Co-regulation and AI-Innovation: Principles for a Sustainable Framework Fostering Innovation and Acceptance of AI

Roeland W. de Bruin

Abstract This contribution focuses on the proposed EU AI-act, and specifically on the role that co-regulation might play in the regulation of AI-innovation. Amongst many other things, the Union legislator aims to promote AI innovation in view of the economic, environmental and societal advantages that could be expected from AI-technology. At the same time, the European Commission acknowledges that AI innovation involves risks. The legislator strives to find a balance between stimulating innovation and the AI-economy on the one hand, and lawful, trustworthy and safe AI, respecting the fundamental rights of EU citizens, on the other hand. This paper illustrates several principles that could be useful for regulators who are seeking to meaningfully involve private actors in the regulatory process, in their balancing act between stimulating innovation in the field of AI and ensuring acceptable results of such innovation for EU-citizens. Both formal and material aspects of the regulatory process will be addressed. Similar to the methodology I used in my dissertation, I address the EU's own "better regulation" principles regarding the formal aspects. As to the material aspects, I evaluate the factors I found to be significant for AI-innovation and acceptance thereof, i.e. stringency, flexibility and legal certainty from an innovators perspective, and risk and trust from a AI-consumers perspective

Keywords AI · Regulation · Innovation · Trust · Trustworthy · Co-regulation · Private actors · Liability · Privacy

R. W. de Bruin (✉)
Utrecht University, Utrecht, Netherlands
e-mail: R.W.deBruin@uu.nl

M. I. Aldinhas Ferreira (ed.), *Producing Artificial Intelligent Systems*,
Studies in Computational Intelligence 1150,
https://doi.org/10.1007/978-3-031-55817-7_8

1 Introduction

Regulating artificial intelligence (AI) stands high on regulatory agendas. Recently, the European Parliament adopted (with some amendments) the AI-act,[1] proposed in 2021 by the European Commission. The *trilogue* between the Parliament, Commission and the Council has now recently been concluded and can soon be expected to enter into force.[2] On the other side of the Atlantic ocean, the Blueprint for an AI Bill of Rights has been issued by the White House.[3] The OECD has issued its recommendations on AI already in 2019,[4] and the Council of Europe is currently working on a multi-faceted approach to AI-regulation—to mention a few examples of AI-regulation in preparation.[5] Meanwhile, the EC's own Executive Vice President Vestager concluded that the regulatory processes run too slowly, and has announced that the EU and the US will investigate the possibilities to draft a voluntary code of conduct regarding (non-binding) international standards and principles for AI-development.[6]

This contribution focuses on the EU AI-act, that is likely to become an important source of law in the not-so-far future, and specifically on the role that co-regulation might play in the regulation of AI-innovation. Amongst many other things, the Union legislator aims to promote AI innovation in view of the economic, environmental and societal advantages that could be expected from AI-technology.[7] At the same time, the European Commission acknowledges that "the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society".[8] The legislator strives to find a balance between stimulating innovation and the AI-economy on the one hand, and lawful, trustworthy and safe AI, respecting the fundamental rights of EU citizens, on the other hand.[9]

---

[1] https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai.

[2] "In this contribution, I mainly used the original texts from 2021, but I have indicated it where the post-trilogue-text implicate significant deviations, in which case I refer to it as AI-Act (Trilogued):" Provisional Agreement resulting from interinstitutional negotiations, 2-2-2024 (COM(2021)0206 - C9-0146(2021) - 2021/0106(COD))

[3] https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

[4] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[5] https://www.coe.int/en/web/artificial-intelligence/home.

[6] https://www.insideprivacy.com/artificial-intelligence/eu-and-us-lawmakers-agree-to-draft-ai-code-of-conduct/; https://www.reuters.com/technology/eus-vestager-sees-draft-code-conduct-ai-within-weeks-2023-05-31/.

[7] See the Explanatory Memorandum to the Proposed AI Act (EC proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM (2021) 206 final, referred to hereinafter as AI Act), pp. 1–2.

[8] Ibidem, p. 1.

[9] Ibidem, p. 3.

As it stands, the Union regulator seeks to find this balance between AI-innovation and acceptable outcomes of such innovation, through a "balanced and proportionate horizontal approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development […]".[10] In that, the Union regulator will strongly rely on private actors from within the AI-sector to fill in certain flexible and principle-based norms that are to be provided under the proposed AI-act, by means of (technical) standards and codes of conduct for compliance with the open norms that are currently being drafted.

My aim is to illustrate several principles that could be useful for regulators who are seeking to meaningfully involve private actors in the regulatory process, in their balancing act between stimulating innovation in the field of AI and ensuring acceptable results of such innovation for EU-citizens. Both formal and material aspects of the regulatory process will be addressed. Similar to the methodology I used in my dissertation,[11] I will address the EU's own "better regulation" principles regarding the formal aspects. As to the material aspects, I will address the factors I found to be significant for AI-innovation and acceptance thereof, i.e. *stringency, flexibility* and *legal certainty* from an innovators perspective, and *risk* and *trust* from a AI-consumers perspective.

In chronological order, I will first sketch how co-regulation could become embedded in the proposed AI-act (Sect. 2). Then, (formal) aspects of regulatory quality will be addressed (Sect. 3), followed by material aspects: Sect. 4 focuses on the innovator's perspective, whereas the consumer's perspective is addressed in Sect. 5. Conclusions are drawn in Sect. 6.

2 Co-regulation Under the Proposed AI-Act

The AI-act distinguishes between three categories of AI-systems, to which a fourth one is added in the EP-proposal, comprising those posing (1) unacceptable risks,[12] (2) high-risks,[13] risks associated with (3) General Purpose AI,[14] and (4) limited

[10] Ibidem.

[11] De Bruin [1].

[12] These include for example cognitive behavioural manipulation mechanisms, or comprise social scoring mechanisms, or contain real-time biometric identifications systems (see article 5 AI-act; and also https://tinyurl.com/2mfajfme).

[13] These systems may negatively affect fundamental rights protection, or safety of citizens, and may include systems to which EU product safety rules apply (for instance cars, aviation technology; toys, medical devices and elevators). Also high-risk will be AI systems allowing for biometrical identification; AI systems connected to critical infrastructure; AI in education; AI related to employment, worker management and access to self-employment; essential services; law enforcement; migration, asylum and border control; assistance to legal interpretation and application of law (Article 6 AI-act and annexes I, II and III; see as well https://tinyurl.com/2mfajfme).

[14] Such as ChatGPT, https://tinyurl.com/2mfajfme. As regulated under Title VIIIA AI-Act (Trilogued)

risks,[15] to citizens. Most heavily regulated will become high-risk AI-systems. The requirements for those systems are set out in Chap. 2 of the AI-act.

