WHY DO WE NEED BOTH SOFT (POST-COMPLIANCE) ETHICS AND LEGAL COMPLIANCE IN THE DIGITAL TRANSFORMATION?

Harald Stelzer / Hristina Veljanova

Professor, University of Graz, Institute of Philosophy, Section Political Philosophy
Heinrichstraße 26/II, 8010 Graz, AT
harald.stelzer@uni-graz.at; https://philosophie-gewi.uni-graz.at/de/politische-philosophie/

Researcher, University of Graz, Institute of Philosophy, Section Political Philosophy
Heinrichstraße 26/II, 8010 Graz, AT
hristina.veljanova@uni-graz.at; https://philosophie-gewi.uni-graz.at/de/politische-philosophie/

Keywords: ***Soft (post-compliance) ethics, hard ethics, legal compliance, digital transformation***

Abstract: *With the adoption of the GDPR and other legal frameworks very high standards have been introduced to ensure data privacy and security. However, just complying with the law does not seem to be sufficient to address all ethical challenges raised by the digital transformation. Soft ethics operates on the post-compliance level and allows us to consider questions of distributive justice and discrimination, the distinction of the private and public sphere, transparency, autonomy, legitimate expectations or trustworthiness.*

1. The age of digital transformation

The digital transformation has undoubtedly introduced novel opportunities and ways to make use of digital technologies in various contexts in society. It has also disrupted and is disrupting many areas such as commerce, healthcare, banking, education, work etc. Moreover, we are constantly enticed by new devices, apps, services and technological advancements. But along with the numerous benefits associated with these new technologies also come novel risks and potential harms to our rights and interests.

All these innovations and technological opportunities mean that regulation has to keep pace with any challenges and risks technology brings about. The same applies to digital ethics. There are many ethical questions and dilemmas that arise in relation to new technologies and services to which answers are needed. Looking at all this, there are two questions in particular that call for urgent consideration: (1) How do we make better use of digital innovation while at the same time making sure that it reflects and respects those values and principles which we as society hold dear?, and (2) How can businesses make better use of digital innovation while staying within the limits of what is considered morally and socially acceptable? This paper will address these two questions by advocating a novel approach known as post-compliance (soft) ethics as a way to complement legal compliance.

2. Soft and hard ethics – setting the stage

In his paper «Soft Ethics and the Governance of the Digital» Luciano Floridi first introduced the distinction between hard and soft (post-compliance) ethics in the context of the digital.[1] His main argument is that in the efforts to steer society in the right direction compliance is necessary but it is not sufficient. Namely, regulation – and in the context of this paper digital regulation – sets up the rules of the game, that is, what the legal and illegal moves are, nevertheless, it does not specify the good and best moves and how one should play the game

[1] Floridi, «Soft Ethics and the Governance of the Digital», *Philosophy & Technology* 31(2018), 1–8.

in order to win. According to him, this is the job of digital ethics and digital governance. Floridi therefore distinguishes between soft and hard ethics. By hard ethics he understands «what we usually have in mind when discussing values, rights, duties and responsibilities – or, more broadly, what is morally right or wrong, and what ought or ought not to be done – in the course of formulating new regulations or challenging existing ones»[2]. So, hard ethics makes and shapes the law, or in other words, it is what goes in parallel with the law. Soft ethics, on the other hand, does not operate on the same level as the law, but it stipulates what ought and ought not to be done beyond the existing regulation. As such it addresses aspects that regulation does not directly or at all address. Therefore, soft ethics is also termed post-compliance ethics.

In a further article «Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage» Floridi applies soft and hard ethics as ethical framework to the General Data Protection Regulation (GDPR).[3] Thereby, he distinguishes five elements. The first element pertains to the ethical, legal and social *implications* the GDPR and its Articles have for businesses, for instance, by dictating how businesses should deal with EU citizens' data privacy. The second element comprises the *GDPR* itself and its 99 Articles. Since Articles in general do not and cannot cover all areas, they might need to be further interpreted in the process of their application. For that purpose, the GDPR contains 173 *Recitals*, which make up the third element. The aim of the Recitals is to facilitate the understanding of the scope and meaning of the Articles. As an ethical framework *soft (post-compliance) ethics* could help interpret the Recitals and «fill in» those gaps which the Articles leave open or unaddressed. This presents the fourth element. The fifth element constitutes the *hard ethical framework* which accompanied the formulation of the Articles and the Recitals in the first place. It is important to emphasize that the soft ethical framework always needs to be consistent with the hard ethical framework.

