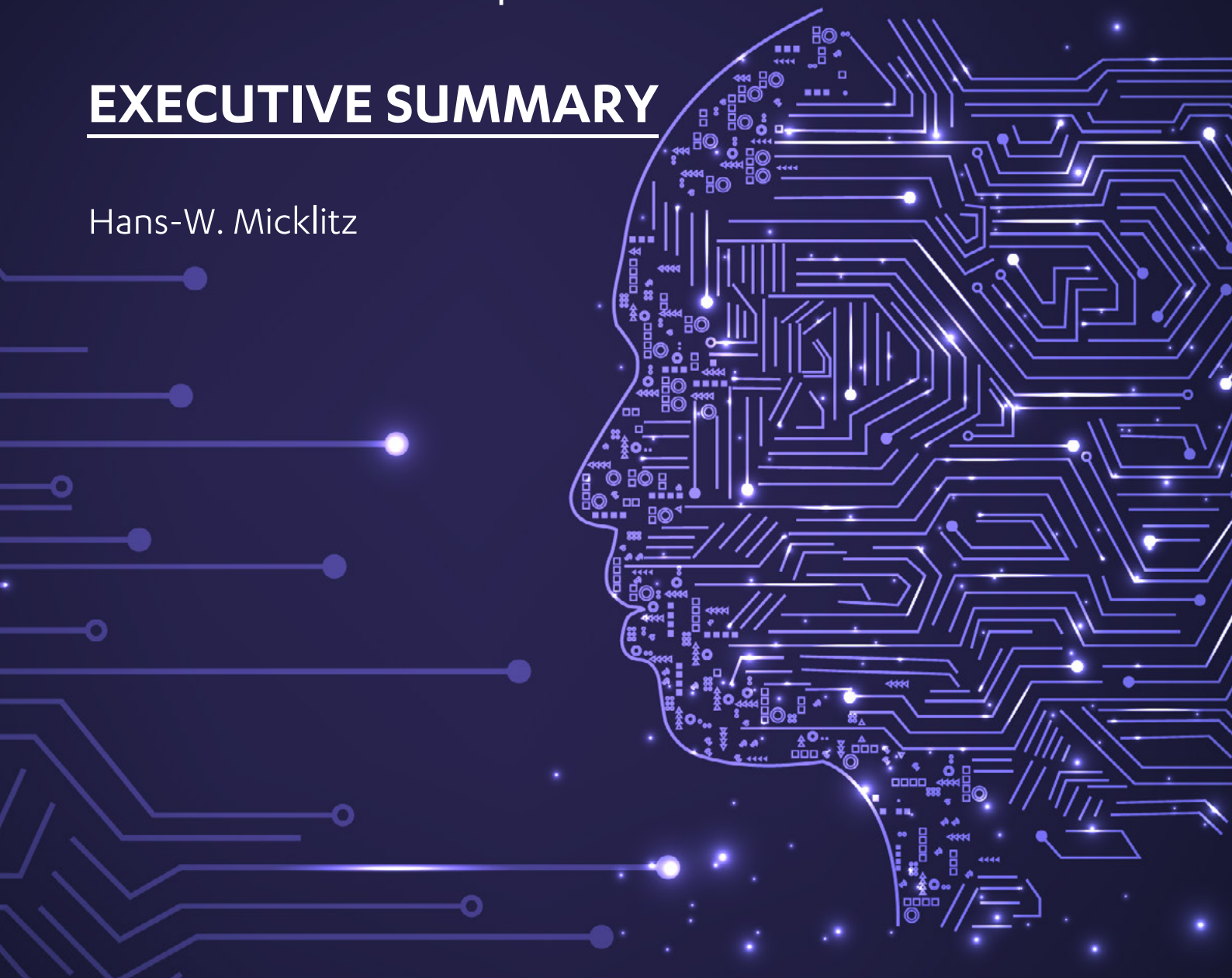
The Role of Standards in Future EU Digital Policy Legislation

A Consumer Perspective

EXECUTIVE SUMMARY

Hans-W. Micklitz



Hans-W. Micklitz is Professor at the European University Institute, Florence, Italy.

The author would like to thank Ursula Pachl, Stephen Russell, Chiara Giovannini, Camille Dornier, and Frederico Oliviera da Silva for their preparedness to support him with whatever information he needed. Without their deep knowledge of and access to all the rather hidden resources, he would have been unable to write a report which does its best to unveil the curtain behind administrative practices in the European Commission and ESOs. His deep thanks go equally to the many interview partners from the European Commission, from national, European, and international standardisation organisations, from business, from the consumer, and from the broader societal and environmental context. Their insights were extremely useful and helped to keep his feet on the ground – in particular, in search of feasible solutions. The author is grateful to his colleagues who commented on an earlier draft: Roger Brownsword, Panos Delimatsis, Martin Ebers, Pete Eisenegger, Alexander Goschew, Sebastian Hallensleben and Harm Schepel. A special thanks is going to Christopher Goddard for turning his Germish into English. That said, all responsibility for errors and omissions is his alone.

ANEC and BEUC would like to thank Stiftung Mercator for providing funding for the development of this publication.

STIFTUNG MERCATOR

Disclaimer: This report has been commissioned by ANEC and BEUC. The research reflects the personal opinion of the author and not the position of BEUC or ANEC.

BEUC The European Consumer Organisation

Rue d'Arlon, 80 Bte 1
B - 1040 Brussels
Tel: +32 2 743 15 90

ANEC

Rue d'Arlon, 80
B - 1040 Brussels
Tel: +32 2 743 24 70

Executive Summary

The Report takes an EU perspective on the role of standards in digital policy legislation through the lenses of consumer law and policy. The EU relies on the successful strategy developed in 1985, the so-called New Approach/New Legislative Framework, of combining binding legal requirements with voluntary technical standards to 'complete the Internal Market'. Regulation 1025/2012 is the key instrument, in which co-operation between the European Commission, the European Parliament, the Member States, the ESOs, and the stakeholder organisations is laid down. The EU is transferring the New Approach/New Legislative Framework from the industrial to the digital economy, prominently in the AIA-P (Artificial Intelligence Act – Proposal), the CRA-P (Cyber Resilience Act-Proposal) through reliance on harmonised European standards. The DSA (Digital Services Act) uses voluntary industry standards instead, here titled as non-harmonised European standards. The transfer is a presuppositional exercise built on the premise that the industrial and the digital economy are comparable.

