# White Paper on Artificial Intelligence – Joint Responses by Centre for Technology, Ethics, Law and Society and Centre of European Law, Dickson Poon School of Law, King's College London:

King's College London, Dickson Poon School of Law, TELOS Research Centre (Centre for Technology, Ethics, Law and Society)

(*Roger Brownsword*

*Mateja Durovic*

*Margarita Amaxopoulou)*

## Introduction

In this paper we are providing some views on behalf of KCL TELOS Research Centre (Centre for Technology, Ethics, Law and Society) in the context of the Commission's consultation on the published White Paper on Artificial Intelligence (AI). This paper is divided in two main parts: a general and a more specific one. First, we provide a general discussion on how the European approach on AI could be advanced, providing our overarching argument on the need to utilise a broader set of regulatory tools. In the second part, we focus on the impact of AI applications' use on specific legal areas. We shed light to legal matters that will need closer examination by the Commission, raising some crucial questions for the policy makers' consideration.

## A. Regulatory options, reimagined: a triple licence

The main purpose of this response to the Commission's White Paper[1] is to argue that the consultation, like the eventual EU regulatory regime for AI, needs to be sensitised to the full range of regulatory responsibilities, reaching back to regulatory stewardship for the global commons' conditions. In this paper, we introduce the idea of a triple licence for emerging technologies (a. whether employed as a regulatory tool or b. applied by regulatees, and c. whether in the public or the private sector), and then (relative to this triple standard) we audit the claimed 'high level' of the EU's protection of consumers and data subjects.[2]

[1] European Commission, *White Paper: On Artificial Intelligence—A European Approach to Excellence and Trust*, COM(2020) 65 final, Brussels, 19.2.2020.

[2] In this response, we are drawing extensively on Roger Brownsword, *Law, Technology and Society—Re-imagining the Regulatory Environment* (Abingdon: Routledge, 2019); *Law 3.0: Rules,*

## *1. The Fundamental Point*

In the EU, there is a regulatory commitment to a high level of protection for both consumers and data subjects as well as to a 'human-centric' approach to innovation. However, in order to assess whether these commitments are being fully met, we need to retrieve a sense of the deep connectedness of humans—not merely as consumers and data subjects in networked societies, or even as members of our particular communities but, crucially, simply as human social beings. Similarly, where there is an emphasis on the importance of emerging autonomous systems being 'trusted' by citizens (lest their benefits will not be exploited) as well as being 'trustworthy' (in the sense, for example, that their application is compatible with the requirements of human rights), we need to place this in the bigger picture of human connectedness.

In this bigger picture, human connectedness informs a three-level scheme of regulatory responsibility and, concomitantly, a triple licence that sets the standard for the legitimacy of regulatory measures. Most importantly, regulators have a responsibility to maintain the global commons, comprising the essential conditions for human existence and the generic context for human agency. It follows that the protection of consumers and data subjects (likewise, the winning of the trust of citizens) demands more than an 'acceptable accommodation' (or 'balancing') of legitimate interests, and more even than compatibility with distinctively European fundamental values. Unless regulators adequately engage with the maintenance of the global commons, they will not fulfil the highest level of their protective and human-centric commitments, the trustworthiness of autonomous technologies will not be assured, and regulators will not fully discharge their responsibilities.

## *3. Regulatory responsibilities*

*Regulation and Technology* (Abingdon: Routledge, 2020); 'Law Disrupted, Law Re-imagined, Law Re-invented' (2019) 1 *Technology and Regulation* 10; 'Law, Technology, and Society: In a State of Delicate Tension' (2020) XXXVI *Politeia* 137, 26; 'Migrants, State Responsibilities, and Human Dignity' (2020) *Ratio Juris* (forthcoming); and 'In Our Connected Societies: Respecting and Protecting Consumers and Data Subjects' (2020) *European Data Protection Law Review* (forthcoming).

Where the regulatory direction of travel is towards a more instrumental approach, with the focus being on what works and how best to serve specified policies, there is a risk that these considerations come to dominate. As Robert Merton put it so eloquently in his Foreword to Jacques Ellul's *The Technological Society*, we need to beware civilisations and technocrats that are 'committed to the quest for continually improved means to carelessly examined ends.'[3]

Arguably, while Merton's warning might be appropriate in relation to the activities of some private corporations who, de facto, act as regulators, it is not yet an urgent concern in relation to public regulators. Nevertheless, there are two striking problems in relation to our public discourse concerning regulatory responsibilities. The first is that we assume that whatever particular principles or purposes we take to be guiding, they are in the final analysis reasonably and rationally contestable; and, the second is that we engage in all manner of balancing exercises (between rights, interests, public policy and so on) without any clear sense of there being a hierarchy that guides deciding between conflicting considerations. In short, we lack foundations; and we lack hierarchy. Accordingly, a priority is to restore some order to our understanding of regulatory responsibilities.