These systems for instance have to be administered (on a continuous, iterative basis in a risk management and mitigation system.[16] Article 10 sets outs data-quality criteria for high-risk AI-systems. It is for instance stipulated that "training, validation and testing data sets shall be subject to *appropriate* data governance and management practices"[17] (emphasis added), which must be "relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose.[18] Furthermore, adequate records shall be kept through logs. Article 12(2) states that "a level of traceability must be ensured that is appropriate to the intended purpose of the system", and certain minimum criteria are given of the AI-system's functioning throughout its lifecycle that is *appropriate* to the intended purpose of the system".[19] Also, it is required that these systems will be designed in such a way that "their operation is *sufficiently* transparent to enable deployers to interpret the system's output and use it appropriately".[20] Furthermore, high-risk systems ought to be "*effectively* overseen by natural persons"[21] during their use, and an "*appropriate* level of accuracy, robustness and cybersecurity"[22] must be ensured. Although the AI-act does at some points provide minimum criteria, the aforementioned norms (there are many others that I did not mention here) are left open, to be filled in by the regulatees and other, private, regulators.

As the Union legislator observed, these principle-based, open norms should contribute to a "robust and flexible legal framework".[23] The legislator sees to the creation of "standards of by other technical specifications […] developed in accordance with general engineering or scientific knowledge at the discretion of the provider of the AI system".[24] In that, the legislator aims to provide flexibility to AI-innovators to choose their own ways to comply with the requirements. This principle is stipulated in article 40:

> High-risk AI systems which are in conformity with harmonised standards […] shall be presumed to be in conformity with the requirements set out in Chapter 2 […] to the extent those standards cover those requirements.

Article 41 adds that where harmonised standards do not exist (yet), or deemed insufficient, that "the Commission may, by means of implementing acts, adopt

---

[15] All other systems in which AI is embedded. See article 3(1) and Annex I AI-act.

[16] Article 9 AI-act.

[17] Section 2.

[18] Section 3.

[19] Emphasis added.

[20] Article 13(1) AI-act, emphasis added.

[21] Article 14(1) AI-act, emphasis added.

[22] Article 15(1) AI-act, emphasis added.

[23] AI-act, p. 3 (explanatory memorandum).

[24] Ibidem, p. 13.

common specifications in respect of the requirements of Chap. 2."[25] The Commission must "consult with an advisory forum in which stakeholders such as industry, start-ups, SMEs, civil society and academia participate, as well as the Fundamental Rights Agency, the Agency for Cybersecurity, CEN, CENELEC and ETSI"[26] when preparing such common specifications. Section 3 establishes that high-risk AI-systems conforming to the respective common specifications, are presumed to be complying with Chap. 2.

Apart from the mandated co-regulation under article 40 and 41, the Union legislator also calls upon private actors to provide voluntary rules, when it concerns limited-risk AI-systems. Article 69 encourages the Union- and Member State legislators to "encourage and facilitate the drawing up of codes of conduct intended [...] to foster the voluntary application to AI-systems other than high-risk AI-systems of [...] the requirements set out in [Chap. 2]".[27] These codes of conduct can be prepared by "individual providers or deployers of AI systems or by organisations representing them or by both, including with the involvement of deployers and any interested stakeholders and their representative organisations, including civil society organisations and academia".[28]

3 Formal Aspects: Regulatory Quality

3.1 EU Perspective

The idea to "mix" policy instruments,[29] i.e., stemming from different governance levels, including different levels and modes of private and public regulation in order to reach certain desired goals, lies at the core of the EU strategy on "Better Regulation" and its (later) REFIT-programme. The European Commission observed from 2001 onwards, that better and faster regulation requires *inter alia* top-down rules issued by the public (EU) legislator, to be "combined with other non-binding tools, guidelines or even self-regulation within a commonly agreed framework […and…] co-regulation [combining] legislative and regulatory action taken by the actors most concerned, drawing on their expertise".[30] Examples of co-regulation as a part of Union legislation,[31] include for instance the General Product Safety Directive, relying on privately

[25] Section 1.

[26] Section 2. jo. article 58a AI-Act (Trilogued)

[27] Section 1.

[28] Section 3.

[29] THIS idea was originally coined by Gunningham and Sinclair [2], pp. 49–76.

[30] European Commission 2001, "European Governance—a white paper", COM (2001) 428 final, pp. 20–21. See for further references De Bruin [1], Sect. 3.3.4.

[31] See for many more: the Database on Self- and Co-regulation initiatives by the European Economic and Social Committee: The Database on Self- and Co-Regulation Initiatives | European Economic and Social Committee (europa.eu).

regulated standardisation regarding product safety,[32] and the General Data Protection Regulation (GDPR), which aims for codes of conduct, industry standards and certification mechanisms to fill-in the many open norms contained in the GDPR.[33]

Often mentioned benefits of co-regulation (more specifically the involvement of private actors) include for example the ability to rapidly respond to societal and technological developments (where pure public regulation mostly lacks this agility),[34] and to "tailor" the respective rules better to the needs and possibilities of those to whom the rules are to apply (*regulatees*),[35] in a transnational, and cost-efficient way.[36]

However, as a part of the regulatory process would be "outsourced" to non-governmental actors, there are several risks connected to co-regulation addressed in literature. Democratic legitimacy is a point of concern. The involvement of private actors in the regulatory process should be well-embedded within the regulatory framework, in order to provide for adequate mandate and democratic justification.[37] Furthermore, transparency is important. As private actors involved in a regulatory process are, as opposed to public regulators, in principle not subject to democratic scrutiny including checks-and-balances (and often not accountable for their regulatory actions), it is most relevant to duly observe the transparency of the co-regulatory process.[38] Also, there is a certain risk that not *all* respective regulatees are duly represented.[39] This would implicate the risk of under-protection of the (core) values, rights or interests of the non-represented actors.[40] Another risk is that the co-regulated framework would not be sufficiently monitored and/or enforced during its lifecycle.[41]

The legislating institutions of the European Union acknowledged these (and other) risks, in different forms throughout the past two decades. For instance in the 2016 Interinstitutional Agreement on Better Regulation, it is stated that the principles on democratic legitimacy, legal certainty, proportionality and subsidiarity should be observed.[42] Also, they stress the importance "to promote the utmost transparency of

[32] See preambles 14, 15, and articles 3(2–3), 4(1) and following of the General Product Safety Directive).

[33] See preambles 81, 100, 166 and articles 24(3), 25(3), 27(5) and following of the GDPR.

[34] Cafaggi, F., "Rethinking private regulation in the European regulatory space", EUI Working Paper LAW No. 2006/13, p. 8–9.

[35] Baldwin et al. [3], p. 139, De Cock Buning and Senden [4], p. 4.

[36] Ibidem Baldwin et al. [3], p. 140, De Cock Buning and Senden [4], pp. 4–5.