1. Summary of the Report

The summary of the major findings is built around four strands:

1. deals with technical standards and product safety in the industrial economy;
2. deals with deficits of EU Digital Policy Legislation seen through consumer lenses;
3. identifies deficits in the formula 'human-centric, secure, trustworthy and ethical AI';
4. identifies gaps and how to close them.

The executive summary concludes with putting the key results together in a nutshell.

a) Technical Standards and Product Safety Regulation in the Industrial Economy

The relative successful management of product safety has been possible because the New Approach/New Legislative Framework was framed by two important pieces of consumer legislation:

- the 1985 Product Liability Directive (currently under revision),
- the 1992 Product Safety Directive

and in the field of standardisation through the institutionalisation of stakeholder participation via ANEC in 1995. Consumer advocacy could therefore rely on a firm EU legislative background and an organisation which brought 'consumers' voice' into the field of technical standardisation. Key to success has been the definition of product safety, enshrined in the formula of

foreseeable use, which requires from co-regulation to combine the normative dimension of product safety with the factual empirical – that is:

- the legitimate expectation that it is not for the manufacturer alone to define 'safe use', thereby releasing itself from liability in case the consumer does not follow instructions, and
- in designing a consumer product the manufacturer has to take into account that the product might be used for purposes for which it was not designed, but where such 'use/misuse' was foreseeable.

This is the bright side of EU policy in the aftermath of the European Single Act.

However, there is also a 'dark side' – which results first and foremost from a long list of open issues, on both sides of co-regulation, both in legislation and in standardisation. The PIP scandal[1] revealed the deficiencies of a policy which primarily aims at opening up markets through harmonised European standards, but which fails to provide the necessary safeguards to ensure that compliance with harmonised European standards is properly tested, and that in cases of non-compliance the victims are properly compensated.

Two pillars of the New Approach/NLF turned out to be insufficient, namely:

- the requirement of conformity assessment through third-party certification and
- insufficient product liability rules.

Less visible are deficiencies on the side of technical standardisation, first and foremost the institutional ones, resulting from the weak position of stakeholder organisations as simply add-on instead of co-operation partners, equipped with arguments only but no rights to make sure that their 'voice' leads to concrete results. The confidential character of technical standards, even in the form of harmonised European standards, is another loose end in the overall construction of the New Approach/NLF. Technical standards, whether non-harmonised or harmonised, whether national, European, or international, are copyright-protected. Production of technical standards is business. Industry is ready to invest through voluntary input because of economies of scale internationally, and the presumption of conformity which guarantees access to the Internal Market. The standardisation organisations are private. CEN-CENELEC are dependent on income through copyright revenues. EU law as it stands leaves copyright issues untouched, which is justified and legitimated through the distinction between 'law' and 'technicity'. Consumer advocates have been challenging the feasibility of drawing a clear line between the two ever since. The specificity of binding legal requirements, which then have to be reflected in a standardisation request from the European Commission, is an ongoing and never-ending battlefield between consumer advocacy and business interests. The adoption of Article 3 (3) d)e)f) RED (Radio Equipment Directive) bears witness to the dimension of the conflict. However, the game changer in the interaction between the European Commission, the ESOs, and the stakeholder organisation has not been the EU legislature, but the Court of

1 Between 2001 and 2010 PIP sold hundreds of thousands of unapproved implants sold globally. They were found to pose a higher risk of rupture or leakage than approved models and of inducing breast cancer, https://en.wikipedia.org/wiki/Poly_Implant_Proth%C3%A8se.

Justice of the European Union through *James Elliott*[2] in 2016, through *Stichting Rookpreventie*[3] in 2022 and through *Public.Resource.Org* to be decided in 2023.[4]

James Elliott forced the European Commission to rearrange distribution of responsibilities in the elaboration of harmonised European standards. The CJEU submitted harmonised technical standards to a – limited – judicial review because they have to be understood as being 'law'. As a consequence, the European Commission decided to publish them in part L of the Official Journal and to take over the selection, management, and the monitoring of the experts in charge of aiding and assessing compliance of elaborated standards with EU law concretised in the standardisation request. The implications of redistribution are subject to a controversial interpretation of *James Elliott*, in particular on the reach of judicial review and its implications for redistribution of responsibilities. What has been long unthinkable has become reality. The CJEU has turned into an actor in terms of surveying and monitoring co-regulation. Not much imagination is needed to expect that more cases will come to the CJEU in the near future and will lead to an even stronger juridification of co-regulation. Whether this is good or bad for the consumer, whether their level of protection will be increased, remains to be seen. So far, the added value of the Court's intervention lies much more in democratic credentials and in making clear that private regulation is not sacrosanct in terms of judicial review.

At the time of writing, the European Commission has not revised the Vademecum which is meant to explain to the interested public how concrete steps in elaborating harmonised European standards are organised, let alone what exactly the technical experts – the so-called HAS consultants – are actually doing. The European Commission has outsourced selection of the HAS consultants to Ernst & Young. Put differently, consultants whose tasks are not clearly described and whose identities are not disclosed are playing a key role at the very bottom line of co-regulation, where the two regulatory levels are merged, binding legal requirements and technical standards through a compliance test. There is no legal certainty as to the legal responsibilities of the European Commission. There are convincing arguments that the European Commission must be ultimately responsible for product safety and that the European Commission could eventually be held liable if fails to exercise its monitoring and surveillance activities in the compliance procedure properly. Such state liability is independent from a producer/AI provider who could be held liable in case of non-compliance with technical standards or in case technical standards fail to meet legitimate consumer expectations.