In that spirit, we suggest that we should frame our thinking by articulating three tiers of regulatory responsibility, the first tier being foundational, and the responsibilities being ranked in three tiers of importance. At the first and most important tier, regulators have a 'stewardship' responsibility for maintaining the pre-conditions for human social existence, for any kind of human social community. These conditions constitute 'the global commons'. At the second tier, regulators have a responsibility to respect the fundamental values of a particular human social community, that is to say, the values that give that community its particular identity. At the third tier, regulators have a responsibility to seek out an acceptable balance of legitimate interests. The responsibilities at the first tier are cosmopolitan and non-negotiable (the red lines here are hard); the responsibilities at the second and third tiers are contingent, depending on the fundamental values and the interests recognised in each particular community. Any conflicts between these responsibilities are to be resolved by reference to the tiers of importance: responsibilities in a higher tier always outrank those in a lower tier.

### *i. The regulatory responsibility for the commons*

[3] Jacques Ellul, *The Technological Society* (New York: Vintage Books, 1964) p. vi.

It is an article of faith in the medical profession that doctors should, first, do no harm (to their patients). For regulators, the equivalent injunction should be, first, to ensure that no harm is done to the generic conditions that underpin the lives and prospects of their regulatees.

This injunction rests on a simple but fundamental idea. This is that it is characteristic of human agents that, as *humans*, they have certain biological needs (the need for a range of life-supporting conditions) and that, as *agents*, they have the capacity to pursue various projects and plans whether as individuals, in partnerships, in groups, or in whole communities. Sometimes, the various projects and plans that they pursue will be harmonious; but, often, human agents will find themselves in conflict or competition with one another as their preferences, projects and plans clash. However, before we get to particular projects or plans, there needs to be a context in which the exercise of agency is possible. This context is not one that privileges a particular articulation of agency; it is prior to, and entirely neutral between, the particular plans and projects that agents individually favour; the conditions that make up this context are generic to agency itself. In other words, there is a deep and fundamental critical infrastructure, a commons, for any community of agents. It follows that any agent, reflecting on the antecedent and essential nature of the commons must regard the critical infrastructural conditions as special. From any practical viewpoint, prudential or moral, that of regulator or regulatee, the protection of the commons must be the highest priority. Indeed, this is so obvious that we really should not need striking schoolchildren and Swedish teenagers or, for that matter, a devastating pandemic, to remind us of such self-evident truths.

Agents who reason impartially will understand that each human agent is a stakeholder in the commons where this represents the essential conditions for human existence together with the generic conditions of both self-regarding and other-regarding agency; and, it will be understood that these conditions must, therefore, be respected. While respect for the commons' conditions is binding on all human agents, it should be emphasised that these conditions do not rule out the possibility of prudential or moral pluralism. Rather, the commons represents the pre-conditions for both individual self-development and community debate, giving each agent the opportunity to develop his or her own view of what is prudent as well as what should be morally prohibited, permitted, or required. However, the articulation and contestation of both individual and collective perspectives (like all other human social acts, activities and practices) are predicated on the existence of the commons.

### *ii. The regulatory responsibility to respect the community's fundamental values*

Beyond the fundamental stewardship responsibilities, regulators are also responsible for ensuring that the fundamental values of their particular community are respected. Just as each individual human agent has the capacity to develop their own distinctive identity, the same is true if we scale this up to communities of human agents. There are common needs and interests but also distinctive identities.

After Covid-19, in the 'new normal', one question to be addressed is whether, and if so how far, a community sees itself as distinguished by its commitment to regulation by rule. In some smaller scale communities or self-regulating groups, there might be resistance to a technological approach. However, where a community is happy to rely on technological features rather than rules, it then has to decide whether it is also happy for humans to be out of the loop. Where the technologies involve AI, the 'computer loop' might be the only loop that there is. The question then (a question that is implicitly posed by Article 22 of the GDPR) is whether the community defines itself by its insistence on humans meaningfully remaining in processes and decisional loops. Furthermore, once a community is asking itself such questions, it will need to clarify its understanding of the relationship between humans and AI-enabled robots—in particular, whether it treats robots as having moral status, or legal personality, and the like.

### *iii. The regulatory responsibility to seek an acceptable balance of interests*

This takes us to the third tier of regulatory responsibility. With the development of a regulatory-instrumentalist mind-set, we find that much of traditional tort and contract law is overtaken by an approach that seeks to promote general policy objectives (such as supporting and encouraging beneficial innovation) while balancing this with countervailing interests. Given that different balances will appeal to different interest groups, finding an acceptable balance is a major challenge for regulators.

