8

Just Don't Get Caught!

Barbora Bad'urová

8.1 INTRODUCTION

We can observe various forms of harm, wrongdoing and crime in the digital environment, violating traditional or newly modified digital human rights.[1] 'Globalisation, digitalisation and smart technologies have escalated the propensity and severity of cybercrime.'[2] A serious increase in cybercrime and cyberattacks has been reported,[3] and estimations for the year 2020 predicted that cybercrime would cost the global economy around US$1 trillion, which is a 50 per cent increase in comparison with 2018.[4] However, the financial impact is not the only problem resulting from the unregulated possibilities in the digital world. For instance, as stated in 2018, around 45 per cent of adult internet users in the UK had experienced some form of online harm;[5] potential harm is affecting not just adults but also children,[6] and not just private individuals but also larger entities such as companies, organisations, and so on. The harm can also be psychological, social, ethical, and medical.

[1] Department for Digital Culture, Media and Sport, 'Online harms feasibility study' (2021), https://assets.publishing.service.gov.uk/media/639b0511e90e072180b2a7c6/DCMS_Online_Harm_Feasibility_study_v2.pdf.

[2] F. Cremer et al., 'Cyber risk and cybersecurity: a systematic review of data availability' (2022) 47 *The Geneva Papers on Risk and Insurance – Issues and Practice*, 698–736, at 698.

[3] E. Decker, 'Full count? Crime rate swings, cybercrime misses and why we don't really know the score' (2018) 5 *Journal of National Security, Law and Policy*, 583–604.

[4] Cremer et al., 'Cyber risk and cybersecurity', p. 698.

[5] Kantar Media, 'Internet users' experience of harm online: summary of survey research' (2018), www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-harms/2018/internet-harm-research-2018-report.pdf?v=323453, 66.

[6] J. Holdoš (ed.), 'EU kids online Slovensko – správy z výskumu' (2022), https://euko.ku.sk/wp-content/uploads/2022/04/EU-Kids-Online-Slovensko-spravy-z-vyskumu_ed_J_Holdos.pdf; V. Gill, L. Monk, and L. Day, 'Qualitative research project to investigate the impact of online harms on children' (2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1167838/Online_Harms_Study_Final_report_updated_51222_updated_290623.pdf; N. Hudson et al., 'Content and activity that is harmful to children within scope of the Online Safety Bill: a rapid evidence assessment', 27 May 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1123421/Content_and_Activity_that_is_Harmful_to_Children_within_Scope_of_the_Online_Safety_Bill__REA__accessible_.pdf.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

Many experts, leaders, stakeholders, even laypeople claim that legal restrictions are what would help. At first glance, legal regulations have several advantages:

- they provide clear guidelines for everyone,
- they set national/international standards,
- the legal system is based on institutions,
- having an authoritative institution facilitates reporting violations of rights.

The legal system clearly has the advantage that rules when well written are transparent and clear to everyone, and provide a set of standards and guidelines about what is prohibited and permitted in the digital realm.[7] The legal rules provide national and international standards of conduct, which can be helpful to orientate agents, citizens, and other legal persons. Rules can be guaranteed by institutions, which represent the distribution of power between the legislature, executive, and judiciary. As pointed out by many social contract theorists (e.g., John Locke),[8] it is reasonable to transfer certain duties; for example, judging and punishing wrongdoers, to an entity that is above individuals and thus independent and acts in a just and commensurate manner. The violation of rights can then be claimed to the authority, and the authority provides protection for individuals. For instance, internet fraud, such as stealing an identity, can be reported to the police, and they can then act accordingly to execute the law.

8.2 PROBLEMS ASSOCIATED WITH THE LEGAL REGULATION OF THE DIGITAL REALM

However, there is also the other side of the coin that legal restrictions are not an ideal and flawless solution. The problems associated with legal rules include, for instance:

- the development of legal regulations is too slow,[9]
- legal standards are not yet developed because the cause of human rights violations in the online realm is not yet adequately understood,[10]

[7] Of course, it depends also on the legal system: some systems are more focused on precedents and also consider the constitution as a living tree.

[8] J. Locke, *Two Treatises of Government* (Cambridge: Cambridge University Press, 1967), p. 525.