Similar uncertainties govern the reach of copyright. *Stichting Rookpreventie* deals with a particular situation where the EU legislature refers to ISO standards in secondary law. The CJEU regarded the ISO standards as being an integral part of EU law, but was not ready to conclude that EU law – even if it appears in the form of ISO standards – has to be freely accessible. The obvious next question will be whether references to ISO/IEC standards and references to harmonised EU standards have to be treated equally and whether harmonised European standards, being part of EU law, must be freely accessible and, if so, what free accessibility should and could look like. *Public.Resource.Org*. will hopefully clarify the accessibility conditions of harmonised European Standards.

---

2 ECJ C-613/14 – *James Elliott Construction*, ECLI:EU:C:2016:63.

3 ECJ Case C-160/20 *Stichting Rookpreventie Jeugd v Staatssecretaris van Volksgezondheid, Welzijn en Sport*, ECLI:EU:C:2022:101

4 Case T-185/19 *Public.Resource.Org*.ECLI:EU:T:2021:445, Appeal Case before the Court of Justice C-588/21 P.

b) Conceptual Deficits of EU Digital Policy Legislation in the Digital Economy

EU Digital Policy Legislation is to be understood as Marktordnungsrecht – establishing a legal order for the digital market. The prime addressees of legislation are public authorities and companies that come under the scope of the law, but the legislation here under review does not deal explicitly with the interaction in b2b and b2c relations. This was different in 1985, when the New Approach/New Legislative Framework was adopted. The EU could rely on and refer to the Product Liability Directive as a safeguard mechanism to protect the interests of the parties against circulation of unsafe products. The Product Liability Directive was regarded – not only in the EU but far beyond – as a promising piece of legislation setting a benchmark for a reasonable compromise between the different interests of the manufacturers and possible victims. The recently *proposed* revision of the Product Liability Directive and the *new* Artificial Intelligence Liability Directive might, if they pass the legislative procedure, increase the level of protection against risks resulting from AI. However, the time gap matters. The EU is promoting digitisation of the economy without a safety net adapted to the digital economy and which addresses the potential liability of standardisation organisations and certification bodies. The lesson from the PIP scandal and the gaps that litigation before the CJEU disclosed are not yet learnt.[5]

aa) Horizontal Legislation on Digital Fairness

Similar to the political situation in 1985, the European Commission does not see the need to accomplish digital policy legislation through what I would like to call a 'Digital Fairness Act', a horizontal piece of legislation which accomplishes EU Digital Policy Legislation. In 2022 the European Commission brought – under political pressure – the Digital Fairness Check[6] on its way. However, the question remains why concerns about digital fairness arise only *after* the DMA, the DSA, the AIA-P and the CRA-P – just to name a few of the many regulations which form part of EU Digital Policy Legislation. It is difficult to predict how many years will pass between adoption of the AIA and the CRA on the one hand and, on the other, adoption of the revised Product Liability Directive and the new Artificial Intelligence Liability Directive, let alone whether there will ever be a 'Digital Fairness Act', which could be understood as a counterpart to the 1992 Product Safety Directive.

The 'Digital Fairness Fitness Check' covers only:

- Directive 93/13 on unfair terms;
- Directive 205/29 on unfair commercial practices and
- Directive 2011/83 on Consumer Rights.

Data protection regulation is not mentioned, nor the mind-blowing difficulties in enforcement of consumer law and consumer data protection law. Even in an optimistic scenario, a Digital Fairness Act in whatever format could not see daylight in the next five years. The obvious conclusion is that the consumer acquis is suggested as providing adequate protection in the digital

5 CJEU Case C-219/15 *Schmitt* ECLI:EU:C:2017:128.

6 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

economy. This is a rather bold assumption in light of the abundant evidence, empirically and academically, on the digital vulnerability of consumers.[7] For sure, there are bits and pieces that pick up certain aspects, such as the Digital Content Directive, the Omnibus Directive, or the Guidelines on the Unfair Commercial Practices Directive. However, where Digital Policy Legislation might reach beyond the existing consumer acquis – such as the rules on dark patterns in the DSA – a potential overreach into b2c relations has been deliberately cut back. What is missing so far is a systematic examination of whether the consumer acquis matches today's political issues – bearing in mind that the acquis itself is deeply embedded in the thinking of the 1960s and 1970s, the Kennedy declaration of 1962, and the first and second European consumer policy programmes from 1975 and 1981.[8]

bb) Foreseeable Use and Use Cases

Similar to the late 1980s debate governing the making of the Product Safety Directive, such a debate should concentrate on the notion of 'digital fairness', which needs to be connected to the 'use case' and how the potential usage of an AI system might affect the consumer in their various economic and social relations. The existing digital policy legislation suffers – in today's world – from its character as the law of the market order. It does not address the consumer/customer directly and therefore does not deal properly with consumer interests. New ground has to be broken. It is not enough to copy-paste 'foreseeable use' but, rather, to offer legislative guidance on what potential 'use cases' might have in common and how they should be taken into account in the use of an AI system. However, the interviewees – technicians, computer scientists and natural scientists, independent of their affiliation – doubted whether it makes sense at all to try to define use cases and pointed to the difficulties in practice.[9] An example might help to understand the difficulties:[10]

> *ChatGPT is about to move from general purpose use into the business environment. ChatGPT might be used in all sorts of interaction which are of high relevance for consumers – financial services to 'replace' professional advice of financial advisors, health services to 'replace' the doctor or the psychotherapist, 'legal services' to replace the lawyer, educational services to 'replace' the teacher. The potential use cases are endless and might easily reach beyond our imagination. In theory it might be possible to standardise potential use cases. However, building use cases will lead to mainstreaming the behaviour and create new types of echo chambers. A potential use outside the mainstream may then be regarded as 'deviant' or as 'discriminatory' depending on the perspective.*