[37] See Baldwin et al. [3], pp. 141–142, De Cock Buning and Senden [4], pp. 4–5; Kulk [5], p. 52.

[38] See Baldwin et al. [3], pp. 142–143.

[39] See Baldwin et al. [3], pp. 141–142, De Cock Buning and Senden [4], p. 5.

[40] De Cock Buning and Senden [4], p. 5.

[41] Ibidem.

[42] Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Lawmaking, 13 April 2016, *OJ* 12 May 2016, L 123 (IIA 2016), p. 2. Via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016Q0512(01)&from=EN.

the legislative process".[43] The relevant stakeholders should be invited to participate in the drafting of regulation in an open and transparent way.[44] Monitoring and evaluation of the rules must be an ongoing activity.[45] Regarding co-regulation specifically, the 2003-edition of the Interinstitutional Agreement on Better Lawmaking, which principles likely still apply to the 2016-edition and the REFIT-toolbox,[46] *inter alia* held that there should always be a solid basis to involve private actors in a legislative act.[47] Furthermore, it was stressed that arrangements should be compliant with (union, then: Community) law.[48]

From the literature and the applicable EU regulatory policy,[49] and summarizing the sections above *inter alia* the following factors can be distilled that could at least be considered from a formal point of view in co-regulatory processes[50]:

i. Ensuring an adequate legislative mandate, and
ii. Ensuring accountability of the public regulator for the co-regulatory activities, in order to guarantee democratic legitimacy;
iii. Ensuring that all relevant stakeholders have access to the process and the outcomes thereof, and
iv. Ensuring that the (private) stakeholder participation is characterised by principles of transparency, equality, fairness and consistency of treatment.

3.2 AI-Act and Co-regulatory Quality

The harmonised standards to which article 40 AI-act refers, will have to be newly drafted. It is likely that the European Committee for Standardization (CEN) and

---

[43] Ibidem. See also the toolbox on Better Regulation (European Commission, "Better regulation 'Toolbox'," complementing Commission Staff Working Document, "Better Regulation Guidelines", SWD(2017) 350 final, available via https://ec.europa.eu/info/sites/info/files/better-regulation-toolbox_1.pdf, and https://ec.europa.eu/info/law/law-making-process/better-regulation-why-and-how_en), p. 4 (transparency).

[44] Ibidem, Sect. 19. See also the Better Regulation toolbox, p. 8 (stakeholder involvement).

[45] Ibidem, Sect. 22. Also, Better Regulation toolbox, pp. 8–9.

[46] De Bruin [1], p. 46.

[47] Interinstitutional Agreement (European Parliament, Council & Commission) on Better Lawmaking, 13 December 2003, *OJ* 31 December 2003, C 32 (IIA 2003), Sect. 18. Via: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003Q1231(01)&from=EN.

[48] IIA 2003, Sect. 20.

[49] As further elaborated in my dissertation, Sect. 3.3, pp. 36–47. See for a useful overview of procedural principles that should be observed in standardization processes also Kanevskaia, O., *The law and practice of global ICT standardization* (diss.) TILT (open access edition, https://research.tilburguniversity.edu/en/publications/the-law-and-practice-of-global-ict-standardization) 2020, who mentions *inter alia* "transparency, openness, consensus, effectiveness, coherence, review and balance of interests" (p. 267).

[50] Many more factors can be indicated of course—what I do not mention here for example is the "internal" agenda-setting of the regulator as well as political validation-; implementation support- and monitoring-; quality control requirements et cetera (see De Bruin [1], p. 47).

the European Committee for Electrotechnical Standardization (CENELEC) will be responsible for developing these standards.[51] CEN-CENELEC has formed a working group (CEN-CENELEC/JTC 21) to that end.[52] As Perarnaud argues, the organisations represented in the participants in (technological) standardisation processes, mainly consist of industry stakeholders.[53] Other stakeholders, such as civil society and fundamental rights organisations are often underrepresented. He furthermore illustrates that the working processes of standardisation organisations are not very transparent, and even "relatively hostile to outsiders".[54]

Nonetheless, the European Commission has called upon CEN-CENELEC in its draft standardisation request, to include small and medium enterprises, civil society organisations, and consumer organisations at EU- and national levels, and should consult experts in the areas of fundamental rights, and to "provide the necessary evidence in the context of interim and final reports provided on the execution of the standardization request".[55] Thus, the EC in fact obliges standardisation organisations to include those actors in the co-regulatory process. Also the Trilogued version of the AI-act provides in article 58a for the inclusion of inter alia start-ups, SMEs, civil society, academia and the Fundamental Rights Agency in the co-regulatory processess (albeit in an advisory role). However, there are doubts whether this would in practice ensure that these voices will be heard.

EDRi stresses *inter alia* that standards should not be used to "take decisions that require democratic scrutiny or legislative interpretation",[56] which would be the case under the proposed article 40 AI-act. They underscore that it is not within the area of expertise of the standardization organizations to provide the standards asked for under the AI-act. Also, they state that the standardization processes are "inaccessible to those without the resources to learn the processes and finance their involvement".[57]

The points made by EDRi and illustrated by Perarnaud, relate *inter alia* to the legislative mandate and democratic accountability of the regulator, stakeholder participation and transparency: they seem to argue that "guaranteeing" due observance of fundamental rights by AI-systems, should not be delegated to standardization organizations. At the same time, the fact that their regulatory processes are not open to the public detriments the democratic public watchdog function—and

---

[51] See Perarnaud [6].

[52] Artificial Intelligence—CEN-CENELEC (cencenelec.eu).

[53] Perarnaud [6].

[54] Ibidem, and see also his reference to Changing minds and machines: a case study of human rights advocacy in the Internet Engineering Task Force (IETF)—ORA—Oxford University Research Archive.

[55] EC 5 December 2022, "A notification under Article 12 of regulation (EU) No 1025/2012, Draft for a Commission Implementing Decision on a standardisation request to the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) in support of safe and trustworthy artificial intelligence" (Draft Standardisation Request) point 14 and article 1 and article 3(5).

[56] The-role-of-standards-and-standardisation-processes-in-the-EUs-Artificial-Intelligence-AI-Act.pdf (edri.org) (EDRi 2023).

[57] Ibidem.

it cannot be guaranteed that all relevant stakeholders will in fact participate in the standardization process.

Regarding the Commission's encouragement to draft voluntary codes of conduct for providers of non-high-risk AI-systems in article 69, the following must be observed. While the legislator aims at broad stakeholder involvement there will always be the risk that not all relevant actors are included in the process. Should it appear that the smaller actors are under-represented when compared to larger organizations, this could have problematic consequences. It may furthermore be easier for the larger actors (with more funds) to eventually comply with the obligations than smaller organizations when codes of conduct will eventually enter into force and become de-facto standards.[58] Similar to the concerns regarding the harmonized standards, it must be noted that the codes-of-conduct drafting processes would not necessarily be characterized by openness and transparency.

