studies and evaluates moral problems related to *information and data* (including generation, recording, curation, processing, dissemination, sharing, and use), *algorithms* (including AI, artificial agents, machine learning, and robots), and corresponding *practices* and *infrastructures* (including, responsible innovation, programming, hacking, professional codes, and standards), in order to formulate and support morally good solutions (e.g., right conduct or right values). This means that the ethical challenges posed by the digital revolution can be mapped within the conceptual space delineated by three axes of research: the ethics of data/information, the ethics of algorithms, and the ethics of practises and infrastructures.

The ethics of data focuses on ethical problems posed by the collection and analysis of large datasets and on issues ranging from the use of Big Data in biomedical research and social sciences (Mittelstadt and Floridi 2016), to profiling, advertising, data donation, and open data. In this context, key issues concern possible re-identification of individuals through data-mining, −linking, −merging, and re-using of large datasets, and risks for so-called "group privacy", when the identification or profiling of types of individuals, independently of the de-identification of each of them, may lead to serious ethical problems, from group discrimination (e.g. ageism, racism, sexism) to group-targeted forms of violence (Floridi 2014; Taylor et al. 2017). Trust (Taddeo 2010; Taddeo and Floridi 2011) and transparency (Turilli and Floridi 2009) are also crucial topics, in connection with an acknowledged lack of public awareness of the benefits, opportunities, risks, and challenges associated with the digital revolution. For example, transparency is often advocated as one of the measures that may foster trust. However, it is unclear what information should be made transparent and to whom information should be disclosed.

The ethics of algorithms addresses issues posed by the increasing complexity and autonomy of algorithms broadly understood (e.g., including AI and artificial agents such as Internet bots), especially in the case of machine learning applications. Crucial challenges include the moral responsibility and accountability of both designers and data scientists with respect to unforeseen and undesired consequences and missed opportunities (Floridi 2012, 2016); the ethical design and auditing of algorithms; and the assessment of potential undesirable outcomes (e.g., discrimination or the promotion of anti-social content).

Finally, the ethics of practices (including professional ethics and deontology) and infrastructures addresses questions concerning the responsibilities and liabilities of people and organisations in charge of data processes, strategies, and policies, including businesses and data scientists, with the goal of defining an ethical framework to shape professional codes that may ensure ethical practises fostering both the progress of digital innovation and the protection of the rights of individuals and groups (Cath et al. 2017). Here four issues are central: solutions by design, consent, user privacy, and secondary use or repurposing.

While they are distinct lines of research, the ethics of data, algorithms, practices and infrastructures are obviously intertwined, and this is why it may be preferable to speak in terms of three axes defining a conceptual space within which ethical problems are like points identified by three values. Most of them do not lie on a single axis. For these reasons, Digital Ethics must address the whole conceptual space, albeit with varying priorities and foci. As such, it needs to be developed from the start as a *macroethics*, that is, as an overall "geometry" of the ethical space that avoids narrow, *ad hoc* approaches, but rather addresses the diverse set of ethical implications of digital realities within a consistent, holistic, and inclusive framework. An example may help to clarify the value of the holistic approach of Digital Ethics. Consider the case of protecting users privacy on social media platforms. In order to be able to understand the problem adequately and to indicate possible solutions, ethical analyses of users' privacy will have to address data collection, access, and sharing. They will have to focus also on users' consent and the responsibilities on online service providers (Taddeo and Floridi 2015, 2017). At the same time, aspects such as ethical auditing of algorithms and oversight mechanism for algorithmic decisions will be central to the analyses, as they may be part of the solution.

In order to give a better sense of the specific issues discussed in Digital Ethics, the following sections focus on two key areas of application: Internet Infrastructure, and Cyber Conflicts. They are not the only ones, but they should provide a clear sense of the scope and significance of this new area of investigation.

2.2 Digital Infrastructure

Increasingly, digital data infrastructures, like the Internet, are part of what makes our societies prosper (Castells 2007). And as this network-of-networks becomes more important—from managing our critical infrastructures like the electricity grid to managing our private lives—so does the ethics of its technical governance (Cath and Floridi 2017).