The example equally shows that 'foreseeable use' in the digital environment cannot be compared to foreseeable use in the old economy. Seen through the lenses of software developers, the possible use cases are hard to overlook. In the analogue world, foreseeable use can be built on a heuristic of how the consumer might use or even misuse a product. In the digital

---

7 N Helberger/ O Lynskey/ H-W. Micklitz/ P Rott/ M Sax/ J Strycharz, EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets, A joint report from research conducted under the EUCP2.0 project, BEUC, March 2021, https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

8 Council Resolution of 14 April 1975 on a preliminary programme of the European Economic Community. for a consumer protection and information policy, OJ No. C 92, 25.4.1975, Council Resolution of 19 May 1981 on a second programme of the European Economic Community for a consumer protection and information policy, OJ No. C 133, 3.6.1981.

9 Interviews with experts from standardisation organisations, companies and stakeholder organisations.

10 I discussed this example with my interview partners from stakeholder organisations.

world, the consumer is the potential addressee of an endless chain of potential uses of an AI system. If use cases cannot be framed so as to allow an assessment of the potential risks, then society at large serves as a guinea pig. In the search for use cases, particular attention should be put on the cognitive interaction between sensors (camera, microphone, and so on) and actors (screens, loudspeaker) and how they affect the consumer.[11] Defining and categorising potential use cases is but a first step. Any potential risk, built around a set of use cases, materialises at the level of a local user of an AI system, to stay with the example of ChatGPT with the financial institutions that decides to replace human advice through technology. In order not to leave the local user of an AI system alone with the risk of fundamental rights infringements, they need support through a toolbox on which they can rely to minimise the risk. This is particularly important as many local users of AI systems will be start-ups or SMEs.

cc) Transformation of the Consumer Acquis through Digital Policy Legislation

Analysis of digital policy legislation indicates a major change in how the European Commission seems to envisage the role of consumer protection in the digital world. Three elements deserve to be highlighted:

- the dismantling of the consumer and the trader,
- the ongoing privatisation of consumer law, and last but not least
- the key role of fundamental rights as a placeholder for consumer protection.

The **dismantling of the consumer** becomes visible through the introduction of ever more categories in EU digital policy legislation:

- customer,
- users,
- natural persons, and
- the individual,

where the concrete meaning depends on the context.

The same is true with regard to **business**, where the traditional counterpart to the consumer – the supplier, the trader, or the manufacturer – is split up in the AIA-P into:

- economic operators,
- provider,
- small-scale provider,
- user,
- operator,
- authorised representative

11 https://de.wikipedia.org/wiki/Kognitives_System, mainly authored by M Bautsch from Stiftung Warentest.

or (in the DSA) into:

- SMEs,
- large online platforms, and
- very large online platforms or economic operators.

There seems no end to possible new categories. Obligations imposed on the different business actors are differentiated according to the size of the company. Similar developments are occurring on the consumer side, but not yet with clear legal consequences. The well-established notion of the consumer in the acquis is gradually being replaced through at least two categories:

- the 'average consumer' and
- the 'vulnerable consumer'.

However, the distinction has not yet led to different rights and duties according to the type of consumer concerned. Digitisation brings back a debate which began in the aftermath of the liberalisation and privatisation of former public monopolies. Here the consumer not only turned into a customer but also – and more importantly – into a citizen-consumer. In EU Consumer Law 2.0[12] we have demonstrated that digitisation is gradually undermining the dividing line between the market and society, and thereby the distinction between the consumer and the citizen. The result is the citizen-consumer, if not the commodification of the consumer themselves,[13] this time not only in the field of regulated markets (finance, energy, telecoms and transport) but in the ever-broader scope of consumer law, which cuts across all economic sectors and intrudes ever deeper into societal relations.

The role and place of technical standards in digital policy legislation fits into the overall process of privatising consumer law through the steadily growing role of due diligence obligations, codes of conduct – and voluntary technical standards. The current regulatory frame on the digital economy – and this cannot be repeated often enough – relies on *voluntary* standards, voluntary in a manifold sense. EU law and the European Commission may base their legislation on technical standards. Each of the following is a decision that each of the parties involved has to take for themselves:

- whether the ESOs are willing to co-operate;
- whether the ESOs are willing to reply to a standardisation request;
- whether companies and stakeholders are ready to invest in a working group; and last but not least,
- whether companies decide to apply harmonised European standards or whether they develop their own way to comply with binding legal requirements.

This willingness can be expected, can be hoped for, but cannot be enforced by the European legislator. It is up to the standardisation bodies and companies to decide for themselves whether they want to follow the path taken by the EU legislature. Both may set incentives

12 N Helberger et al Consumer Protection 2.0. (n 8)

13 This has been quite a common theme in digital rights events and publications, see an extract at https://www.youtube.com/watch?v=Aucb5tJMi70; https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/ https://powazek.com/posts/3229 https://www.linkedin.com/pulse/youre-paying-product-you-faiz-shaikh/

through regulatory tools, such as the presumption of conformity in cases of compliance that grants access to the Internal Market, and through financial contribution. However, financial input from the European Commission does not seem to be an incentive for companies. The costs of elaborating one standard are estimated at about one million Euros.[14] The contrary is true for the stakeholder organisations in Annex III. Their participation depends on EU funding, perhaps not as much as 100%, but they are on the EU's drip: if the EU stops paying, they will have to fear for their existence and the continuation of a societal voice in the drafting of such tools of a legal nature.[15]