When presenting the two ethical frameworks in the context of the GDPR Floridi stays on the more general level without going further into details and giving concrete examples, nevertheless, his papers provide an important insight into how the interaction between regulation, hard and soft ethics should be understood.

3. Going beyond legal compliance – what does it mean in the context of the digital transformation?

Floridi's hard/soft ethics distinction brings to the surface one important message, namely, ethics should be part of making the law but it should also complement the law afterwards.[4] In that sense, ethical aspects play a role already at the level of the formulation of the regulation and they stay to be relevant after it has been put in place. This is a very important observation in light of the efforts to strengthen the presence and relevance of ethics in both the regulation area (hence the need to distinguish between hard/soft ethics) as well as in the technology design process by advocating «ethics by design». An early inclusion of normative aspects in the development of new technologies can help to prevent conflicts and foster acceptability. Therefore, post-compliance ethics is also part of the design process of those services, products and processes that then need to be regulated by law and hard ethics. Especially for information technology Wright has developed an Ethical Impact Assessment (EIA).[5] EIA looks at how technologies may be used in the future as components of a larger technological framework. It therefore extends towards a broader assessment of emerging technologies. It aims at finding workable conceptualizations of ethical impacts and ethical values and principles which apply to them, in order to assess the relative importance and the likelihood of the occurrence of ethical impacts and

2 Ibid, p. 4.

3 Floridi, «Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage», *Philosophy and Technology* 31 (2018), 163–167.

4 Ibid.

5 Wright, «A Framework for the Ethical Impact Assessment of Information Technology», *Ethics and Information Technology* 13(3) (2011), 199–226.

to locate potential value conflicts and, where possible, to resolve these.[6] EIA can also help to deal with the so-called «dilemma of control» or «Collingridge dilemma»: «The social consequences of a technology cannot be predicted early in the life of the technology. By the time undesirable consequences are discovered, however, the technology is often so much part of the whole economic and social fabric that its control is extremely difficult»[7]. This is the dilemma of control. «When change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult and time consuming»[8]. To escape the need to put hard regulation into place once a technology is fully developed it would be preferable «to provide indicators of negative ethical implications at an early stage of technological development»[9]. Post-compliance ethics should therefore be systematically involved in technology development throughout the entire process. Furthermore, the balancing act of the positive and negative effects of introducing new technology is not to be seen as the responsibility of political processes but rather distributed *throughout* the innovation enterprise.[10] The particular distribution of responsibility has also consequences for the governance of the respective field and relates to questions concerning the purpose, motivation, goal and direction of innovation and the provided social and political framework. So, by looking into the compliance/post-compliance distinction the idea is to add more to the value of ethics and the reason why we really need it in the process of constructing and governing the digital realm.

Let us now further develop Floridi's understanding of hard and soft ethics. In the context of digital regulation, it is in particular the GDPR as well as other legal frameworks that have tried to keep pace with current technological innovations and have set high standards to regulate data protection. So, if we have the law which dictates the compliance level and sets legally defined and adopted rules and regulations, then why do we need post-compliance ethics as well? Or, to ask the question more concretely: What could post-compliance ethics offer more than the existing law? What are the benefits businesses can reap if they do decide to put more effort into being post-compliant?

If we look at the developments in law and the ethical discourse in the past years one might easily get the impression that law and ethics are trying to be more reactive to technological innovation and address those challenges which innovation seems to raise. Having this in mind, going beyond compliance has the aim to encourage a more proactive approach and stimulate businesses to consider the moral acceptability of their actions before carrying them out. There are some good reasons for that. First, as Floridi argues, the law does not cover everything nor does it give straightforward answer to all issues.[11] Second, even though something is considered legal it is not necessarily ethical. This is closely correlated with the next reason. Third, in times of great distrust of users and consumers towards businesses and how they deal with their data (privacy and security scandals in the past years such as Cambridge Analytica have just re-confirmed and re-justified the declining level of trust), just acting within the legal framework might not be enough to compensate for the low level of trust. Having in mind these three reasons, post-compliance ethics allows us to consider questions and address challenges raised by the digital transformation that go beyond the law. In what follows, few such examples will be elaborated which should shed more light into why, where and how businesses can and should act beyond compliance.

---

6 Reijers/Brey/Jansen/Rodrigues/Koivisto/Tuominen, *A Common Framework for Ethical Impact Assessment,* Satori, 2016.

7 Collingridge, *The social control of technology*, Palgrave, Macmillan, 1981, 11.

8 Ibid.

9 Palm/Hansson, «The case for ethical technology assessment», *Technological Forecasting & Social Change* 73 (2006), 543.