Today, we have the perfect example of this challenge in the debate about the liability (both criminal and civil) of Internet intermediaries for the unlawful content that they carry or host. Should intermediaries be required to monitor content or simply act after the event by taking down offending content? In principle, we might argue that such intermediaries should be held strictly liable for any or some classes of illegal content; or that they should be liable if they fail to take reasonable care; or that they should be immunised against liability even though the content is illegal. If we take a position at the strict liability end of the range, we might worry that the liability regime is too burdensome to intermediaries and that on-line

services will not expand in the way that we hope; but, if we take a position at the immunity end of the range, we might worry that this treats the Internet as an exception to the Rule of Law and is an open invitation for the illegal activities of copyright infringers, paedophiles, terrorists and so on. In practice, most legal systems balance these interests by taking a position that confers an immunity but only so long as the intermediaries do not have knowledge or notice of the illegal content. Predictably, now that the leading intermediaries are large corporations with deep pockets, and not fledgling start-ups, many think that the time is ripe for the balance to be reviewed. However, finding a balance that is generally acceptable, in both principle and practice, is another matter.

While finding an acceptable balance might be messy and provisional, and while it might be the best that we can do at the time, it is critically important that do not make the mistake of thinking that balancing is always the best that we can do. Where the stewardship of the commons or the values that define a particular community are at stake, there are clear priorities and regulators have very different responsibilities.

## 4. The triple licence

Following on from our sketch of the regulatory responsibilities, we propose that new technologies (such as AI) should not be employed (whether for regulatory or non-regulatory purposes) unless they have a triple licence: a (global) commons licence, a community licence, and a social licence.

### *i. The (global) commons licence*

The first element of the triple licence is that the measures in question must be compatible with respect for the pre-conditions for human social existence, with the maintenance of the global commons. As we have said, determining the nature of the commons' conditions will not be a mechanical process and we do not assume that it will be without its points of controversy. In particular, where a community has formally expressed its commitment to a range of fundamental values, we can debate which of those values relate to the essential commons' conditions and which to the distinctive aspirations of the particular community. For example, in the EU, the Charter of Fundamental Rights opens with the striking declaration that human dignity is to be respected and protected as 'inviolable'. However, it is not clear whether this declares what is distinctively most important for Europeans *as Europeans* or whether it declares what is most important for Europeans *as humans*, thereby

connecting back in some way to the existence or the agency preconditions or both. This is a matter to which we will return in the next part of our discussion. At this stage, though, we can give an indication of how we might understand the distinctive contribution of each segment of the commons.

In the first instance, the natural ecosystem for human life must be protected and preserved.[4] At minimum, this entails that the physical well-being of humans must be secured; humans need oxygen, they need food and water, they need shelter, they need protection against contagious diseases, if they are sick they need whatever medical treatment is available, and they need to be protected against assaults by other humans or non-human beings. It follows that the intentional violation of such conditions may be viewed as a crime against, not just the individual humans who are directly affected, but humanity itself.[5]

Secondly, the conditions and context for meaningful self-development and agency need to be constructed: there needs to be a sufficient sense of self and of self-esteem, as well as sufficient trust and confidence in one's fellow agents, together with sufficient predictability to plan, so as to operate in a way that is interactive and purposeful rather than merely defensive. In such a context, human life becomes an opportunity for agents to be who they want to be, to have the projects that they want to have, to form the relationships that they want, to pursue the interests that they choose to have and so on. In this light, we can readily appreciate that—unlike, say, Margaret Atwood's post-apocalyptic dystopia, *Oryx and Crake*—what is dystopian about George Orwell's *1984* and Aldous Huxley's *Brave New World* is not that human *existence* is compromised but that human *agency* is compromised.

Thirdly, the commons must secure the conditions and context for an aspirant moral community, whether the particular community is guided by teleological or deontological standards, by rights or by duties, by communitarian or liberal values, by virtue ethics, and so on. The generic context for moral community is impartial between competing moral visions, values, and ideals; but it must be conducive to 'moral' development and 'moral' agency in a

---

4 Compare, J. Rockström et al, 'Planetary Boundaries: Exploring the Safe Operating Space for Humanity' (2009) 14 *Ecology and Society* 32 (http://www.ecologyandsociety.org/vol14/iss2/art32/) (last accessed November 14, 2016); and, Kate Raworth, *Doughnut Economics* (Random House Business Books, 2017) 43-53.

5 Compare Roger Brownsword, 'Crimes Against Humanity, Simple Crime, and Human Dignity' in Britta van Beers, Luigi Corrias, and Wouter Werner (eds), *Humanity across International Law and Biolaw* (Cambridge University Press, 2014) 87.

formal sense. Crucially, there is more to moral development than acting in a way that aligns with what is generally taken to be the right thing to do. Agents must freely choose to do the right thing, implying that they need to have the practical option of doing the *wrong* thing. This is the message of Anthony Burgess' dystopian novel, *A Clockwork Orange*; and it is also the concern raised by the supposedly utopian model community introduced to readers by B.F. Skinner in *Walden Two*—a concern now re-kindled by Shoshana Zuboff in her view that the long game of surveillance capitalism is not simply to be able accurately to profile consumers' preferences but actually to control and shape those preferences.[6]

### *ii. The community licence*

The second strand of the triple licence, the community licence, demands that, within a particular community, the application of regulatory measures should be compatible with the fundamental values of that community—with the values, so to speak, that give the community its distinctive identity, that make it the particular community that it is.