The – so far – last determinant of change is perhaps the most visible and the most obvious: the constant reiteration of fundamental rights in the AIA-P, the CRA-P, and the DSA. The new market order is rhetorically linked to compliance with fundamental rights both far more strongly and far more explicitly than in the market order for the old economy. The addressees of fundamental rights are not only those to whom the different Acts speak – an addressee can be anybody who is in some way or the other affected.[16] The respective recital in the AIA-P even lists the various individual rights as well as the principles, including Article 38 EUCFR on consumer protection. The DSA equally includes fundamental rights, this time without referring to Article 38 EUCFR. Read together, the AIA-P, the CRA-P, and the DSA demonstrate that fundamental rights reach beyond protection of health and safety. They cover the economic interests of rightholders, their autonomy, and their dignity. None of the legislative initiatives under consideration offers a more specific insight into why fundamental rights are given such a prominent role, let alone the missing guidance on how this objective can be achieved through standardisation. This is particularly relevant with regard to consumer protection because the AIA-P and the DSA do not address the consumer directly. Fundamental rights are hovering over the new market order, though without any tangible effect. One might therefore wonder what kind of place the EU legislation attributes to them and what exactly is behind the constant references to fundamental rights, in the recitals and in some but not all of the articles, sometimes with a general proviso, in others without a general proviso. The political objective is outspoken, the EU intends to become a '*global leader in a secure, trustworthy and ethical AI*' and a key role is attributed to fundamental rights.

c) Acid Test: Human-centric, Secure, Trustworthy and Ethical AI

EU digital policy legislation as well as international standardisation organisations, ISO/IEC and IEEE along with the European standardisation organisations (ESOs) are putting 'trustworthy and ethical AI' at centre stage, connected to human and fundamental rights. However, despite major attempts undertaken both inside and outside the EU legislative machinery, the high-flying rhetoric lacks clear-cut contours and stands far away from a legal concept in the academic environment as well as in standardisation bodies.[17] The lack of clarity on what the term 'trustworthy and ethical AI' might mean is reflected in efforts by international standardisation to develop concrete AI standards from which to derive the substance of what 'trustworthiness'

---

14 Interview with representative from the European Commission. The sum goes back to a Roland Berger study from the year 2000, probably calculated in ECUs, and might be much higher now.

15 See the figures on the financial contribution of the EC to stakeholders, though without indicating the percentage of EU money in their overall budget.

16 The Report does not discuss the horizontal effects of fundamental rights.

17 The European Parliament is working on a definition of trustworthy AI. It remains to be seen what it looks like, whether it makes it into the final version, and if it will have an effect on the New Approach/NLF at all.

actually means. The European Commission is a latecomer meeting a highly crowded field in its intention to make the EU a 'global leader' in standards and to promote 'core values'.[18] The two working programmes from 2022 and 2023 as well as the just published standardisation request demonstrate that the grand formula of *'human-centric, secure, trustworthy and ethical AI'* ends up in loose references to fundamental rights.

aa) Search for a Concept in EU Digital Policy Legislation and Socio-technical Standards

The intellectual background to the formula of *'human-centric, secure, trustworthy and ethical AI'* which governs EU Digital Policy Legislation derives from the High Level Expert Group (HLEG) set up by the European Commission with the mandate to elaborate ethical guidelines for trustworthy AI in 2018. Trustworthiness is a catch-all term, which intermingles political, legal, economic and social thinking but without having clear contours, though with a strong normative message. Seeking guidance on the meaning of trustworthiness through ethics amounts to levelling up the search to the more abstract philosophical level, which, however, does not mean that there are no politics in the search for ethical AI. Indeed, quite the contrary is true.

A proliferation of AI principles has been developed by different actors around the world. Notwithstanding their origin, they carry a common core, which seems acceptable in the Western World, that is, the Global North:[19]

- human rights including privacy,
- promotion of human values (beneficial to society),
- professional responsibility (human control of technology, accountability),
- fairness and non-discrimination,
- transparency and explainability,
- safety and security.

The HLEG Guidelines, whilst overall very much in line with the common core, are more concrete in what ethical principles could contribute to give trustworthiness contours:

> *Trustworthiness should be lawful, ethical, robust and holistic (the latter one is my own interpretation of the Guidelines).*

Two of the four components deserve particular attention as they are crucial for an analysis of how trustworthiness is handled in EU digital policy legislation and in the various international projects which aim at defining trustworthiness. The first is **lawfulness**. This component is missing in most of the international standardisation projects and for obvious reasons: there is no

18 New Standardisation Strategy, under 13: 'The EU needs to be a global leader in the development of secure, trustworthy and ethical Artificial Intelligence. The European Council invites the Commission to: propose ways to increase European and national public and private investments in Artificial Intelligence research, innovation and deployment; ensure better coordination, and more networks and synergies between European research centres based on excellence; provide a clear, objective definition of high-risk Artificial Intelligence systems'. https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf

19 Fjeld, J, Achten, N. Hilligoss, H, Nagy, A and Srikumar, M. (2020). 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI.' [Online] Available from: http://nrs.harvard.edu/urn-3:HUL.InstRepos:42160420

consensus on what 'lawfulness' means in international law, perhaps with the exception of the 1948 Declaration of Human Rights, which, however, was never ratified and is given effect as customary law only. In the European context, lawfulness matters. The EU is a product of law, operates through law and provides a legal system[20] – as the envisaged digital policy legislation amply demonstrates. What is the Union law to which trustworthiness should abide by? Here the Charter of Fundamental Rights comes into play.

The second component, where the HLEG differs, is **holism**, which refers to the descriptive and descriptive/applied side of ethics. The HLEG guidelines suggest that trustworthiness is not only related to the AI system (think of the definition in the AIA-P) but that '*trustworthiness* (should include) *all processes and actors that are part of the system's life cycle*.[21] Translated into more colloquial language, trustworthiness covers a normative – these are the principles – the common core – and a descriptive/applied dimension. The other two components, namely ethics and robustness, form a common denominator of all AI principles.