The management of the infrastructure of the Internet depends on choice (Lessig 2006) and control (Deibert et al. 2008; Choucri and Clark 2012). It is about how one decides to build the infrastructure through which data travels, and how it does so. The Internet influences who can connect to whom, and how (Denardis 2014). In turn, these choices can have a fundamental impact on the Internet's ability to foster the public interest, especially in terms of social justice, civil liberties, and human rights (Chadwick 2006; Denardis 2014). Control matters too. Internet infrastructure is increasingly becoming 'politics by other means' (Abbate 2000). Understanding the ethics of the practices embedded in the technology underlying the Internet's digital information flows is vital in order to understand and ultimately improve societal and political developments.

To understand this specific axe of digital ethics we need to address professional responsibilities and deontology (Floridi 2012) of those actors involved in coding, maintaining, and updating the Internet's infrastructure, including its applications and platforms. This requires an in-depth understanding of the inner-workings of the Internet. The Internet is not one network but a global network of networks that are bound together through standards and protocols, relying on hardware and software for information flows. Its decentralized, complex, and multi-layered character explains why its maintenance takes many actors and organizations. Considering the complexity of this system, a taxonomy that explains the Internet by dividing it into three distinct layers provides the needed level of abstraction: content, logical, physical (Benkler 2000). This model divides the Internet into three layers: the content layer (information to interact with), the logical infrastructure layer (software), physical infrastructure (wires, cables).

Layer	Description
Content	News, social media posts, videos on streaming platforms, content generated in collaborative tools like Wikipedia or on digital labour platforms
Logical	The technology that makes the Internet interoperable, its digital infrastructure
Physical	The tangible Internet, its physical infrastructure: Computers (servers, personal computers, mobile phones, etc.), telecommunications cables, routers, data centres

Each layer raises specific ethical questions about data, but not all the associated discussions have dedicated institutional homes, and often cut across the various layers and organizations (Mathiason 2008). There has been a concerted political effort over the last decade to highlight how human rights frameworks apply to the Internet. Yet more work remains to be done about how the ethics of data and associated ethics of practices of the various actors mentioned in the taxonomy (Cath and Floridi 2017). There is also limited engagement with the ethical questions surrounding material infrastructures through which data flows. Addressing these questions could alleviate some of the concerns surrounding private ordering of data flows and information control by the Internet's technical and business community, increase trust in the decisions of these private actors (Taddeo and Floridi 2011), and make the overall technical infrastructure of the network more stable, as it combines moral values with an ethical infrastructure to support the instantiation of moral behaviour (Floridi 2012). Such an analytical manoeuvre is particularly important as the infrastructure of the Internet increasingly enacts its social ordering upon the world (Denardis 2014; Hofmann et al. 2016).

2.3 Cyber Conflicts

Cyber conflicts arise from the use of digital technologies for immediate (tactic) or intermediate (strategic) disruptive or destructive purposes. When compared to conventional warfare, cyber conflicts show fundamental differences: their domain ranges from the virtual to the physical; the nature of their actors and targets involves artificial and virtual entities alongside human beings and physical objects; and their level of violence may range from non-violent to potentially highly violent phenomena.

These differences are redefining our understanding of key concepts like harm, violence, combatants, and weapons. They also pose serious ethical and policy problems concerning *risks*, *rights*, and *responsibilities* (the 3R problems) (Taddeo 2012). Start from the risks. Estimates indicate that the cyber security market will be worth US$170 billion by 2020 (Markets and Markets 2015), posing the risk of a progressive weaponisation of cyberspace, which may spark a cyber arms race and competition for digital supremacy, further increasing the possibility of escalation and conflicts (Taddeo 2017a, b; Taddeo and Floridi 2018). At the same time, cyber threats are pervasive. They can target, but can also be launched through, civilian infrastructures. This may (and in some cases already has) initiate policies of higher levels of control, enforced by governments in order to detect and deter possible threats. In these circumstances, individual rights, such as privacy and anonymity, come under devaluing pressure (Arquilla 1999). Ascribing responsibilities is also problematic, because cyber conflicts are increasingly waged through autonomous systems (Cath et al. 2017). Two good examples are the Active Cyber Defence programmes developed in the US and UK, and 'counter autonomy' systems, which are autonomous machine-learning systems able to engage in cyber conflicts by adapting and evolving to deploy and counter ever-changing attack strategies. In both cases, it is unclear who or what is accountable and morally responsible for the actions performed by these systems.