[9] See, e.g., L. B. Moses, 'Adapting the law to technological change: a comparison of common law and legislation' (2003) 26 *UNSW Law Journal* 2, 394–417; S. Greenstein, 'Preserving the rule of law in the era of artificial intelligence' (2022) 30 *Artificial Intelligence and Law*, 291–323, at 396.

[10] T. Pajuste (ed.), 'Specific threats to human rights protection from the digital reality: international responses and recommendations to core threats from the digitalised world' (2022), https://graphite.page/gdhrnet-threats-to-human-rights-protection/, p. 9; A. Strowel and W. Vergote, 'Digital platforms: to regulate or not to regulate? Message to regulators: fix the economics first, then focus on the right regulation' (2016), https://ec.europa.eu/information_society/newsroom/image/document/2016-7/uclouvain_et_universit_saint_louis_14044.pdf.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

- the field and the legal context is country specific,[11]
- there can be vagueness, limited scope, and conflicting interpretations of the law,[12]
- law enforcement can be problematic,[13]
- some crimes go unreported.[14]

The problem of the regulation of digital issues stems from the rapid exponential growth of what is possible with digital technology and the comparatively slow development of legal restrictions. 'As technological developments take place faster than regulation can catch up, the guidelines and rules that have been adopted have not provided solutions to many of the issues, including the human rights implications of digital activities."[15]

A related problem is that the restriction of certain areas focusing on, for instance, the regulation of digital human rights is not yet fully understood, and thus the regulation is not yet developed in some areas at all. As an example, we could mention that 'a threat of cancel culture and social engineering in the context of elections where the harm of manipulated voting is obvious but how exactly the prohibited acts should be defined or how they could be prevented is an open question. Similarly, a question to what extent the risk of addiction to the Internet could provide entitlements to health care services."[16]

A more general problem of the law and legal restrictions is that situations are often country specific, and it is difficult to find common ground for legal norms in the international global context. Countries have citizens and inhabitants with various beliefs and they represent the plurality of diverse cultures. Other problems related to legal rules stem from how they are written and presented, and this is related to uncertainty, limited scope, or divergent interpretations of law. Another interesting aspect of law, the legal system, and the state distribution of power is law enforcement. The problem is thus not only whether the legal rules are well made, timely, and targeting relevant issues, but also whether the violation of the law is treated in a relevant manner and the criminals punished.

[11] See, e.g., Y. Shany, 'Digital rights and the outer limits of international human rights law' (2023) 24 *German Law Journal* 3, 461–72, at 464; J. Kleijssen and P. Perri, 'Cybercrime, evidence and territoriality: issues and options' (2017) 47 *Netherlands Yearbook of International Law*, 147–73, at 155.

[12] Pajuste (ed.), 'Specific threats to human rights protection', p. 9; M. Greenberg, 'Legal interpretation' (2021), *Stanford Encyclopedia of Philosophy*, https://plato.stanford.edu/entries/legal-interpretation/.

[13] A. Ivanov, D. Gorelik, and K. Prokofiev, 'Law enforcement in the context of digitalization: problems and prospects for improving efficiency' (2020) 171 *Advances in Economics, Business and Management Research, volume*, Proceedings of the 1st International Scientific Conference 'Legal Regulation of the Digital Economy and Digital Relations: Problems and Prospects of Development' (LARDER 2020); V. Ceccato, 'Special issue: crime and control in the digital era' (2019) 20 *Criminal Justice Review* 10, 1–6, at 3.

[14] US Department of Justice, 'Report of the Attorney General's cyber digital task force' (2018), www.justice.gov/archives/ag/page/file/1076696/dl.

[15] Pajuste, 'Specific threats to human rights protection', p. 4.

[16] Ibid., p. 9.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

Similarly, the detection of a violation of the law needs to be well monitored in order to catch the criminal. If the system fails, for instance, if the victim does not report a bully because the victims are not aware of their rights or are afraid to do so, the legal regulation does not fully help diminish the problem. In the digital world, the problem of unreported violations and harms can be quite fruitful owing to its potential for anonymity. According to the US Federal Bureau of Investigation (FBI), approximately only one in seven cybercrimes were reported in 2017.[17]

This prompts a question: How can we achieve better regulation of the digital realm?

It seems there are multiple possible solutions, and they can be summed up as follows within the framework of a better legal system:

- better regulation, better laws, and law enforcement,
- developing better legal standards,
- better law enforcement,
- stricter regulation and control.