4 Material Aspects: Innovators Perspective

4.1 Legal Certainty, Stringency, and Flexibility in Theory

In the past decades, the interplays between the contents of regulatory frameworks and innovation have increasingly been the subject of academic research.[59] Albeit there are many factors enshrined in the bodies of legislation that might influence innovation that are mentioned in the literature, largely varying in kind and nature, mainly two "strands" can be identified. Firstly, there are factors that might influence the ability, capacity and/or willingness of innovators to develop novel technology and bring it to the market. The most important factors within this *innovator's perspective* that I found in my research, include *legal certainty*, *stringency,* and *flexibility* (discussed below).[60] From a *consumer's perspective*, the factors *risk* and *trust* play an important role in the acceptance of innovative technology (discussed in Sect. 5).[61]

a. Legal certainty

Legal certainty implies that rules should be formulated precise, unambiguous, and predictable for all *regulatees*, over a longer period of time.[62] This material legal certainty,[63] comprises of two parts: *predictability* and *stability* of rules and judicial decisions. Predictability implicates that the contents of a regulatory framework

[58] See De Bruin [1], pp. 309–310; De Cock Buning and Senden [4], pp. 4–5.

[59] See for a high-level overview: De Bruin [1], pp. 47–49; also Pelkmans and Renda [7]; Ranchordás [8].

[60] See De Bruin [1], Sect. 3.4.2.

[61] Ibidem, Sect. 3.4.3.

[62] De Bruin [1], p. 50 and the references there in footnote 274.

[63] Which can be distinguished from formal material certainty, relating to the legibility, clarity and public availability of rules and judicial decisions.

(which may consist of laws and rules) and judicial decisions "must meet the reasonably foreseeable and calculable expectations of those actors to whom these apply".[64] Thus, *regulatees* should be able to plan and adapt their behaviour according to the applicable rules. Also, predictability implicates that it is clear how one should behave to comply with the respective rules.

Stability implies that rules should not deviate too much over time—as that would not be beneficial *inter alia* in terms of predictability: predictions should remain valid as long as possible. When regulating new technologies, stability and predictability may appear to be contradictory in some situations. On the one hand, a regulator should aim for clear and precise instructions regarding the expected behaviour with or towards the novel technology. In that, it may seem necessary to specifically address the technology in the rule. On the other hand, when that technology would change over time, the rule may no longer be accurate—which is a disadvantage in sense of stability. Thus, it is advisable to refrain from technology specific regulations as much as possible,[65] and to draft rules that are technology-independent.[66] Rules should therefore be technology-neutral, i.e. focussing on the results of technology rather than on the technology itself—while at the same time aiming for maximum predictability.

It is observed that legal certainty is crucial for innovation,[67] and that legal uncertainty could impactfully hinder innovation,[68] which should thus be avoided or resolved as much as possible.

b. Stringency

Stringency sees to the (financial) efforts for regulatees to comply with the applicable rules. Ashford, Ayers and Stone even find this to be "the most important factor influencing technological innovation".[69] Pelkmans and Renda observe a rule to be stringent, when "firms need to significantly change their behavior or to develop new technology in order to comply with the regulation", which would have significant financial implications for them.[70] Stringent regulation is not necessarily bad: there may be very good reasons for reaching changes in behaviour, or certain technological innovation—for instance to reach societal or environmental goals, and stringency could even positively impact consumer trust.[71]

According to Ashford, Ayers and Stone, regulation should be as stringent as feasible in order to reach maximal results.[72] However, high compliance costs that

[64] De Bruin [1], p. 51.

[65] Cock Buning [9], p. 224, 228.

[66] Koops [10], p. 6; Pelkmans and Renda [7], pp. 11–12.

[67] de Bruin [11], 1–55,republished under the same title by Northwestern University School of Law, *Faculty Working Papers* 2010, Paper 108.

[68] Pelkmans and Renda [7], p. 12.

[69] Ashford et al. [12], p. 426.

[70] Pelkmans and Renda [7], p. 11.

[71] See below, Sect. 4c, and Blind [13], p. 395.

[72] Ashford et al. [12], pp. 463–464.

should be made to reach (maximal) compliance, could be too burdensome, especially for small businesses. In turn, this could be bad for innovation, as "the innovation-enhancing potential of stringent rules is replaced by a discouraging effect on existing firms",[73] and it could be prohibitively difficult for starting companies to enter into a certain business due to too high compliance costs.[74] Overly stringent rules could furthermore have as undesired effects that regulatees start to seek ways to avoid the rules, or never go beyond minimum compliance.[75]

Thus, *stringency* can be problematic for innovation when compliance burdens are too high, as it then would become unlikely that the regulatory goals will be met.

c. Flexibility

There are two types of *flexibility* that must be distinguished here. The first type relates to the "number of implementation paths firms have available for compliance".[76] A larger of implementation paths (thus more flexibility) would be preferable over a smaller number (less flexibility), as companies should be able to choose the route towards compliance that is most suitable for them, and their business processes. Less flexibility may implicate higher compliance costs (i.e. higher *stringency*) in order to adapt the business processes to the desired compliance route, which in turn would limit the innovation budget.[77] In this sense, performance- or outcome-based standards can be argued to offer more flexibility than rules prescribing the ways to attain the desired results.[78]

The second form relates to the capacity of regulation to adapt to technological or societal changes.[79] Also from this perspective, standards which aim for a certain outcome or behaviour provide for a higher level of flexibility than for instance technology-specific or otherwise prescriptive rules. The latter would be less sustainable, and thus (also in terms of *legal certainty* cq *stability*) less preferable from an innovator's perspective.

Both types of *flexibility* can impact innovation, whereby regulation allowing for multiple potential compliance paths for innovators and technology-neutral, non-prescriptive standards are preferable over rigid, technology- or prescriptive rules.

[73] Pelkmans and Renda [7], p. 11.

[74] See for instance [13], p. 394.

[75] Stewart [14], p. 2.

[76] Pelkmans and Renda [7], p. 5, quoting Stewart [14], p. 3.

[77] Stewart [14], p. 5.

[78] Luppi and Parisi [15], pp. 43–53; Van der Heijden [16], pp. 727–728, Gunningham and Sinclair [17], p. 711; and Stewart [14], p. 5, 23.

[79] SEE for example Ranchordás [8], p. 143.

4.2 Legal Certainty, Stringency, and Flexibility in the AI-Act

a. *Legal Certainty*

The Union legislator seems to provide certainty for innovators through a layered regulatory approach of "open" norms enshrined in the proposed AI-act which are to be filled in through harmonized standards and common specifications established through implementing acts. This implicates *stability* on the level of the AI-act, while enabling flexibility to adapt the rules to technological and societal developments via lower regulatory levels.