From the middle of the Twentieth Century, many nation states—not least in Europe—have expressed their fundamental (constitutional) values in terms of respect for human rights and human dignity.[7] These values (most obviously the human right to life) clearly intersect with the commons conditions and there is much to debate about the nature of this relationship and the extent of any overlap—for example, if we understand the root idea of human dignity in terms of humans having the capacity freely to do the right thing for the right reason,[8] then human dignity reaches directly to the commons' conditions for moral agency.[9] However, those nation states that articulate their particular identities by the way in which they interpret their commitment to respect for human dignity are far from homogeneous. Whereas, in some communities, the emphasis of human dignity is on individual empowerment and autonomy, in others it is on constraints relating to the sanctity, non-commercialisation, non-commodification, and non-instrumentalisation of

---

6 Shoshana Zuboff, *The Age of Surveillance Capitalism* (London, Profile Books, 2019).

7 See Roger Brownsword, 'Human Dignity from a Legal Perspective' in M.Duwell, J. Braavig, R. Brownsword, and D. Mieth (eds), *Cambridge Handbook of Human Dignity* (Cambridge University Press, 2014) 1.

8 For such a view, see Roger Brownsword, 'Human Dignity, Human Rights, and Simply Trying to Do the Right Thing' in Christopher McCrudden (ed), *Understanding Human Dignity* (Proceedings of the British Academy 192) (The British Academy and Oxford University Press, 2013) 345.

9 See, Roger Brownsword, 'From Erewhon to Alpha Go: For the Sake of Human Dignity Should We Destroy the Machines?' (2017) 9 *Law, Innovation and Technology* 117.

human life.[10] These differences in emphasis mean that communities articulate in very different ways on a range of questions prompted by new technologies, some familiar (such as beginning of life and end of life questions) others novel (such as many of the questions provoked by the development of smart machines equipped with AI).

While the fundamental values to which a particular community commits itself must be consistent with the commons' conditions, the community licence is about maintaining fidelity with the community's own constitutive values, and, to this extent, it is internal to the commitments of the particular community. Accordingly, in principle, there can be a plurality of communities each with their own distinctive community licence.

### *iii. The social licence*

Within each community, there will be many debates about questions that do not implicate either the commons' conditions or the community's particular fundamental values. Judgments about benefits and risks, and about the distribution of benefits and risks, might be varied and conflictual.

In many communities, these questions will be managed by a process of inclusive consultation and democratic deliberation structured by a concern that the governing regulatory framework should not 'over-regulate' and risk stifling potentially beneficial innovation but nor should it 'under-regulate' and expose citizens to unacceptable risks. As the Commission says, when discussing the regulation of the Internet of Things in the context of preparing consumer policy for future challenges:

> It is forecast that there will be at least 6 billion internet-connected products in the EU and 25 billion worldwide by 2020. It is important to make sure that these products and technologies are safe for consumers, while ensuring wide choice and not stifling innovation. [11]

---

[10] See Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (Oxford: Oxford University Press, 2001); and Roger Brownsword, *Rights, Regulation and the Technological Revolution* (Oxford: Oxford University Press, 2008).

[11] European Commission, Communication from the Commission to the European Parliament, the Council, and the European Economic and Social Committee, *A New Deal for Consumers*, COM(2018) 183 final, Brussels 11.4.2018, p 14.

At the conclusion of this process of consultation and deliberation, a regulatory position will be taken that reflects a 'balancing' and 'accommodation' of various competing and conflicting interests, often with supportive appeals to 'proportionality'.[12] The position taken will not be one to which everyone ideally would subscribe; however, provided that the position is within the range of 'acceptability', it should be respected by all as having a social licence.

So much for the benchmarks of regulatory legitimacy—benchmarks that indicate that, before technological tools should be used by either regulators or regulatees, there will need to be a triple licence for the particular use or application. Our next step is to consider how these licensing conditions might be applied to questions of consumer protection and the fair collection and processing of personal data.

## 5. Respecting and Protecting Consumers and Data Subjects

If the regulatory environment is to pass muster in relation to respecting and protecting consumers and data subjects, the relevant measures must satisfy the conditions of the triple licence; and, the absence of measures must also be compatible with the discharge of regulatory responsibilities. Accordingly, the key questions for any regulatory audit would be whether consumers and data subjects are properly respected and protected (i) as human agents (relative to the conditions of the global commons), (ii) as Europeans (relative to fundamental European values), and (iii) as consumers and data subjects simpliciter.

In what follows, our focus will be particularly on the first of these questions because, if there were to be a blind spot in the protective regime in the EU, this would be the most serious place for it to be located—if this were to be the case, the level of protection of consumers and data subjects would not be high enough.