10 Fisher/Rip, «Responsible Innovation: Multi-level dynamics and soft intervention practices.», in: *Responsible innovation: Managing the responsible emergence of science and innovation in society*, edited by R. Owen / M. Heintz, / J. Bessant (Chichester: Wiley, 2013), 165.

11 Floridi, «Soft Ethics and the Governance of the Digital», *Philosophy & Technology* 31(2018), 5.

3.1. Trustworthiness

Trustworthiness and trust take up a very important place in EU's efforts to build the Digital Single Market and the European digital economy. For instance, trust and trustworthiness play a crucial role as part of the Digital Single Market Strategy for Europe.[12] Additionally, in the Cybersecurity Act trust finds its place in the context of trust in digital technologies, trust in digital solutions or trust in the Digital Single Market.[13] Against this background, having trustworthy infrastructure as well as trustworthy businesses can be considered as the backbone of the digital transformation.

So, investing and doing more than just what the law demands represents a long-term investment in business's trustworthiness. Moreover, it can also be interpreted by consumers as a confidence-booster sign, as a dedication and commitment displayed by a business regarding its consumers and how it deals with their data. Of course, doing more than what the law requires also implies that businesses should invest more money. However, this can pay off in the future. As Floridi notes, «Ethics can be expensive, but this is a clear case in which those who spend more spend less»[14]. In that sense, one could argue that post-compliance ethics has the goal to enhance the trustworthiness of technology and businesses by providing a space for not just a mere adherence with existing law and regulation but rather to serve as a guidance and help businesses choose their actions wisely and anticipate the consequences their actions might lead to. Trustworthiness can therefore be seen as a final goal of post-compliance ethics. The next few sections pertain to few aspects where and how businesses can go beyond compliance and hence invest in their trustworthiness. These include some of the most pertinent ones: (a) (distributive) justice, fairness and non-discrimination, (b) transparency, (c) autonomy, (d) privacy. The list is, however, not exhaustive.

3.2. (Distributive) Justice, fairness and non-discrimination

At the heart of the concept of justice lie the notions of fairness, equality, desert. When talking about justice, we generally ask questions such as (a) What do we owe to other people?, or (b) What makes someone or something unjust? So, what could justice considerations add to the post-compliance level of the digital transformation?

The (automated) collection, analysis and use of data by businesses can have several implications, both positive and negative. Not seldom are cases where certain individuals or groups are being discriminated against based on their data. So, data can be a source of both discrimination and bias – in such cases we talk about data-based discrimination and biased decision-making. We distinguish two types of discrimination. Direct discrimination occurs when a person or a group is discriminated based on some features (or also called sensitive attributes) it possesses such as age, gender, religion, race, ethnicity etc. Indirect discrimination covers situations where, for instance, non-sensitive attributes are included in the decision-making, but a correlation exists between sensitive and non-sensitive which allows for indirect discrimination to occur. For instance, indirect discrimination could occur when postal codes are included in the decision-making which could reveal information about the neighborhood and people living there and hence stand in a strong correlation with ethnicity or race. For post-compliance ethics of particular interest are cases of indirect discrimination as very often it is more difficult to detect and fight them.

---

12 See European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee to the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, 2, 3, 4, 12.

13 See European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the «EU Cybersecurity Agency», and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification («Cybersecurity Act»), 29 May 2018.

14 Floridi, «Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage», *Philosophy and Technology* 31 (2018), 167.

With this in mind, for the domain of justice of importance are cases of information-based harm, informational inequality[15], informational injustice etc. Additionally, as data-based decision-making could also influence or determine who gets access to what benefits, opportunities, services, technology etc., distributive justice and the idea of fair distribution of benefits and fair treatment of people and groups within society are of relevance as well. It is clear though that not all of these issues can be regulated by law. Also due to problems of detection and attribution it may be preferable, if possible, to establish social practices that hinder or decrease forms of discrimination and unfair treatment. Post-compliance ethics can contribute to the establishment of such practices not only by analyzing the underlying ethical values, but also by awareness raising.

3.3. Transparency

Transparency presents a key component in building trustworthy infrastructure and enhancing trust among users in the digital transformation. It is no surprise that greater demands for transparency are considered to be so essential. After all, transparency can provide answers as to who does what and how.[16] This, furthermore, creates more openness and ensures accountability, which is a valuable asset in times of increasing informational asymmetry between users and businesses as it shifts the control more towards the users' side of the scale.

