Philos. Technol. (2018) 31:163–167
https://doi.org/10.1007/s13347-018-0315-5

EDITOR LETTER

Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage

Luciano Floridi[1,2]

Published online: 3 June 2018

1 Hard and Soft Ethics

In a previous article (Floridi 2018), I introduced the distinction between *hard* and *soft ethics*. Since the reader may not be familiar with it, let me quickly summarise it here. I will then be able to use it to clarify two issues: the application of soft ethics to the General Data Protection Regulation (henceforth GDPR) and the idea that soft ethics has a *dual advantage*.

Hard ethics is 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 making choices or taking decisions in general and of formulating new legal norms or challenging existing ones in particular. In short, *hard ethics is what may contribute to making or shaping the law*. In hard ethics, it is not true that "ought" implies "may"; it is perfectly reasonable to expect that "ought" may be followed by "even if not". Call this the Rosa Parks Principle, for her famous refusal to obey the law and give up her bus seat in the "coloured section" to a white passenger, after the whites-only section was filled.

Soft ethics covers the same normative ground as hard ethics, but it does so by considering what ought and ought not to be done *over and above* the existing norms, not against them, or despite their scope, or to change them, or to by-pass them, e.g. in terms of self-regulation. In other words, *soft ethics is post-compliance ethics* because, in this case, "ought implies may" (or at least implies the absence of a "may not"). Call this the Matthew Principle, from Matthew 22:15–22: "Render to Caesar the things that are Caesar's".

Now, both hard and soft ethics presuppose *feasibility* or, in more Kantian terms, assume that "ought implies can", given that an agent has a moral obligation to perform

✉ Luciano Floridi
luciano.floridi@oii.ox.ac.uk

[1] Oxford Internet Institute, University of Oxford, 1 St Giles, Oxford OX1 3JS, UK

[2] The Alan Turing Institute, 96 Euston Road, London NW1 2DB, UK

an action only if this action is possible in the first place. It follows that soft ethics also assumes a *post-feasibility* approach. Add that any ethical approach, at least in the EU, accepts, as its minimal starting point, the implementation of the Universal Declaration of Human Rights (UDHR) and The Charter of Fundamental Rights of the European Union. And the result is that the space of soft ethics is only partially bounded. To see why, I suggested to visualise it in the shape of a trapezoid (see Fig. 1), with the lower side representing a feasibility base that is ever-expanding through time—we can do more and more things thanks to technological innovation—and the two constraining sides, left and right, representing legal compliance and human rights, while the open upper side represents the boundless space where what is morally good may happen in general and, in the context of this article, may happen in terms of shaping and guiding the ethical development of our mature information societies.

Soft digital ethics can be rightly exercised in places of the world where digital regulation is already on the good side of the moral vs. immoral divide. But it would be a mistake to argue for a soft ethics approach to establish a normative framework when agents (especially governments and companies) are operating in contexts where human rights are disregarded, e.g. in China, North Korea or Russia, or in contexts where hard ethics is precisely what is needed to change some current regulation, e.g. in the USA when it comes to net neutrality, and, a fortiori, in the three countries already mentioned. In all these cases, we need *hard ethics*. It is really within the European Union (EU) that post-compliance soft ethics can currently be exercised, to help individuals, companies, governments and other organisations to take more and better advantage, morally speaking, of the opportunities offered by digital innovation. Because even in the EU, legislation is necessary but insufficient. It does not cover everything (nor should it), and agents should leverage digital ethics in order to assess and decide what role they wish to play in the infosphere, when regulations provide no simple or straightforward answer, when competing values and interests need to be balanced (or indeed when regulations provide no guidance) and when there is more that can be done over and above what the law strictly requires. This is why it is in the EU that a good use of soft ethics could lead to companies to exercise "good corporate citizenship"