[12] For example, in Recital 27 of Directive (EU) 2019/2161 (on the better enforcement and modernisation of consumer protection rules), we read:

> The information requirements for providers of online marketplaces should be proportionate. Those requirements need to strike a balance between a high level of consumer protection and the competitiveness of providers of online marketplaces.

### *i. The first element of the licence*

Are consumers and data subjects in the EU adequately respected and protected simply as human agents? The key questions here are whether the regulators have put in place, first, an environment that is safe for the consumption of goods and services and, secondly, a context that is supportive of agency.

While consumers in the EU have been exposed to dangerous products (including pharmaceuticals, food, and implants, and so on), and while debates about GMOs remain unresolved, the regulatory culture is famously precautionary, there is a major emphasis on ex ante safety checks, and product liability sets a strict standard. Against this backcloth, the concern is not so much that the activities of the surveillance capitalists will kill us but that they will compromise the essential conditions for agency. Thus, according to Frank Pasquale, the danger with today's dataveillance practices, is that they might be 'doing less to deter destructive acts than [slowly to narrow] the range of tolerable thought and behaviour.'[13] Or, as Zuboff puts it, the 'instrumentarian' society fostered by the big tech surveillance capitalists,

> suffocate(s) the individually sensed inwardness that is the wellspring of personal autonomy and moral judgment, the first-person voice, the will to will, and the sense of an inalienable right to the future tense.[14]

And, more specifically, 'Facebook has learned to bite hard on the psychological needs of young people, creating new challenges for the developmental processes that build individual identity and personal autonomy.'[15] What should we make of this? Is the essential context for agency a blind spot in the law? By way of response, we can offer four short thoughts.

---

13 Frank Pasquale, *The Black Box Society* (Cambridge, Mass., Harvard University Press, 2015) at 52.

14 Zuboff (n 1) at 444.

15 Ibid, at 446.

First, while it is widely accepted that our privacy interests (in a broad sense) are 'contextual',[16] it is important to understand not just that 'there are contexts and contexts' but that there is a Context in which we all have a common interest and, concomitantly, that there are Privacy conditions in the agency-supporting dimensions of that Context. As Bert-Jaap Koops has so clearly expressed it, privacy has an 'infrastructural character', 'having privacy spaces is an important presupposition for autonomy [and] self-development';[17] without such spaces, there is no opportunity to be oneself.[18] On this reading, respect for privacy is not so much a matter of protecting goods (informational or spatial) in which one has a personal interest, or demanding that one be 'left alone', but protecting infrastructural goods that are intimately associated with the connectedness of humans.[19] Arguably, the separate specification of privacy and data protection in the Charter of Fundamental Rights, and the foregrounding of the latter right in Article 1 of the General Data Protection Regulation (GDPR)[20], are hostages to fortune. Granted, privacy is still very much part of the rhetoric around the GDPR[21], but regulators should protect those conduits that lead from data processing to the essential conditions for the self-development of agents.[22]

Secondly, let us suppose that smart environments might compromise the context for moral development by making it more difficult for agents to make their own moral judgments. On this view, we might be particularly concerned about the proliferation of smart digital assistants that start by guiding and making recommendations to their users but which, insidiously, take over the independence of their users. It is one thing for agents to use their smart device as a moral 'critical friend', quite another to delegate moral decision-making to

---

16 See, for example, Daniel J. Solove, *Understanding Privacy* (Cambridge, Mass.: Harvard University Press, 2008), and Helen Nissenbaum, *Privacy in Context* (Stanford: Stanford University Press, 2010).

17 Bert-Jaap Koops, 'Privacy Spaces' (2018) 121 *West Virginia Law Review* 611, at 621.

18 Compare, too, Maria Brincker, 'Privacy in Public and the Contextual Conditions of Agency' in Tjerk Timan, Bryce Clayton Newell, and Bert-Jaap Koops (eds), *Privacy in Public Space* (Cheltenham: Edward Elgar, 2017) 64; and, similarly, see Margaret Hu, 'Orwell's *1984* and a Fourth Amendment Cybersurveillance Nonintrusion Test' (2017) 92 *Washington Law Review* 1819, at 1903-1904.

19 Compare the discussion of 'mass surveillance' in the White Paper (n 1), p. 11.

20 Regulation EU 2016/679, Article 1 (where it is the right to data protection that is highlighted).

21 See, e.g., GDPR.EU, 'What is GDPR, the EU's new data protection law?' (listing 8 privacy rights in the GDPR) https://gdpr.eu/what-is-gdpr/ (last accessed April 24, 2020).

22 Compare Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' in Hielke Hijmans and Herke Krannenborg (eds), *Data Protection Anno 2014: How to Restore Trust?* (Cambridge: Intersentia, 2014) 83.

it (or habitually to rely on its 'expert' judgment).[23] In a similar vein, Shannon Vallor is rightly concerned that any employment of digital technologies to foster prosocial behaviour should respect the importance of conduct remaining 'our *own conscious activity and achievement* rather than passive, unthinking submission.'[24] Quite simply, where technologies do too much work for their users, there is a risk that moral agency will be compromised. If the task of maintaining the context for independent moral judgment falls to regulators, it needs to be on their agenda.

