



The Role of Standards in Future EU Digital Policy Legislation

A Consumer Perspective

Hans-W. Micklitz



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

The author would like to thank Ursula Pahl, 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.



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

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

The Role of Standards in Future EU Digital Policy Legislation



A Consumer Perspective

Commissioned by ANEC and BEUC

Hans-W. Micklitz

July 2023

Contents

| | |
|--|----|
| Glossary | 8 |
| Disclaimer | 10 |
| Executive Summary | 11 |
| 1. Summary of the Report..... | 11 |
| a) Technical Standards and Product Safety Regulation in the Industrial Economy | 11 |
| b) Conceptual Deficits of EU Digital Policy Legislation in the Digital Economy | 14 |
| aa) Horizontal Legislation on Digital Fairness..... | 14 |
| bb) Foreseeable Use and Use Cases..... | 15 |
| cc) Transformation of the Consumer Acquis through Digital Policy Legislation | 16 |
| c) Acid Test: Human-centric, Secure, Trustworthy and Ethical AI | 18 |
| aa) Search for a Concept in EU Digital Policy Legislation and Socio-technical Standards | 19 |
| bb) Difficulties in Concretising Trustworthy AI Standards..... | 21 |
| cc) Gaps to be Closed..... | 23 |
| 2. Key Results in a Nutshell..... | 24 |
| I. Purpose, Methodology, Argument, and Note to the Reader | 27 |
| II. The Industrial Economy, Technical Standards, and EU Product Safety Regulation | 31 |
| 1. New Approach, Comitology, Consumer Participation, Product Safety..... | 33 |
| a) Foundations of the Regulatory Frame – the New Legislative Framework..... | 33 |
| b) Constitutional Conflicts over Power Sharing | 35 |
| c) Governance Structure..... | 35 |
| d) Extension to Standardisation of Services | 37 |
| e) Safety, Intended, Foreseeable Use or Misuse..... | 38 |
| 2. From New Approach/NLF to Regulation 1025/2012..... | 38 |
| a) Regulation on European Standardisation | 39 |
| b) Formalisation of Governance Structure..... | 40 |
| aa) Institutional Requirements..... | 40 |
| bb) Procedural Requirements..... | 44 |
| cc) Stakeholder Participation..... | 46 |

| | | |
|-------------|---|-----------|
| c) | Governance Structure after <i>James Elliott</i> | 47 |
| aa) | Part of EU Law | 47 |
| bb) | Redistribution of Responsibilities..... | 49 |
| d) | European (harmonised) standards between national and international standards..... | 50 |
| aa) | European and national standard bodies | 51 |
| bb) | European and International Standards..... | 54 |
| cc) | Next Judicial Blow: Public Accessibility of ISO and Harmonised EU Standards?..... | 56 |
| e) | A New Governance Structure under a revised Regulation 1025/2012? | 57 |
| aa) | Roadmap, E&Y Report, and Five-year Implementation Report..... | 57 |
| bb) | Pressuring Core Values into the Governance Structure | 60 |
| f) | Revision of the Governance Structure through the New Legislative Framework?..... | 61 |
| 3. | Lessons to be Learned | 61 |
| III. | The Digital Economy, Technical Standards, and EU Legislation – Conceptual Deficits ... | 63 |
| 1. | AIA-P and Harmonised Standards..... | 65 |
| a) | Consumer Protection – Missing..... | 65 |
| b) | Fundamental Rights – Omnipresent but Underdeveloped | 69 |
| c) | Harmonised Standards, Common Specifications – Inconsistencies and Uncertainties | 71 |
| d) | Common Specifications – Conflicts of Interest..... | 73 |
| e) | Conformity Assessment, Self- and Third-party Certification | 76 |
| 2. | CRA-P and Harmonised Standards..... | 78 |
| a) | Consumer Protection – Missing..... | 79 |
| b) | Fundamental Rights – Less Prominent but Still Underdeveloped | 81 |
| c) | Common Specifications – Without Compensating for Risks to Fundamental Rights..... | 82 |
| d) | Conformity Assessment – Self-Assessment by the Back Door..... | 82 |
| 3. | DSA and Non-harmonised European Standards..... | 83 |
| a) | Consumer Protection – Incomplete and Privatised | 84 |
| b) | Non-harmonised European Standards, Protection of Minors, Stakeholder Participation | 87 |
| c) | Fundamental Rights – Reach and Uncertainties | 89 |
| d) | Compliance – Institutional and Procedural Safeguards | 90 |
| 4. | Concept of Safety, Intended, Foreseeable Use or Misuse in the Digital Economy | 92 |
| 5. | Lessons to be Learned | 95 |

| | |
|---|-----------|
| IV. Acid Test: Secure, Trustworthy, and Ethical AI | 98 |
| 1. ISO/IEC, IEEE, and CEN-CENELEC..... | 99 |
| 2. Trustworthy AI in the EU, ISO/IEC, IEEE – Search for a Concept..... | 101 |
| a) Trustworthiness in the AIA-P, the CRA-P and the DSA..... | 103 |
| aa) <i>Trustworthiness in the AIA-P</i> | 103 |
| bb) <i>Background to Recital 5 AIA-P</i> | 105 |
| cc) <i>Trustworthy AI and Generally Acknowledged State of the Art</i> | 107 |
| dd) <i>Trustworthiness in the CRA-P and the DSA</i> | 108 |
| b) HLEG Guidelines and Ethical Principles..... | 108 |
| aa) <i>Four Components of Trustworthy AI</i> | 109 |
| bb) <i>Giving Shape to Human Agency and Oversight</i> | 110 |
| c) ISO/IEC and IEEE’s Search for a Concept..... | 113 |
| d) Evaluation and Consumer Concerns..... | 116 |
| 3. ISO/IEC, IEEE – Concretising Trustworthy AI through Technical Standards..... | 117 |
| a) ISO/IEC JTC 1/SC 42 on Artificial Intelligence..... | 117 |
| aa) <i>Seven AI Standards Shaping Trustworthiness</i> | 119 |
| bb) <i>AI Draft Proposals on Shaping Trustworthiness</i> | 121 |
| b) IEEE Global Initiative..... | 125 |
| c) Evaluation and Consumer Concerns..... | 128 |
| 4. European Commission Working Programme on Trustworthy AI Standards..... | 129 |
| a) 2023 Working Programme, Call for Proposals..... | 129 |
| aa) <i>Working Programme</i> | 130 |
| bb) <i>Call for Proposals</i> | 131 |
| b) 2022 Working Programme, Call for Proposals..... | 134 |
| c) Implementing Decision on a Standardisation Request..... | 135 |
| aa) <i>Trustworthy AI and Generally Acknowledged State of the Art</i> | 136 |
| bb) <i>Ten Mandated Standards</i> | 138 |
| c) Evaluation and Consumer Concerns..... | 142 |
| 5. CEN-CENELEC, ETSI on Trustworthy AI Standards..... | 143 |
| a) CEN-CENELEC Initiatives in the Field of AI..... | 143 |
| b) ETSI initiatives in the field of AI..... | 147 |
| c) Evaluation and Consumer Concerns..... | 148 |
| 6. Comparison ISO/IEC, IEEE, CEN-CENELEC Trustworthy AI Standards with EC WP..... | 150 |

| | |
|---|------------|
| V. Lessons to be Learned and Conclusions to be Drawn | 154 |
| 1. Legacy of the New Approach/NLF Designed Made for the Industrial Economy..... | 154 |
| a) Participation by Stakeholders – Consumer Organisations and ANEC..... | 154 |
| b) Conformity Assessment, Presumption of Conformity, and Certification..... | 156 |
| 2. Unquestioned Transfer of the New Approach/NLF to the Digital Economy..... | 158 |
| a) Passing the Buck, Normative and Descriptive/Applied Ethics, Use Cases..... | 158 |
| b) Technical Standards, Deliverables, and Socio-technical Standards..... | 159 |
| c) Red Lines on Standardisability in both the Industrial and the Digital Economy..... | 161 |
| d) Technical Standards, Fundamental Rights and the Consumer Acquis..... | 163 |
| e) HAS Consultants, Standardisation Scrutiny Board, Accessibility..... | 164 |
| f) Civil Society Participation as Core Values..... | 166 |
| g) Geopolitics..... | 168 |
| 3. Options for Change..... | 169 |
| a) First Option – No Change..... | 170 |
| b) Second Option – Amendment of Regulation 1025/2012..... | 172 |
| aa) Red Lines on Standardisability..... | 173 |
| bb) Institutional Governance..... | 173 |
| cc) Procedural Governance..... | 176 |
| dd) Substantive Governance..... | 178 |
| c) Third Option – Amending the AIA-P, the CRA-P and the DSA..... | 181 |
| VI. Proposal for a Standardisation Governance Act | 182 |
| 1. Recitals..... | 182 |
| 2. Text of the Proposed Amendment..... | 190 |

Glossary



- **AFNOR** – Association Française de Normalisation
- **AI** – Artificial Intelligence
- **AIA-P** – Artificial Intelligence Act Proposal
- **ANSI** – American National Standards Institute
- **ANEC** – The Consumer’s Voice in Standardisation
- **CEN** – Comité Européen de Normalisation
- **CENELEC** – Comité Européen de Normalisation Électrotechnique
- **CEN/CWA** – Workshop Agreement, which aims at bringing about consensual agreements based on deliberations of open Workshops with unrestricted direct representation of interested parties
- **CEN/TS** – Technical Specification, that serves as a normative document in areas where the actual state of the art is not yet sufficiently stable for a European Standard
- **CEN/TR** – Technical Report for information and transfer of knowledge
- **CEN/CWA** – Workshop Agreement, which aims at bringing about consensual agreements based on deliberations of open Workshops with unrestricted direct representation of interested parties
- **CRA-P** – Cyber Resilience Act Proposal
- **CRD** – Consumer Rights Directive
- **DA-P** – Data Act Proposal
- **DGA** – Digital Governance Act
- **DIN** – Deutsches Institut für Normung
- **DMA** – Digital Market Act
- **DSA** – Digital Services Act
- **EC** – European Commission
- **EC WP** – European Commission Working Programme
- **EID** – European identity framework
- **EN** – European Standard
- **ESOs** – European Standardisation Organisations
- **ETSI** – European Telecommunication Standards Institute
- **EUCHR** – European Charter of Fundamental Rights

- **GDPR** – General Data Protection Regulation
- **HAS** – Harmonised Standards Consultant
- **HLEG** – High Level Expert Group
- **IEC** – International Electrotechnical Commission
- **IEC/SRD** – Systems Reference Deliverable
- **IEEC** – Institute of Electrical and Electronics Engineers
- **IEEE ICAID** – Global Initiative on Ethics of Autonomous and Intelligent Systems Industry Connections Activity Initiation Document
- **ISO** – International Organization for Standardization
- **ISO/IEC AWI** – Approved Work Item Proposal (the majority of the national mirror committees supports the proposal since November 2022)
- **ISO/IEC CD** – Committee Draft (which has not yet reached the stage at which the public comment takes place)
- **ISO/IEC DIS** – Draft International Standard
- **ISO/IEC FDIS** – Final Draft International Standard
- **ISO/IEC TR** – Technical Report
- **ISO/IWA** – International Workshop Agreements
- **ISO/PAS** – Publicly Available Specifications,
- **ISO TS** – Technical Specifications,
- **JTC** – Joint Technical Committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- **ML** – Machine Learning
- **NLF** – New Legislative Framework
- **PLD** – Product Liability Directive
- **RGPS** – Regulation on General Product Safety
- **SMEs** – Small and Medium-Seized Enterprises
- **UCPD** – Unfair Commercial Practices Directive
- **UCTD** – Unfair Contracts Term Directive
- **WG** – Working Group
- **WP** – Working Programme

Disclaimer



This Report is written at time when it is highly likely that the AIA and the CRA will be adopted in the near future. Interinstitutional negotiations on the AIA will take place before the summer. However, the Report takes for granted that the two Acts will be adopted in one form or the other and that they will rely on technical standards. That is why the report does not engage with the fundamental critique raised against the overall approach of the European Commission to regulate AI, but focuses instead on the technical standards which are supposed to play a crucial role in EU Digital Policy Legislation. The Report rests on the premise that there is no viable alternative to technical standards and that the competence of the AI industry is needed to build those standards. The focus is therefore laid on the potential challenges that this reliance poses, in particular to consumer agency.

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 scandal¹ 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 Check⁶ 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 2.0¹² 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=Aucb5tJM70>; <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 system²⁰ – 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. IEEE 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 be 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 be 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 as 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

I. Purpose, Methodology, Argument, and Note to the Reader

The EU Draft Regulations AIA-P, CRA-P on the digital economy and digital society rely heavily on European technical standards elaborated through the European Standardisation Organisations (ESOs) – CEN, CENELEC and ETSI – in order to complement the binding legal requirements of secondary EU law through harmonised European standards. These standards must not only take into account the physical safety of persons but also their mental health and the Charter of Fundamental Rights.²⁵ Standardisation organisations have a long-standing tradition in dealing with the standardisation of product characteristics, including product safety. However, the envisaged integration of mental health and the pertinent call to respect fundamental rights go far beyond their existing experience. The (draft) Regulations raise *serious political* and legal concerns,²⁶ which can be overcome only through a review of the existing European Legal Framework on Standardisation, and its replacement through a ‘*Standardisation Governance Act*’. There is abundant literature on what ‘governance’ means; however, when it comes to concretising its scope and reach there is agreement that governance comprises three different layers²⁷ namely:

- *institutional* – between the EU institutions and the standardisation organisations,
- *procedural* – transparency, participation, voting, conflict resolution and
- *substantive* – in this dimension, an assemblage of technology and societal implications – in our context, the *socio-technical*²⁸ character of AI technical standards.

This is the terminology ever more often used in the field of AI standardisation. Implementation of the new Standardisation Strategy, initiated by the European Commission in February

25 This is recognised by the European Commission in its recent Standardisation Strategy: Com (2022) 31 final An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market <https://ec.europa.eu/docsroom/documents/48598> ‘More than ever, standards do not only have to deal with technical components, but also incorporate core EU democratic values and interests, as well as green and social principles.’

26 K Vieweg, Technische Normung und Wirtschaftsrecht – Zu den ethischen Anforderungen beim Einsatz ‚Künstlicher Intelligenz‘, in Festschrift für W E Ebke, Deutsches, Europäisches und Vergleichendes Wirtschaftsrecht, Hrsg B P Paal, D Poelzig, O Fehrenbacher, C H Beck München, 2021, 1025; M Ebers, Standardizing AI – The Case of the European Commission’s Proposal for an Artificial Intelligence Act (August 6, 2021). The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, Available at SSRN: <https://ssrn.com/abstract=3900378> or <http://dx.doi.org/10.2139/ssrn.3900378>; Sybe de Vries, Olia Kanevsk, AIA-P and Rik de Jager, Internal Market 3.0: the Old ‘New Approach’ for Harmonising AI Regulation, forthcoming, on file with the author.

27 F Möslin/K Riesenhuber, Contract Governance – A Draft Research Agenda, European Review of Contract Law (ERCL) 5 (2009), 248–289.

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

2022,²⁹ offers the opportunity to identify current deficiencies, and to look for ways and means to overcome legal and constitutional concerns in the envisaged use of standardisation for regulating AI and other digital technologies in Europe. This Report is written through the lenses of consumer advocacy, building on experience in product safety regulation, and interaction between EU legislation and technical standardisation.

The law on standards,³⁰ despite its academic attractiveness, is still difficult to access. Intensive desk research allows the researcher to find the policy documents of the European Commission and of the ESOs. The websites, however, are produced for insiders and they vary considerably in the way they provide access to documents and at what stage in the elaboration process. Without the help and support of BEUC and ANEC, I would have had to spend much more time and energy to bring the necessary information together, nor am I even sure whether I would have found all the documents. BEUC/ANEC enabled me to find competent interview partners in DG Grow, DG Connect, CEN-CENELEC, ETSI, IEEE, AFNOR, DIN, VDE, Stiftung Warentest, Microsoft and IBM/BITCOM. All in all, I took 20 interviews over roughly 30 hours. My interview partners provided me not only with all sorts of material often at the crossroads with confidentiality, but more importantly allowed me to gain deep insights not only into the politics and policy of standardisation, but also on the concrete problems that the working groups are facing in elaborating AI technical standards. A final barrier remained, though. Few AI technical standards are made available for free. In their vast majority, they are protected through copyright. The same is true with regard to ongoing work on draft projects at whatever stage. Whilst access to existing standards can be bought, access to the inner machinery is limited to the members of the respective working groups. The various interviews helped me to close the knowledge gap, if not with regard to all the technical details then at least definitely with regard to the politics behind the different exercises.

This Report is broken down into six parts:

- The *first* part identifies the purpose and the methodology, demonstrates the argument and leaves the reader a note for guidance.
- The *second* part looks into the *politics* of European law on standardisation in the industrial economy, how the law on standardisation developed from the 1985 New Approach into the 2008 New Legislative Framework and the 2012 Regulation on European Standardisation, and how these interact with product safety regulation. Only such a look back explains the path dependency of the European approach, of using a combination of binding legislation and voluntary standards in sensitive fields such as product safety, which had its merits in the old economy, despite well-known and highly debated deficiencies.
- The *third* part analyses how the New Approach/NLF is integrated into EU Digital Policy Legislation and what kind of role technical standards are supposed to play in EU Digital Policy Legislation, in the AIA-P, CRA-P, and the DSA, although the latter relies on non-harmonised European standards. The three acts are screened in order to get a picture of how promotion of harmonised standards is connected to consumer protection, to fundamental rights, and to a common specification as a substitute for harmonised European standards.

29 Com (2022) 31 final An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market

30 Still seminal: H Schepel *The Constitution of Private Governance* (Oxford: Hart Publishing, 2005), with a recent revival, O Kanevsk *AIA-P, The Law and Practice of Global ICT Standardization*, CUP 2023, M Gérardy, *The 'Standards Effects': The Public Instrumentalisation of technical standards in EU law*, PhD University of Luxembourg, 2023.