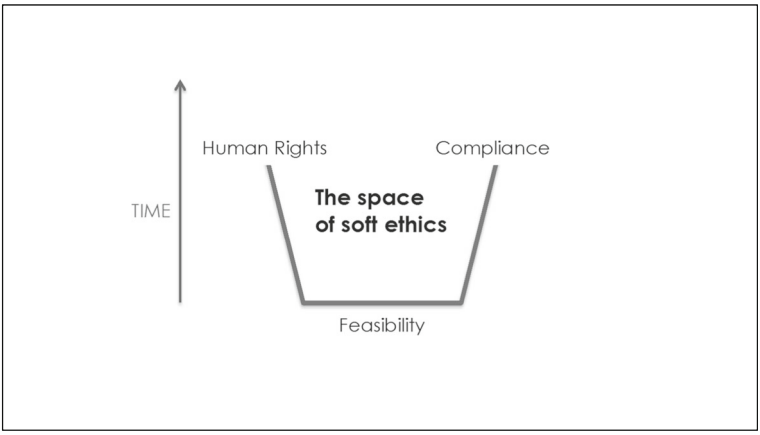

Fig. 1 The space of soft ethics

within a mature information society. The next question is then: given that digital regulation in the EU is now determined by the GDPR, what is the relation of soft and hard ethics with regard to it?

2 Soft Ethics as Ethical Framework

To understand the role of hard and soft ethics with regard to law in general and the GDPR in particular, five components need to be introduced. I shall do so in logical order, from left to right (see Fig. 2).

First, there are the ethical, legal and social implications (ELSI) of the GDPR, e.g. for organisations. This is the impact of the GDPR on business, for example. Then, there is the GDPR itself. This is the legislation that replaces the Data Protection Directive 95/46/EC. It is designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy, independently of geographical location, and to improve the way organisations across the EU approach data privacy. The GDPR comprises 99 Articles; this is the second element. As it is often the case with complex legislation, the Articles leave grey areas of normative uncertainty uncovered, are subject to interpretations and may require updating when applied to new circumstances, especially in a technological context where innovation develops so quickly and radically; think for example of face recognition software, or the so-called "deep fake" software. So, to help understand their meaning, scope and applicability, the Articles are accompanied by 173 Recitals. This is the third element. Recitals, in EU law, are texts that explain the reasons for the provisions of an act, but are not legally binding, and are not supposed to contain normative language. Normally, Recitals are used by the Court of Justice of the European Union (CJEU) in order to interpret a directive or a regulation and reach a decision in the context of a particular case.[1] But in the case of the GDRP, it is important to note that Recitals can also be used by the European Data Protection Board (the EDPB, which replaces the Article 29 Working Party), when ensuring that the GDPR is applied consistently across Europe. The Recitals themselves will require an interpretation, and this is the fourth element, namely the ethical framework that can contibute to interpret the Recitals. Finally, the Articles and the Recitals were formulated thanks to a long process of negotiations between the European Parliament, The Council of Europe and the European Commission (the so-called Formal Trilogue meeting), resulting in a joint proposal. This is the fifth element, namely the perspective or hard ethics that also informed the elaboration of the GDPR. It may be seen in action by looking at a comparative analysis of drafts from the European Parliament and European Commission and the amendments to the Commission's text proposed by the European Council.[2] So, here is a summary of what we need to consider (Fig. 2):

[1] See for example "C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González" http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&. or domestic CCTV and Directive 95/46/EC (European Court of Justice (ECJ) Judgment in Case C-212/13 Ryneš): http://amberhawk.typepad.com/amberhawk/2014/12/what-does-the-ecj-ryne%C5%A1-ruling-mean-for-the-domestic-purpose-exemption.html

[2] European Digital Rights, *Comparison of the Parliament and Council Text on the General Data Protection Regulation* https://edri.org/files/EP_Council_Comparison.pdf