The HLEG Guidelines may be easily linked to the various fundamental rights in the EUCHR. However, one particularity deserves particular attention – human-centrism. This term can mean protection of the human being against risks resulting from AI, but human centrism can also mean that control over AI should ultimately remain in the hands of the human being. The second strand needs to be guaranteed so as to preserve human dignity. The EU digital policy framework does not explicitly refer to the HLEG Guidelines – which would have been possible and what the European Parliament was obviously striving for. This omission has had far-reaching consequences on the design of the AIA-P, the CRA-P, and the DSA. There are two major gaps: the first is the underdetermined meaning of human-centric. EU Digital Policy Legislation builds on human oversight, but does not state explicitly that human control over AI systems is a necessary requirement for protection of human dignity. It remains to be seen whether the European Parliament will also sharpen the understanding of human-centrism. The call for humans to have the last word requires defining red lines which cannot be crossed in technical standardisation. The second gap results from the missing link of the formula to the 'real world', to descriptive/applied ethics. All three acts under scrutiny are by and large limited to the normative side but do not stress the need to engage with the factual side, with the concrete impact of AI systems on society. This deficit needs to be overcome.

The regulatory tool to link the normative and the descriptive/applied side are the '*use cases*'. There is no deeper reflection on what it means for digital policy legislation to integrate possible use cases into the regulatory design, thinking about a possible choice of use patterns – or, at the very extreme, to reflect on the consequences for trustworthy AI, if experts are right, who claim that the potential risks are not foreseeable in concreto and that it is therefore not possible to define potential uses cases of AI systems. Such a finding, if correct, shatters the assumption that trust and ethics can be built through EU Digital Policy Legislation, more concretely through a combination of binding legal requirements in secondary EU law and voluntary harmonised European standards to be elaborated by the ESOs under participation of stakeholder organisations. The EU regulatory approach is limping – the normative side of trustworthy ethical AI

---

20 In the words of W Hallstein, Europe in the Making (translated from German by C. Roetter; originally published under the title Der unvollendete Bundesstaat (Düsseldorf; Wien: ECON, 1969)) (London: George Allen & Unwin Ltd, 1972), at 30. The German title says: 'The Incomplete Federal State'.

21 HLEG, Ethics Guidelines for Trustworthy AI, 2019. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

is overstretched, the descriptive/applied side of trustworthy AI – its acceptability in society – is underdeveloped and flows into the rather naïve belief that EU law alone is able to create trust and that no additional means are needed to engage in possible use cases, their chances and their limits in the real world. There is a strong need to engage into a deeper discussion on the feasibility to define use cases. The best would be to mandate the ESOs accordingly and ask them to develop an AI standard on use cases. This would be the appropriate way to find out whether the AI experts are right or whether there is an opportunity to develop use cases in the digital economy, maybe in a different format compared to the industrial economy.

The very same gap equally shows up in international efforts by ISO/IEC and IEEE to lend trustworthiness a meaning which could guide standardisation activities. However, the ISO/IEC and IEEE standards do not refer to law outside the overall claim that users of standards should respect the law of the country where they reside. This makes sense because international standards will be applied in different countries around the world, each of them having specific national legislation. If they refer to law at all, they do so by mentioning human rights, occasionally by listing various laws from around the world – typically the USA, the UK, and the EU. There is one exception: the GDPR is nearly omnipresent even in international documents, not necessarily as a benchmark but as a reference point. All of them neglect the descriptive and applied side of AI and do not engage with the difficulties which run around use cases. If any, they touch upon the empirical side through definitions of the life-cycle. These definitions, though, whilst they could theoretically include consumers, are written through business lenses. The focus lies on the lifecycle determined through the intended use.

bb) Difficulties in Concretising Trustworthy AI Standards

ISO/IEC and IEEE on trustworthy AI already firmly occupy the field. For more than five years they have been working on elaboration of AI standards, which are meant to concretise how the – incomplete – concept of trustworthy AI could operate in practice. ISO/IEC alone have already adopted 17 AI standards, with another 27 under way. IEEC has come up with another 20, often with content overlapping ISO/IEC. These AI standards, so far mostly in the form of technical reports, are not really technical in nature. All standardisation organisations working on trustworthy AI standards, independent of their origin, have elaborated a kind of *meta-norms*, standing in between binding law and truly technical standards. In standardisation-speak these are called *socio-technical* standards.[22] They are elaborated by technicians, engineers, computer scientists, or mathematicians, but at the same time providing definitions on categories with a strong legal flavour – for instance, 'transparency' and 'explainability', strongly overlapping with the EU consumer law acquis. This is the key result of the stock-taking of AI standards sailing under the flag of trustworthiness, which covers hundreds of pages of ISO/IEC and IEEE AI standards. A disclaimer needs to be added, though. IEEE standards are partly open access, and a preview of ISO/IEC standards allows for studying roughly one-half of the text. These socio-technical standards might certainly help non-lawyers to understand the implications, the difficulties, and the uncertainties, which result from the need to integrate trustworthiness into technical standards. However, these socio-technical standards, at least in what is freely accessible, do not suffice to reach the level of concreteness that certifiability requires so as to trigger the presumption of conformity under the New Approach/NLF. More

22 The term came up in my interviews with representatives from the European Commission, from standardisation organisations, and from companies.

is needed to meet the component of lawfulness, set out in the HLEG Guidelines and translated into EU Digital Policy Legislation.

A similar lack of clarity on how trustworthy AI should be pinned down in elaboration of AI standards shines through the regulatory means undertaken by the European Commission and the ESOs, EU 2022/2023 work programmes, calls for proposals, the 2023 standardisation request, and projects that ESOs have already set up. There is no explicit mandate on making sure that AI systems have always to remain in the control of humans and there is no mandate to test the standardisability of use cases. Trustworthiness seems to be equated by reference to fundamental rights. The further down the ladder, the further away from the legislative level, and the closer to concrete AI standardisation projects, the fewer and the less outspoken are references to fundamental rights. Put differently, the EU measures are aiming at translating binding legal requirements into a concrete mandate given to the ESOs which can then be checked by the HAS consultants and the European Commission. Respect for fundamental rights forms an integral part of binding legal requirements. It looks as if the European Commission intends to leave adjustment of binding legal requirements under inclusion of fundamental rights to the expertise of what the ESOs are able to deliver, thereby drawing the line between the law and technical standards. However, the ESOs are ill-equipped to handle fundamental rights in technical standardisation and they are not necessarily keen to take this burden on board, either.[23] This understanding of the EU regulatory approach is confirmed by the ten mandated standards which the European Commission is calling for.