The consumer lenses demonstrate that deficiencies in the existing governance structure are aggravated through unquestioned transfer into the digital economy, which is particularly apparent in the missing conceptualisation of a comparison between foreseeable use in product safety and foreseeable use in EU Digital Policy Legislation.

- The *fourth* part moves from the *legal* dimension of EU Digital Policy Legislation to the *socio-technical* dimension of EU Digital Policy Legislation, from the foreground to the underground, from top-down to bottom-up, so to say. The standard formula which is meant to guide elaboration of technical standards is ambitious: harmonised European standards are to establish ‘human-centric, secure, ethical, and trustworthy AI’. The purpose of the *fourth* chapter is to conceptualise the content of the formula at the more abstract level in law and policy documents and use the benchmark thereby developed to analyse AI standards on the trustworthiness of international standardisation organisations, ISO/IEC, IEEE and of the European Standardisation Organisations (the ESOs). It will have to be demonstrated that ISO/IEC and IEEE have already established a dense net of AI standards which occupy a field into which the European Commission and the ESOs are currently trying to drag their feet. In a geopolitical perspective, the EU is playing out its regulatory power, the power which stands behind a supranational entity covering 500 million potential consumers.³¹
- The *fifth* part summarises the overall findings, the lessons to be learnt from technical standardisation in the industrial economy, from the top-down regulatory approach in EU Digital Policy Legislation and from bottom-up efforts to lend shape to trustworthiness through technical standards. The deficiencies of the existing governance structure thereby identified serve as a starter in the search for potential solutions at the institutional, the procedural, and the substantive levels.
- The *sixth* part develops key elements of a model for a ‘Governance Act on Standardisation’. The proposed act is intended to overcome existing deficiencies and to lay down a governance structure adapted to the needs of a regulatory approach which combines binding legal requirements and technical standardisation in ever more policy fields, product safety, environmental protection – and now Artificial Intelligence. The proposed Governance Act on Standardisation aims at a revision of the current Regulation 1025/2012 with regard to harmonised European standards.

The Report takes a European perspective, with a particular focus on the role and function which consumers are expected to play in the digital economy; how their interests are taken care of in EU Digital Policy Legislation and what a revised governance structure in its threefold dimension – substance, procedure, and institutions – should look like. In what follows, I am relying on our joint study of EU Consumer Protection 2.0, commissioned by BEUC in 2020.³² Here we have developed and explained the concept of digital vulnerability, which includes the structural, the architectural, and the relational, and which can and should be translated into the legal concept of ‘structural asymmetries in digital consumer markets’. The digital economy, so the key message goes, endangers consumer autonomy. Neither the AIA-P nor the CRA-P addresses autonomy upfront. The AIA-P prohibits practices that materially distort a person’s behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm, which is a rather narrow concept. The DSA goes further as its Recital 67 requires that decision-making autonomy shall not be distorted or impaired through dark

³¹ A Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

³² N Helberger et al. *EU Consumer Protection 2.0* (n 8)

patterns.³³ The explanatory memorandum to the AIA-P refers to ‘digital autonomy’, though without specifying what is meant. Translated into the context of this Report, EU Digital Policy Legislation should aim at restoring the autonomy of the consumer in providing them with a technology that serves first and foremost the interests of the people and ensures that humans remain in control. This in turn harnesses the great potential that lies in AI to increase equality, and enables a better life – hopefully not only in Europe.³⁴

33 Dark patterns in online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of service recipients to make autonomous and informed choices or decisions. These practices can be used to persuade service recipients to engage in unwanted behaviours or come to undesired decisions which have negative consequences for them. Providers of online platforms should therefore be prohibited from deceiving or nudging service recipients and from distorting or impairing the autonomy, decision-making, or choice of service recipients via the structure, design or functionalities of an online interface or a part thereof.

34 O Lobel, *The Equality Machine: Harnessing Digital Technology for a Brighter, More Inclusive Future*, 2022.

II. The Industrial Economy, Technical Standards, and EU Product Safety Regulation

The leading industrial states established national standardisation organisations in the early years of the twentieth century: the UK in 1901, Germany in 1917, the USA in 1918,³⁵ and France in 1926.³⁶ They promoted the foundation of international counterparts, ISO in 1947 and IEC in 1906. Their European counterparts were set up after the foundation of the EEC: CEN in 1961, CENELEC in 1973, and ETSI in 1988. Yet standardisation is at least two thousand years old. The Romans are said to have invented standardisation in the building of their warships. Initially, standardisation was about measuring: making sure that the different bits and pieces which are needed for the same device fit together. The age of industrialisation boosted standardisation. Think of Charlie Chaplin in *Modern Times* The competent ministries in the rapidly industrialising states were not able to cope with the speed and need of a standardised production process. However, industries took standardisation into their own hands and – this is crucial – the public authorities in the wider sense began to rely on the expertise enshrined in each and every technical standard.³⁷ This is worth remembering in terms of designing a new governance structure. Putting technical standardisation back into the hands of administrations would mean turning the clock back by more than a hundred years. This is undoubtedly not a viable alternative.³⁸

Industrialisation went hand in hand with electrification and so went standardisation, too. Whenever products were electrified, safety issues were on the agenda. This is visible even today in the bifurcation between the different standardisation organisations, ISO and IEC; CEN and CENELEC; and, with the same specialisation at the national level in Germany, DIN and DKE/VDE. However, standardisation did not touch upon product quality. Quality was and should be left – this is the rationale of capitalist production – to the market. However, in the second half of the twentieth century technical standardisation reached beyond mere measuring techniques and came ever closer to quality by regulating ‘design’, although in terms of policy the emphasis is laid on performance as process.³⁹ The transformation of technical standards

³⁵ NIST is the US government department dealing with standards etc.

³⁶ Engineering Standards Committee (now British Standards Institution); Deutsches Institute für Normung; American Engineering Standards Committee (now American National Standards Institute); Association Française de Normalisation.

³⁷ K-H Ladeur, *The Evolution of General Administrative Law and the Emergence of Postmodern Administrative Law* (2011) *Comparative Research in Law & Political Economy*. Research Paper No 16.

³⁸ Forcefully, H Schepel, *The Constitution of Private Governance*, 2006, 414: similar R van Gestel/P van Lochem, *Private Standards as a replacement for public policy making?* In M Cantero Gamito/ H-W Micklitz (eds), *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes*, Edward Elgar Publishing, 2020, 27.

³⁹ T Büthe and W Mattli, *The New Global Rules, The Privatisation of Regulation in the World Economy* (Princeton, Princeton University Press 2011); J L Contreras (ed), *Cambridge Handbook on Technical Standardisation, Further*

– from mere measuring into quality and process standards – is well documented and has led to ever more sophisticated categorisations.⁴⁰

Only gradually did standardisation make its way into EU law. Standardisation – and this has to be constantly reiterated – started more or less simultaneously in the leading industrial states of the late nineteenth/early twentieth centuries with a strong focus on developing international standards in order to facilitate cross-border trade. Like CEN, CENELEC and ETSI, the EU is a latecomer in a heavily regulated field. The EU aimed at developing European standards in order to build the common – and later the internal – market. This necessarily created tensions between European institutions, the EU, and the ESOs, with national standardisation organisations in and beyond the Member States, as well as with international standardisation organisations. The geopolitical dimension of standardisation is abundant in the regulatory framework of European standardisation. It is well documented in the interaction, the co-operation, and the friction between the ESOs and the international standardisation organisations, in particular ISO.⁴¹

However, a vitally significant factor in the context of this Report consists in the telling difference between the old and the new economy. In the old economy, the Western industrialised states had taken the lead and the EU has used European standardisation, not only to promote the internal market, but also to open up new markets for its industries outside the EU.⁴² This is different in the digital economy. Here the major players are located outside the EU: they are in the USA, in China, and in India. The key actors are striving for international standards, if any. The many fields to be standardised are already occupied by ISO/IEC and IEEE standards or by ISO/IEC and IEEE initiatives. The EU is using its regulatory power to influence standardisation, not only to keep the door open for European companies, but also to defend and to promote ‘core European values’ – fundamental rights – in the standardisation of AI, so as not only to become a ‘global standard setter’⁴³ but a ‘*global leader in the development of secure, ethical, and trustworthy AI*’⁴⁴ Compliance with European harmonised standards ensures access to a market of 500 million customers/consumers. In this twofold dimension, European standardisation of AI is just another variant of the Brussels effect.⁴⁵ The call for a ‘Standardisation Governance Act’ has to take the geopolitical dimension seriously, though not thereby easing the strengthening of consumer policy in European standardisation. Theoretically and conceptually, the EU/EC undertaking could be put under ‘good governance’ in external relations. The EU does not want to carry the burden of the former colonial ‘hegemon’ but would like to be seen as a ‘gentle civiliser’.⁴⁶ Growing critique from the Global South against EU/European-cen-

Intersections of Public and Private Law (Cambridge, CUP 2019) – Art 2.8 TBT Agreement, P Mavroidis, *The Regulation of International Trade*, Volume I, Cambridge Massachusetts, 2016, 52,

40 P Marburger, *Die Regeln der Technik im Recht*, (Tübingen, Mohr Siebeck 1979).

41 Seminal: P Delimatsis (ed), *The Law, Economics and Politics of International Standardisation*, CUP 2015.

42 H-W Micklitz, *The European Transnational Private Law on Regulated Markets*, in A Beckers, H-W Micklitz, R Vallejo and P Letto Vanamo (eds), *The Foundations of European Transnational Private Law*, Hart Publishing forthcoming 2023.

43 J Bjerkem/ M Harbour, *Europe as a global standard-setter: The strategic importance of European standardisation*, EPS policy project, 2020, https://www.epc.eu/content/PDF/2020/EPE_JB_Europe_as_a_global_standard-setter.pdf

44 Roadmap for a European Standardisation Strategy May 2021 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy_en with regard to standardisation and Rec. 5 AIA-P with regard to the regulation of Artificial Intelligence.

45 A Bradford, *Brussels Effect* (n 32).

46 H-W Micklitz, *The Role of the EU in the External Reach of Regulatory Private Law – Gentle Civilizer or Neoliberal Hegemon? An Epilogue*, in: M Cantero Gamito/ H.-W. Micklitz (eds), *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes*, (n 39), 298–20.

trism ‘for good’ reaches far beyond the purpose of this Report but will be touched upon in terms of stakeholder participation.

1. New Approach, Comitology, Consumer Participation, Product Safety

The crucial importance of technical standards for building the EU common market – later the internal market – became clear after the EEC managed to abolish customs. As far back as 1969, the EEC set up its first programme to do away with technical standards as ‘non-tariff barriers to trade’. It promoted adoption of secondary EU law to overcome potential barriers to trade through harmonising technical requirements.⁴⁷ The 1969 programme ended in deadlock. Harmonising technical standards by way of EU directives burdened the legislature with political debates about technical specifications. In 1985, in line with the Single European Act, the European Commission developed the ‘New Approach to technical harmonisation and standards’ – which became known simply as the ‘New Approach’⁴⁸ as compared with the ‘Old Approach’ which had preceded it. The regulatory model gained attention far beyond the EU. It raised concern in the OECD and triggered the GATT TBT Agreements, which levelled up the use of technical standards in the international economic order. The rules in the WTO and the Agreement on Sanitary and Phytosanitary Products are heavily influenced by the European initiative. This is not the place to evaluate the effect of the GATT/WTO rules, let alone the Agreement on Sanitary and Phytosanitary Products, but the example shows that the EU is powerful enough to influence rule production at the international level.

a) Foundations of the Regulatory Frame – the New Legislative Framework

What kind of politics has the EU pursued, what kind of regulatory frame has the EU established that shaped the governance structure of European standardisation? In the 1980s, the EU underwent one of its many crises. The New Approach must be seen in the wider context of the 1985 White Paper on the Completion of the Internal Market and the 1986 amendment of the Treaty in the Single European Act. The aim of eliminating barriers to trade is inherently intertwined with the necessity to guarantee an appropriate level of product safety for European consumers. The EU prepared the ground for the New Approach with Directive 83/189 (today Directive 2015/1535). The Information Directive required Member States to notify the EC when they were developing new national technical regulations. National standardisation organisations were obliged to notify CEN-CENELEC of national standardisation projects, and to refrain from initiating or continuing work that could frustrate European standardisation. In order to support harmonisation efforts at the European level, the Directive also establishes a request procedure enabling the European Commission, after consultation with the Member States, to mandate a European Standardisation Organisation to develop technical standards corresponding to a

⁴⁷ Ch Joerges/ J Falke/ H-W Micklitz/ G Brüggemeier, *Die Sicherheit von Konsumgütern und die Entwicklung der Europäischen Gemeinschaft*, Band 2, ZERP Schriftenreihe, 1988; Joerges, Ch, Falke, J, Micklitz, H-W and Brüggemeier, G ‘European Product Safety, Internal Market Policy and the New Approach to Technical Harmonisation and Standards’ (1991) EUI Working Paper Law No. 10–14 = with a new foreword reprinted in (2010) 6 *Hanse Law Review* 109

⁴⁸ The so-called New Approach was approved by the Council on 7 May 1985 in its ‘Resolution on a New Approach to technical harmonisation and standards’, OJ 1985 C 136/1

specific aspect of legislation. Step by step these rules were further elaborated. The 1985 Memorandum of Understanding formalised the relationship between the European Commission and the European Standardisation Organisations: CEN, CENELEC and later ETSI (replaced in 2003 through the Guidelines for Co-operation⁴⁹). The 1985 New Approach provided a model of what the future of European standardisation should look like.

The EU legislature should limit itself to formulating legally binding legal requirements, to be concretised through voluntary technical standards. Manufacturers are not obliged to apply technical standards to prove compliance with requirements. They remain free to choose a different technical option, as long as it complies with ‘binding legal requirements’.⁵⁰ Compliance with European standards, notwithstanding their origin, sets a presumption of conformity, hence making it much easier to show compliance with legal requirements. As a rule, it is for the manufacturer to ensure that products respect technical requirements and to document compliance through CE marking. The EU may require, via secondary EU law, the involvement of third parties, so-called Notified Bodies; these are accredited certification bodies which substitute self-certification. The riskier the product, the greater the tendency in EU law to rely on third-party certification instead of self-certification. The regulatory philosophy is laid down in what has become known as the New Legislative Framework (NLF).⁵¹ Whether or not a particular regulatory project is suitable for New Approach-type legislation is laid down in Decision 90/683 (then 93/465, today Decision 768/2008). According to this Decision, products can be placed on the market only if they comply with applicable European legislation (Article 1) and, in particular, with the essential requirements aimed at protecting public interests (Article 3(1)). According to the same provision, the essential requirements must be expressed in terms of the results to be achieved. Regulation 93/393 (today Regulation 765/2008) specified the requirements on accreditation and market surveillance (amended by Regulation 2019/1020). The three together – Decision 768/2008, Regulation 765/2008, and Regulation 2019/1020 – form the NLF.⁵²

Initially, the European Commission started from the premise that the Product Liability Directive 85/374, also adopted in 1985, would suffice to handle potential risks which might result from unsafe consumer products, either as a deterrent or by way of providing a solid ground for compensation claims. However, it turned out that the ‘New Approach’ needed to be counterbalanced by a Product Safety Directive. This was adopted after fierce debates in 1992 as Directive 92/59 (today 2001/95, to be transformed in Regulation 2023).⁵³ The Directive operates like a safety net. It only applies in the absence of sectoral legislation. Its purpose is to fill gaps. Within its scope of application, the Directive obliged manufactures to bring only safe products on to the market and established a system of post-market control in order to take unsafe products off the internal market through competent national authorities. Step by step, the European Commission succeeded in introducing technical standards into product safety

49 General Guidelines for the Cooperation Between CEN, CENELEC and ETSI and the European Commission and the European Free Trade Association 28 March 2003 (2003/C 91/04) <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2003:091:0007:0011:EN:PDF>

50 However, non-harmonised European standards may unfold a de facto binding effect, ECJ Case C-171/11 *Fra.bo* [2012] ECLI:EU:C:2012:453 to be discussed below.

51 https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

52 Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products, OJ 2008 L 218/30; Decision 768/2008 on a common framework for the marketing of products, OJ 2008 L 218/82; and Regulation (EU) 2019/1020 on market surveillance and compliance of products, OJ 2019 L 169/1.

53 <https://www.europarl.europa.eu/committees/en/general-product-safety-regulation/product-details/20220904CDTI0083>

regulation. Originally lacking, Article 6 Regulation 2023 provides for a presumption of conformity so long as the manufacturer complies with European standards.

b) Constitutional Conflicts over Power Sharing

Efforts by the European Commission to abolish technical barriers to trade through New Approach-type secondary EU law led to tensions between the EU and the Member States on the one hand and the EU institutions – the European Commission, the Council, and the European Parliament – on the other. The involvement of ESOs was heavily criticised as an unlawful delegation of power reaching beyond the then Article 155 EEC (Treaty of Rome). There has been – and remains – intense debate on the reach of the *Meroni* Judgment⁵⁴ and whether and to what extent elaboration of technical standards should be regarded as rule making, which is reserved for the EU legislature. The 1987⁵⁵ Council Decision on the implementing powers of the European Commission was based on Article 145 of the Treaty, which was not amended by the Single European Act. The Decision introduced a distinction between different types of committees according to their regulatory function and the degree of influence that the Member States and the European Parliament might exercise. The 1987 Council Decision did not settle conflicts, though. The Lisbon Treaty introduced a distinction between Articles 290 (delegating acts) and 291 (implementing acts) TFEU and lifted the conflict to the ‘constitutional’ level. The revised comitology regulation 182/2011 is based on Article 291 (3) TFEU and defines the possibilities of the Member States and the European Parliament to influence, supervise, and control mandating and publication of harmonised standards. This does not mean, however, that the debate on whether the involvement of ESOs requires application of Article 290 TFEU is over, in particular in light of recent developments in the case law of the CJEU, which is about to tighten its grip on judicial control of harmonised European standards.⁵⁶

c) Governance Structure

The institutional dimension rests on the interaction between the European Commission and the ESOs. The European Commission recognised the ESOs – at the time CEN and CENELEC only – as the key actors. The ESOs on the other hand were ready to co-operate with the European Commission in promoting European standards as industry would benefit from easy access to the internal market due to the presumption of conformity. The 1985 mechanism was a memorandum of agreement, which could be classified as a kind of contract between two institutions on a level playing field. The shift from a memorandum to guidelines in 2003 in order to include the newly established ETSI set a slightly different tone. The mutual element is reduced. A memorandum differs from guidelines. Both the memorandum and the guidelines were signed by the two parties.