There are many emerging developments in the national and international context of aiming to better regulate the digital environment.[18] However, as ideal as it may seem at first sight, these approaches also have their Achilles heels, including:

- not all societies and citizens are developed enough to be able to follow the law and manage proper law enforcement,[19]
- the motivation for action is mostly – not to get caught.

It is obvious that some societies are suffering with greater problems of law enforcement. For instance, this is related to the high level of corruption that affects the impartiality, justness, and fairness in the decision-making of responsible agents.[20]

[17] FBI, 'Internet crime: IC3 a virtual complaint desk for online fraud' (2017), www.fbi.gov/news/stories/ic3-virtual-complaint-desk-for-online-fraud.

[18] See, e.g., M. L. Chiarella, 'Digital Markets Act (DMA) and Digital Services Act (DSA): New rules for the EU digital environment' (2023) 9 *Athens Journal of Law* 1, 33–58; 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 acts (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206; Council of the EU, Press Release, 'DSA: Council gives final approval to the protection of users' rights online' (2022), www.consilium.europa.eu/en/press/press-releases/2022/10/04/dsa-council-gives-final-approval-to-the-protection-of-users-rights-online/.

[19] This can be illustrated by the differences in the trust that citizens have in the police in different countries, see, e.g., D. Schaap and P. Scheeper, 'Comparing citizens' trust in the police across European countries: an assessment of cross-country measurement equivalence' (2014) 24 *International Criminal Justice Review* 1, 82–98; R. I. Mawby, 'Comparing police systems across the world', in G. Bruinsma and D. Weisburd (eds.), *Encyclopedia of Criminology and Criminal Justice* (New York, NY: Springer, 2014), pp. 478–88.

[20] See, e.g., Transparency International, 'Corruption Perceptions Index' (2022), www.transparency.org/en/cpi/2022.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

8.3 THE PROBLEM OF SURVEILLANCE

One option would be to say, all right, we can still make it work and focus on the following:

- monitoring agents,
- even stricter regulations – cameras, tracking devices everywhere, use of facial recognition,[21]
- provide better control and data about who is doing what, so that the responsible institutions can protect citizens and other stakeholders.

There is quite a fruitful debate currently regarding surveillance systems, for instance in China, but also other countries. As pointed out by Peter Königs, non-democratic states nowadays and in recent history 'known for their extensive surveillance systems include the GDR, the People's Republic of China, the Soviet Union, and North Korea. In the past few decades, however, established liberal democracies have been increasingly ready to monitor their citizens on a massive scale. One notorious surveillance program run by an alliance of democracies was uncovered by Edward Snowden.'[22] The proponents of surveillance present arguments regarding greater safety and crime prevention, and the resulting benefits for everyone involved. Unfortunately, such Big Brother concepts are not ideal.[23] 'Government surveillance and the erosion of privacy it is associated with are being discussed as a cause of distrust and feelings of vulnerability, as a potential source of discrimination and unjust domination, and as a threat to democracy and the integrity of the public sphere, to name but a few concerns.'[24] Therefore, as mentioned earlier, reducing harms in the digital realm by increasing surveillance also has its downsides, which stem from:

- the right to privacy,[25]
- possible abuses of information, data, systems.[26]

The concept of the protection of privacy is central in relation to human rights, and relates to the threat of the abuse of information, its manipulation, use in an

[21] See, e.g., A. M. Jansen et al., 'The influence of the presentation of camera surveillance on cheating and pro-social behavior' (2018) 9 *Frontiers in Psychology*, Article 1937; T. Golda et al., 'Perception of risks and usefulness of smart video surveillance systems' (2022) 12 *Applied Sciences* 20, Article 10435; C. Ziller and M. Helbling, 'Public support for state surveillance' (2021) 60 *European Journal of Political Research* 4, 994–1006.

[22] P. Königs, 'Government surveillance, privacy, and legitimacy' (2022) 35 *Philosophy & Technology*, 1, Article 8.

[23] For educational aspects regarding surveillance see workshop proposal related to the Erasmus+ project PLATO'S EU, that I got a chance to test at the University of Skovde, Sweden and Frederick University, Cyprus.

[24] Königs, 'Government surveillance, privacy, and legitimacy', section 1.

[25] See, e.g., S. Quach et al., 'Digital technologies: tensions in privacy and data' (2022) 50 *Journal of the Academy of Marketing Science* 6, 1299–323.