However, since the many open norms mainly contain principles on a procedural level, but are lacking guidance in a material sense, the *predictability* of the current set of rules is strongly dependent on the standards and specifications still to be co-regulated—and for now to be evaluated as "low". This unpredictability can prove problematic for high-risk AI-providers who need to comply with requirements regarding for instance the implementation of risk management systems (article 9); data quality (10) and -governance; logging (12); transparency and information provision (13); human oversight (14); accuracy, robustness and cybersecurity (15); quality management (17) and conformity assessments (19)—to name a few. The Draft Standardisation Request calls on CEN-CENELEC to adopt standards on *inter alia* aforementioned points, before the end of January 2025. Whether this date would be maintained in an eventual Standardisation Request remains to be seen, but it is a 'tight deadline' as it stands. Should the provisions of the Regulation be enacted *before* the respective standards have been adopted, the unpredictability and therefore *legal uncertainty* would remain.

Although being less strict in its standardization requirements (the drafting of codes of conduct and certification mechanisms was just "encouraged" by the legislator),[80] it must be noted that the GDPR might not serve as a good example in this respect. More than 5 years after the GDPR entered into force,[81] only 4 codes of conduct have been approved by the European Data Protection Board, and 0 certification mechanisms, seals, or marks.[82]

b. *Stringency*

The AI-act contains implicates a whole new set of rules to be complied with by AI-innovators, in order to protect consumers from negative outcomes of the application of AI-systems. There is a strict enforcement mechanism foreseen in the proposed AI-act, which seems inspired by the enforcement mechanisms enshrined in the GDPR. Compliance can be enforced in several ways, for instance by Member State authorities through "appropriate measures to restrict or prohibit the high-risk AI system

[80] See article 40(1) and 42(1) GDPR.

[81] https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en.

[82] https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en.

being made available on the market or ensure that it is recalled or withdrawn from the market",[83] through warnings and non-monetary measures, and/or to fine the respective innovator. Non-compliance with article 5 (regarding forbidden practices) or article 10 (regarding data quality and -governance) can be fined with a penalty of € 35.000.000 of 7% of the annual worldwide turnover, whichever amount is higher.[84] Non-compliance with the other provisions of the AI-act, can be subject to fines up to € 15 million, or 3% of the annual worldwide turnover.[85] Lying to a notified body, or national competent authorities can result in a € 7.5 million penalty, or 1% of the annual worldwide turnover.[86] Given the facts that innovators will likely have to invest heavily to comply with the norms, while the (to be co-regulated) norms are not clear (yet), and the fines are potentially astronomous, can lead to the assumption that the *stringency* of the proposed regulatory framework is "high".

Furthermore, it must be noted here that although the AI-act does not contain a civil-liability regime (comparable for instance to the regime stipulated in article 82 GDPR), the advent of AI has brought the Union legislator to propose changes to the Product Liability Directive,[87] (PPLD) and to draft a entirely new set of rules regarding the non-contractual liability for AI, also in the form of a directive, (AILD).[88] As I have elaborated in other contributions on the PPLD,[89] and the AILD,[90] mainly the PPLD may arguably lead to increased *stringency* for innovators.

Software (including AI-algorithms) will be brought under the scope of the PPLD,[91] and virtually all actors in the supply chain of AI-systems will become subject to the risk-based liability rules.[92] This implicates *inter alia* that consumers who suffer damage from "defective" AI, can claim compensation. Products under the PPLD are defective, when a product does not "provide the safety which the public at a large is entitled to expect",[93] taking all relevant circumstances into account, including for instance "the effect on the product of any ability to learn after deployment",[94] the manufacturer's ability to control the product after it has been marketed, for instance through updates or upgrades,[95] as well as "product safety requirements, including safety-relevant cybersecurity requirements".[96] This implicates that when

[83] Article 68(2) AI-act.

[84] Article 71(3) AI-act.

[85] Section 4.

[86] Section 5.

[87] COM (2022) 495 final, 2022/0302, Proposal for a Directive on liability for defective products.

[88] COM (2022) 496 final, 2022/0303, Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence.

[89] See de Bruin [18–20], pp. 89–106.

[90] De Bruin [21].

[91] Article 4(1) PPLD.

[92] Article 7 PPLD.

[93] Article 6(1) PPLD.

[94] Sub c.

[95] Sub e.

[96] Sub f.

an AI-product does not conform to the applicable safety requirements (including for instance those to be co-regulated under the AI-act) may play a role in the determination of "defectiveness", although non-compliance does not automatically lead to a presumption of defectiveness.[97] It is up to the victim to prove defectiveness, the damage and causality between the defectiveness and the damage occurred.[98] This implies that a victim would need access to meaningful information regarding the (non-) functioning of an AI-product, in order to successfully argue that it might have been defective, and that it may caused damage. In order to alleviate the burden of proof, the Union legislator will obligate users and providers if AI-systems to disclose the necessary information to a victim who has a plausible claim under the PPLD.[99] Should a defendant refuse a court order to disclose certain information, this may lead to the *presumption* that the respective product was defective.[100] Defectiveness should also be presumed when the claimant can establish "that the product does not comply with mandatory safety requirements […] that are intended to protect against the risk of the damage that has occurred",[101] or when there was an "obvious malfunction of the product during normal use under ordinary circumstances".[102] Further procedural aids for victims are stipulated regarding the causal link between defectiveness and damage, when the defect has been established, and the damage is "typically consistent" therewith.[103] Judges may even presume both causality and(/or) defectiveness when victims face "excessive difficulties due to technical or scientific complexity"—be it that the victim should demonstrate "on the basis of sufficiently relevant evidence" that "the product contributed to the damage", and that it was likely defective, and/or that the "defectiveness is a likely cause of the damage […]".[104] Where producers can traditionally fend off a liability claim with defences based *inter alia* on the argument that the defect came into existence after putting the product on the market, or that the technological or scientific knowledge at the time of marketing did not allow for detection of the defect, these cannot be upheld when the producer still exercises control over the (AI-endowed) product, or failed to provide updates or upgrades that are necessary to maintain safety.[105]

The PPLD thus significantly increases *stringency* when compared to the currently existing product liability rules. However (as will further discussed in Sect. 5) this would implicate a positive and necessary change from a both the *risk and trust* perspective—as it will become easier, and fairer, for victims to successfully claim

[97] See consideration 24 to the PPLD.

[98] Article 9(1) PPLD.

[99] Article 8 PPLD.

[100] Article 9(2)(a) PPLD.

[101] Sub b.

[102] Sub c.

[103] Section 3.