At that time, consumer associations in whatever sense were not forming part of the institutional structure. There were no triangular negotiations. However, the memorandum and later the 2003 Guidelines insisted on the need to strengthen participation by stakeholder organisations, such as consumers’ and workers’ organisations. The two key actors had the authority and

⁵⁴ Cases C-9/56 and C-10/56 *Meroni v High Authority* [1957/1958] ECR 133.

⁵⁵ Council Decision of 13 July 1987 laying down the procedures for the exercise of implementing powers conferred on the Commission (87/373/EEC)

⁵⁶ For a deeper analysis M Chamon, *The European Parliament and Delegated Legislation, An Institutional Balance Perspective*, Hart 2021.

were ready to 'grant' stakeholder organisations some participatory rights. The only two consumer institutions were the Consumer Consultative Committee (CCC today CPAG⁵⁷) and BEUC, the umbrella organisation of consumer associations. The EC and CEN-CENELEC involved the Consumer Consultative Committee in the negotiations on consumer participation in technical standardisation, which led to tensions between the CCC and BEUC. In the end, BEUC took over the so-called Secretariat for Co-ordination (SeCo) and received additional funding from the EC. BEUC was in charge of organising the potential input of consumer organisations in technical committees and handling possible reimbursement of travel costs to meetings. However, participation was not yet institutionalised but proceeded on an ad hoc basis. The proposal by the European Commission to establish a consumer committee in parallel to the standing committee of the Member States (the predecessor of comitology) failed and it took until 1995 before ANEC was established.⁵⁸

Procedural mechanisms were still in the making. However, the two sides drew a clear line between, on the one hand, a harmonised (European) standard responding to a Commission mandate and, on the other hand, other European standards. The European Commission could require elaboration of standards through a mandate and the Commission was entitled to cite their references in the Official Journal. At the time, the European Commission rejected any responsibility for assessing compliance of technical standards with binding legal requirements, let alone with a mandate.⁵⁹ Indeed, the Commission understood that the ESOs are in charge of the compliance procedure. They were the ones who hired the New Approach Consultants who were in charge of advising the technical committees developing standards on compliance. The exact details of their responsibilities were laid down in CEN-CENELEC Guide 15, which was withdrawn after the European Commission had taken over management of consultants in the aftermath of the *James Elliott* judgment.⁶⁰

Still in 1998, the European Commission used forceful language:

Responsibility for presenting European standards as 'harmonised' standards under the New Approach has been given to the European standards organisations. At the same time, public authorities have committed themselves to not insisting on approving the technical content of such standards; no positive decision is required by which authorities approve the standards, even if previously such technical aspects were subject of regulation.⁶¹

The 2000 Guide is more ambiguous in terms of publication of an EN:⁶²

The objective of publishing the reference in the Official Journal is to set the earliest date for the presumption of conformity to take effect. Before the Commission publishes the reference, it may verify that the terms of the mandate are fulfilled.

57 https://commission.europa.eu/strategy-and-policy/policies/consumers/consumer-protection-policy/our-partners-consumer-issues/consumer-policy-advisory-group-cpag/european-consumer-consultative-group-eccg_en

58 For details, see H-W Micklitz in Joerges et al. (f. 58), at 413 German version.

59 H Schepel (n 31), at 524.

60 See under II 2 c).

61 Report from the Commission to the Council and the European Parliament of May 13 1998, on efficiency and accountability in European standardisation under the New Approach, COM(1998)0291, at 3, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51998DC0291&from=FR>

62 2000 Guide for the implementation of New Approach and Global Approach directives available at <https://op.europa.eu/en/publication-detail/-/publication/4f6721ee-8008-4fd7-acf7-9d03448d49e5> at 28.

A conflict was set up here at a very early stage – a conflict that still awaits a clear solution.

The New Approach triggered and augmented adoption of directives where the EU legislature refrained from laying down detailed technical requirements and instead relies on binding safety requirements to be concretised through technical standards elaborated by the ESOs as European standards. Whilst the New Approach-type directive unblocked the elimination of technical barriers to trade – even those with a product safety component – the European Commission failed more or less in transposing the New Approach to the field of services, where safety is less dominant and where standardisation interferes more generally in the concretisation of the rights and duties of the parties.

d) Extension to Standardisation of Services

The ‘law of standards’ came even closer to consumer policy and law when the EU adopted the Services Directive 2006/123/EC.⁶³ The original political attention of the EU was to set up an overall frame for all those services that are not subject to particular sectoral or subject-related rules. Here we have to think of all those services that consumers require in their daily lives, such as craftsmen, repair services, dry cleaning, cleaning and maintenance, home and leisure activities, and so on. In the field of services, technical specifications easily transgress legal boundaries in formulating legal rights and obligations which determine the scope and content of services to be performed. Through the lenses of consumer advocacy, the borderline between technical standards and standard contract terms becomes blurred.

One might understand the interaction between the rules in the Service Directive and the underpinning standardisation of these down-to-earth services as an early attempt by the European Commission to compensate for a lack of common rules on contracts for services, a deficit which is equally visible in the Draft Common Frame of Reference.⁶⁴ However, the European Commission did not succeed in pushing technical standardisation of services either in b2b or in b2c relations. Some 70% of EU gross income results from services, though, whereas only 2% of all EU standards deal with services.⁶⁵ The few existing standards on services are nevertheless of major interest for consumer lawyers as they demonstrate to what extent technical standards can substitute private law rules, thereby providing for a much broader understanding of ‘contract’ covering both the pre-contractual and the post-contractual stage.⁶⁶ In its Roadmap for a new Standardisation Strategy, the European Commission refers to universal services as a potential field of standardisation.⁶⁷ The other envisaged areas of activities are those with a shaky competence in the Treaty: social policy, education, sport, and health. This looks like a mixture – a revitalisation of the old, though failed, strategy from 2006, and a reply to the servification of society with regulated markets taking the lead.

⁶³ Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market OJ L 376, 27.12.2006, 36–68.

⁶⁴ [https://max-eup2012.mpipriv.de/index.php/Common_Frame_of_Reference_\(CFR\)](https://max-eup2012.mpipriv.de/index.php/Common_Frame_of_Reference_(CFR))

⁶⁵ Figures referenced in the Roadmap (n 45).

⁶⁶ H-W Micklitz, *Services Standards: Defining the Core Elements and Their Minimum Requirements*, study commissioned by ANEC, 2007, <http://www.anec.eu/attachments/ANEC-R&T-2006-SERV-004final.pdf>; V Leeuwen, B, *European Standardisation of Services and its Impact on Private Law* (Oxford: Hart Publishing, 2017)

⁶⁷ Roadmap for a European Standardisation Strategy (n 45) at 2.

e) Safety, Intended, Foreseeable Use or Misuse

The Product Liability Directive (PLD) was adopted in 1985, the Product Safety Directive (PSD) in 1992. One of the crucial issues in the legislative process was the extent to which the concept of safety could be determined by the manufacturer or by the consumer, the user of the product.⁶⁸ Article 6 PLD 92/59 starts from the premise that a:

product is defective when it does not provide the safety which a person is entitled to expect.

The PSD says in Article 2 (b):

safe product shall mean any product which, under normal or reasonably foreseeable conditions of use, including duration, does not present any risk or only the minimum risks compatible with the product's use, considered as acceptable and consistent with a high level of protection for the safety and health of persons,...

The formula remained the same in the recently adopted Regulation on General Product Safety (RFPS) 2023/988, Article 2 (3).

The Product Safety Regulation sends a clear message to the standardisation organisations: normal or 'reasonably foreseeable conditions of use' – to be added by the consumer/user – must be taken into account when developing technical standards with an impact on product safety. The formula contains both a normative and an empirical message: the normative is the obligation imposed on the manufacturer; the empirical is the need to build a heuristic on the way in which the consumer might use the product beyond the intended use. The history of European technical standards is full of conflicts which document that the level of safety – meaning the degree to which the user perspective has to be taken into account – is a constant and ongoing battleground. Annex I to this Report reconstructs one of the success stories, where ANEC managed to strengthen the level of safety through a re-wording of the standard concerned.⁶⁹ On the other end stand unresolved conflicts, such as that on accessibility to elevators by people with disabilities, where the European Disability Forum criticises the ESOs for having pushed a European standard through the procedure which contradicts both the spirit and the purpose of the European Accessibility Act.⁷⁰ One might conclude that the concept of 'foreseeable use' made its way into the New Approach type of legislation and technical standards, or in today's language, binding legal requirements and technical standards have to take 'use cases' into account.

2. From New Approach/NLF to Regulation 1025/2012

The New Approach turned into a win-win solution. The European Commission needed the ESOs as industry alone had the necessary skills to develop such standards and to break the deadlock, while the ESOs needed the European Commission in politically prioritising and subsidising

⁶⁸ Hans-W Micklitz in Ch Joerges/ J Falke/ H-W Micklitz/ G Brüggemeier, Die Sicherheit von Konsumgütern und die Entwicklung der Europäischen Gemeinschaft, (n 58), at 42.

⁶⁹ ANEC Case study on the EN 60335 series Safety of electrical household appliances, 2023. Available on request.

⁷⁰ The point of conflict is EN 81-70 on the accessibility of lifts. The stumbling block is ICT standard EN 301 549 https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf

technical standards, compliance with which guarantees access to the Internal Market. Both sides – the European Commission and the ESOs – praise the success of the New Approach and its reflection in the development of further harmonised European standards.⁷¹ The more harmonised European standards are available, the more likely it is that industry refrains from using the option to provide compliance with binding legal requirements through a rather costly and administratively burdensome self-assessment or third-party assessment. The old stories about technical standards as barriers to trade which preoccupied the European Commission, the Member States, and industry in the 1980s vanished from the political agenda. During recent decades, the European Commission has been using harmonised European standards ever more often to implement European policy objectives, such as sustainability. This is well documented in the four regulated markets: finance, energy, telecoms, and transport.⁷² Very few standards that respond to the EC mandate are not harmonised.

a) Regulation on European Standardisation

Regulation 1025/2012 adapted the ‘New Approach’ to a ‘Regulation on European Standardisation’,⁷³ often somewhat misleadingly equated with the New Legislative Framework (NLF). Whether or not EU legislation is aligned with the NLF always needs to be specified. The AIA-P and the CRA-P are part of the NLF.⁷⁴ Some 27 years after adoption of the New Approach, the European Union put the established co-operation between the European Commission and the ESOs on firm legal ground. The Regulation pins down established practice into law and formulates a mandate for the objectives to be achieved. Article 1 defines the overall purpose in amazingly telling language:

This Regulation establishes rules with regard to the cooperation between European standardisation organisations, national standardisation organisations, Member States and the Commission, the establishment of European standards and European standardisation deliverables for products and for services in support of Union legislation and policies, the identification of ICT technical specifications eligible for referencing, the financing of European standardisation and stakeholder participation in European standardisation.

Article 2 (1) brings clarity to often confusing language and draws a distinction between European harmonised standards (HEN), which are mandated, and other European standards. Whilst all European standards are voluntary – even mandated harmonised European standards – non-harmonised European standards are often called ‘purely voluntary’ by practitioners. Harmonised European standards mandated by the European Commission grant presumption of conformity, though. Here is the definition:

b) ‘European standard’ means a standard adopted by a European standardisation organisation;

⁷¹ Brussels, 11.11.2022 SWD(2022) 364 final Commission Staff Working Document evaluation of the New Legislative Framework {SWD(2022) 365 final} at 20 The majority of stakeholders among all stakeholder groups in the targeted consultations (84.1%, 174/207) considered the use of harmonised standards to have been effective as a voluntary mechanism for achieving conformity with the essential requirements.

⁷² H-W Micklitz, The European Transnational Private Law on Regulated Markets, (n 43).

⁷³ See for useful background information on the history Reg 1025/2012 M Eliantonio (2017). Alternative forms of regulation: are they really ‘better’ regulation? A case study of the European standardisation process. European Journal of Law Reform, (1/2), 141–163, <https://doi.org/10.5553/EJLR/138723702017019102008>

⁷⁴ https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

(c) ‘harmonised standard’ means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation;

The following explains and analyses the work programme of the European Commission, standardisation requests, the conditions of its operation, participation by stakeholders and quite extensively the financing of the ESOs and stakeholder organisations, distinguishing between operating grants and action grants. All these rules are further specified in the so-called ‘Vademecum’, meant to explain and concretise the various procedural steps to the benefit of the ESOs and stakeholder organisations.

b) Formalisation of Governance Structure

All those participating in the process – the European Commission, the members of the Committee on Standards, the members of the committee established under EU legislation, the ESOs, and the Annex III organisations – are building a kind of ecosystem on standardisation. From a sociological perspective, the result is an epistemic community⁷⁵ which develops its own communication patterns and informal mechanisms that are hard to grasp by simply studying Regulation 1025/2012, the explanations provided by the European Commission in the Vademecum, or the bulk of ESO bylaws.

aa) Institutional Requirements

The most important *institutional* change is recognition of the ESOs as the major co-operation partners in the development of harmonised standards. These are the Annex I organisations. They are mentioned already in the recitals and then listed: CEN, CENELEC and ETSI. This is an astonishing regulatory technique. Whilst the three benefit from long-standing co-operation with the European Commission, it is nevertheless striking that legislation does not define criteria to be met but lists them and names them. The three enjoy a kind of monopoly as the EU legislator decided to tie the hands of the European Commission. Other standardisation institutions, such as IEEE, which have played a significant role in developing standards ever since the industrial age, are thereby excluded. The list is exhaustive.

The Regulation is less clear with regard to stakeholder organisations. Here nobody is named but criteria are laid down which have to be met by those who would like to benefit from legal status. Article 5 together with the relevant passages of Annex III deserves to be quoted in full:

Article 5

Stakeholder participation in European standardisation

1. European standardisation organisations shall encourage and facilitate an appropriate representation and effective participation of all relevant stakeholders, including SMEs, consumer organisations and environmental and social stakeholders in their standardisation activities. They shall in particular encourage and facilitate such representation and participation through the

⁷⁵ J Klabbers, On Epistemic Universalism and the Melancholy of International Law, *European Journal of International Law*, Vol 29, Issue 4, November 2018, 1057–1069, <https://doi.org/10.1093/ejil/chy073>; F Cardenas, J d’Aspremont, Epistemic Communities in International Adjudication, *Oxford Public International Law* <https://opil.ouplaw.com/display/10.1093/law-mpeipro/e2425.013.2425/law-mpeipro-e2425>

European stakeholder organisations receiving Union financing in accordance with this Regulation at the policy development level and at the following stages of the development of European standards or European standardisation deliverables: (a) the proposal and acceptance of new work items; (b) the technical discussion on proposals; (c) the submission of comments on drafts; (d) the revision of existing European standards or European standardisation deliverables; (e) the dissemination of information of, and awareness-building about, adopted European standards or European standardisation deliverables.

2. In addition to the collaboration with market surveillance authorities in the Member States, research facilities of the Commission and the European stakeholder organisations receiving Union financing in accordance with this Regulation, European standardisation organisations shall encourage and facilitate appropriate representation, at technical level, of undertakings, research centres, universities and other legal entities, in standardisation activities concerning an emerging area with significant policy or technical innovation implications, if the legal entities concerned participated in a project that is related to that area and that is funded by the Union under a multiannual framework programme for activities in the area of research, innovation and technological development, adopted pursuant to Article 182 TFEU.

Annex III then specifies the requirements which an organisation representing consumers has to fulfil in the context of Regulation 1025/2012:

2. A European organisation representing consumers in European standardisation activities which: (a) is non-governmental, non-profit-making, and independent of industry, commercial and business or other conflicting interests; (b) has as its statutory objectives and activities to represent consumer interests in the standardisation process at European level; (c) has been mandated by national non-profit consumer organisations in at least two thirds of the Member States, to represent the interests of consumers in the standardisation process at European level.

Regulation 1025/2012 is legally binding and directly applicable. Article 5 speaks of ‘shall encourage and facilitate’ – this is not yet an obligation. There is no ‘must’. However, there is a stick behind the door – the ESOs have an interest in developing harmonised standards, not so much because of potential co-financing⁷⁶ but because of getting access to the market. The European Commission will tie any mandate to appropriate involvement by stakeholder organisations – these are the ones that comply with the criteria and which as a consequence may request financial support from the European Commission. Therefore Article 5 Regulation 1025/2012 interferes in the self-regulatory autonomy of the ESOs. They have no true choice. They have to adjust their bylaws to the satisfaction of the European Commission and meet the criteria of Article 5 (1) a) to e). These criteria are sufficiently vague so as to leave discretionary power to the European Commission to tighten the grip, if it is politically advantageous to do so. The legislative history informs of a conflict between the European Commission and the European Parliament on voting rights of stakeholders, including a right to veto. The EP rejected voting rights.⁷⁷ The compromise is still found in Recital 23:

⁷⁶ Interview with representative of the European Commission. They co-operate because they want access to the market. The elaboration of a standards is said to come up to 1 Mio € on average.