It is also the case with transparency that post-compliance ethics can provide very useful guidance as to what more could be done. As users get only very little peak into what businesses are doing with their data or how the digital services and products they are using collect their data, investing more into transparency measures could be an important trust card for many businesses. For instance, post-compliance ethics would demand taking additional measures for the purpose of ensuring transparent dealing with users' data and with users in general. This could take the form of issuing (additional) transparency reports or any other similar activities that serve the same purpose. However, any efforts to increase transparency would be in vain unless the information itself is provided in a manner that is useful, understandable for and easily accessible by users. Nevertheless, transparency should be understood as just the first step towards building a more trustworthy digital infrastructure which paves the way for other important aspects such as autonomy, privacy, justice etc. The reason for this is simple, transparency alone does not guarantee trustworthiness but it is an essential component of it.

3.4. Autonomy

Briefly put, autonomy rests upon the idea of self-determination and freedom from manipulation. Today businesses have access to an immense pool of digital data as well as dispose of much more sophisticated tools to collect, analyze and use that data than ever before. Additionally, users interact daily with different technologies with built-in AI that have a decision-making capacity. Moreover, they also daily use numerous digital services and interact with businesses. With that in mind, the line is getting thinner between users' great dependence on digital services and products and the benefits they get from all them, and how this impacts users' autonomy and their capacity to make autonomous decisions.

Today, the «nudging» done by many AI products and services through personalized and individually tailored advertising or digital environment is undoubtedly one of the most successful means to influence and hence direct users' decisions and choices. In addition to this, the personalization and tailoring of the digital environment creates personalized «filter bubbles» i.e. algorithmic filters which filter out the information that reaches

[15] Van den Hoven and Rooksby talk about distributive justice in the context of access to information. For more on this see Van den Hoven, Jeroen, / Emma Rooksby, «Distributive justice and the value of information: A (broadly) Rawlsian approach.» In: *Information Technology and Moral Philosophy*, edited by J. van den Hoven / J. Weckert, 376–396. Cambridge, Cambridge University Press, 2008.

[16] European Group on Ethics in Science and New Technologies, *Opinion No.28, Ethics of Security and Surveillance Technologies,* Brussels, 20 May 2014, 75.

each individual.[17] Despite the convenience this might bring to users in their capacity as consumers, at the same time it does diminish their autonomy and decision-making possibility. This stands opposite to the expectation that to some extent and in particular contexts people should let technology such as personal assistants, search engines, navigation systems etc. make decisions for them or assist them in their daily activities.[18] In that sense, the added value of post-compliance ethics would be to point at the necessity of creating a free of manipulation decision-making area and thus put emphasis on enhancing users' autonomy. This would imply that users should be given an environment in which their self-determination will be supported and in which technology will serve only to support and enhance their autonomy. This would also allow users to individually adjust the degree to which they prefer a decision should be «made» in their name.

3.5. Public and private sphere

With the digitization of all aspects of social life as well as the increased presence of users in the digital realm the line between our public and private life is getting even more blurred. Under such circumstances privacy concerns understandably gain more and more importance. Since the data we leave behind by using digital products and services can include both personal and non-personal, it can tell a lot about ourselves, our interests, habits, preferences. In many cases it can reveal even much more information about ourselves that we are aware of.

Currently under European Union law the GDPR is considered as one of the strictest regulations on data protection and privacy as it imposes very high standards by covering many privacy-related aspects and challenges. Nevertheless, as Floridi argues, as with any other legislation, the GDPR cannot cover everything. It is here that one should make greater use of digital ethics to fill in any gaps which legislation leaves uncovered, any questions it leaves unanswered, or simply to point out what more could be done beyond the bare legal minimum.[19] For instance, current privacy regulations place great value on informed consent. The aim of informed consent is to embody and enhance users' autonomy and privacy amidst increased data mining processes by businesses. But as data mining processes are expected to increase even more in the future and data mining techniques to become even more sophisticated and complex, just providing informed consent may have its limits. For users to be able to make informed decisions, merely providing users with the possibility to consent based on previously provided information might not suffice. What could also be done is to think about redesigning the process of informed consent and making it more visual, user-friendly and easily comprehensible for users without overburdening them with just one more box to tick it off. If we look a bit broader, informed consent is just one area where post-compliance could say what more could be done. There are other aspects of privacy as well where post-compliance measures could be taken.

4. Legal compliance and post-compliance ethics as a way to ease the digital transformation

If legal compliance presents the minimum legal standard that has to be accounted for and respected by businesses, post-compliance ethics allows businesses to showcase users that they are trying and willing to do more than just what the law requires. As already mentioned, in time of numerous privacy and cybersecurity breaches and where trust in technology stands on shaky grounds, in order to reap the full benefits of technological innovation Europe needs users and consumers that can trust and have confidence in the products and services they use while at the same time are aware of the potential and possible harms and risks. One way to earn and

---

17 Pariser, *Beware online «filter bubbles»* (Video file), TED2011, retrieved December 2018, https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript.