[26] See, e.g., Königs, 'Government surveillance, privacy, and legitimacy'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

inappropriate context, even stealing an identity. For instance, the idea of transparency is helping not to conflate the protection of privacy by masking other inappropriate actions, such as cheating, stealing, and other forms of wrongdoing.

8.4 MOTIVATIONS

Another aspect of this problem relates to what motivates a person or agent in the digital world. The motivation not to get caught.

If the agents are mostly motivated to not do certain things (e.g., cheat online) by the idea of not getting caught, they may try to find ways to avoid punishment. The problem is in the system but also in human character. For instance, the ancient philosopher Aristotle already sketched the problem of the human character in relation to the state.[27]

Even with controlling devices and greater surveillance, there is a danger that the people who work with them can manipulate the data or evidence, and can be bribed to do so. So there is the question of who controls those who are in power and those who should control others. Of course, there again the solution of the division of power emerges, but as we can observe even that can be abused if individuals with an unsuitable character end up in these roles.

When we consider the legal restrictions, we may ask: What is the motivation to act legally?

It seems that the motivation is, as already sketched out, not to get caught. We can, of course, speculate and consider that in the end it is not important to act based on certain motives, but the consequences are what matters. Even if we act in compliance with the law and out of a fear of punishment, we can still act well and the consequences can be good. Nevertheless, it seems this is not always optimal either, as there is still room to act in ways that are not so beneficial for society if we expect no one can catch us.

Therefore, we may go further and ask: What if no one can see us?

The digital world offers us several potential threats that are often not so prevalent offline, related to anonymity, the idea of 'no identity', or creating a 'new' identity.[28] It seems to be easier to remain anonymous using a fake identity online than offline. Of course, even in the pre-digital era, we could send anonymous (paper) letters, or wear masks, or modulate our voice; however, nowadays the possibilities in the online world are more numerous and can have a much greater impact. It is possible to identify an IP address or other digital traces; however, at the same time there are ways to avoid being spotted.

[27] Aristotle, *The Nicomachean Ethics* (London: Penguin Books, 2004).

[28] See, e.g., A. Lareki et al., 'Fake digital identity and cyberbullying' (2022) 45 *Media, Culture & Society* 2, 338–53.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

8.5 INDIVIDUAL REGULATION

There are various forms of regulation online, but they are also related to different motivations. Since the idea of regulation presented here is not flawless, we should consider other options. Therefore, there emerges the issue of individual regulation.

Our motivation should be more than just to not get caught and could also include:

- individual responsibility,
- internal/intrinsic regulation/ motivation.

By individual responsibility, we mean the responsible behaviour of an individual, considering the consequences of his or her actions and being aware and able to be held accountable for them. The responsible person is aware of his or her own actions and makes qualified judgements and decisions. He or she does not rely only on external forms of authority, telling him or her what to do and what not, but also on rational understanding of the situation.

The idea of internal or intrinsic regulation and motivation exists in contrast with external, extrinsic regulation and motivation. An example of external, extrinsic regulation is a police officer standing at an intersection regulating the traffic, where it affects motivation, and people act in the requested manner in the given situation in order to not incur a fine or end up in jail.

On the other hand, the idea of intrinsic or internal regulation is about regulation not from outside but rather from inside. Therefore, to put it simply, there is no policeman on the street but our internal policeman or conscience tells us we should not exceed the speed limit. The reason is, for instance, because it will very likely endanger other passengers, pedestrians, or even ourselves, and it is not good to take such a risk without sufficient justification.

To imagine a situation in the digital realm, we can think of examples such as an authority checking the identity of a user by validating their credentials (e.g., password, biometric data, phone number) as a form of external regulation preventing users accessing another person's account. The motivation for not trying to access someone else's account is the fear of punishment. On the other hand, internal regulation in this situation is when the user is aware that it is not right to hack into another person's account and steal his or her identity or finances.

However, we may ask whether there is a necessary connection between internal regulation and internal motivation, or external regulation and external motivation. Of course, it seems it is not so straightforward, since it is possible to have, for instance, external regulation and at the same time internal motivation to act in compliance with the law.

At the same time, we also need to be aware that internal or intrinsic motivation and the related regulations also have some limits; for instance, they:

- need time and effort to develop,
- rely on people's conscience.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

There are also problems with regulations set and adopted by private companies; they can set their own standards and create diverse responses, as there are many (often mostly financial) interests. Then such rules are often referred to as 'ethics washing'; that is, they pretend the company is regulated to the benefit of society but in fact the benefit is only aimed at a narrow group of people. Despite the fact that this area is an interesting topic, in this chapter I will focus on the ethical regulation of individuals.