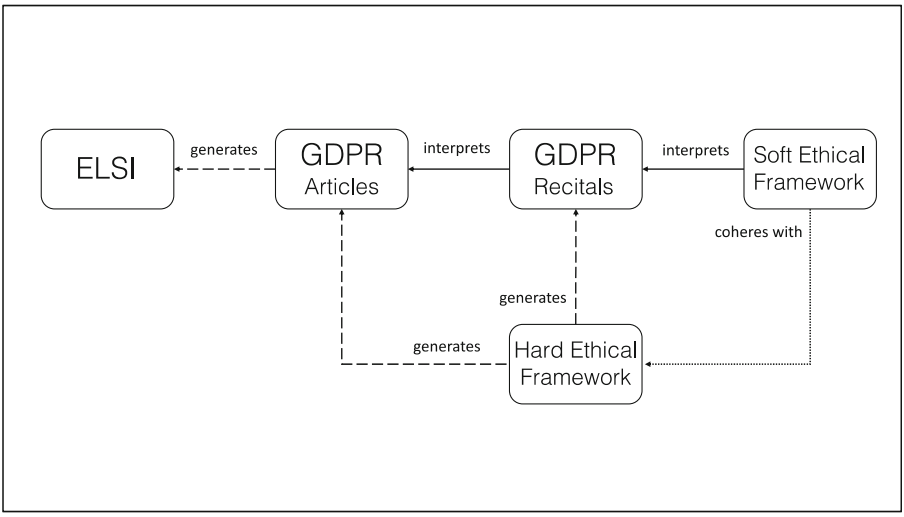

Fig. 2 Soft and hard ethics and their relation to regulation

(A) the Ethical Legal and Social Implications (ELSI) generated by the Articles in (B);
(B) the Articles of the GDPR that generate (A);
(C) the Recitals of the GDPR that help interpret the Articles in (B);
(D) the Soft Ethical Framework that help interpret the Recitals in (C) and is coherent with the Hard Ethical Framework in (E);
(E) the Hard Ethical Framework that helped generate the Articles in (B) and the Recitals in (C).

Hard ethics in (E) is what contributed to the process leading to the elaboration of the law, in this case, the GDPR. Soft ethics in (D) is the framework that contributes to enable the best interpretations of the Recitals in (C). For Soft Ethics in (D) to work well in interpreting the Recitals in (C), it must be coherent with, and informed by, the Hard Ethics in (E) that contributed to their formulation in the first place.

Clearly, the place of ethics is both before (hard) and after (soft) the law, as what contributes to make it possible first and may complement it afterwards. Let us now turn to its dual advantage.

3 Soft Ethics' Dual Advantage

Digital technologies offer many opportunities but also associated challenges and potential risks. Ensuring socially preferable outcomes means resolving the tension between incorporating the benefits and mitigating the potential harms, in short, promoting these technologies while avoiding their misuse, underuse and harmful use. This is where the value of an ethical approach becomes obvious. I argued above that compliance is merely necessary, but significantly insufficient. Adopting a soft ethical approach to digital innovation, over and above what is legally required, confers what I would like to define as a "*dual advantage*", echoing the "dual use" terminology popular in philosophy of technology at least since the debate on civil and military uses of nuclear power. Let me explain.

On the one hand, soft ethics can provide the advantage of an *opportunity strategy*, enabling actors to take advantage of the social value of digital technologies. This is the advantage of being able to identify and seize new opportunities that are socially acceptable or preferable, balancing any precautionary principle with the duty not to omit what could and ought to be done, e.g. to take advantage of the wealth of data accumulated, or the forms of smart automatic agency available.

On the other hand, soft ethics also provides the advantage of a *risk management solution*. It enables organisations to anticipate and avoid costly mistakes (the Cambridge Analytica scandal involving Facebook data is an unfortunate example). This is the advantage of prevention and mitigation of courses of action that turn out to be socially unacceptable and hence rejected, even if they are not illegal. In this way, soft ethics can also lower the opportunity costs caused by choices not made or opportunities not seized for fear of mistakes.

Soft ethics' dual advantage can only function in an environment of public trust and clear responsibilities more broadly. Public acceptance and adoption of digital technologies, including artificial intelligence, will occur only if the benefits are seen as meaningful and risks as potential, yet preventable, minimisable or at least something against which one can be protected. These attitudes will depend in turn on public engagement with the development of digital technologies, openness about how they operate and understandable, widely accessible mechanisms of regulation and redress. The clear value to any organisation of the dual advantage of an ethical approach amply justifies the expense of engagement, openness and contestability that such an approach requires. Ethics can be expensive, but this is a clear case in which those who spend more spend less.

Reference

Floridi, L. (2018). Soft ethics and the governance of the digital. *Philosophy & Technology, 31*(1), 1–8.