If left unaddressed, the 3R problems will daunt attempts to regulate cyber conflicts, favour escalation, and jeopardize international stability. Digital ethics offers a valuable framework to address the 3R problems, as these span across the conceptual space identified at the beginning of this chapter, namely data, algorithms, and practices.

More specifically, as state-run cyber operations will rely on machine learning and neural network algorithms, focusing on ethics of algorithms will be crucial to mitigate issues concerning the risks of escalation. This is because ethical analyses of algorithms foster the design and deployment of verification, validation, and auditing procedures that can ensure transparency, oversight, on autonomous systems deployed for threat detection and target identification. The ethics of data offers the conceptual basis to solve the friction between cyber conflicts and rights. For it sheds light on the moral stance of digital objects, (artificial) agents, and infrastructures involved in cyber conflicts and, in doing so, it facilitates the application of key principles of Just War Theory—such as proportionality, self- defence, discrimination—to cyber conflicts (Taddeo 2014, 2016). The ethics of practices plays a central role in the regulation of cyber conflicts, as it fosters the understanding of roles and responsibilities of the different stakeholders (private companies, governmental agencies, and citizens) and, thus, shapes the ethical code that should inform their conduct. These problems need to be addressed now, while still nascent, to ensure fair and effective regulations.

2.4 Conclusion

This chapter provided an overview of digital ethics, a new and fast developing field of research that is of vital importance to develop our information societies well, to improve our interactions among ourselves and with our environments, to protect human dignity and to foster human flourishing in the digital age. Much work lies ahead, and progress will require multidisciplinary collaboration among many fields of expertise and a sustained, unflinching focus on the value that ethical thinking can and should make in the world and in technological innovation.

References

Abbate, Janet. 2000. *Inventing the internet*. Cambridge, Mass: The MIT Press.

Arquilla. 1999. Ethics and information warfare. In *Strategic appraisal: The changing role of information in warfare*, ed. Zalmay Khalilzad and John Patrick White, 379–401. Santa Monica, CA: RAND.

Benkler, Yochai. 2000. From consumers to users: Shifting the deeper structures of regulation towards sustainable commons and user access. *Federal Communications Law Journal* 52: 3.

Bynum, Terrell. 2015. Computer and information ethics. In *The Stanford encyclopedia of philosophy*. http://plato.stanford.edu/archives/win2015/entries/ethics-computer/.

Cath, Corinne, and Luciano Floridi. 2017. The design of the internet's architecture by the Internet Engineering Task Force (IETF) and human rights. *Science and Engineering Ethics* 24 (2): 449–468.

Castells, Manuel. 2007. Communication, power and counter-power in the network society. *International Journal of Communication* 1 (1): 238–266.

Cath, Corinne, Sandra Wachter, Brent Mittelstadt, Mariarosaria Taddeo, and Luciano Floridi. 2017. Artificial intelligence and the "Good society": The US, EU, and UK approach. *Science and Engineering Ethics*: 1–24.

Chadwick, Andrew. 2006. *Internet politics: States, citizens, and new communication technologies*. Oxford: Oxford University Press.

Choucri, N., Clark, D. 2012. *Integrating cyberspace and international relations: The Co-Evolution*. Working Paper No. 2012–29, Political Science Department, Massachusetts Institute of Technology. Retrieved from http://ssrn.com/abstract=2178586

Deibert, Ronald. 2008. *Access denied: The practice and policy of global internet filtering*. Cambridge, Mass: MIT Press.