There have been quite fruitful discussions about the nature of intrinsic and extrinsic motivation.[29] The debate is not just at the conceptual level but also explores the emerging problem of how to deal with this in practice. The obvious question, therefore, is how we can implement internal regulation.

One plausible answer is that agents internalise existing rules and act according to them.[30] This seems quite a good idea at first sight. Citizens, agents become informed and educated about the legal norms in relation to the digital environment and understand the importance of them for themselves and others, and also understand that violating them will be punished, and they will internalise such rules and act accordingly.

Regarding the regulation and compliance motivation, there are many interesting ideas.[31] However, unfortunately, there are also some problems with this approach, as mentioned at the beginning of the chapter, such as the fact that:

- legal norms regarding the digital realm are evolving slowly,
- the legal system is evolving, but the legal norms are not always right,
- people can manipulate the rules,
- there is a problem with freedom and autonomy,
- internalising the rules may not be effective or efficient.

[29] See, e.g., F. Gomez and M. Artigot i Golobardes, 'Intrinsic and extrinsic motivations to comply with legal rules: comment on B. Deffains and D. Demougin, "Class Actions, Compliance, and Moral Cost"', in S. Grundmann, F. Möslein, and K. Riesenhuber (eds.), *Contract Governance: Dimensions in Law and Interdisciplinary Research* (Oxford: Oxford Academic, online edn., 2015), pp. 241–8; L. S. Morris et al., 'On what motivates us: a detailed review of intrinsic v. extrinsic motivation' (2022) 52 *Psychological Medicine* 10, 1801–16; R. Ryan and E. L. Deci, 'Intrinsic and extrinsic motivations: classic definitions and new directions' (2000) 25 *Contemporary Educational Psychology* 1, 54–67; R. Bénabou and J. Tirole, 'Intrinsic and extrinsic motivation' (2003) 70 *Review of Economic Studies* 3, 489–520; A. Van den Broeck et al,. 'Beyond intrinsic and extrinsic motivation: a meta-analysis on self-determination theory's multidimensional conceptualization of work motivation' (2021) 11 *Organizational Psychology Review* 3, 240–73; A. Turner, 'How does intrinsic and extrinsic motivation drive performance culture in organizations?' (2017) 4 *Cogent Education* 1, Article 1337543.

[30] See, e.g., S. Larcom et al., 'Follow the leader? Testing for the internalization of law' (2019) 48 *The Journal of Legal Studies* 1, 217–44; J. Benka et al., 'Internalization of rules and risk-behavior among early adolescents and relevance for public health' (2019), 29 *European Journal of Public Health*, Issue Supplement 4, 367–8; M. Kim, 'Legalization and norm internalization: an empirical study of international human rights commitments eliciting public support for compliance' (2019) 7 *Journal of Law and International Affairs* 2, 337–81.

[31] See, e.g., P. J. May, 'Regulation and compliance motivations: examining different approaches' (2005) 65 *Public Administration Review* 1, 31–44; P. J. May, 'Compliance motivations: affirmative and negative bases' (2004) 38 *Law & Society Review* 1, 41–68.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

Therefore, even this approach is problematic and is not a flawless solution.

It seems that we need something more. One idea is to use various nudges to motivate people to act in a desirable way; however, this can also be understood as manipulation and can be abused by the authorities or certain people.[32]

8.6 DIGITAL ETHICS AND EDUCATION

It seems that we need something else. And that could be ethics and moral norms.[33] What more do they add to legal regulation? They are often oriented towards internal regulation, and therefore can help even in situations when agents are in a setting where no one can see them, when there is no surveillance, and it can even help them deal with situations when there are no existing legal rules regulating their actions.

Therefore, when mentioning digital ethics as a solution, the question of whether it should fully replace legal regulation of the digital realm can emerge.[34] Of course not – both have their pros and cons, and therefore their mutual enrichment could be beneficial. They should be understood as complementing each other – internal should complement external regulation.