⁷⁷ Amendment n°54 on Article 5 – paragraph 1a new proposal regulation 1025, see more on the EP’s proposed amendments(6.10.2010 – (2010/2051(INI))): https://www.europarl.europa.eu/doceo/document/A-7-2012-0069_FR.html?redirect and more on the EP’s reports on the draft proposal of regulation 1025: [https://www.europarl.europa.eu/RegData/commissions/inta/avis/2012/478355/INTA_AD\(2012\)478355_EN.pdf](https://www.europarl.europa.eu/RegData/commissions/inta/avis/2012/478355/INTA_AD(2012)478355_EN.pdf) [https://www.europarl.europa.eu/RegData/commissions/itre/avis/2012/476047/ITRE_AD\(2012\)476047_EN.pdf](https://www.europarl.europa.eu/RegData/commissions/itre/avis/2012/476047/ITRE_AD(2012)476047_EN.pdf)

The obligation of the European standardisation organisations to encourage and facilitate representation and effective participation of all relevant stakeholders does not entail any voting rights for these stakeholders unless such voting rights are prescribed by the internal rules of procedure of the European standardisation organisations.

The prominent position of the European Commission is equally present in its relationship to the stakeholder organisations. In contrast to Annex I, the Annex III organisations are not enumerated in the Regulation. Annex III ties this selection to the criteria that have to be met and which are subject to possible amendments through an implementing act by the European Commission. It is for the European Commission to decide which organisation meets the criteria set out in Annex III. The criteria are far-reaching and they even interfere in the relationship between the European stakeholder and the national consumer organisations. Candidates need to be mandated by two-thirds of ‘non-profit consumer organisations in the Member States’. One might draw a parallel here to EU Directive 1828/2018 on Representative Action under which ‘qualified entities’ have to register so as to take action for an injunction or for collective redress. In theory, Article 5 Regulation 1025/2012 leaves space for a new body representing the interests of consumers in standardisation, in practice seen through consumer lenses. Annex III legitimated ANEC as the appropriate stakeholder organisation. This was possible because ANEC was occupying the space when Regulation 1025/2012 was adopted, and its experience and knowledge have allowed it to continue to be the organisation recognised. However, ANEC does not have a monopoly like that enjoyed by the ESOs. Annex III was not shaped to suit ANEC or the other Annex III organisations.

Participation is bound to those stakeholder organisations which receive financing. This lies in the hands of the European Commission. Annex III organisations, including ANEC, have to apply for financial support and the EC is empowered to implement the Annex III (2) requirements. Others can – and do – apply through a public call for a new Framework Partnership Agreement. The original draft of the European Commission provided for rules on financing Annex III organisations for ‘*the verification of the quality, and conformity to the corresponding policies and legislation of the Union, of European standards and European standardisation deliverables.*’ Due to pressure by the European Parliament, the sentence was deleted.⁷⁸

The ESOs had to adapt their bylaws. The relevant rules of CEN and CENELEC can be found in Guide 25⁷⁹ and in the Internal Regulations Part 1 and 2.⁸⁰ The bylaws reiterate the rationale of Article 5 Regulation 1025/2012 in combination with Annex III. Consumer organisations have to apply to be granted the status of a partner organisation. In order to submit a request, consumer organisations have to provide evidence as to the criteria which are spelt out in Guide 25 under 1.3.⁸¹ The General Assembly of CEN or CENELEC has to rule on the application. Merely meeting

⁷⁸ <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52011PC0315>, Amendment 83 on the deletion of Article 12 paragraph 1 – point of proposal for regulation 1025.

⁷⁹ <https://www.cenelec.eu/media/Guides/CEN-CLC/cenclguide25.pdf>

⁸⁰ <https://boss.cen.eu/reference-material/refdocs/pages/>

⁸¹ An organisation wishing to become a Partner Organisation of CEN and/or CENELEC is: a) an independent European or international European based sectoral organisation representing, within its defined area of competence, a sector or subsector. In the case of CENELEC, the Partner Organisation is expected to represent a sector or subsector in the electro-technical field; or b) a recognised European pan-sectoral organisation promoting, within its defined area of competence, the interest of a defined category of stakeholders, such as SMEs, or societal interests, such as consumers, social or environmental stakeholders. In addition, the organisation: — is able to represent a very significant part of the European interest groups related to its defined area of competence across the geographical scope of CEN and CENELEC; — is willing and able to provide on an active basis relevant inputs to the work of one

the criteria does not convey a right of partnership according to the bylaws. Nevertheless, whether the bylaws could be interpreted as a right to become a partner organisation, provided the conditions are fulfilled, would have to be decided under the Belgian Law of Associations. Once accepted as a partner organisation, the stakeholder organisation has to pay a fee. Guide 25 spells out the rights and the obligations of partner organisations, thereby distinguishing between participation at the corporate level (general assembly, presidential committee, other working groups, and advisory boards) and at the technical level. Partner organisations have the right to access the corporate and the technical level as observers. Whilst the bylaws are clear with regard to participation in the General Assembly, access to all other bodies, whether corporate or technical, is subject to limitations. The partner organisations ‘can’ participate in ‘other working groups or advisory boards’, ‘where such participation is envisaged in the relevant Group’s Terms of Reference or on the Chair’s invitation’ (1.2.1.). Special rules are foreseen on the access to technical boards:

The Partner Organisation may request observership at any time in specific CEN and/or CENELEC Technical bodies. Such requests are decided upon by the CEN and/or CENELEC Technical Boards in line with the CEN-CENELEC Internal Regulations Part 2 upon advice of the concerned Technical bodies or groups when appropriate (1.2.2.). However, in a footnote to exactly this sentence, the Guide clarifies ‘that the organisations listed in Annex III of (EU) Regulation 1025/2012 that have entered into partnership with CEN-CENELEC, are entitled to participate in any Technical Committee and its relevant working groups and this without any restriction.

Access is bound to respect a whole series of ‘obligations’ on non-disclosure and on respect for copyright (1.3) and can be withdrawn ‘when it clearly emerges that the partner organisation is not actively contributing to the corresponding work’ (1.2.) or – one has to add – if the partner organisation does not respect the non-disclosure and copyright rules. The threat is a powerful instrument to tie the hands of stakeholder organisations. Even setting aside the sensitive issue of confidentiality and copyright, it is hard to find in the dense net of CEN-CENELEC bylaws a spirit of ‘partnership’, as the power lies in the hands of CEN-CENELEC whereas the stakeholder organisations are grantees, not holders of rights. The rules exercise pressure on ANEC to be ‘friendly critics’ of CEN-CENELEC and also to ETSI. In theory a ‘bad partnership’ could be sanctioned, as the European Commission controls access. The institutional dimension is designed to integrate a politically imposed necessary burden rather than as an opportunity to give standardisation a direction, which in turn takes seriously the societal dimension of an increasingly politicised technology. Contrasting Article 5 (1) Regulation 1025/2012 with the bylaws of CEN-CENELEC raises doubts as to whether the bylaws are in compliance with EU law. The bylaws are stricter with regard to the status of a partner organisation and stricter with regard to access to technical boards.

or more CEN and/or CENELEC technical bodies in the development of standards or other technical deliverables; — is willing and able to actively contribute, as appropriate, with inputs and proposals in dialogue with CEN and/or CENELEC corporate bodies and their working or advisory groups; — is open to membership of appropriately qualified national organisations in the countries from the Members of CEN and CENELEC; — has a legitimate interest in European standardisation in general, or with regard to the sector/subsector of its activity; — does not perform any activity that is regarded as in conflict or in competition with the CEN and CENELEC activities; — can effectively and representatively support CEN and CENELEC objectives through the contribution of its own members and their internal organisations, including at the national level.

bb) Procedural Requirements

Articles 10 and 11 Regulation 1025/2012 lay down the *procedural* requirements for a request for harmonised standards, on their publication in the Official Journal, and on the conditions under which and by whom the harmonised standard can be rejected.

In the *ex-ante* procedure, formulation of a standardisation request (SReq), the Committee on Standards gives an opinion under the examination procedure (Article 22 (1), with the Committee established under Regulation 182/2011 (Article 22 (3)). If the Committee delivers a positive opinion by qualified majority voting, the Commission adopts the implementing act and notifies it to the ESOs. Thus, the Commission has the obligation *ex ante* to formulate the request as precisely as possible to provide a strict framework within which ESOs have to act. ESOs should only focus on defining the technical means through which the policy goals set by the legislator can be achieved. The ESOs and Annex III organisations are involved in consultation, Article 10 (2). Where a harmonised standard satisfies the requirements which it aims to cover and which are set out in the respective EU legislation, the European Commission will publish the harmonised standard in the Official Journal, Article 10 (6).

In the *ex-post* procedure, once the standards are published in the Official Journal, the Committee takes a decision by qualified majority of the Member States. The Commission is obligated to follow that opinion, Articles 11, 22, Regulation 1025/2012, referring to Articles 4 and 5 of Regulation 182/2011 (comitology). ESOs and Annex III organisations are not empowered to initiate the objection procedure. The European Commission has established a website which carries information on objections and makes the reasoned opinions of the Member States or the European Parliament available to the public.⁸² The benchmark for objections is rather high. Complainants have to provide clear-cut evidence, not only via arguments but also via facts to underpin potential shortcomings.⁸³

Further details of the standardisation request, on the role and use of harmonised standards in harmonisation legislation for products (the so-called 'Blue Guide') and on methods of referencing standards in European legislation can be found in the '*Vademecum for European standardisation*'.⁸⁴ The *Vademecum* provides deep insights into the various stages of the standardisation request, of the conformity assessment procedure and on publication, as well as on the role associated with the different actors during the overall process. However, when it comes to specifying the role and function of Annex III organisations, the *Vademecum* remains rather vague. Part I reiterates what is written in the recitals of the Regulation and in Article 5.⁸⁵ Part II is slightly more helpful. The European Commission should compensate for missing voting rights by listening to weaker parties – those of the Annex III organisations.⁸⁶ Part III Guidelines for the execution of a standardisation request are addressed to the ESOs only but does not even mention Annex III organisations.⁸⁷ The *Vademecum* dates back to 2015 and reflects

82 https://single-market-economy.ec.europa.eu/single-market/european-standards/notification-system_en#formal-objections-to-harmonised-standards

83 See, e.g., Paris, le 26 septembre 2022 La Note Des Autorités Françaises Objet : Objection formelle contre la norme harmonisée EN 15997 :2011/AC : 2012 relative aux véhicules tout terrain (ATV – Quads)

84 https://single-market-economy.ec.europa.eu/single-market/european-standards/vademecum-european-standardisation_en

85 <https://ec.europa.eu/docsroom/documents/13507/attachments/1/translations> Part 1 under 4.6.

86 <https://ec.europa.eu/docsroom/documents/13508/attachments/1/translations> Part 2 under 2.5.3.

87 <https://ec.europa.eu/docsroom/documents/13509/attachments/1/translations>.

neither adjustments made by the European Commission after the *James Elliott*⁸⁸ judgment nor the call for more inclusiveness in the New Standardisation Strategy of February 2022. That is why the Vademecum needs to be read in conjunction with the Communications of the European Commission from 2018 and 2022. However, before we embark on an analysis of *James Elliott*, it is necessary to look deeper into the bylaws and to connect them to the procedural requirements which concretise the position of Annex III stakeholders in the elaboration of a technical standard within the ESOs.

The criteria in Article 5 (1) are more interesting in what they do not require. Annex III organisations do not enjoy voting rights, at least not in CEN-CENELEC. In ETSI they are members with voting rights. In light of the overall spirit, it is not surprising that Guide 25 reiterates that Annex III organisations have no voting rights. They are partner organisations and observers, with a right to access documents. Annex III organisations are in charge of finding out which of the possible projects under way are of consumer relevance. They are not automatically informed on all ongoing projects, although this would be technically easy to manage. The voting itself is weighted. A proposed standard developed in a CEN TC will be adopted if:

1) 55.00 % or more of the votes cast (abstentions not counted) are in favour, and 2) if the population of the countries of the Members having voted positively reaches 65.00% or more of the population of the countries of all Members having voted (abstentions not counted).

A proposed standard developed in a CENELEC TC will be adopted if:

*1) if a simple majority of the votes cast (abstentions not counted) is in favour, and 2) if 71.00 % or more of the weighted votes cast (abstentions not counted) are in favour.*⁸⁹

CEN-CENELEC gives voting rights to countries that are not members of the EU but does not give voting rights to an organisation that represents over 450 million European consumers. If one gives voting rights to ANEC, European business organisations might want the same, and then the national delegation principle starts to fail. This has to be kept in mind when it comes to a possible revision.

The most powerful instrument of stakeholder organisations seems to be able to intervene during the elaboration stage through comments or opinions. In practice this seems to work pretty well, as 75% of ANEC opinions on draft standards are 'favourable'.⁹⁰ It has to be recalled though that Annex III organisations are observers only and that they cannot lead a technical body. CEN-CENELEC interpret the existing rules to allow an Annex III organisation to be the Chair of a Technical Committee (but not the Secretariat), and to hold a WG convenorship. The agenda is set by the ESOs within the respective technical body. Annex III organisations are entitled:

*to submit comments on draft European Standards submitted to formal approval (vote) or submit an "Opinion" on draft European Standards undergoing public enquiry or submitted for formal approval (vote)."*⁹¹

⁸⁸ See under II 2 c).

⁸⁹ Internal Regulations under 3.4.

⁹⁰ Information provided by ANEC.

⁹¹ CEN-CENELEC Guide 25 Clause 1.2.2

The second major ‘right’ – provided the first can be construed as a right – is to lodge an appeal⁹² against a decision considered not to be in accordance with the CEN Statutes or the Internal Regulations. In theory this would be a powerful tool in the hands of Annex III organisations, a kind of last-resort control, even if they have missed participation in elaborating a standard. However, it is exactly this that is not possible. The right to lodge an appeal is severely restricted:⁹³ (is) *limited to matters associated with work carried out by CEN and/or CENELEC Technical Bodies to which the Partner Organisation has contributed.*

cc) Stakeholder Participation

The following chart sums up the major findings as far as they appear on paper. In reality there is an ongoing exchange between the European Commission and the ESOs not only where it is explicitly foreseen but also in terms of a call for a proposal on the basis of an approved working programme.⁹⁴ The so-called SMARRT (the Standards Market Relevance Roundtable) was created to allow a ‘structured dialogue’ between the Commission, industry, and stakeholders – not only but also ahead of meetings of the Committee on Standards. SMARRT was set up because Regulation 1025 overlooked the business interest and its voice in the Committee on Standards. Business made a proposal to create a representative platform which would be allowed to send a representative to the CoS, alongside the Annex III representatives. That was thrown out by Member States. In the end, the SMARRT suits the multitude of business interests far more as it allows a bilateral (and private) forum with the EC before every CoS meeting. Indeed, this arrangement certainly seems to suit the business associations.⁹⁵ Such informal exchanges make perfect sense in light of the co-operative spirit. Neither stakeholder organisations nor the ESOs are involved in the exchange and they are not allowed to attend. The relationship between the European Commission and the stakeholder organisations is not limited to formalised positions or to participation in open fora. In practice, the European Commission operates as a kind of mediator between the ESOs and the stakeholders, if the stakeholders do not manage to penetrate one of the ESOs with their concerns, politically as much as technically.⁹⁶

⁹² Internal Regulations Part 1 under 6.1.

⁹³ Guide 25 under 1.2.1.

⁹⁴ Interview with representative from the European Commission.

⁹⁵ Documented in a leaflet ‘The Joint Initiative on Standardisation’

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjPg2DE3NTAhX4gv0HHZ6GBjMQFnoECAsQAw&url=https%3A%2F%2Fec.europa.eu%2Fdocsroom%2Fdocuments%2F35781%2Fattachments%2F1%2Ftranslations%2Fen%2Frenditions%2Fnative&usq=AOvVaw2YrJKUZZl2Y2fO_6TAw-o4&opi=89978449

⁹⁶ Interview with representatives from the European Commission and the stakeholder organisations.

| | Legal Basis | Participation | Decision |
|-------------------------|--|--|---|
| Working Programme | Art 8 (4) Reg 1025/2012 | Art 8 (4) Reg 1025/2012 ESOs and stakeholders Stakeholders are invited to committee meetings but have to leave the room when it comes to a vote ⁹⁷ | Art 8 (4) with Art 22 Reg 1025/2012 Committee Procedure (unspecified) |
| Call for Proposals | Art 17 Reg 1025/2012 Distinguishing between institutional and action grants | | |
| Standardisation Request | Art 10 (2) Reg 1025/2012 | Art 10 (2) Reg 1025/2012 ESOs and Stakeholders Corresponding committees or sectoral experts Stakeholders are invited to committee meetings but have to leave the room when it comes to a vote ⁹⁸ | Art 10 (3) with Art 22 (3) Examination procedure |
| Compliance | Art 10 (5) Reg 1025/2012 | Art 10 (5) Reg 1025/2012 Commission together with ESOs to assess compliance No stakeholder participation | |
| Publication | Art 10 (6) Reg 1025/2012 | Art 10 (6) Reg 1025/2012 In case of compliance Commission publishes in OJ | Since James Elliott implementing decision |
| Objection Procedure | Art 11 Reg 1025/2012 | Art 11 (1) Reg 1025/2012 Member States and European Parliament No right to objection for ESOs and stakeholders | Art 12 (4) and (5) together with Art 22 (2) or (3) depending on the objective of the decision |

c) Governance Structure after *James Elliott*

The *James Elliott* judgment of the CJEU,⁹⁹ decided on 26 October 2016, shattered the standardisation community: legally speaking, the firm belief in business circles that harmonised technical standards are ‘sacred’ and free from the risk of being submitted to judicial control; conceptually speaking, the procedural requirements of the governance structure, the inner mechanics of the distribution of work and responsibilities between the ESOs and the European Commission. It will have to be shown, though that, in implementing the judgment, the European Commission used the required changes in the procedure to adapt the institutional requirements of the current governance structure.

aa) Part of EU Law

The CJEU held that harmonised standards come under its jurisdiction. In a series of further and pending judgments, the CJEU will have to clarify the exact scope of its jurisdiction as they form ‘part of EU law.’¹⁰⁰ *James Elliott* triggered fierce debates in legal scholarship as well as a change

⁹⁷ Information from ANEC.