[104] Section 4. See for a critical review E.R. de Jong, "Europeanisering van bewijs en aansprakelijkheid", *NTBR* 2023/8, afl. 3.

[105] Article 10(1)(e) and (2) PPLD.

damages from innovators.[106] Besides the PPLD, the AILD aims to improve the position of victims even further.

The AILD contain procedural rules that victims of AI-related damages may aid in seeking remuneration from a provider or user of an AI-system, on the basis on (non-harmonised) national tort liability rules. It must be noted, that at this point no *material* liability rules are harmonised by the AILD. Comparable with the system in the PPLD (yet more elaborate), the AILD regulates the obligation for AI-users or -providers to store and disclose information on the request of (potential) claimants, to underpin a non-contractual liability claim.[107] Requests may be "enforced" by a national court upon first refusal of the provider of a high-risk AI-system, who may order the respective information to be disclosed to the claimant. When the defendant refuses to comply with a court order to preserve or disclose evidence, a "fault" i.e. "the defendant's non-compliance with a relevant duty of care" under the applicable tort regime must be presumed. Article 4 states more circumstances that should lead to the assumption of a "causal relationship" between a fault of the defendant and the output of an AI-system (or the failure produce an output).[108] This must be the case when:

(A) a *fault* has been established or presumed by (or attributable to) the defendant, "consisting in the non-compliance with a duty of care laid down in Union or national law directly intended to protect against the damage occurred"[109];
(B) it is likely that the *fault* influenced the (failure of an) output by the AI-system[110]; AND
(C) the claimant can demonstrate the causal relationship between the (failure of an) output and the occurred damage.[111]

While the practical improvement for victims can be questioned (see further Sect. 5), the scope of these procedural aids is limited further in Article 4(2) when the defendant is the provider or user of a high-risk AI-system. The presumption of "causality" (i.e. "attribution" to the high-risk AI-provider) may only be done when the *fault* consists in an established violation of certain to be co-regulated norms provided in the AI-act. The norms referred to include those regarding data quality (10(2) and (4) AI-act); transparency (13); human oversight (14); accuracy, robustness and cybersecurity (15 and 16(a)); corrective actions, withdrawal or recall (16(g) and 21). When the defendant is the user of a high-risk AI-system, the same presumption may only be made when the defendant a) failed to monitor the AI-system or to

[106] See De Bruin (2022), Chaps. 7 and 8.

[107] Article 3(1) AILD. The plausibility of the claim must however be underpinned through facts and evidence. Claimants should have "undertaken all proportionate attempts" to get hold of the information out-of-court Sect. 2.

[108] It must be noted that this is *not* the causal relationship between a fault and damage—which is often referred to in the liability doctrine: this notion of causality rather sees (in my opinion) to the *attributability* of a damage-inflicting output to a defendant.

[109] Article 4(1)(a) AILD.

[110] Sub b.

[111] Sub c.

suspend its use according to the instructions (article 29 AI-act), or b) exposed the AI-system to irrelevant input-data (29(3)).

Given the limited scope of the AILD, and that it will often remain difficult for victims to prove a) a norm-violation and b) the "real" causal relationship between norm-violation and occurred damages, I do not think that the AILD-regime will significantly increase *stringency*.

c. *Flexibility*

Albeit the open norms must still be filled in through co-regulatory processes, the entire system of the AI-act sees to maximise flexibility for innovators to comply with the norms-to-be-developed in a non-prescriptive, thus *flexible* way. The envisaged system also provides the means to adapt the norms when technological developments would demand so.[112]

It remains to be seen to what extent the eventual standards and common specifications allow innovators to choose the most suitable compliance paths—and cannot be further evaluated at this point.

5 Material Aspects: Consumers Perspective

5.1 Risk and Trust in Theory

Innovation can hardly be successful if the results thereof are not accepted and adopted by the market. One of the leading theories on (consumer) acceptance of innovations, is the Diffusion Of Innovation (DOI) theory, developed by E.M. Rogers in 1962 (and revised in 2003).[113] He distinguishes five factors (*relative advantage* of the innovation over the established products/ideas etcetera to be replaced; *compatibility* with the existing values, experiences and needs of the consumers; the perceived *complexity* of the innovation; the *triability* of the innovation before adoption and the *observability* of the (results of the) innovation).[114] From a legal/regulatory point of view, the additions to the DOI-literature by Ostlund—relating to perceived *risk*,[115] as well as Carter & Belanger[116] and Van Slyke et al.—relating to *trust*,[117] are worthwhile to elaborate.

[112] See consideration 6 to the AI-act.

[113] Rogers [22] (5th edition), which builds upon the first edition that was published in 1962.

[114] Rogers [22], pp. 229–230, 240–248; 257–259.

[115] Ostlund [23], 23–29.

[116] Carter and Bélanger [24], pp. 5–25.

[117] Van Slyke et al. [25], pp. 32-49.

a. Risk

Perceived *risk*—of different natures, including for instance physical and financial risks, can refrain consumers from adopting innovation.[118] Regarding autonomous vehicles (AVs) for example, Fagnant and Kockelman observe that

> regardless of how safe AVs eventually become, there is likely to be an initial perception that they are potentially unsafe because the lack of a human driver. Perception issues have often been known to drive policy and could delay implementation. Moreover, if AVs are held to a much higher standard than human drivers, which is likely given perception issues, AV costs will rise and fewer people will be able to purchase them.[119]

Although it is impossible from a legal research perspective to investigate consumer *perceptions*, it is possible to study the actual risks for consumers as the result of the application novel AI-technology against the backdrop of existing or future regulation, in terms of for instance financial or physical risks.

b. Trust

Trust is a multi-facetted concept.[120] Relating to innovation, *trust* regards the mental state of those who are to adopt innovative technology. As Rousseau et al. put it: "a psychological state comprising the intention to accept vulnerability based on positive expectations or behaviour of another".[121] This implicates that, despite certain risks that may result from the application of certain innovative products or services, a consumer would still consider adopting it, based on his (safety) expectations, or the behaviour of an innovator to mitigate certain risks. Trust is often associated—at least from a legal perspective—with safety, security and the protection of core values for citizens, such as those enshrined in fundamental rights.[122]

Risk and *Trust* are correlated concepts, but not the same. Albeit *trust* would not be needed without *risk*,[123] *trust* may be behaving independent of *risk*: even if risks are high, trust could be high—or low, and vice versa. While in terms of this contribution, *risk* relates to the potential financial or physical losses by consumers, *trust* is more-encompassing: trust would relate to a higher level of guarantees for consumers, including for instance fundamental rights protection, safety, integrity and reliability.

---

[118] See also Hirunyawipada and Paswan [26], p. 187.

[119] Fagnant and Kockelman [27], p. 177.

[120] See also de Bruin [28], pp. 47–60.

[121] Rousseau et al. [29], p. 395.