Similarly, we could mention Lawrence Kohlberg and his theory of moral development here, where he speaks about associating the lower stages with external regulation and the higher stages with the internal regulation of moral actions.[35] For instance, the pre-conventional level is oriented towards avoiding punishment and focused on obtaining praise, while the other stages are more oriented towards compliance with rules, the law for the benefit of society, and the highest stages are related to greater moral competence in moral judgements. How can we put ideas about digital ethics into practice?

There seem to be quite a rich debate regarding digital ethics regulating agents online, and many companies show they have a code of conduct dealing with such issues or that ethics committees exist; however, there is a risk of using this merely as

[32] L. Congiu and I. Moscati, 'A review of nudges: definitions, justifications, effectiveness' (2022) 36 *Journal of Economic Surveys* 1, 188–213.

[33] 'Ethics is generally understood to be the study of "living well as a human being". This is the topic of works such as Aristotle's Nicomachean Ethics, in which the aim of human beings is to exemplify human excellence of character.' – J. Driver, 'Moral theory' (2022), *Stanford Encyclopedia of Philosophy*, https://plato.stanford.edu/entries/moral-theory/. However, it is often understood more broadly as a discipline of practical philosophy dealing with right and wrong conduct.

[34] Digital ethics can be understood as a branch of practical or applied ethics, which deals with ethical issues related to digital technologies. As in other areas of practical ethics it is highly interdisciplinary and overlaps with or includes other areas of investigation as well as other areas of practical ethics (e.g., ethics of technology, ethics of AI, environmental ethics, ethics of law). Digital ethics is sometimes falsely interpreted as dealing only with etiquette online, so called netiquette. However, ethics is not possible to conflate with etiquette. Both deal with questions regarding right conduct but ethics deals more with the idea of harm, which is not that important in etiquette.

[35] L. Kohlberg, *The Philosophy of Moral Development* (New York, NY: Harper and Row, 1981).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

marketing to wash their hands so consumers do not question their actions.[36] At the same time, as mentioned earlier, although I think well-made self-regulation of companies can supplement the overall regulation of digital issues, here I will focus more on the regulation of individuals. So how can we make digital ethics work?

There is room for digital ethics education to help to implement the ideas of digital ethics. It should focus on:

- the development of internal regulation,
- critical thinking and moral judgement,
- a deeper understanding of ethical dilemmas in the digital realm.

There are various approaches to digital education and digital ethics education,[37] and various challenges emerge related to the following:

- targeting individuals on different levels – children, adults,[38]
- the means of teaching,
- dealing with disagreements,
- having qualified teachers,
- having good teaching materials.

It seems reasonable to focus not just on children but also on adult education in the area of digital ethics. There are several approaches to teaching ethics,[39] but I propose that ethics education be oriented towards the development of critical thinking and not merely training about ethics – indoctrination or rules without any critical examination and reflection. Reflection and critical analysis has the advantage of being flexible in seeking the best solution to moral dilemmas. Digital ethics

[36] In relation to AI digital ethics see, e.g., B. Wagner, 'Ethics as an escape from regulation. From "ethics-washing" to ethics-shopping?', in E. Bayamlioğlu, I. Baraliuc, and L. Janssens (eds.), *Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen* (Amsterdam: Amsterdam University Press, 2018), pp. 84–8.

[37] See, e.g., B. O'Brien, 'Digital ethics in higher education' (2020) *Educause Review*, https://er.educause.edu/articles/2020/5/digital-ethics-in-higher-education-2020; E. Zvereva, 'Digital ethics in higher education: modernizing moral values for effective communication in cyberspace' (2023) 13 *Online Journal of Communication and Media Technologies* 2, e202319; E. Wulandari and W. Triyanto, 'Digital citizenship education: shaping digital ethics in society 5.0' (2021) 9 *Universal Journal of Educational Research* 5, 948–56; D. Olcott, Jr et al., 'Ethics and education in the digital age: global perspectives and strategies for local transformation in Catalonia' (2015) 12 *RUSC* 2 Special Issue.

[38] See, e.g., K. Moore, 'The three-part harmony of adult learning, critical thinking, and decision-making' (2010) 39 *Journal of Adult Education* 1, 1–10; H. Boxler, 'Quest for the grail? Searching for critical thinking in adult education' (2002) *Adult Education Research Conference*, Conference Proceedings; D. R. Garrison, 'Critical thinking and adult education: a conceptual model for developing critical thinking in adult learners' (1991) 10 *International Journal of Lifelong Education* 4, 287–303; H. Tinmaz et al., 'A systematic review on digital literacy' (2022) 9 *Smart Learning Environments*, Article 21; T. Ott and M. Tiozza, 'Digital media ethics: benefits and challenges in school education' (2022) 14 *International Journal of Mobile and Blended Learning* 2, 1–8.