Thirdly, even if regulatory technologies do not interfere with one making one's own moral judgment (agents can still have an independent view of what is morally right and wrong), they can find themselves acting in technologically managed environments where there is simply no option other than to do what one can do. For example, consumers who are the end-users of products or devices that have been designed for digital rights management, can only act in ways that are compliant with the technological management of IP rights. Given what seems to be a technological direction of travel, regulators need to recall Ian Kerr's evocative remark that moral virtue is simply not something that can be automated.[25]

Fourthly, EU consumer law wavers between paternalistically protecting consumers against making choices that might prove damaging to their well-being or that they might seriously regret and trying to improve the conditions for consumers to make their own free and informed choices. The objection to the former protective approach, as Antonios Karampatzos, has recently highlighted, is that this might evince a lack of respect for the autonomy of consumers—and, particularly so for poorer consumers who would not freely have chosen the protections for which they now have to pay.[26] Accordingly, Karampatzos argues that, in the interests of autonomy, rather than nudging consumers towards a right to withdraw (or embedding a mandatory right to withdraw) it would be better to operate with a regime of mandated choice. While Karampatzos' interest is primarily in nudges as default *rules*, there are plenty of examples of nudges to consumers that are not in the rules as such

---

23 For extended discussion, see Roger Brownsword, 'Disruptive Agents and Our Onli*f*e World: Should We Be Concerned?' (2017) 4 *Critical Analysis of Law* 61 (symposium on Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Cheltenham: Elgar, 2015).

24 Shannon Vallor, *Technology and the Virtues* (Oxford: Oxford University Press, 2016) 203 (emphasis in original).

25 Ian Kerr, 'Digital Locks and the Automation of Virtue' in Michael Geist (ed), *From 'Radical Extremism' to 'Balanced Copyright': Canadian Copyright and the Digital Agenda* (Toronto: Irwin Law, 2010) 247.

26 Antonios Karampatzos, *Private Law, Nudging and Behavioural Economic Analysis* (Abingdon: Routledge, 2020).

but in practical information, settings, or in the design of products, processes, and places. In other words, the 'choice architecture' of which nudging might be a part has both a rule dimension and a design dimension. With regard to the latter, we can certainly agree with Karampatzos that it is important that nudges of this kind should be transparent. At the very least, consumers should know that, with each click and each purchase, data is being collected that will then be deployed to make the nudges even more effective in serving the interests of both suppliers and others in the data economy. However, even with transparency, is this a sufficient exercise of regulatory stewardship? If the marketplace is being structured in ways that compromise the agency conditions of the commons, regulators need to intervene.

### *ii. The second element of the licence*

For consumers and data subjects, connectivity is increasingly and ubiquitously enabled by AI; it starts with smart phones and wearables, smart devices in smart homes, smart transportation, and smart cities, and it ends we do not know where. It is axiomatic that the application of AI should be compatible with European values, and no one doubts that there will be major challenges involved in ensuring such compatibility.[27]

In an attempt to get to grips with the basic conditions of this element of the triple licence, the independent high-level expert group on artificial intelligence has highlighted the importance of AI being 'trustworthy' and, crucially, that the development and use of AI should be 'human-centric'.[28] However, to the extent that trustworthiness signifies only that the AI will be compatible with European values and compliant with whatever regulatory requirements are put in place, and to the extent that human-centricity signifies only that AI should be applied in the service of humanity or that the human rights that are recognised in Europe will be applicable, all the hard work remains to be done. Key regulatory provisions (such as the much-debated Article 22 of the GDPR, protecting data subjects against solely automated decisions where those decisions have legal or similarly significant effects) pose

[27] For an outstanding discussion of one such challenge, see Philipp Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law' (2018) 55 *Common Market Law Review* 1143.

[28] European Commission, *Ethics Guidelines for Trustworthy AI*, Brussels, April 8, 2019. For example, at p 4, we read that 'AI systems need to be human-centric, resting on a commitment to their use in the service of humanity and the common good, with the goal of improving human welfare and freedom.'

more questions than they answer[29]; the principles that the expert group identifies as key to the governance of AI—namely, respect for human autonomy, prevention of harm, fairness, and explicability—are open to interpretation; and, any tensions between the principles will need to be resolved (as the expert group proposes by 'methods of accountable deliberation' involving 'reasoned, evidence-based reflection rather than intuition or random discretion'[30]).