[122] Privacy is for instance explicitly mentioned by Van Slyke et al. [25], p. 2. See in a similar vein Balboni [30], p. 9; and Fagnant and Kockelman [27], pp. 177–178.

[123] Ibidem, p. 395.

5.2 Risk and Trust in the AI-Act

a. Risk

The AI-act aims amongst other things to minimise the risk of citizens to be confronted with damage-causing AI. To that end, the Union legislator has drafted a layered framework of norms, to be specified and detailed further through co-regulation. It has been stated above, that at this moment, where standards and common specifications do not yet exist, where the norms thus are very open, the precise obligations for innovators to be complied with, are rather uncertain. This implicates that AI-innovators cannot reasonably calculate their risks, while being confronted with significant enforcement risks. How this uncertainty and stringency that may result from the current text of the proposed AI-act impact the behaviour of innovators is not clear. However, as the legislator aims at the swift development of (sector-specific) standards, and the imminent threat of fines for non-complying innovators, it could be argued that when the standards (and common specifications) are developed soon, and when it would not be too hard to implement these, this may have a positive impact of *risk*, i.e. a reduction of the risks that consumers are currently exposed to by the exploitation of AI-systems *without* any specific regulations being applicable thereto.

When consumers suffer damage resulting from the deployment of AI-systems, they might want to seek remuneration based on the PPLD and the proposed AILD (after enactment). The PPLD entails significant improvements for consumers compared to the "old" product liability rules. The enlarged scope, the newly embedded obligations to keep (AI-)software safe and the procedural aids will lead thereto that successful product liability claims will be more likely than it used to be under the current product liability regime: the *risk* of non-remuneration, and thus that the victim will have to bear its damages himself, will likely decrease significantly.

A similar statement cannot be made regarding the AILD. Despite the embedded procedural aids, it will for instance not be easy for victims to successfully call upon a presumption of "causality" between an AI-system's output and a norm-violation, as *inter alia* the norm-violation and the causal relationship between the norm-violation and the damage still have to be proved by the victim (which would require in-depth technological knowledge and the means to interpret the data used or generated by the AI-system).

b. Trust

The creation of *trust* is one of the drivers for the Union legislator to regulate AI, in order to provide good conditions for the adoption of AI-innovation.[124] Therefore, it is deemed necessary to protect *inter alia* the health, safety and fundamental rights. The layered approach proposed by the AI-act should establish a regulatory framework through which amongst other important things, fundamental rights are solidly (and ex-ante) embedded in AI-systems. There are however questions whether

[124] See consideration 5 to the AI-act.

this should be "outsourced" to standardisation organisations and thus the dominant players represented in the co-regulatory processes.[125]

As long as there are no harmonised standards (or common specifications) in place, it is however hard to establish to what extent these will be in conformity with the fundamental rights catalogues, and whether these may contribute to health and safety of EU citizens.

Another aspect of *trust* relates to the "reparative capacities" of the regulatory framework should the application of AI-systems have led to damage. It must be noted again that the proposed revision of the product liability framework could implicate a very significant improvement of the capacities of the system to remunerate damages resulting from defective AI-products. The AILD however still offers ample room for improvement: the presumptions embedded therein, could be more "generous" for victims: comparable to the envisaged system under the PPLD, it can be recommended that the presumptions are extended to causality between a norm violation and the damage that occurred.

6 Conclusions and Recommendations

In this contribution, I have reviewed to what extent the co-regulation mechanisms embedded in the proposed AI-act contain certain factors that might influence innovation and acceptance of AI-systems in the European Union. The Union legislator envisages co-regulation to fill in many of the AI-act's open norms, through harmonised standards or common specifications. By adhering to these standards or common specifications, providers of high-risk AI-systems can illustrate their compliance with the requirements stipulated by the AI-act. The legislator furthermore encourages the drawing up codes of conduct for voluntary compliance by those who offer other forms of non-prohibited (low-risk) AI-systems.

From a formal perspective regarding "regulatory quality", it has been observed that the legislative mandate and democratic accountability of the regulator, stakeholder participation and transparency within the standardization processes can be questioned, as it appears in practice that mainly larger innovators are represented therein, and that accessibility is a point of concern. It is argued that "guaranteeing" due observance of fundamental rights by AI-systems should not be delegated to standardization organizations. At the same time, the fact that their regulatory processes are not open to the public detriments the democratic public watchdog function—and it cannot be guaranteed that all relevant stakeholders will in fact participate in the standardization process. The backup mechanism proposed in article 41 AI-act may offer more guarantees in this respect: where the Commission adopts common specifications, it would at least be the democratic legislator drafting the specifications itself, using their open and transparent regulatory processes, while being obliged to involve the relevant stakeholders.

[125] See Perarnaud 2023 l EDRi 2023.

With a view to the voluntary codes of conduct, it must be observed that it might be easier for the larger actors (with more funds) to comply with the obligations than smaller organizations when codes of conduct will eventually enter into force and become de-facto standards.

The following recommendations can be made regarding the regulatory quality of the co-regulatory mechanisms:

- Regulate more accessibility and transparency: any interested actor/regulatee should be able to participate without prohibitive costs to the process.
- Make standards (con)testable against fundamental rights, also after these have been adopted.
- Codes of Conduct processes should be examined for openness and inclusivity: not only should it be possible for anyone to participate in the regulatory process, but compliance must also be de facto possible for all regulatees.

In a material sense, from an *innovator's perspective*, the factors *legal certainty* (in terms of predictability and stability of rules), *stringency* (referring to the compliance-efforts to be made in relation to the societal goals to be achieved) and *flexibility* (regarding the number of implementation paths available for innovators to comply, and regarding the capacity to adapt to changing technological and societal circumstances) have been evaluated.

The co-regulation mechanisms aim to offer *high flexibility* for innovators to comply with the requirements, although this can be better evaluated when harmonized standards or common specifications have been eventually drafted. The layered, co-regulatory approach should result in a resilient, technology-neutral and *stable* regulatory framework, although as it stands, it lacks *predictability* as the standards and common specifications yet have to be drafted. To the extent that the open norms are not filled in before the AI-act becomes law, this might result in a framework that is too *stringent*, taking the harsh public enforcement mechanisms into account. Stringency might decrease when standards/specifications are adopted that can be complied with throughout the sector. Furthermore, the civil enforcement mechanisms, provided for *inter alia* under the proposed Product Liability Directive and the newly proposed AI Liability Directive may impact the *stringency* factor. The PPLD implicates a more effective mechanism for victims of defective AI-products to successfully claim damages, from virtually any actor in the supply chain of AI-systems, leading to (justified) increased *stringency*. As the effectiveness of the (procedural) rules proposed under the AILD can be questioned, the latter framework does not necessarily implicate *stringency*.