[39] See, e.g., the forthcoming book that I am editing with J. Irwin – *Ethical Education Across European Systems – Concepts, Practices, Dilemmas* (Lausanne: Peter Lang Publishing, 2025).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

education should be oriented towards critical thinking, where the focus is not primarily on what to think but rather on method or how to think.[40] It is also about focusing on understanding why. The potential for disagreements about what is right and what is wrong also needs to be taken into account; however, this approach should also help us learn how to communicate clearly, effectively, logically, and how to evaluate arguments.

However, what if the critical thinking collides with legal norms? It seems that in open societies it can even be desirable to have citizens who are able to critically evaluate the existing legal system and norms.[41]

Of course, the problem may be in finding qualified teachers and having good teaching materials and manuals. The lack in these areas is addressed for instance by various initiatives and projects: digital education is often oriented towards the technical or psychological aspects of using digital technologies, which is important since based on empirical findings in Slovakia, for example, 20 per cent of children do not know that they can block a contact on social media and 40 per cent do not know that they can report a case when someone is bullying them online.[42] At the same time, it is also important to address digital ethics with regard to what is right and what is wrong and why, and what we should do in a given situation. The problem of digital ethics education has been addressed by various projects, for instance, Erasmus+ PLATO'S EU, where the team has developed teaching materials and manuals for teachers as well as organizing workshops for students in order to promote philosophical methods of thinking as a tool for dealing with issues online.[43]

8.7 CONCLUSION

This chapter has explored the problem of digital regulation, and the idea of digital ethics and education has been proposed as a complementary solution.[44] The main idea presented is that we need to focus not just on external regulation and the

[40] See, e.g., L. M. Murawski, 'Critical thinking in the classroom … and beyond' (2014) 10 *Journal of Learning in Higher Education* 1, 25–30; K. Larsson, 'Understanding and teaching critical thinking – a new approach' (2017) 84 *International Journal of Educational Research*, 32–42; O. L. U. Enciso et al., 'Critical thinking and its importance in education: some reflections' (2017) 19 *Rastros Rostros* 34, 78–88; Y. E. L. Zuluaga et al., 'A study of critical thinking in higher education students' (2020) 16 *Revista Latinoamericana de Estudios Educativos* (Colombia) 2, 256–79; L. Campo et al., 'Methodologies for fostering critical thinking skills from university students' points of view' (2023) 13 *Education Sciences* 2, Article 132; J. Huang and G. Sang, 'Conceptualising critical thinking and its research in teacher education: a systematic review' (2022) 29 *Teachers and Teaching* 6, 638–60.

[41] See, e.g., B. Sheehy et al., 'Shifting from soft to hard law: motivating compliance when enacting mandatory corporate social responsibility' (2023) 24 *European Business Organization Law Review* 4, 693–719; A. S. Rosenberg, 'Motivational law' (2008) 56 *Cleveland State Law Review* 1, 111–36.

[42] Holdoš, 'EU kids online Slovensko', pp. 120, 137.

[43] Plato's EU website, https://platos-eu.org.

[44] As presented also in earlier material on the topic under GDHR – Pajuste, 'Specific threats to human rights protection', pp. 20–2.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

motivation to act in compliance with legal norms out of fear of being caught and punished, but also on the development of an internal moral compass in our citizens. Various advantages and disadvantages to the different approaches to regulation have been presented.

Legal norms are not considered in contrast with digital ethical regulation but as complementary. As mentioned in an earlier publication of the COST Global Digital Human Rights Network project: 'there is the inherently multidimensional nature of compliance with human rights in the digital realm, which requires a multidimensional response, including in the context of awareness raising and training. Law should be complemented by ethics and the training on cyber ethics should be provided along with training on digital human rights law.'[45]

Internal regulation and intrinsic autonomous motivation seem to be an important area for further development towards the regulation of the digital realm. The topic of internal regulation is very fruitful, and has been investigated by philosophers and ethicists since ancient times also in terms of people flourishing and realising their full human potential.

[45] Pajuste, 'Specific threats to human rights protection', pp. 9–10.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 11:23:39, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009606295.010