That said, the expert group emphasises that there might be cases where 'no ethically acceptable trade-offs can be identified. Certain fundamental rights and correlated principles are absolute and *cannot be subject to a balancing exercise* (e.g. human dignity).'[31] On one reading, this makes the important point that fundamental rights are to be privileged against the mere (legitimate) interests that consumers and data subjects might have; but, on another reading, this makes the even more important point that some fundamental values, such as human dignity, should not be balanced against either (third-tier) legitimate interests or even distinctively (second-tier) European values—in other words, given the analysis in this article, that these values are 'absolute' in that they represent the (first-tier) commons' conditions themselves. Again, though, disentangling which fundamental values—including which (if any) aspects of 'trustworthiness' and 'human centricity'—relate to the global commons and which to the community's distinctive aspirations is a major and, no doubt, ongoing jurisprudential exercise.

Building on the expert group's report, the Commission proposes a risk-based approach such that 'the new regulatory framework for AI should be effective to achieve its objectives while not being excessively prescriptive [and disproportionately burdensome].'[32] It follows that regulators should focus on high-risk uses of AI. Paradigmatically, such uses will involve some high-risk activity in a high-risk sector. Thus, for example, while health care is a high-risk sector, some uses of AI are less risky than others. As the Commission notes, 'a flaw in the

---

29 For discussion, see, e.g., Roger Brownsword and Alon Harel, 'Law, Liberty and Technology—Criminal Justice in the Context of Smart Machines' (2019) 15 *International Journal of Law in Context* 107; and Orla Lynskey, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' (2019) 15 *International Journal of Law in Context* 162; and, for the vexed question of whether there is 'a right to an explanation', see Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76.

30 (n 28) p. 13.

31 Ibid., emphasis added.

32 European Commission (n 1) at 17.

appointment scheduling system in a hospital will not normally pose risks of such significance as to justify legislative intervention.'[33] Presumably, this would contrast with, say, the use of AI in surgical procedures where a patient's life might be at stake if 'something goes wrong' or, possibly, with reliance on AI to triage patients who test positive for Covid-19. In these paradigmatically high-risk cases, human oversight is required. In the Commission's own words, 'The objective of trustworthy, ethical and human-centric AI can only be achieved by ensuring an appropriate involvement by human beings in relation to high-risk applications.'[34] But, again, we do not know what this means until the jurisprudence that develops around the community element of the triple licence specifies precisely what level and kind of involvement by humans is to be treated as a matter of fundamental rights, or respect for human dignity.

### *iii. The third element of the licence*

Finally, we can expect there to be ongoing adjustments to the regulatory environment for consumption of goods and services and for the collection and processing of personal data, such adjustments reflecting shifts in views about a reasonable accommodation of competing or conflicting interests.

In recent years there have been, as it were, 'new deals' for both consumers and data subjects in the EU.[35] Indeed, for consumers, there have been in some respects a succession of new deals as a variety of adjustments (both upwards and downwards) to the protective provisions of earlier Directives are made. For example, the original rights to withdraw ('cooling-off' periods) that were introduced in a number of Directives were modified by EU Directive 2011/83 on Consumer Rights and fine-tuned again in the recent EU Directive 2019/2161. Throughout, there are balances to be struck between bright line rules and qualified rights, between protection of consumer vulnerability and restriction of consumer opportunism, and between the legitimate interests of both suppliers and consumers.[36] At

---

33 Ibid.

34 Ibid. at 21.

35 European Commission (n 11), Section 7.

36 For discussion of such balances, see e.g., Marco Loos, 'Rights of Withdrawal' in Geraint Howells and Reiner Schulze (eds.), *Modernising and Harmonising Consumer Contract Law* (Munich: Sellier European Law Publishers) 237 (concluding that, all things considered, the balance is rather too favourable to the interests of business contractors), and 'The Modernization of European Consumer Law: A Pig in a Poke?' (2019) 27 *European Review of Private Law* 113 (for an overview of the latest

much the same time, in the GDPR, the new deal adjusts the balance (for the better protection of data subjects) where consent is the basis for the processing of data.[37] However, so long as consent is merely a sufficient rather than a necessary condition for processing personal data—a point that the Commission emphasises—it is arguable that the supposedly fundamental rights of Europeans to privacy and data protection are undersold.[38]

Within the (third-tier) range of acceptability, a commitment to a high-level of protection has to be put in perspective. Whether the adjustments involve more or less protection, this is regulatory business as usual. These protections are side constraints on general regulatory objectives—as the Commission put it when introducing the new deal for consumers, 'A healthy consumer environment is a key factor for economic growth'[39]; and, there is a bandwidth for such protections to be acceptably tuned up or tuned down. Crucially, in the bigger picture, the social licence is the least important element: quite simply, there is much more to respecting and protecting consumers and data subjects than routinely rebalancing the economic interests and preferences of, on the one side, suppliers and data processors and, on the other, consumers and data subjects.