⁹⁸ Information from ANEC

⁹⁹ C-613/14 – *James Elliott Construction*, ECLI:EU:C:2016:63.

¹⁰⁰ At 40 ‘It follows from the above that a harmonised standard such as that at issue in the main proceedings, adopted on the basis of Directive 89/106 and the references to which have been published in the Official Journal of the European Union, forms part of EU law, since it is by reference to the provisions of such a standard that it is established whether or not the presumption laid down in Article 4(2) of Directive 89/106 applies to a given product.’

in the way in which the European Commission handles the process that leads from the standardisation request up to the publication of harmonised European standards. Interestingly, the change is not immediately recognisable on the Commission website, or in the Vademecum or in the Blue Guide. Part 1 of the Vademecum – the guidelines for a standardisation request – date back to 2015. They present the state of the law prior to *James Elliott*. The Blue Guide was updated in 2022, but nevertheless contains only sibylline language which in no way addresses the implication of harmonised standards being ‘part of EU law’:¹⁰¹

Harmonised standards never replace legally binding essential requirements. A technical specification given in a harmonised standard is not an alternative to a relevant essential or other legal requirement but only a possible technical means to comply with it...

Publication of references is not an automatic action and the Commission must perform certain checks and assessments before publication takes place. The Commission may thus refuse to publish the references or, where appropriate, may set certain restrictions which are published together with the references....

The crucial document to understand the change in policy is a Communication from the European Commission to the Council, the European Parliament and ECOSOC of 22 November 2018.¹⁰² This document with the telling title ‘*Harmonised standards: Enhancing transparency and legal certainty for a fully functioning Single Market*’ addresses the practical consequences of *James Elliott*, *Global Garden*, and *Anstar*¹⁰³ for the elaboration of harmonised standards. It is worth contrasting the wording of Article 10 Regulation 1025/2012 with that in the Communication that ‘*Certain improvements to the practical implementation of this framework need to be made swiftly, notably in light of the case of law of the Court of Justice of the European Union*’:

Art. 10 (5) 2nd sentence Reg. 1025/2012: The Commission together with the European standardisation organisations (emphasis added HWM) shall assess the compliance of the documents drafted by the European standardisation organisations with its initial request.

Communication on Harmonised Standards 2018: Once the European Standardisation Organisations have developed a harmonised standard, the Commission assesses (emphasis added HWM) whether it complies with the requirements of corresponding Union legislation and the original standardisation request. If the Commission concludes (emphasis added HWM) that the standard is in compliance with the request and Union legislation, it will decide to publish its reference in the Official Journal of the European Union. As a result, and following a Commission decision to publish the reference in the Official Journal, the standard will produce legal effects under the relevant Union legislation.

The Commission changed the procedure, thereby interpreting the CJEU judgment as an obligation to set out its final responsibility.¹⁰⁴ Until November 2018, New Approach Consultants operated under the auspices of CEN and CENELEC. Their task was to accompany the elaboration process so as to make sure that harmonised standards comply with binding legal requirements in the secondary legislation concerned.

¹⁰¹ COMMISSION NOTICE, The ‘Blue Guide’ on the implementation of EU product rules 29.6.2022 OJ 2022/C 247/01, under 4.1.2.2. and 4.1.2.3. pages 50 and 52

¹⁰² COM 2018 764 final, 22.11.2018 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A764%3AFIN>

¹⁰³ GC *Global Garden* T-474/15 and CJEU *Anstar* C-630/16.

¹⁰⁴ Interview with representative from the European Commission.

bb) Redistribution of Responsibilities

The European Commission took over selection, management, and monitoring. The first step was to launch a tender in order to appoint consultants. A new category was born: the HAS consultant. The construction leads to an overlap between public and private law, in that the European Commission's responsibility derives from the interpretation of Regulation 1025/2012, whereas the relationship between the European Commission and the consultants is based on a contract. The tender launched by the European Commission was won by Ernst and Young (E&Y).¹⁰⁵ This does not necessarily mean that the consultants themselves are different. E&Y immediately established a website where all those who are interested – meaning also the former experts hired by CEN-CENELEC – could register.¹⁰⁶ The responsibility shifted from the ESOs to the European Commission. This is a change in the institutional design and precisely this change lies at the heart of the conflict among the ESOs, the industry standing behind the ESOs, and the European Commission.¹⁰⁷

The final decision under Article 10 (6) to publish a harmonised standard is taken by the College of Commissioners via an implementing act. From November 2018 onwards, references to harmonised standards are published in part L of the Official Journal as they are supposed to be regarded as 'law'.¹⁰⁸ The legal implications of this shift in the distribution of responsibilities are far from clear. There are two camps – the private law camp and the public law camp. The private law camp, defending the position of the industry, criticises the move as being unlawful as it does not do justice to the differences between Article 10 (5) and Article 10 (6) Regulation 1025/2012. In an opinion written by a well-known German law firm on behalf of the German Ministry of Economic Affairs and Energy, the authors argue that the compliance test is conclusively regulated in Article 10 (5) as a joint exercise to be undertaken by the ESOs and the European Commission, and that Article 10 (6) instead does not leave room for an additional test to be exercised by the European Commission alone.¹⁰⁹ The counter-position is taken in a legal opinion commissioned by ECOS (Environmental Coalition on Standards), executed by Eliantonio and Volpato.¹¹⁰ *James Elliott* is said to have triggered a radical change:

the standard-setting process and its outputs have today an undeniable public law relevance, which implies the need to abide by essential constitutional requirements and general principles of the Treaties, including general principles of administrative law.

ECOS represents environmental interests and is recognised as the respective stakeholder in Annex III (2) Regulation 1025/2012. It is equally funded by the European Commission and actively

¹⁰⁵ For details see COM (2022) 30 final under 2.7.1. the link referred to in fn. 29 on the HAS contract is no longer accessible though.

¹⁰⁶ Call for expression of interest for Harmonised Standards (HAS) Consultants, https://assets.ey.com/content/dam/ey-sites/ey-com/en_be/topics/advisory/ey-has-call-for-expression-of-interest.pdf

¹⁰⁷ ETSI Technical Report, Study into the challenges of developing harmonised standards in the context of future changes to the environment in which products are being developed and operated, 2022 with a detailed critique of the consequences.

¹⁰⁸ Explicitly mentioned in COM (2022) 30 final, at 10.

¹⁰⁹ Redeker/Sellner/Dahs, executed by K Dingemann, and M Kottmann, Legal Opinion On the European System of Harmonised Standards Commissioned by the German Federal Ministry for Economic Affairs and Energy (BMWi) August 2020, https://www.bmwk.de/Redaktion/EN/Downloads/L/legal-opinion-on-the-european-system-of-harmonised-standards.pdf?__blob=publicationFile&v=3

¹¹⁰ M Eliantonio and A Volpato, The European System of Harmonised Standards. Legal Opinion for ECOS (March 11, 2022). Available at SSRN: <https://ssrn.com/abstract=4055292> or <http://dx.doi.org/10.2139/ssrn.4055292>

contributes to the development of European harmonised standards.¹¹¹ So far, the CJEU has had no opportunity to clarify the shift and it seems that even industry is not seeking clarification, as no case has been initiated which would examine the lawfulness of the interpretation of the *James Elliott* judgment by the European Commission. The long-standing ties between the ESOs and the European Commission and their mutual dependence speak in favour of finding amicable solutions.

Nevertheless, the story is not yet over and the two parties to the conflict may be waiting for a political solution, perhaps in the form of a revision of Regulation 1025/2012. It is indeed strange that the European Commission did not take the opportunity of the 2022 revision of Regulation 1025/2012 to clarify things in the aftermath of the *Elliott* judgment. The 2018 Communication de facto complements the *Vademecum*.¹¹² Given the degree of detail which governs the guidelines on a standardisation request and its execution, one would have expected that the European Commission would provide for a more sophisticated explanation of the procedure in a commonly accessible document. This is particularly true with regard to the exact role of the HAS consultants in the procedure, from what stage on they are involved and what exactly they are doing. The European Commission does not disclose their names, not even to the standardisation organisations.¹¹³ My efforts to interview a HAS consultant failed: emails were simply not responded to. It seems, however, that the HAS consultants operate as ‘crit-sit-handling’ to mediate critical situations and as ‘crit-sit managers’ throughout the overall process.¹¹⁴ Since even the Blue Guide adopted in 2022 does not take a clear position on what the procedure will look like, it seems as if the conflict is postponed and that all interested parties have concluded a de facto stand-still agreement, despite all the loose ends.¹¹⁵

d) European (harmonised) standards between national and international standards

The focus on the European level, on European regulation, on the ESOs, the European Commission and the Annex III stakeholder organisations – in short on European harmonised standards – presents an incomplete if not distorted picture. European standardisation is sandwiched between national and international standardisation. That is why it is indispensable to analyse the interaction between European harmonised standardisation and national standardisation (AFNOR, BSI, DIN, etc) as well between European harmonised standards and international standardisation (ISO, IEC, IEEE).

¹¹¹ Details on the role of ECOS can be found in the E&Y Study on implementation of Regulation (EU) No. 1025/2012 (Article 24) <https://doi.org/10.2873/504681> and <https://doi.org/10.2873/593923>

¹¹² COM (2018) 764 final, at 6.

¹¹³ Interview with experts from standardisation organisations.

¹¹⁴ Interview with a former representative of an internationally operating company, having been and still being involved in a number of technical standard committees.

¹¹⁵ ETSI Technical Report, Study into the challenges of developing harmonised standards in the context of future changes to the environment in which products are being developed and operated, 2022 with a detailed critique of the consequences, preview <https://cdn.standards.iteh.ai/samples/63987/c543c6b3133648629b7b7f1c50c84070/ETSI-TR-103-880-V1-1-1-2022-11-.pdf>

aa) European and national standard bodies

The principle of national delegation lies at the core of the European (ESOs) and the International standardisation system (ISO/IEC but not IEEE). With the financial support of the European Commission and EFTA, CENELEC has set up a website, giving the following explanation on the three constitutive elements:¹¹⁶

National delegation: 'International and European standards are developed according to the National Delegation Principle: each national standardisation body sends a delegation of experts to represent the national standpoint.

Mirror Committees: The national standpoints are drawn up in national committees that "mirror" the Technical Committees at European or international level. Stakeholder Organisation:

*Stakeholders" in standardisation include manufacturers and services providers, consumers, trade unions, researchers and scientists, academia, businesses, public administrations, testing bodies and laboratories, associations, NGOs, etc. Companies and organisations nominate their experts to participate in the relevant technical bodies of standardisation organisations. **All stakeholders can take part in standardisation work** (bold letters on the website).*

However, it is much more difficult to find out how the national delegation principle works in practice; how the mirror committees are designed, and how the input of stakeholders at the different levels is organised. The Internal Regulations of CEN-CENELEC do not illuminate a rather opaque picture. Part II states that each member of CEN-CENELEC (meaning each national standardisation organisation) is entitled to send to the technical body (TB) a national delegation composed of between one and up to three representatives of national interest in order to negotiate a standard.¹¹⁷ Seen this way, ESOs are platforms where meetings are organised, where information is shared, where different national viewpoints are co-ordinated, and where the final voting procedure takes place.

The members of the ESOs (that is, national standardisation organisations) are responsible for the development of European standards. So it is necessary to look into the statutes that govern the national standardisation organisations, which are not homogenous. It suffices to compare the statutes of AFNOR and DIN to understand the difference, in particular in the way the responsibilities between private and the public actors are distributed. Regulation 1025/2012 does not take sides on whether technical standardisation should be in the hands of private or public bodies. Article 7 explicitly encourages the involvement of public bodies in national standardisation organisations. EU law has no grip on the way in which national standardisation is organised, private or public, let alone whether or not stakeholder organisations have a say. However, Regulation 1025/2012 also deals with participation at the national level. Recital 2 sets the tone: *National standardisation organisations should also encourage and facilitate the participation of stakeholders*. The Regulation shies away from putting national standardisation organisations and ESOs on an equal footing with regard to participation by consumers, workers, and non-governmental organisations. Astonishingly enough, SMEs are directly targeted in Article 6. EU law imposes a whole series of obligations on national standardisation organisations in order to increase the input from SMEs in the development of technical standards.

¹¹⁶ <https://www.standardspluselearning.eu/b-1-3-national-delegation-principle>

¹¹⁷ Under 2.3. together with 3.2.2.

DIN was established in 1917 by the German Government, German industry, and the association of German engineers to increase production by the military industry. Today's relationship between DIN and the German Government is laid down in a contract, concluded in 1975.¹¹⁸ This contract served as a blueprint for the Memorandum of Understanding concluded between the European Commission and CEN-CENELEC in 1984 and is governed by the same spirit – public subsidies against political influence through the possibility to mandate standards and through stakeholder participation. Details of consumer participation are laid down in the statutes of the DIN president.¹¹⁹ In principle, the DIN Consumer Council has no special rights. DIN 820 (the equivalent to the CEN-CENELEC Internal Regulations) applies, as it does with regard to every other participant in standardisation. However, procedural instruments are mentioned in the presidential decision and these deserve to be highlighted.

If public interest objectives of occupational health and safety, environmental protection, health or consumer protection and protection of the environment are concerned, if health or consumer protection and building safety are affected, then the Consumer Council can introduce a so-called closed vote. No decision can be taken against the Consumer Council in the national committee: the national committee must abstain. The closed vote procedure only plays a role in European or international standardisation projects (where there are short voting periods). If a DIN mirror committee discusses the position of a European or international draft standard and if important objections raised by the DIN's Consumer Council (for instance, safety concerns against the European draft) are not taken into account by the mirror committee, then the DIN Consumer Council may invoke a closed vote and the German mirror committee would have to abstain from voting at the European level. However, the mechanisms do not prevent adoption of a European standard. If the criteria for adoption of a standard are fulfilled, that is, enough CEN-CENELEC members vote positively, the EN must then be adopted in the national body of standards. So far, this presidential decision has only been used very rarely. It is also linked to further conditions. Just like under Guide 25, the DIN Consumer Council can only invoke the procedure if it had collaborated beforehand, submitted corresponding comments/objections, and made efforts to find a consensus. If this is impossible, DIN 820 foresees an in-house dispute settlement mechanism.¹²⁰ The DIN rules do not require that the German delegation speak with one voice. Possible dissent can therefore be laid bare by communicating the disagreement. In practice, this could mean abstention until a consensus has been found. Theoretically it would be possible to reach agreement on disagreement and to lay bare that there are two different positions. Whether and to what extent this possibility has been used in practice is open to further investigation.¹²¹

In France, the foundations were laid down after World War I, in 1926.¹²² In contrast to Germany, standardisation had been integrated into the administration and understood as a statutory

¹¹⁸ J Falke, in Joerges et al (n 58), under 3.4.2. Normenvertrag and under 3.4.5. on the DIN Verbraucherrat, more comprehensively same author, J Falke, *Rechtliche Aspekte der Normung in den Mitgliedstaaten und der EFTA*, Band 3 Deutschland, 2000.

¹¹⁹ Presidential Decision of 1974, on file with the author.

¹²⁰ DIN 820-4 Abschnitt 5.

¹²¹ Something similar is said to exist in BSI but, when its 'consumer council' tried to force a vote of abstention on an EN for mini-motorbikes, the Chair of the BSI mirror committee threatened such retaliation that the 'consumer council' backed down. Information provided by ANEC.

¹²² H-W Micklitz, in Joerges et al. (n 58) at 61 and 84, comprehensively, J Champigneulle Mihailov, *Les aspects juridiques de la normalisation en droit français*, in J Falke and H Schepel, *Legal Aspects of Standardisation in the Member States of the EC and EFTA Volume 2 Country Reports*, 2000, 231–321.

task. The ultimate responsibility of the French state has not changed over time despite various ministerial amendments. However, within that frame a gradual strengthening of redistribution of competences took place, away from the state to industry. In 1984 the French Government opened up the management level for stakeholder organisations, mainly trade unions and consumers. The idea was to legitimate the partial retreat of the state through stronger involvement by civil society organisations. The current organisational design results from 2009.¹²³ The message enshrined in Article 5 is crystal clear:

The French Association for Standardisation guides and coordinates (emphasis added HM) the development of national standards and participation in the development of European and international standards¹²⁴

The Consumption Committee (COSAC) has to advise the AFNOR Board of Directors. The Committee is made up of national consumer associations, representatives of the Ministry of Industry, the DGCCRF, the National Consumer Institute (INC), the testing network represented by the National Laboratory for Metrology and Testing (LNE), and professional sectors. It has to gather the demands and needs of consumers, define priorities, contribute to the development and monitoring of standardisation programmes, and represent consumers in French, European, and international standardisation organisations (IOSCO).¹²⁵ COSAC is only occasionally involved in elaborating concrete standards.

Comparing DIN Verbraucherrat (Consumer Council) and AFNOR COSAC discloses the well-known though rarely openly addressed problem of the unbalanced input by stakeholder organisations at the national standardisation level. Among Member States, for example, in Germany the DIN Verbraucherrat is a well-established and solidly financed body which may exercise its influence at the European level, too. The German Consumer Council might in theory speak on behalf of all European consumers looking beyond the specific interest of German consumers, or the very same German Consumer Council might join forces with German industry so as to push German interests through at the European level against the interests of consumers in other Member States.¹²⁶ The uneven spread of input in technical bodies at the national level affects co-ordination at the European level and quite unavoidably leads to frictions. The European technical body is composed of national representatives. These may be representatives from industry or – as in the case of Germany – two representatives, one from industry, and one from the DIN Consumer Council. Such a tandem might put pressure on representatives from other Member States. The ‘over-representation’ of one Member State, whichever it is, might bring about a difficult situation at ANEC, whose task is to develop a collective position on behalf of all European consumers. What happens if there is disagreement between the national consumer representatives and the European ones? The answer could only be found in deeper empirical research. Essentially, ANEC brings together national experts to set a common position which is communicated directly to the ESOs and shared with ANEC members.¹²⁷ However, one might wonder whether the solution is not more research but a redesign of the governance structure so as to guarantee that all Member States have at least

¹²³ Décret no 2009–697 du 16 juin 2009 relatif à la normalisation.