From a *consumer perspective* it has been observed that with the PPLD, the risk of under-compensation will significantly decrease, which positively impacts the *risk* factor. The same is not necessarily true for the AILD. Despite the procedural aids embedded therein, it will for instance remain hard for victims to successfully call upon a presumption of "causality" between an AI-system's output and a norm-violation, as *inter alia* the norm-violation and the causal relationship between the norm-violation and the damage still have to be proved by the victim. The *trust* factor can fully be evaluated when the harmonised standards and common specifications have been

eventually developed and adopted. It seems that the "reparative capacities" of the regulatory framework will increase, after the PPLD (and to a less significant extent, the AILD) are enacted.

The following recommendations can be derived regarding the material factors:

- Standards and common specifications must be adopted before the AI-act enters into force as much as possible, in such a way that the current legal uncertainties are resolved where possible.
- The eventual standards/specifications should not be prohibitively hard or costly to comply with and should offer plenty routes that innovators may take to ascertain compliance.
- The procedural aids for victims basing their claim on a fault-based liability regime, should be extended. At least presumptions regarding the causal relationship between norm-violation and damage must be (effectively) enabled.

References

1. de Bruin, R.W.: Regulating Innovation of Autonomous Vehicles: Improving Liability & Privacy in Europe (diss.), Amsterdam: deLex (2022a)
2. Gunningham, N., Sinclair, D.: Regulatory pluralism: designing policy mixes for environmental protection. Law & Policy **21**(1), 49–76 (1999)
3. Baldwin, R., Cave, M., Lodge, M.: Understanding Regulation—Theory, Strategy & Practice, 2nd edn. Oxford University Press, Oxford (NY) (2012)
4. De Cock Buning, M., de, Senden, L.A.J. (eds.): Private Regulation and Enforcement in the EU. Hart Publishers, Oxford (2020)
5. Kulk, S.: Internet Intermediaries and Copyright Law—Towards a future-proof EU legal framework, Dissertation, Utrecht (2018)
6. Perarnaud, C.: With the AI Act, we need to mind the standards gap. CEPS 25 April 2023, via https://www.ceps.eu/with-the-ai-act-we-need-to-mind-the-standards-gap
7. Pelkmans, J., Renda, A.: Does EU regulation hinder or stimulate innovation. CEPS Special Report No. 96/2014
8. Ranchordás, S.H.: Sunset Clauses and Experimental Legislation: Blessing or Curse for Innovation? p. 143. Zutphen: Koninklijke Wöhrmann (2014)
9. de Cock Buning, M.: *Auteursrecht en informatietechnologie* (diss.), p. 224, 228. Otto Cramwinckel Uitgever, Amsterdam (1998)
10. Koops, B.J.: Should ICT regulation be technology-neutral. In: Koops, B.J., et al. (eds.) Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners, IT & Law Series Vol 9, The Hague: T.M.C. Asser Press (2006)
11. D'Amato, A.: Legal Uncertainty. California Law Review (1983), 1–55
12. Ashford, N.A., Ayers, C., Stone, R.F.: Using regulation to change the market for innovation. Harvard Environmental Law Review **9**(2), 426 (1985)
13. Blind, K.: The Impact of Regulation on Innovation. Nesta Working Paper No. 12/02, January 2012, available on the Internet, p. 394. https://www.nesta.org.uk/sites/default/files/the_impact_of_regulation_on_innovation.pdf
14. Stewart, L.A.: The Impact of Regulation on Innovation in the United States: a Cross-Industry Literature Review. paper commissioned by the Institute of Medicine Committee on Patient Safety and Health IT, June (2010). http://www.itif.org/files/2011-impact-regulation-innovation.pdf, p. 2.

15. Luppi, B., Parisi, F.: 3. Rules versus Standards. In: G. de Geest (ed.) Encyclopedia of Law and Economics, Cheltenham: Edward Elgar Publishers, pp. 43–53 (2017)
16. Van der Heijden, J.: Urban sustainability and resilience. In: Drahos, P. (ed.) Regulatory theory: foundations and applications, pp. 727–728. ANU Press, Canberra (2017) (e-book version, via: press.anu.edu.au)
17. Gunningham, N., Sinclair, D.: Smart Regulation. In: Drahos, P. (ed.), Regulatory theory: foundations and applications. ANU Press, Canberra (2017)
18. de Bruin, R.W.: European Commission proposes AI liability rules: the Product Liability Directive. UCALL-blog 25 November 2022 (2022b). https://ucallblog.sites.uu.nl/2022/11/25/european-commission-proposes-ai-liability-rules-the-product-liability-directive/
19. de Bruin, R.W.: Nieuwe productaansprakelijkheidsregels en AI: goed voor innovatie en acceptatie? *Verkeersrecht* forthcoming (2023a)
20. de Bruin, R.W.: Europese regelgeving voor zelfrijdende auto's. In: Kolder et al. Over de grens?!, Den Haag: Boom Juridisch, forthcoming 2023, pp. 89–106 (2023b)
21. de Bruin, R.W.: European Commission proposes AI liability rules: the AI Liability Directive. UCALL-blog, 16 November 2022 (2022c). https://ucallblog.sites.uu.nl/2022/11/16/european-commission-proposes-ai-liability-rules-the-ai-liability-directive/
22. Rogers, E.M.: Diffusion of Innovations. Free Press, New York (2003)
23. Ostlund, L.E.: Perceived innovation attributes as predictors of innovativeness. J. Consumer Res. **3**(1), 23–29 (1974)
24. Carter, L., Bélanger F.: The utilization of e-government services: citizen trust, innovation and acceptance factors. Info Systems J. 15, 5–25 (2005)
25. Van Slyke, C., Belanger, F., Comunale, C.L.: Factors influencing the adoption of web-based shopping: the impact of trust. ACM SIGMIS Database: the DATABASE for Advances in Information Systems 35(2), Spring 2004, 32–49
26. Hirunyawipada, T., Paswan, A.K.: Consumer innovativeness and perceived risks: implications for high technology product adoption. J. Consum. Mark. **23**(4), 187 (2006)
27. Fagnant, D.J., Kockelman, K.: Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendation. Transp. Res. Part A **77**, 177 (2015)
28. de Bruin, R.W.: Informational privacy and trust in autonomous intelligent systems. In: Aldinhas Ferreira, M.I., Tokhi, M.O. (eds.) Towards Trustworthy Artificial Intelligent Systems—Intelligent Systems, Control and Automation: Science and Engineering Series, Vol. 102: Springer, pp. 47–60 (2022)
29. Rousseau et al.: Not So Different After All: A Cross-discipline View of Trust. The Academy of Management Review, p. 395 (1998)
30. Balboni, P., Trustmarks: Third-party liability of trustmark organisations in Europe, Tilburg (diss), p. 9 (2008)