18 The European Commission's High-Level Expert Group on Artificial Intelligence, Draft Ethics Guidelines for Trustworthy AI, Working Document for stakeholders» consultation, Brussels, 18 December 2018, 17.

19 Floridi, «Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage», *Philosophy and Technology* 31 (2018), 164.

strengthen that trust is by investing more than the bare minimum prescribed by the law. If businesses just act within the legal framework, then they will manage to avoid any penalties and stay out of court, which users might perceive as simply businesses acting out of purely self-interested reasons. Of course acting according to the law is non-negotiable, but it presents only the first step.

It should be emphasized that post-compliance ethics does not exclude legal compliance nor should it be understood as an alternative to it. The best way is to see both legal compliance and post-compliance ethics as mutually reinforcing and complementing our efforts to build a digital society that is based on trust and trustworthiness. We need businesses to equally pay attention and make efforts to consider both of them. In that way, businesses can show users that they respect the law but also at the same time that they care about them, their interests and rights. It is here that the greatest value of post-compliance ethics lies. Finally, post-compliance ethics should also be seen as an integral part of responsible innovation. It possesses the great potential to encourage progress and technological advancement but in a responsible and morally acceptable manner, something which is very much needed in times of extremely speedy digital transformation.

5. Conclusion

The main goal of this paper was to shed some light on the need to consider post-compliance ethics as part of the digital transformation and to share some ideas where post-compliance ethics could be applied. This is a work in its inception that will be further developed.

The main message we wanted to share is that in light of a «trust crisis» in Europe and in the world in general regarding technological innovation, privacy, cybersecurity etc., we need both legal compliance and post-compliance ethics in order to deal with all challenges and ease the process of digital transformation. As argued before, post-compliance ethics would demand from businesses to do more than the bare legal minimum. This would be a more costly approach, nevertheless, investing in beyond compliance could also open up new opportunities for businesses to make better use of digital innovation as seen morally acceptable and use all the benefits innovation brings.

Additionally, even though post-compliance ethics (as it is the case with ethics in general) is not enforceable by law and hence voluntary and more aspirational, we also wanted to argue that it has a great potential and could bring to businesses much more, sometimes even more than what compliance would bring. In that sense, legal compliance should be understood as just one step which paves the way for post-compliance ethics.

6. Literature

Collingridge, David, *The social control of technology,* Palgrave, Macmillan, 1981.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee to the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final.

European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the «EU Cybersecurity Agency», and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification («Cybersecurity Act»), 29 May 2018.

European Group on Ethics in Science and New Technologies, *Opinion No.28, Ethics of Security and Surveillance Technologies,* Brussels, 20 May 2014.

Floridi, Luciano, «Soft Ethics and the Governance of the Digital.», *Philosophy & Technology* 31(2018), 1–8.

Floridi, Luciano, «Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage.», *Philosophy and Technology* 31 (2018), 163–167.

Fisher, Erik / Rip, Arie, «Responsible Innovation: Multi-level dynamics and soft intervention practices.», in: *Responsible innovation: Managing the responsible emergence of science and innovation in society*, edited by R. Owen / M. Heintz, / J. Bessant, 165–183, Chichester, Wiley, 2013.

Palm, Elin / Hansson, Sven Ove, «The case for ethical technology assessment.», *Technological Forecasting & Social Change* 73 (2006), 543–558.

Pariser, Eli, *Beware online «filter bubbles»* (Video file), TED2011, retrieved December 2018, https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript.

Reijers, Wessel / Brey, Philip / Jansen, Philip / Rodrigues, Rowena / Koivisto, Raija / Tuominen, Anu, *A Common Framework for Ethical Impact Assessment,* Satori, 2016.

The European Commission's High-Level Expert Group on Artificial Intelligence, Draft Ethics Guidelines for Trustworthy AI, Working Document for stakeholders consultation, Brussels, 18 December 2018.

Van den Hoven, Jeroen, / Emma Rooksby, «Distributive justice and the value of information: A (broadly) Rawlsian approach.», in: *Information Technology and Moral Philosophy*, edited by J. van den Hoven / J. Weckert, 376–396. Cambridge, Cambridge University Press, 2008.

Wright, David, «A Framework for the Ethical Impact Assessment of Information Technology.» *Ethics and Information Technology* 13(3) (2011), 199–226.