## 6. Conclusion

The central point of this response is that the regulatory environment for AI needs to be self-consciously and explicitly orientated to the full range of regulatory responsibilities. Essentially, there are three take-home messages. First, notwithstanding the attention paid in the EU to the protection of consumers and data subjects, there is a danger that we focus too much on routine adjustments to the balance of interests that qualifies for a social licence. Secondly, if we are to fulfil the promise of a high level of protection for consumers and data subjects, particularly so where connectivity is AI-enabled, the regulatory environment must be clearly and firmly anchored to the values that Europeans distinctively regard as fundamental and constitutive of their collective identity. Rethinking the

---

new deal and, particularly, for criticism of the *proposal* to exclude the right of withdrawal in distance and off-premises contracts where consumers have actually used the goods rather than simply trying them out).

37 See GDPR, Article 4 (11) (defining consent).

38 Compare the critique in Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Oxford: Hart, 2007).

39 European Commission (n 11), para 1.1.

community licence in the EU in response to the latest technological developments is, as we have said, a major challenge. Thirdly, and most importantly, in our connected societies, the highest risks relate to the maintenance of the global commons, to the pre-conditions for the existence of humans and the exercise of their agency. Labels such as 'human-centric', 'trustworthy', and the like might have some utility but care needs to be taken that they do not divert us from asking, and trying to answer, the most important questions on the regulatory agenda.

## 2. Lessons from EU data protection past experience: The Way Forward

In the last five years, developments around Artificial Intelligence (AI) have been at the epicentre of policy and legal scholarship on the regulation of new technologies. The scholarship is abound with critical appraisals of AI applications that redefine the terms of trade policies, create novel economic incentives and aspire to improve social welfare. In some cases, the analytical emphasis is laid on requirements for realising AI's revolutionary potential for productivity and economic growth, whereas other accounts prefer to caution against the risks for users caused by AI. Being aware of these issues, European Commission needs now sketch a novel path for the regulation of AI on the European level. For this purpose, we suggest that the European policy makers consider any lessons that can be learned from the 2-years GDPR experience.

This comparative avenue (between Data protection and AI regulation is likely to prove fruitful for strategy planning. Both frameworks aim at enforced accountability and strengthening the protection of existing EU principles. Both of them intend to empower users and highlight the obligations of the data controllers on the one hand, and the AI deployers on the other. Protection of personal data was urgent, as it is now the case with AI applications. With AI technology, companies now can 'super-profile' consumers, i.e. predict their needs even before such needs arise, often without providing sufficient information as to their particular collection and processing practices within AI applications. Given that AI technology supports the intensity of processing the EU legislature should consider whether the new regulatory framework should have an *ex ante* focus regarding the AI deployers obligations to protect the rights of AI applications' users, as the GDPR has with regard to the data controllers obligations. The same applies to the GDPR's reactive approach with regard to compliance- this reactivity to reaffirm and enhance AI deployers' responsibility must be an integral part of the new AI framework.

The White Paper adopts a risk-based approach and limits its scope to *high-risk* AI applications. This is crucial for the comparative line of analysis that is suggested in this paper. First, the concept of 'risk' should be clear in the context of AI regulation. Then, the concept of 'high risk' should be clarified further. For these purposes there is a possible comparison that can be made on notion of 'high risk' in the two frameworks of GDPR and the future AI framework. On the concepts' definitions, must the 'quality' and 'severity' of risk in the GDPR be a part of the 'critical sector and critical use' assessment in the future AI framework? It is essential for EU harmonisation purposes that there is a common understanding of the notion of risk. Since the Commission confirms that there will be an exhaustive list of 'high risk' sectors (in contrast with the non exhaustive approach adopted in the GDPR), they should carefully think and delineate the assessment processes for high risk, as well as whether this assessment will be 'objective' as proposed in the GDPR context.

Going further, there are a few issues relating to article 35 GDPR can be useful in the AI context. Will the interpretation of 'high' risk approach proposed in the White Paper relate to factors that need to be considered when deciding whether a type of processing is going to result in a high risk? In other words, what is the relation of the considerations on 'nature, scope, context and purposes' with the 'sector' and 'use' in the new AI framework? Will the affirmation of a 'high -risk sector' be informed by the interpretations on the GDPR'S context (art 35)? Is the 'critical use' in the new framework to be interpreted in accordance with the interpretations on the 'purposes' of data processing?

Given that both in the GDPR and in the forthcoming framework on AI there will the obligation to perform impact assessments, there should be sufficient clarity with regard to how this will work in practice for companies. In other words, if the new AI framework is to put forward obligations on the AI deployers to mitigate potential high risks after impact assessments (as GDPR does with introducing the obligation of data controllers to conduct DPIAs) the Commission should make sure that the guidelines provided by the legislature will be clear enough for the AI deployers to follow.

Finally, a few questions emerge on the intersection of AI application and different legal disciplines. How would we calculate the degree of risk for the purposes of each legal field eg for consumer protection, IP rights protection? How would impact assessment work for these different legal fields? What are potential cases of high-risk applications in these fields and how would individuals benefit from the application of the new framework? If the EU aspires for an effective framework, that protects individuals' rights in the context of AI applications, the aforementioned questions should be considered by the Commission's legal teams before the implementation of the new AI framework.