¹²⁴ Art 5 L’Association française de normalisation oriente et coordonne l’élaboration des normes nationales et la participation à l’élaboration des normes européennes et internationales.

¹²⁵ <https://www.inc-conso.fr/content/association-francaise-de-normalisation-afnor>

¹²⁶ It is hard to find evidence; one of the interviewees criticised the German CC for defending the interests of German industry much more than those of European consumers.

¹²⁷ Information from ANEC.

comparable participation by stakeholder organisations at the national level. Such a common structure seems to be the condition for co-ordinating input at the European level bottom-up, at least as long as the national delegation principle forms the core of the European standardisation policy.

bb) European and International Standards

Integrating the international dimension of standardisation highlights difficulties brought about in establishing the European Economic Community in 1957, and CEN in 1961, CENELEC in 1973, and ETSI in 1988. Under the leadership of the United States, institutions were built which even today form the core of international economic law: on the one hand, GATT, the IMF; on the other, the United Nations with all its specialised sub-units and last but not least ISO¹²⁸ – IEC existed already. The EU as a political entity and CEN-CENELEC had to find their places in a field which was either dominated by national rules and/or by international rules. What should be the place for the EU, CEN-CENELEC and later on ETSI?

Development and promotion of European standards governing the Common Market and later the Internal Market was already complicated enough. Creation and invention of European harmonised standards simply added a new layer. The ever-stronger intermingling – among EU legislation; the European Commission as the executive branch; the Member States; national and European standardisation organisations, and last but not least the involvement of stakeholder organisations – is unique and produces frictions not only with GATT/WTO but also with ISO/IEC. The weakening of GATT/WTO due to the partial retreat of the United States which is blocking further juridification of the international economic order and the strong rise of bilateral trade agreements are – strangely enough – accommodating the intentions of the EU to become a key actor in standardisation. Thereby the frictions were shifted from GATT/WTO to ISO/IEC in particular. ISO/IEC has long been one of those international organisations which are hugely important but are never in the limelight. This has changed, mainly due to the role China is playing within ISO/IEC.¹²⁹

Today, the European institutions are at first sight fully integrated into international economic law. The EU, together with the Member States, is a member of the WTO. ISO is built around ‘one country, one member’. That is why the EU cannot be a member, but the European Commission (and more recently the European Parliament) belongs to a long list of institutions with whom ISO is co-operating.¹³⁰ CEN and CENELEC built close ties with ISO through the 1991 Vienna Agreement¹³¹ and with IEC through the 1991 Lugano Agreement (the latter becoming the Dresden Agreement in 1996, and the Frankfurt Agreement in 2016). The European legislature is interweaving the different levels of standardisation in the New Approach type of legislation. The standard formula is the following:

¹²⁸ On the ISO more generally C Murphy and J Yates, *The International Organisation for Standardisation (ISO): Global Governance through voluntary consensus*, (Routledge 2009).

¹²⁹ M Cantero Gamito, *From private regulation to power politics: the rise of China in AI private governance through standardization*, manuscript 2022 on file with the author.

¹³⁰ The European Commission as 185 A-to-C types of co-operation <https://www.iso.org/organisations-in-cooperation-with-iso.html?f=E>, as to the difference between the three https://www.iso.org/sites/directives/current/part1/index.html#_idTextAnchor083

¹³¹ https://boss.cen.eu/media/CEN/ref/vienna_agreement.pdf

Wherever appropriate priority is given to cooperation with ISO provided that international standards meet European legislative and market requirements and that non-European global players implement these standards.

This is an important proviso as it indicates that the EU reserves the right and the authority to examine whether ISO/IEC standards meet European legal requirements – what might be called the juridification of technical standards through EU law. This proviso is to be remembered when it comes to existing ISO/IEC standards¹³²

Regulation 1025/2012 is less outspoken. The spirit is expressed in Recital 2:

European standardisation reinforces the global competitiveness of European industry especially when established in coordination with the international standardisation organisations, namely the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU)

and Rec. 6:

The Union should seek to promote cooperation between European standardisation organisations and international standardisation organisations.

Regulation 1025/2012 does not lay down rules or recommendations on what co-operation between the European Commission and ISO/IEC or between the ESOs and ISO/IEC should look like. The 2021 Standardisation Strategy is much more outspoken in how the EU looks at international standardisation and what kind of values should be promoted:¹³³

4) Setting international standards is critical for the EU's competitiveness. The geopolitical landscape has significantly changed in recent years, with increasingly complex value chains and more assertive actions by trading partners in setting standards for which we need a more strategic approach. This has led to a situation where the respect for core European values and freedoms, in particular in the setting of internet standards and new technologies like artificial intelligence, blockchain, data or online platforms, is being challenged. At the same time, setting international standards is key to promoting the EU's strategic capacity in areas like raw materials, space data, batteries, hydrogen or microchips. The coordination of EU stakeholders and available resources should be improved to ensure that standards are set in line with EU values.

Currently it looks as if the EU and/or the European Commission leaves it to the ESOs to take the necessary measures. The overall purpose of the Vienna and Frankfurt Agreements is to co-ordinate so as to avoid duplication and to leave elaboration to the most specialised team of experts. However, cooperation is taken to another level when it comes to adoption by one organisation of existing publications of the other organisation, or when cooperation takes place through mutually agreed allocation of work with parallel approval and voting on technical standards.¹³⁴

There is no equivalent to Annex III stakeholder participation in ISO/IEC. COPOLCO – ISOs Committee on Consumer Policy – is to be located at the policy level similar to the French regulatory

¹³² See under IV. 2. c).

¹³³ Roadmap for a European Standardisation Strategy (n 45).

¹³⁴ Sections 4 and 5 of the agreement on technical cooperation between ISO and CEN (Vienna Agreement).

approach, not at the standard-setting level. Some 128 ISO members are members of COPOL-OCO, a consumer policy body whose task is to:

- study means of helping consumers to benefit from standardisation;
- study means of improving consumer participation in national and international standardisation;
- provide a forum for exchange of information on the experience of consumer participation in the development and implementation of standards in the consumer field;
- advise the ISO Council as to the consolidated viewpoints of consumers on matters relevant to ISO's current and potential standardisation and conformity assessment work, and
- advise the ISO Council on the need for new or revised policies or actions within ISO as they relate to consumers' needs.

It needs to be stressed here that national standards bodies are members of COPOLCO, not consumer organisations. Indeed, some national standards bodies do not include a member from a consumer organisation in their delegations.¹³⁵ The only possible means for stakeholder organisations to contribute to elaboration of a technical standard in an ISO/IEC technical committee seems to be to apply for special liaison status, which means as observers. ISO has published guidance for liaison organisations which determine the requirements for admission and the possibilities for stakeholder organisations to contribute to ISO work.¹³⁶ ANEC as well as Consumers International are among organisations that can fulfil ISO requirements.¹³⁷

In its new Standardisation Strategy, the European Commission stresses the importance of inclusiveness and broad stakeholder participation (including civil society, vertical sectors, SMEs), and says: *'this approach should also be consolidated at international level'*. The hidden claim seems to be that CEN and CENELEC should renegotiate the Vienna and Frankfurt Agreement so as to strengthen inclusiveness.

cc) Next Judicial Blow: Public Accessibility of ISO and Harmonised EU Standards?

One may wonder whether the CJEU might promote inclusiveness through its preparedness to submit ISO standards to its jurisdiction provided EU law explicitly refers to them. The facts behind *Stichting Rookpreventie* are of utmost interest.¹³⁸ The EU Tobacco Directive¹³⁹ put a ceiling on cigarette emissions requiring that, in order to access the EU internal market, emissions are necessarily calculated on the basis of ISO 4387, ISO 10315, ISO 8454 and ISO 8243. Quite unusually, the ISO standards are explicitly mentioned in the Directive. The specific measurement methods were developed by an ISO committee predominantly composed of members representing the tobacco industry. The complex case raised questions on the public accessibility of technical standards which are integrated into EU law and are made mandatory, though; on the reach of judicial review by the CJEU over international standards which are being criticised

¹³⁵ <https://www.iso.org/committee/55000.html>

¹³⁶ Guidance for ISO liaison organisations Engaging stakeholders and building consensus, 2011 https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/guidance_liaison-organisations.pdf

¹³⁷ <https://committee.iso.org/sites/tc322/home/about/liaisons.html>

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

¹³⁹ Directive 2014/40/EU on the manufacture, presentation and sale of tobacco and related products.

as being industry-biased; on a possible infringement of copyright in case ISO standards are made public; and last but not least on whether the dynamic reference is in compliance with the *Meroni* judgment.¹⁴⁰

Two of many questions have to be highlighted – the jurisdiction of the Court and public accessibility. The AG and the CJEU disagreed on both issues. The AG drew a distinction between binding law and mere technical specifications and rejected the need to make ISO standards publicly available. However, the Court instead confirmed that, through direct reference, ISO standards are becoming part of EU law. One might feel tempted to stress the parallel with *James Elliott*. However, there is a difference between European harmonised standards whose use is voluntary and the very particular situation where the EU legislature references ISO standards in secondary EU law. While the Court took a bold decision with possibly far-reaching consequences, it shied away from drawing the obvious conclusion, namely that in such circumstances technical standards have to be freely accessible. There are many loose ends in the judgment, which triggered fierce academic debate, but what matters in the broader political context is that the CJEU sent a message to ISO and to the EU. International standards are not sacrosanct. This message might be well heard and might incentivise CEN and CENELEC to engage in negotiations with ISO/IEC on a revision of the Vienna and Frankfurt Agreements so as to increase inclusiveness, which in turn could help to overcome at the least potential deficiencies in the measuring technique. Whether or not and, if so, under what conditions harmonised European standards have to be freely accessible is to be decided in *Public.Resource.Org*. Two environmental organisations have sued the European Commission under Regulation (EC) No 1049/2001 on public access to European Parliament, Council and Commission documents. The General Court rejected the claim, but the appeal is now pending before the CJEU.¹⁴¹

e) A New Governance Structure under a revised Regulation 1025/2012?

The reluctance to revise the Vademecum might have to do with intensive efforts by the European Commission to prepare the ground for a substantial reform of the regulation on technical standards. At least, this is how the Communication from February 2022 could be understood, which points to an evaluation in order to test whether the Regulation is still ‘*fit for purpose*’.¹⁴² Two different strands are coming together – evaluation and revision of Regulation 1025/2012 and of Decision 768/2008 and Regulation 765/2008.

aa) Roadmap, E&Y Report, and Five-year Implementation Report

The European Commission launched the political process with the Roadmap for a new Standardisation Strategy, published on 28 June 2021,¹⁴³ which goes back to the 2020 New Industry Strategy.¹⁴⁴ The Roadmap addressed six major issues to be discussed:

¹⁴⁰ *Meroni* (n 55).

¹⁴¹ Case T-185/19 *Public.Resource.Org*. ECLI:EU:T:2021:445, Appeal Case before the Court of Justice C-588/21 P.

¹⁴² COM (2022) 31 final Com (2022) 31 final An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market, at 6, the Commission ‘Will launch the evaluation of Regulation (EU) 1025/2012 to assess whether it is still fit for purpose’

¹⁴³ Roadmap for a European Standardisation Strategy (n 21).

¹⁴⁴ COM (2021) 350 final.

1. the fitness of the ESS (European Standardisation System) for dealing with sustainability and the digital economy,
2. the fitness of the regulation on harmonised standards,
3. consolidation of stakeholder participation at the international level,
4. strengthening of ‘core European values and freedoms’ in the geopolitical environment of standardisation,
5. the rise of the importance of vocational training and
6. the increase in standards for services.

Public consultation included,¹⁴⁵ it took the European Commission less than a year to draw the necessary conclusions and to come up with a proposal for reform. The first four issues touch upon the governance structure – at least, the communication could be read that way. The duty under Article 24 (3) to report every five years to the European Parliament and the Council on implementation of the Regulation might trigger far-reaching action.

On 2 February 2022, the European Commission published its second report on the implementation of Regulation 1025/2012 for the period 2015–2019.¹⁴⁶ In order to fulfil its reporting obligation, the European Commission commissioned from E&Y an ‘*independent study*’.¹⁴⁷ Ernst & Young, this has to be recalled, won the tender by the European Commission to exercise compliance by HENs with binding legal requirements through HAS consultants. One might wonder whether it is a politically sound choice to entrust the same body which is in charge of selecting HAS consultants with such a task. ETSI complained along these very lines, but the EC answered that the two parts of E&Y were ring-fenced.¹⁴⁸

The E&Y study had three main objectives:

firstly to analyse the implementation of Regulation (EU) 1025/2012 according to the reporting requirements in Article 24, which apply to the European Standardisation Organisations and the European stakeholder organisations eligible for Union financing representing SMEs, consumers, environmental and social interests (Annex III organisations). Secondly, to evaluate the relevance of the standardisation activities receiving Union financing, and thirdly to assess opportunities and provide recommendations to simplify Union financing and reduce administrative burden.

The E&Y study is mainly quantitative in nature: it lists all the activities of Annex III organisations over the reporting period. The figures on financial support of the ESOs and Annex III organisations are highly informative, distinguishing between operating (institutional) and action (project-related) grants, see Article 17 Regulation 1025/2012. In 2019, the three ESOs received some EUR 5 million as an operating grant and roughly EUR 10 million in action grants, with CEN receiving EUR 7 million. The EC provided EUR 15 million in 2019, which is EUR 5 million less than in 2015. With regard to Annex III organisations, SBS (Small Business Standards) and ANEC were the main beneficiaries. In 2019 ANEC received EUR 1.4 million, which is 100T more than in 2015 in institutional grants but no action grants, in contrast to SBS, which got EUR1.8 million.

¹⁴⁵ On the consultation see the different steps undertaken https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy_en

¹⁴⁶ Brussels, 2.2.2022 COM(2022) 30 final Standardisation package report from the Commission to the European Parliament and the Council on the Implementation of Regulation (EU) No 1025/2012 from 2016 to 2020.

¹⁴⁷ Study on the implementation of Regulation (EU) No. 1025/2012 (Article 24) <https://doi.org/10.2873/504681> and <https://doi.org/10.2873/593923>.

¹⁴⁸ Information provided by ANEC.

In contrast to the other Annex III organisations, ANEC depends almost exclusively on the EC (95%, presented in the table above) and EFTA (5%) funding, as ANEC does not receive membership fees and the foundation of its General Assembly on a natural person to represent the interests of perhaps numerous legal persons in that country (the national consumer organisations) makes collection of membership fees impossible in practice. Interestingly, the E&Y report points to the need for ANEC to raise money outside and beyond the current budget: *'The European Commission has, at numerous times, invited ANEC to invest in looking for possible partners able to co-fund the organisation.'*¹⁴⁹ ANEC, this is to be added, has diversified its funding by EUR 1.75 million since 2011, with most of that sum being raised in the past few years. Nevertheless, most of the sum reflects transfer payments to experts and others but does not represent a (large) financial benefit for ANEC. ANEC has difficulty in finding private funders, given the perceived public nature of 'consumer protection' and the uncertainties of standards versus regulation.¹⁵⁰ Next, the study focuses on the relevance of EU financing and insists that the contribution of the Annex III organisations depends on public funding, with particular emphasis on ANEC.¹⁵¹ The last part of the study analyses the costs which result from production of interim and final reports of operation grants and aims at facilitating reporting.

The follow-on report of the European Commission to the European Parliament and the Council, published on 2 February 2022, is relatively short and is comprehensible only when taking the much more comprehensive 'independent study' into account. The Commission report points to new initiatives within CEN and CENELEC to increase inclusiveness through the right of opinion. If there is a non-favourable opinion, the technical committee responsible for drafting the standard in question *'shall consider the justification provided for the opinion and provide feedback'*.¹⁵² A similar mechanism does not exist within ETSI. The Commission report refers to the critique raised by Annex III organisations and quotes them rather extensively. It has to be recalled that Annex III organisations are full members within ETSI and have voting rights, although voting rights are unevenly spread. More in passing, the Commission report notes that national standardisation organisations enjoy only 2% of ETSI voting rights. The contract on services with HAS consultants is presented as a success. The Commission Report pinpoints that the HAS consultants' sole task is to assess compliance of draft standards with binding legal requirements, but that it is for the Commission alone to take a final decision on publication of harmonised European standards in the Official Journal, without referring to *James Elliott* or the Communication of November 2018. Interestingly, out of roughly 3000 assessment requests only one-third passed the benchmark due – for the other two-thirds – to 'inadequacy with EU law'.¹⁵³

However, the Commission report does not provide any further detail which would allow one to get a clearer picture of where the inadequacies are resulting from, in particular what kind of binding requirements were not fully taken into account or whether inadequacy simply refers to non-compliance between the mandate and technical standards. The rest of the Commission report deals with the reasons behind delayed publication, where there are contradictory views between the ESOs and the EC, and the number of formal objections initiated by the Member States and/or the European Parliament, again without further analysis. A formal objection leads on average to a delay of three years.

¹⁴⁹ E&Y report (n 148) at 45.

¹⁵⁰ Information provided by ANEC.

¹⁵¹ E&Y report (n 148) at 53.

¹⁵² COM(2022) 30 final, 4.

¹⁵³ At 8.

bb) Pressuring Core Values into the Governance Structure

One might need to distinguish between the Roadmap for a New Standardisation Strategy and evaluation of Regulation 1025/2012. The Roadmap set ambitious targets, which might need further investment in a search for appropriate solutions; the evaluation report is no more than the late redemption of a legal obligation. However, the two are intertwined through the geopolitical dimension and this is where the European Commission took action.