Denardis, Laura. 2014. *The global war for internet governance*. New Haven: Yale University Press.

Floridi, Luciano. 2006. Information ethics, its nature and scope. *SIGCAS Computer Society* 36 (3): 21–36.

———. 2008. The method of levels of abstraction. *Minds and Machines* 18 (3): 303–329.

———. 2011. "The philosophy of information". Oxford/New York: Oxford University Press.

———. 2012. Distributed morality in an information society. *Science and Engineering Ethics* 19 (3): 727–743.

———. 2013. *The ethics of information*. Oxford: Oxford University Press.

———. 2014. Open data, data protection, and group privacy. *Philosophy & Technology* 27 (1): 1–3. https://doi.org/10.1007/s13347-014-0157-8.

———. 2016. Faultless responsibility: on the nature and allocation of moral responsibility for distributed moral actions. *Philosophical Transactions of the Royal Society A* 374 (2083): 20160112.

Hoare, Charles Antony Richard. 1972. Structured programming. In *Structured programming*, ed. O.J. Dahl, E.W. Dijkstra, and C.A.R. Hoare, 83–174. London: Academic. http://dl.acm.org/citation.cfm?id=1243380.1243382.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. 2016. Between coordination and regulation: Finding the governance in internet governance. *New Media & Society* 19 (9): 1406–1423.

Lessig, Lawrence. 2006. *Code: And other Laws of cyberspace, version 2.0*. New York: Basic Books.

Markets and Markets. 2015. 'Cyber security market by solutions & services - 2020'. http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gclid=CNb6w7mt8MgCFQoEwwodZVQD-g.

Mathiason, John. 2008. *Internet governance: The new frontier of global institutions*. Routledge.

Mittelstadt, Brent Daniel. 2016. In *The ethics of biomedical big data*, Law, governance and technology series, ed. Luciano Floridi, vol. 29. Cham: Springer.

Moor, James H. 1985. What is computer ethics? *Metaphilosophy* 16 (4): 266–275.

Parker, Donn B. 1968. Rules of ethics in information processing. *Communications of the ACM* 11 (3): 198–201. https://doi.org/10.1145/362929.362987.

Taddeo, Mariarosaria. 2010. Trust in technology: A distinctive and a problematic relation. *Knowledge, Technology & Policy* 23 (3–4): 283–286. https://doi.org/10.1007/s12130-010-9113-9.

———. 2012. Information warfare: A philosophical perspective. *Philosophy and Technology* 25 (1): 105–120.

———. 2014. Just information warfare. *Topoi* 35 (1): 213–214.

———. 2016. On the risks of relying on analogies to understand cyber conflicts. *Minds and Machines* 26 (4): 317–321.

———., ed. 2017a. *The responsibilities of online service providers*. New York/Berlin/Heidelberg: Springer.

———. 2017b. Cyber conflicts and political power in information societies. *Minds and Machines* 27 (2): 265–268.

Taddeo, Mariarosaria, and Luciano Floridi. 2011. The case for E-trust. *Ethics and Information Technology* 13 (1): 1–3.

———. 2015. The debate on the moral responsibilities of online service providers. *Science and Engineering Ethics* (November). https://doi.org/10.1007/s11948-015-9734-1.

———, eds. 2017. *The responsibilities of online service providers*. New York: Springer Berlin Heidelberg.

———. 2018. Regulate artificial intelligence to avert cyber arms race. *Nature* 556 (7701): 296–298. https://doi.org/10.1038/d41586-018-04602-6.

Taylor, Linnet, Luciano Floridi, and Bart van der Sloot, eds. 2017. *Group privacy: New challenges of data technologies*. Hildenberg: Philosophical Studies, Book Series, Springer.

Turilli, Matteo, and Luciano Floridi. 2009. The ethics of information transparency. *Ethics and Information Technology* 11 (2): 105–112.