These ten mandated standards mirror more or less literally the different topics regulated in the Second Chapter of the AIA-P on high risks. They meet three out of the four components of trustworthy and ethical AI in the meaning of the HLEG Guidelines, that is:

- they are lawful (based on the AIA-P),
- they are ethical (they all can be attributed to the common core of ethical principles in general and to the HLEG in particular, with the exception of the underdetermined respect for human dignity as a red line) and
- they are robust (robustness forms part of the standardisation request).

However, the regulatory design lacks guidance on how the ESOs should handle fundamental rights. As a result, compliance with the AIA-P and CRA-P does not necessarily mean that technical standards do not infringe individual rights or Article 38 EUCFR – the principle of consumer protection. Through the implicit equation between ethical standards and the binding requirements enshrined in the AIA-P, and through thinning out the importance of fundamental rights down the ladder, the European Commission enables the ESOs to downgrade use cases and to delegate the fundamental rights test to the next actors in the chain – the certification bodies and/or local AI providers/users. True, the integration of fundamental rights into technical standardisation faces uncharted territory. However, it would have been the responsibility of the EU legislature – and, in implementing the New Approach/NLF the European Commission – to address open questions around the integration of fundamental rights upfront.

The ten mandated European standards by and large overlap with existing ISO/IEC or IEEE standards and if they are not yet existing, work is under way already and partly quite advanced. As

23 This is the result of the interviews with representatives and experts of the standardisation organisations.

the ESOs are in the process of accepting the mandate, the now set-up ESO working groups have to juridify international standards, bringing them into line with EU law and turning them from technical reports into certifiable harmonised European standards. All that remains from the claim of 'trustworthy and ethical AI' is the need to make sure that ISO/IEC and IEEE standards comply with EU fundamental rights, to be equated with 'core values'. However, as it is neither clear what exactly the EC is expecting from the ESOs, nor what the fundamental rights test implies (in particular due to lack of emphasis on use cases), the ESOs – just like the stakeholders – find themselves in an awkward situation. They have a clear mandate to integrate fundamental rights but how this could be done is left open. There is an additional, more psychological, difficulty in that the ESO working groups are or will be composed by and large of the same people who have already participated in elaborating ISO/IEC standards. It will not be easy for the very same people to admit that the ISO/IEC standards they have elaborated are *not* in compliance with human and/or fundamental rights. Work on 'inclusiveness' within CEN-CENELEC JTC 21 WG 2 is ongoing, although at an early stage. Ethical issues have been dominating debates in the various AI committees around the world since 2018. Interviewees reported that there is no gulf between the Europeans defending core values and the rest of the world. If there are conflicts, compromises are sought.[24] Whether the levelling up of international standards to core European values is feasible without friction, can only be said once the standardisation request is adopted and once the work started to transform ISO/IEC standards into harmonised European standards

cc) Gaps to be Closed

Analysis of the New Approach/NLF in the two economies, the industrial and the digital, revealed a series of gaps, uncertainties, and loose ends which need to closed. The New Approach/NLF set up in 1985 was gradually completed over the last nearly forty years, having the industrial economy in mind. To put the process into a metaphor, the plan for the house was there but it took decades to build the house – step by step, governed by the same corporate spirit – a strong alliance between the European Commission and the ESOs, under gradual acceptance of the (still under-represented) stakeholders as an add-on to the standardisation community, but without granting them the status of a partner and without adjusting Regulation 1025/2012 to the overall policy of the European Union to ensure compliance of secondary EU law with the EUCHR. The revision of Regulation 1025/2012 provides the opportunity to – finally – level up the stakeholder organisations and grant them the same status as the ESOs, by naming them in Annex I and by equipping them with appropriate rights and remedies to make sure that their voices are not only heard but make their way into harmonised European standards.

The unquestioned transfer of the New Approach/NLF from the industrial to the digital economy has not only put long-standing deficits into the limelight – the shaky status of stakeholder participation and compliance with fundamental rights – and has also added a whole series of additional problems which call for action. The list starts with lack of giving due consideration to the descriptive/applied dimension of AI ethics. The focus on the normative implications is comprehensible in a supranational institution which operates through law, but the emphasis on law and regulation would have made it necessary to dive into the 'foreseeability of AI risks', which nearly automatically leads to 'use cases'. Use cases belong to a new category of technical standards, socio-technical standards, which have to be integrated into the current legal

24 Interviews with an expert taking part in the standardisation organisations.

structure of Regulation 1025/2012. This cannot be done without discussing free access and without identifying the limits which result from socio-technical standards that are not certifiable. On a deeper level, though, the transfer should have tackled the problem of human-centric AI upfront, clarified its meaning and the need to draw red lines for concretising binding legal requirements on AI systems through harmonised technical standards. The long overdue need to submit *all* harmonised technical standards to a fundamental rights impact assessment leads directly to the question whether the red line approach for AI systems needs to complemented through a kind of second layer test that sets limits to the standardisation of technology which is strongly intertwined with the public interest. As there is no fundamental rights free zone in EU law, the relationship between consumer protection-related fundamental rights and the EU consumer law acquis needs to be adjusted. The mandated projects on elaboration of harmonised European standards largely overlap with the EU consumer law acquis, for example, in the rules on transparency. This begs the question whether and to what extent the consumer law acquis can be integrated into individual consumer-related fundamental rights as well is into Article 38 EUCHR.