On the same day, 2 February 2022, together with the Roadmap for a new Standardisation Strategy and the report on the evaluation of Regulation 1025/2012, the European Commission published a proposal for amending Regulation 1025/2012.¹⁵⁴ The proposal reiterates the concern of the European Commission that ‘core European values’ have to be given greater weight in the internal procedure on developing technical standards through the ESOs:

Greater clarification is therefore needed to ensure that the whole internal decision-making process in issuing standards and standardisation deliverables, requested by the Commission on the basis of Article 10(1) of the Standardisation Regulation, is in line with what the EU institutions expect from a standards-developing body officially recognised as a European standards organisation.

The proposal ran through the legislative process in record time and was approved in December 2022.¹⁵⁵

Article 10 of Regulation (EU) No 1025/2012 is amended as follows:

(1) paragraph 1 is replaced by the following:

1. The Commission may, within the limitations of the competences laid down in the Treaties, request that one or more European standardisation organisations draft a European standard or European standardisation deliverable within a set deadline, provided that the European standardisation organisation concerned complies with paragraph 2a. European standards and European standardisation deliverables shall be market-driven, take into account the public interest as well as the policy objectives clearly stated in the Commission’s request and be based on consensus. The Commission shall determine the requirements as to the content to be met by the requested document and a deadline for its adoption.;

(2) the following paragraph is inserted:

‘2a. Without prejudice to other advisory opinions, each European standardisation organisation shall ensure that the following decisions concerning European standards and European standardisation deliverables referred to in paragraph 1 are taken exclusively by representatives of the national standardisation organisations within the competent decision-making body of that organisation: (a) decisions on the acceptance and refusal of standardisation requests; (b) decisions on the acceptance of new work items that are needed for the fulfilment of the standardisation request; and (c) decisions on the adoption, revision and withdrawal of European standards or European standardisation deliverables’

¹⁵⁴ Brussels, 2.2.2022 COM(2022) 32 final 2022/0021 (COD) Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 1025/2012 as regards the decisions of European standardisation organisations concerning European standards and European standardisation deliverables.

¹⁵⁵ Regulation (EU) 2022/2480 19.12.2022, amending Regulation (EU) No 1025/2012 as regards decisions of European standardisation organisations concerning European standards and European standardisation deliverables.

The revised version of Article 10 (1) is directed against ETSI in barely veiled language and aims to amend the internal statutes in order to curb the influence of non-European players.¹⁵⁶ The message is clear: if ETSI wants to remain within the named Annex I organisations, it has to amend its statutes. As the rumour goes, ETSI is ready to comply and to introduce a kind of split voting, depending on whether the elaboration of harmonised European standards is involved or ‘only’ a non-mandated standard. The other objectives set out in the Roadmap are not yet dealt with, in particular a serious analysis of whether Regulation 1025/2012 is fit for the digital age, while another issue not yet tackled is whether the current Annex III suffices to guarantee the input of European stakeholders.

f) Revision of the Governance Structure through the New Legislative Framework?

The stocktaking would be incomplete without the Commission Staff Working Document on the Evaluation of the New Legislative Framework, dating back to 11 November 2022 and being closely connected to the Roadmap for a new Standardisation Strategy.¹⁵⁷ The scope of the report is of limited importance for the regulatory frame on standardisation, as it:

does cover the aspects of harmonised standards relevant to the NLF, such as having technologically neutral essential requirements and relying on harmonised standards for presumption of conformity. However, it does not address the EU standardisation system beyond those aspects. The Evaluation of the standardisation system should be a stand-alone process.

Overall, the report underlines the importance of harmonised standards and their availability once legislation is in place so as to save costs of third-party assessment. Both conditions have to be kept in mind when it comes to analysis of the role of harmonised standards in the digital framework. This might explain why the European Commission, already prior to formal adoption of the AIA-P, has started to initiate the necessary procedural steps to promote the development of technical standards which are meant to concretise the AIA-P. However, the long and extensive report is crucial for another reason. The ESOs and the National Standardisation Organisations are heavily relying on certification bodies to make sure that harmonised standards comply with fundamental rights and mental health. That is why detailed analysis of conformity assessment is of utmost relevance for the role and function of certification and accreditation bodies under the AIA-P and the CRA-P.¹⁵⁸

3. Lessons to be Learned

Seen through consumer lenses, the review of the New Approach in the field of product safety produces mixed feelings. While there is certainly progress to be reported, much of it results from the framing of the New Approach through European product safety regulation and – last but not least – from the CJEU judgment in *Elliott*, which triggered a change in the distribution of responsibilities. However, what remains unresolved so far is the gulf between the call for inclusiveness, on the one hand, and, on the other, the hard reality of participation within

¹⁵⁶ Interview with a representative from the ESOs.

¹⁵⁷ Brussels, 11.11.2022 SWD(2022) 364 final Commission Staff Working Document Evaluation of the New Legislative Framework {SWD(2022) 365 final}

¹⁵⁸ This Report does not go into depth in terms of assessment of conformity via self- or third-party certification.

the ESOs and within the European decision-making process on technical standardisation. The European stakeholder organisations continue to lead a shadowy existence. The reconstruction of the last decades showed that they have to fight for every inch of ground and that they are considerably restricted in their scope of action, especially by the statutes of the ESOs. There is no true spirit of partnership on a level playing field. The rules of the ESOs are more obstacles than bridges for better integration of consumer interests. It is clear that the ESOs only act when put under massive pressure from the political side, more concretely via binding EU regulation.

In terms of legal policy, it remains to be criticised that the various CJEU rulings have not prompted the Commission to fundamentally revise the relevant provisions in Article 10 (5) and (6), in particular with regard to clarifying the distribution of responsibilities between the ESOs and the European Commission, not to mention the pending issue on the reach of copyright with regard to harmonised European standards. One might even go further and raise the question whether qualifying harmonised standards as 'law' affects the collective rights of the so-called qualified entities under Directive 1828/2020 on representative actions. Taking their legal character seriously implies integrating harmonised standards in the list of European legislation against which qualified entities may take action, be it an action for an injunction or in the case of an infringement collective redress. The list of pending issues can easily be prolonged. A crucial point, not so much at the centre of this Report, is the potential liability of standardisation and certification bodies. The PIP scandal¹⁵⁹ and the CJEU judgment in *Schmitt*¹⁶⁰ disclosed the liability gap which could only be closed through targeted regulation in (for instance) the EU Digital Policy Legislation or in the envisaged revision of the Product Liability Directive. The loose ends and open issues are neatly transferred to regulation of the digital economy.

A final rather striking point or perhaps observation is the missing reference to fundamental rights in EU legislation, in particular after 'codification' of the New Approach in Regulation 1025/2012. This is all the more astonishing as the Declaration on fundamental rights dates back to the year 2000 and as health and safety are undoubtedly coming under the umbrella of fundamental rights. The current EU regulatory approach on harmonised standards insinuates that a clear divide exists between standardisation 'without' fundamental rights in the old economy and standardisation 'with' fundamental rights in the new digital economy.

¹⁵⁹ Between 2001 and 2010 PIP sold hundreds of thousands of unapproved implants sold globally. They were found to involve a higher risk of rupturing or leaking than approved models and of inducing breast cancer, https://en.wikipedia.org/wiki/Poly_Implant_Prosth%C3%A8se

¹⁶⁰ CJEU Case C-219/15 *Schmitt* ECLI:EU:C:2017:128.

III. The Digital Economy, Technical Standards, and EU Legislation – Conceptual Deficits



Strongly interlinked to the Roadmap – in fact one of the reasons for the Roadmap – is the ongoing attempt by the European Commission to lay down an overall framework for the digital economy and digital society (sic) through the Digital Governance Act (DGA), the Digital Market Act (DMA), the Digital Services Act (DSA), the Data Act (DA-P), the Artificial Intelligence Act (AIA-P), the Cyber Resilience Act (CRA-P) and the Electronic Identification and Trust Services Regulation (eIDAS 2-P).¹⁶¹ Turned into the language of the ESS, the seven proposals mirror the New Approach rationale, so that broadly worded binding legal requirements will have to be specified and concretised through harmonised standards and non-harmonised standards. EU Digital Policy Legislation is built on a risk-based approach in line with the New Legislative Framework, in essence on the distinction between health and safety on the one hand and non-health and non-safety related issues on the other. Harmonised standards come into being only as tool to manage particularly ‘risky’ products and services, which might have an impact on health and safety. Here lies the parallel to the role of the New Approach in the old economy in product safety regulation.

The inherent risk to health and safety is claimed to legitimate the threefold function of the European Commission in mandating harmonised standards, in monitoring the process of standard-setting, and in examining compliance of harmonised standards before they are cited in the Official Journal. The rationale can be turned upside down. When there are no risks to health and safety, there is no room for the European Commission and therefore elaboration of technical standards remains in the hands of the ESOs. Seen through the eyes of the European Commission, the distinction is reflected in the differences between the AIA-P and the CRA-P – where harmonised standards play a crucial role – and the DSA, where the EU relies on non-harmonised standards, as will be analysed below. This does not mean that the EU leaves the level of protecting service recipients/users to those who develop and apply non-harmonised standards. It only implies that the European Commission stays away from intermingling in standardisation, and leaves it to the ESOs and the respective businesses to comply with binding legislation to protect the economic interests of recipients/users.

In contrast to the New Approach/NLF in the industrial economy, fundamental rights are supposed to play a key role in EU Digital policy legislation. The abundant reference to fundamental rights in the various regulations blurs the distinction between risky products (namely, risks to health and safety) and non-risky products and services; or between protection against

¹⁶¹ 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, 21.4.2021.

risks to health and safety and protection against economic risks. The Charter of Fundamental Rights covers both dimensions. However, in terms of the core of economic interests, the Charter looks biased. There is no counterpart to the ‘right to do business’ in Article 16 EUCFR by way of a ‘right to consumer protection’ or a ‘right to protection against economic harm’. The Charter covers consumer economic interests through the ‘principle of a high level of consumer protection’ in Article 38 EUCFR only. Consumer rights, if any, have to be integrated into those rights of the Charter which provide space for inclusion of economic interests, such as the right to dignity (Article 3), the right to liberty (Article 6), Article 7 (respect for private and family life), Article 8 (protection of personal data), Article 10 (freedom of thought, conscience, and religion) Article 11 (freedom of expression), Article 17 (the right to property) as well as the whole of Title III aiming at equality.¹⁶²

The concentrated power of fundamental rights has to be coordinated with a body of digital law, here AIA-P, the CRA-P, and the DSA, which first and foremost establish rules for an EU digital market. The various acts frame the conditions under which the various actors in the digital market are operating. They are to be understood as what is called in German legal terminology *Marktordnungsrecht*, that is, something like ‘market order law’. Market order law does not deal with the relationship between private parties, b2b or b2c, at least not directly.¹⁶³ This is exactly what happened in the AIA-P, the CRA-P, and the DSA. The regulatory approach imposes rules in particular on professional actors top-down, but does not engage in the complex relationship between the various professional actors and their different capabilities, let alone the relationship between professional actors and consumers. I do not want to be misunderstood – the rules of the three acts under scrutiny affect private parties in whatever perspective, but the three acts would look very different if they had been written and conceptualised through the lenses of private actors. The categorisation of the AIA-P, the CRA-P, and the DSA as market order law is crucial to understanding the design of their law and the particular role and function of harmonised standards.

The following analysis has to be put into the context of our research on the ‘universal, structural and relational vulnerability of consumers’.¹⁶⁴ The envisaged dominance of harmonised standards, provided the pending proposals find political support, will have to integrate not only physical harm, but partly psychological harm and always fundamental rights so as to build a ‘*human-centric, secure, ethical, and trustworthy AI*’.¹⁶⁵ In short, the different Regulations and Draft Regulations will strengthen the regulatory ‘underground’, now in the form of algorithms.¹⁶⁶ The screening of the AIA-P, the CRA-P, and the DSA aims at elaborating on the conceptual deficits which result from the bold but not very well thought-through transfer of the New Approach/NLF from the industrial to the digital economy, under three parameters: missing consumer protection, conceptual unclarity on the role of fundamental rights in the

¹⁶² This is not the place to go through the various ‘rights’ one by one or to analyse *in abstracto* the potential reach of the consumer protection ‘principle’ in Art 38 EUCFR, but see B Kas/ H-W. Micklitz, *Judge Made Private Law and the European Polity*, in: B Kas and Ch Mak (eds), *Judges in Utopia*, forthcoming 2023.

¹⁶³ This is somewhat different with regard to the Digital Market Act, the Data Governance Act and the Data Act, which, however, do not form part of the closer analysis undertaken in Ch III.

¹⁶⁴ For a first account of the importance of standardisation; N Helberger/ H.-W. Micklitz/ P Rott, *EU Consumer Protection 2.0: The Regulatory Gap: Consumer Protection in the Digital Economy: Addendum to the report ‘Structural Asymmetries in Digital Consumer Markets’*, December 2021, https://www.beuc.eu/publications/beuc-x-2021-116_the_regulatory_gap-consumer_protection_in_the_digital_economy.pdf.

¹⁶⁵ See under IV 2 b) bb)

¹⁶⁶ H-W Micklitz, *Soft Law, Technical Standards and European Private Law*, in: E Korkea-aho (ed), *Handbook of Soft Law*, Edward Elgar Publishing, forthcoming 2023.

regulatory design, and the potential consequences which result from the residual power of the European Commission to substitute harmonised European standards through common specifications.

1. AIA-P and Harmonised Standards

The draft uses forceful language so as to drive home the risk-based approach through extensive reference to technical standardisation:

(61) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation. Compliance with harmonised standards as defined in Regulation (EU) No 1025/2012 of the European Parliament and of the Council should be a means for providers to demonstrate conformity with the requirements of this Regulation. However, the Commission could adopt common technical specifications in areas where no harmonised standards exist or where they are insufficient.

(64) Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for the remote biometric identification of persons, for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.

The AIA-P rules Title III Chapter 2 (Requirements for High-Risk AI) establish ‘general binding requirements’ in the meaning of the New Approach with regard to ‘high-risk’ AI systems on:

- creation of a risk management system (Article 9 AIA-P);
- on the quality criteria for training, validation and testing data in relation to relevance, representativeness, accuracy and completeness (Article 10 AIA-P);
- inter alia to avoid biases and discrimination (Article 11, Annex IV AIA-P);
- record-keeping (Article 12 AIA-P);
- provisions on transparency and user information (Article 13 AIA-P);
- on human oversight (Article 14) and
- obligations on system accuracy, robustness, and cybersecurity (Article 15 AIA-P).

These general requirements need to be concretised through harmonised technical standards. High-risk AI systems which are in conformity with harmonised standards and which are cited in the Official Journal of the European Union will be presumed to be in conformity with the requirements of the AIA-P, Article 40 AIA-P. In case the general requirements or the harmonised standards are insufficient, or when there is a particular need to respect safety and fundamental rights, the European Commission may, by means of implementing acts, adopt common specifications which concretise the general requirements, Article 41 AIA-P.

a) Consumer Protection – Missing

Regulation of technical standards is deeply connected to consumer policy issues through the merging of technicity with product safety. The AIA-P is aligned with the New Legislative

Framework (NLF) that defines the rules for placing a product on the market. The AIA-P copies the regulatory technique in the old economy and transfers it to the new economy. The European Commission had to face strong criticism on its risk-based approach, which embraces AI broadly and breaks it down into four different categories, according to the degree of risk. Much ink has been spilt on the AIA-P proposal, not only from the theoretical conceptual aspect,¹⁶⁷ but also with regard to how business could implement the very openly drafted legal concepts.¹⁶⁸ None of the critique changed the minds of the European Commission, the European Parliament, or the Council. In the meanwhile, the European Parliament and the Council have agreed on a position. However, interinstitutional negotiations have not yet started. Neither of the two challenged the broad risk-based approach. That is why it does not make much sense to reiterate the overall critique. This Report takes the risk-based approach for granted and tries to highlight the consumer protection gap, which cannot be – or can only partially be – compensated through reference to fundamental rights.

The AIA-P does not address consumers directly, nor can it be seen as a piece of consumer law. Nonetheless, the rules it establishes do affect consumers considerably, if indirectly, through the establishment of a particular market order. The primary addressee is the professional ‘user’, Article 3 (4). There is one notable and extremely relevant exception: namely, Article 52 (1) and (2) reaches out to ‘natural persons’, which also means consumers. The AIA-P distinguishes between different levels of risk. ‘Certain risks’ are all those which are neither prohibited risks nor high risks – in essence all risks which result from commercial transactions which do not touch upon health and safety issues. In daily life, these are by far the majority of commercial and non-commercial activities. Consumers should be *‘informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use’*. The deficits of endless stringing together of information obligations are well known. Here they are all the more serious as the regulation does not provide for the obligation to explain either the AI system as such, or what the possible result of interaction might be. This gap is partly filled through ISO/IEC and IEEE standards in a way that forestalls future European harmonised standards, but that raises even more questions.¹⁶⁹

The European Commission has indirectly confirmed the gap through its pending initiative on digital fairness.¹⁷⁰ At the time of writing, the outcome of the initiative is still open. It is highly likely that the current Commission will not take any action. This would mean that the EU will have adopted an extremely comprehensive and complex set of regulations on the digital economy – but without taking consumer concerns seriously. The timing is worth remembering. In 1997, the EU adopted Directive 97/7/EC on distance selling, a predecessor of the Consumer Rights Directive, aiming at guaranteeing an adequate level of consumer protection in upcoming – and then still infant – e-commerce. Three years later the EU adopted the e-commerce Directive 2000/31/EC, which remained the key document for 22 years until adoption of the DSA. In 1997, consumer protection preceded the rules governing the internet; in 2023 consumer law lags behind.

¹⁶⁷ Out of an abundant literature, see M Veale and F Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, (2021) 22(4) *Computer Law Review International*, 97

¹⁶⁸ And the just-published report *Open Loop Artificial Intelligence Act: A Policy Prototyping Experiment Revisiting the Taxonomy of AI Actors*, April 2023, file:///C:/Users/Mi-PC-SFF/Downloads/Artificial_Intelligence_Act_A_Policy_Prototyping_Experiment_Taxonomy_AI_Actors.pdf

¹⁶⁹ See under IV.3.