The issues brought up so far already sound complicated enough but at least two if not three further problems remain to be added: the first problem results from the opaque role of the HAS consultants and the need to sharpen distribution responsibilities among the European Commission, the ESOs, and the stakeholder organisations as partners. This is all the truer as the compliance test will have to involve fundamental rights. The Regulatory Scrutiny Board provides a viable model to be tested as a substitute for HAS consultants. Whilst the upgrading of stakeholder organisations to partners on a level playing field offers new opportunities, the redesign of stakeholder participation should go one step further and open the door for NGOs which represent independent technical knowledge, so urgently needed in the digital economy, but not only there. The double valorisation of stakeholder organisations, the naming of ANEC as a partner and the NGOs bringing in independent expertise would allow the EU to base promotion of core values not only on fundamental rights but on the need to include civil society in elaboration of harmonised European standards, which might clash with existing ISO/IEC and IEEE standards. The geopolitical dimension of harmonised European standards, in particular in the field of AI, raises additional issues which are underlit, such as cooperation agreements between the ESOs and ISO/IEC as well as potential co-operation with IEEE.

2. Key Results in a Nutshell

International standardisation institutions, above all ISO/IEC and IEEE, already occupy the field of trustworthy and ethical AI standards:

- ISO/IEC and IEEE AI standards are elaborated in the form of technical reports, not in the form of certifiable standards proper;
- ISO/IEC and IEEE AI standards (technical reports) are socio-technical standards defining normative ethical principles with loose references to international law and without red lines;
- ISO/IEC and IEEE AI standards do not take use cases into account, so they are of limited value for assessing whether an individual technical standard is trustworthy and ethical

- ISO/IEC and IEEE AI standards (technical reports) were elaborated with very limited stakeholder participation;
- ISO/IEC and IEEE AI standards claim to be focused on the technical side, whereas in reality they produce normative interpretations of legal concepts, sometimes with loose reference to international law.

European Digital Policy Legislation is directed towards elaboration of certifiable harmonised standards which are secure, trustworthy, and ethical, built firmly on the New Approach/NLF. The current legal framework:

- relies on the New Approach/NLF without getting to grips with key deficiencies despite the rupture resulting from digitisation of the economy and society, such as drawing red lines, insufficient stakeholder participation; unsolved distribution of responsibilities between the EU and the ESOs; the opaque role of HAS consultants; liability of standardisation and certification bodies;
- starts from the presuppositional premise that human-centric, secure, trustworthy, and ethical AI to the benefit of society at large can be established through the interaction of binding legal requirements and voluntary harmonised European standards;
- overstates the normative dimension of trustworthy and ethical AI but neglects the descriptive and applied dimension of trustworthy and ethical AI;
- in the normative dimension intermingles trustworthiness, ethics, and fundamental rights, thereby insinuating that compliance with the EUCFR indicates trustworthy and ethical AI;
- sets aside the descriptive and applied dimension of trustworthy and ethical AI by excluding use cases from elaboration of harmonised European standards;
- although relying heavily on the normative dimension, fails to provide guidance on how and by whom fundamental rights should be integrated into certifiable harmonised European standards;
- thereby delegates implementation of the AIA-P, CRA-P and DSA de facto to private standardisation organisations, namely the ESOs;
- establishes a highly risky 'pass the buck' policy, where the individual local AI provider runs the risk of being held liable for infringement of fundamental rights despite certified compliance, which can backfire on the ESOs and the certification bodies in case of liability claims.
- where consumers or better the society as a result of the 'pass the bucket' policy has to bear the risks stemming from being subject to products and services that have been released based on industry driven implementation.

Existing ISO/IEC, IEEE AI standards have to be coordinated with development of harmonised EU standards. The first-mover advantage creates legal, technical, and psychological barriers which need to be overcome, as the EU working programme and the pending standardisation request greatly overlap with ISO/IEC and IEEE standards:

- in the relationship between CEN-CENELEC and ISO/IEC: the Vienna and Frankfurt Agreements do not legally bind the EU but tie the hands of CEN-CENELEC in stipulating that CEN-CENELEC and ISO/IEC should not develop standards in the same area of application, which in turn means that CEN-CENELEC may fill gaps with purely European projects, though in co-operation with ISO/IEC, where the same national members are present;
- in the relationship between ISO/IEC, CEN-CENELEC and the AIA-P as well as the CRA-P: the need to include fundamental rights in harmonised European standards leads to tensions between EU projects and existing ISO/IEC and IEEE standards, not only in terms of

substance but also due to the fact that by and large the same people are meeting in ESO working groups who have elaborated the ISO/IEC standards;
- in the relationship between the ESOs, stakeholder organisations at national and European level, and ISO/IEC: participation by civil society in elaborating technical standards belongs to the core values which the European Commission would have to promote to justify why existing ISO/IEC and IEEE standards are insufficient.

In sum:

- transfer of the New Approach/NLF to the digital economy considerably increases the impact of EU law on the standard-making process, which has to be organised so that harmonised European standards are not only lawful but are acceptable in European society;
- standardisation organisations do not have the necessary institutional, procedural, and substantive governance structure to answer hard normative questions, which the building of a human-centric secure, trustworthy, and ethical AI requires, such as the definition of where to draw the red line;
- that is why the governance structure of the interaction among the European Commission – more broadly the EU – standardisation organisations, and stakeholder organisations has to be reorganised in order to better address the new challenges posed by the digital economy;
- the spirit which should guide any call for change is the universal, structural, architectural, and relational vulnerability of citizen-consumers, thereby taking into account the known deficiencies of the New Approach/NLF in the old economy

Published in July 2023 by BEUC, Brussels, Belgium

BEUC – The Consumer Voice in Europe

ANEC – The European Consumer Voice in Standardisation

Rue d'Arlon 80 - B - 1040 Brussels