¹⁷⁰ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

The European Commission – and this is the overall logic behind EU Digital Policy Legislation – seems to start from the premise that the existing body of consumer law rules, developed with a strong focus on the old analogue economy, suffices to meet the consumer problems of the new digital economy. True, the Consumer Rights Directive was already revised in 2011, though with minimal changes, and Directive 2019/770 lays down rules on digital content in consumer sales contracts. However, these adjustments could not set aside the fact that the European Commission focused all its resources on the ‘A’ acts, the DMA, DSA, DGA, DA, AIA-P, CRA-P, but forgot about taking consumer problems seriously and initiating a debate on the need for and feasibility of a ‘Digital Fairness Act.’¹⁷¹ The fitness check could in theory be turned into a substitute. However, its scope is limited to the Consumer Rights Directive (CRD), the Unfair Contract Terms Directive (UCTD), and the Unfair Commercial Practices Directive (UCPD), though excluding – for instance – the General Data Protection Regulation (GDPR) and, perhaps even more importantly, ‘enforcement’.¹⁷²

The regulatory gap is abundantly clear and again it seems that there is no political will to introduce consumer concerns in the final version of the AI Act.¹⁷³ The risk-based approach, the transfer of health and safety regulation to the digital economy, sets aside the economic interests of consumers. Potential effects on the economic situation of consumers are not regarded as being ‘high-risk’. In light of the adverse impact of AI on consumer agency – here, recall the universal, structural, and relational vulnerability – this is astonishing to say the least. ANEC proposed an amendment to Article 6 (1) which expresses consumer concerns and which, if accepted, would broaden the potential scope of high-risk AI and would change the perspective from intended use defined by the provider through foreseeable use defined by the consumer,¹⁷⁴ a tension which goes like a red thread through the whole analysis.

In addition to the high-risk AI systems referred to in paragraph 1, an AI product shall be deemed high-risk, as far as the aspects covered by this Regulation are concerned, when, in the absence of specific provisions of Union Harmonisation legislation in Annex II, it presents a risk based on the criteria of likelihood of the harm occurring, immediacy of the harm and the intended purpose and foreseeable use of the AI product. This provision shall be applied taking due account of the precautionary principle.

Justification:

As the European Commission’s study of product safety and liability legislation showed, there are gaps in present legislation and new AI related aspects such as explicability require new legal provisions, especially for enforcement purposes. Any AI system has the potential to cause harm so identifying a limited group as high-risk and ignoring the rest can result in dangerous systems slipping through.

Therefore, in addition to the proposed classification criteria, in order to assess whether the AI system is posing a high or low risk, criteria such as likelihood of the harm occurring, immediacy of the harm, the foreseeable use of the AI system (and not only the intended use which is not covering the potential effects of machine learning) have to be taken into account too.

¹⁷¹ A BEUC study is under way, which will be publicly available in late autumn 2023.

¹⁷² This topic is subject to a larger project initiated by BEUC in which I am participating.

¹⁷³ Helberger et al, Consumer Protection 2.0 (n 8) at 158; BEUC Position Paper AIA-P under 4.3. p. 6.

¹⁷⁴ BEUC Position Paper, at 4.

However, even this proposal does not overcome the problem that the AIA-P puts the European Commission in pole position, as the European Commission alone decides on a potential amendment of what it classifies as high-risk. Two examples might underpin the importance of AI for consumers, the first being the impact of biometrics:

A Big Apple lawyer was banned from Madison Square Garden sporting events, as the camera identified him as belonging to the law firm which represented a client in a case against the Garden. He therefore went to court as he could no longer see his favourite basketball team¹⁷⁵

Article 5 d) AIA-P prohibits the ‘use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement,’ subject to a number of exceptions. The point is not so much to discuss whether similar market behaviour would be prohibited,¹⁷⁶ but to demonstrate that a technology which seems to be far removed from the daily life of consumers may affect them. Transferred to Europe, can a sports club bar access by hooligans or other unwanted visitors with the help of face recognition?¹⁷⁷ Article 52 (3) AIA-P suggests that it suffices if fans are properly informed. It is difficult not to be cynical about such a naïve legislative approach. Provided screening of visitors to a sporting event is allowed, it would suffice to put a sign at the entrance telling the customer that everybody is automatically screened. Article 6 AIA-P legalises public use of biometric identification under certain conditions – what if the ESOs are elaborating technical standards and what if the European Commission is mandating elaboration of such a standard?

The second example concerns another area where consumer concern is crystal clear – credit scoring. Article 6 (2) AIA-P in combination with Annex III classifies them as high-risk:

AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use.

Recital 37...In particular, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons’ access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, disabilities, age, sexual orientation, or create new forms of discriminatory impacts...

Credit scoring was classified as high risk, not least in light of the ‘open Schufa campaign’, which is referred to explicitly in the impact assessment.¹⁷⁸ The political agreement introduces additional requirements in Article 6 (3). These have to be met so as to qualify credit scoring as high-risk. The result together with a narrowing of the definition of AI will limit high-risk scoring to the use of ML techniques and knowledge-based approach. Statistical methods would not qualify as AI.¹⁷⁹ At first sight, it looks as if consumers enjoy a higher degree of protection against (narrowed) AI-based credit scoring, in particular when read in light of Article 5 (1) which

¹⁷⁵ New York Post 8.3.2023 <https://nypost.com/2023/03/07/nyc-lawyer-banned-from-msg-i-had-to-go-to-miami-to-see-knicks/>

¹⁷⁶ Convincingly, M Veale and F Borgesius (n 168) at 7.

¹⁷⁷ German Constitutional Court, BVerfGE 148, 267. Beschluss vom 11.04.2018–1 BvR 3080/09.

¹⁷⁸ AIA-P impact assessment, <https://artificialintelligenceact.eu/wp-content/uploads/2022/06/AIA-P-COM-Impact-Assessment-1-21-April.pdf> at 20.

¹⁷⁹ The EC website informs on the state of affairs <https://artificialintelligenceact.eu/documents/>

prohibits social scoring.¹⁸⁰ However, on a closer look it is far from clear where to place the data mining of credit bureaus which collect a broad range of demographic, socio-economic, and behavioural data. Article 5 (1) AIA-P seems to relate to input data concerning interactions with public authorities only, which would mean that the business activities of credit bureaus are out of scope. Article 6 (2) AIA-P in combination with Annex III ties the use of AI in credit scoring to the standard mechanism of self- or third-party assessment. While it looks as if for the time being credit bureaus are not yet using AI, their potential competitors – payment services providers – might very well do so. There is a grey area between social scoring, which is prohibited, and credit scoring, which is lawful subject to the conditions that all high-risk AI has to meet. In consequence, the AIA-P does not offer an additional layer of protection if credit bureaus use AI in assessing creditworthiness. In his recent opinion, AG Pikamae¹⁸¹ held that credit scoring has to be regarded as ‘profiling’ in the meaning of Article 22 GDPR. The ‘Open Schufa’ campaign might welcome the opinion. However, the legal assessment by the AG stands on shaky legal grounds with regard to the facts from which it starts and with regard to the missing analysis that profiling can be justified under Article 22 Paragraph 2 GDR.¹⁸²

b) Fundamental Rights – Omnipresent but Underdeveloped

The AIA-P mentions fundamental rights 80 times. Fundamental rights are omnipresent. The most outspoken reference can be found in Recital 28. Here all the potential rights are enumerated, in between consumer protection. In contrast to Article 1 DSA, the AIA-P does not tie the scope of the Regulation to respect for fundamental rights more generally. However, title II-IV in which the various types of risks are regulated – prohibited risks, high risks, and certain risks – contains references to fundamental rights. Title II dealing with prohibited practices mentions not only fundamental rights but also psychological harm, which is a novelty. Two aspects are worth stressing. The AIA-P does not define mental health or clarify why mental health is not covered by ‘health and safety’, although Recital 16 seems to suggest that physical harm is different from psychological harm. Clearly the latter is different and may be closer to consumer agency and therefore to consumer economic interests. However, psychological harm is mentioned neither in the context of high risks nor of certain risks. The problem is the same as with consumer issues. Psychological harm can only be integrated into the other two risk categories if upgraded to the fundamental rights level.

Title II High Risk is not consistent with regard to the way in which the different chapters integrate fundamental rights. Article 7 (1) b) Chapter 1 Classification ties possible amendments:

to pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

Chapter 2 Requirements mentions fundamental rights only in Articles 10 (data governance), 13 (transparency and provision of information to users) and 14 (human oversight), while Chapter

¹⁸⁰ See Michael Veale and Frederik Borgesius (n 169) at 7.

¹⁸¹ Priit Pikamae, 16. März 2023 Case C-634/21 OQ gegen Land Hessen, Beteiligte: SCHUFA Holding AG

¹⁸² S Schulze and L Konrad (Law Firm Haerting Berlin) Pimp your creditscore – demnächst als Howto aus Luxemburg? Warum der erneute Abgesang auf den SCHUFA-Score verfehlt ist <https://haerting.de/wissen/pimp-your-creditscore-demnaechst-als-howto-aus-luxemburg-warum-der-erneute-abgesang-auf-den-schufa-score-verfehlt-ist/>

3 lays down obligations ‘of providers, users and other parties’, but does not refer to fundamental rights at all, which seems to contradict Recital 58. The same is true for Chapter 4. In Chapter 5, dealing with standards and conformity assessment, fundamental rights show up only with regard to delegated acts in Article 43 (6) AIA-P which specify the requirements of conformity assessment. Title III certain risk refers to fundamental rights in Article 52 (3) but only with regard to AI systems which generate or manipulate image, audio, or video content.

The unsystematic references beg the question whether fundamental rights have to be taken into account only when explicitly mentioned in one of the articles, which would mean that harmonised standards to be developed to concretise the open-ended rules would have to respect fundamental rights incrementally. This is hard to imagine. But is it untidy drafting or is it a new form of legislating, where the democratic authorities point to respect for fundamental rights explicitly, beyond and outside the universal obligation? Or is the differentiation due to the different addressees, public authorities and/or particular parties as in Chapter 3, due to whether fundamental rights are directly applicable or indirectly applicable? What remains, though, is a high degree of uncertainty. It seems hardly likely that the European Commission intends to differentiate between various levels of observance in binding legal requirements, independent of the fact that the Charter of Fundamental Rights remains applicable whether it is mentioned in a particular piece of secondary EU law or not.

However, what remains and what will remain in all probability is the problem that consumer concerns – in particular those that reach beyond physical integrity (health and safety) such as psychological harm or economic harm (!) – can be integrated into the scope of the AIA-P only through either Article 38 (consumer principles) or via the various individual fundamental rights. There has been much discussion on the potential impact of Article 38 EUCFR.¹⁸³ In practice, individual fundamental rights are of much greater importance. They need to be studied one by one in order to test the potential impact on consumer law in a particular context. The two examples on the use of biometric identification and on credit scoring may serve as examples to demonstrate the difficulties.¹⁸⁴ As the AIA-P does not provide for individual rights, consumers would have to rely on national law and then try to upgrade national law through reference to the Charter. What matters in our context is the uncertainty with regard to the importance of fundamental rights in the elaboration of technical standards.

Let us assume that the ESOs, as well as the national standardisation organisations, are full of good intentions to take fundamental rights into account and let us equally assume that they are also prepared to go beyond health and safety and to look after constitutionally protected economic rights. What exactly should they do – and what kind of rights should they take into account? Each and every standardisation project would in theory require a fundamental rights impact analysis. The AIA-P lacks any guidance. Abundant references to fundamental rights do not compensate for the lack of a clear-cut policy which explains the interaction between binding legal requirements and harmonised technical standards.

¹⁸³ Out of the many contributions, see in particular the series of commentaries, published by Ch. Beck and by Nomos.

¹⁸⁴ See above under III 1 a).

c) Harmonised Standards, Common Specifications – Inconsistencies and Uncertainties

On this reasoning, one might seek a solution at the other end, that is, not in the rules on fundamental rights but in those dealing with harmonised standards and common specifications and their interaction. Articles 40 and 41 AIA-P deserve to be quoted in full as they explain the inner mechanics of the Regulation:

Article 40 Harmonised standards

High-risk AI systems which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those standards cover those requirements.

Article 41 Common specifications

1. Where harmonised standards referred to in Article 40 do not exist or where the Commission considers that the relevant harmonised standards are insufficient or that there is a need to address specific safety or fundamental right concerns, the Commission may, by means of implementing acts, adopt common specifications in respect of the requirements set out in Chapter 2 of this Title. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2). 2. The Commission, when preparing the common specifications referred to in paragraph 1, shall gather the views of relevant bodies or expert groups established under relevant sectorial Union law. 3. High-risk AI systems which are in conformity with the common specifications referred to in paragraph 1 shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those common specifications cover those requirements. 4. Where providers do not comply with the common specifications referred to in paragraph 1, they shall duly justify that they have adopted technical solutions that are at least equivalent thereto.

There is some inconsistency with regard to the potential scope of harmonised standards. Article 9 AIA-P alone refers to harmonised standards as a tool to concretise risk management systems. There is no reference to harmonised standards with regard to:

- Article 10 (data governance),
- Article 11 (technical communication),
- Article 12 (record keeping),
- Article 13 (transparency and information for users),
- Article 14 (human oversight), and
- Article 15 (accuracy, robustness and cybersecurity).

This reads as if there is no room for harmonised European standards beyond Article 9, which sounds surprising. On the other hand, Article 40 refers as a whole to Chapter 2, which covers Articles 6–15. A further inconsistency results from Article 17 on quality management systems, which belongs to Chapter III but refers to harmonised standards. It will have to be shown that the European Commission mandates harmonised standards independently of whether they are explicitly mentioned or not.¹⁸⁵

¹⁸⁵ Under IV. 4. and 5.

The very same inconsistency is transferred to the residual power of the European Commission in Article 41 AIA-P to elaborate technical standards itself through so-called ‘common specifications’, which should not be mixed up with ‘technical specifications’. The latter is a kind of umbrella term for national standards, non-harmonised European and international standards, or individual technical specifications. Article 3 (2) AIA-P provides a definition for common specifications:

common specifications’ means a document, other than a standard, containing technical solutions providing a means to, comply with certain requirements and obligations established under this Regulation;

This is a posh way of describing the fact that the European Commission is taking into its own hands development of the rules that concretise binding legal requirements. Two questions immediately emerge – when and how? The ‘when’ is rather vaguely defined in Article 41 AIA-P which grants the European Commission three options: a) harmonised standards do not exist, b) harmonised standards are insufficient, c) there is a need to address specific safety or fundamental right concerns. In a non-paper,¹⁸⁶ which is circulated widely but not officially accessible, the European Commission clarifies – at least to some extent – the background and reasons behind fall-back competence. The non-paper spells out the context. This is not the first time that the European Commission has been granted such a competence. There are rules in place with regard to fertiliser products, medical devices and web-accessibility laws. So far, however, the Commission has never initiated or adopted common specifications via implementing acts. The non-paper equally mentions the various proposals under way where such a competence will be introduced, in between the AIA-P.¹⁸⁷

Of particular relevance are attempts to specify the substantive and procedural requirements which have to be met in order to activate the mechanism. The non-paper refers to Article 291 TFEU, the Comitology procedure, and the opportunity for stakeholders to comment on a draft implementing act. The Commission promises to inform the Committee on Standards and the recently established High Level Forum on Standardisation.¹⁸⁸ The conditions would be as follows:

1. There is no reference to harmonised standards already published in the Official Journal of the European Union related to the essential requirement(s), unless the harmonised standard in question is an existing standard that must be revised; and

¹⁸⁶ Non-paper-horizontal approach on common specifications complementary to harmonised European standards (on file with the author. The non-paper does not have an author and does not indicate the date).

¹⁸⁷ 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); Proposal for a Regulation concerning batteries and waste batteries, repealing Directive 2006/66/EC and amending Regulation (EU) No 2019/1020 (COM/2020/798); Proposal for a Regulation of the European Parliament and of the Council on machinery products (COM(2021)202), Proposal for a Regulation on the internal markets for renewable and natural gases and for hydrogen (recast) (COM(2021) 804); Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) (COM(2022) 68); Proposal for a Regulation establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC (COM(2022) 95); but not Proposal amending Regulations (EU) 2016/424, (EU) 2016/425, (EU) 2016/426, (EU) 2019/1009 and (EU) No 305/2011 as regards emergency procedures for the conformity assessment, adoption of common specifications and market surveillance due to a Single Market emergency.

¹⁸⁸ https://single-market-economy.ec.europa.eu/single-market/european-standards/standardisation-policy/high-level-forum-european-standardisation_en

2. The Commission has requested one or more European standardisation organisations to draft a harmonised standard for the essential requirement(s)

3. And one of the following conditions must be fulfilled: a) The request has not been accepted by any of the European standardisation organisations; or b) There are undue significant delays in the establishment of an appropriate harmonised standard; or c) The standard provided does not satisfy the requirements of the relevant EU legislation, or does not comply with the request of the Commission.

The non-paper mentions three examples where a request by the European Commission to elaborate such a standard suffers from significant delay – helmets for equestrian activities (since 1995); particular requirements for grills, toasters and similar portable cooking appliances (since 2014), and pyrotechnic firework items (since 2007). The very last condition 3.c) which is of relevance in our context is complemented via a rather cryptic footnote:

In some emerging areas (e.g. standards dealing with fundamental rights), given that the full ability and competence of standardisation organisations remains to be fully assessed, the conditions for invoking the Commission's empowerment to opt for common specifications may need to be set in a more flexible manner.

The message seems to be that the European Commission is ready to provide the ESOs with some credit to develop the necessary competences in the field of fundamental rights and will adopt a rather lenient approach. Last but not least, the European Commission points in Annex III of the Non-Paper to a more sophisticated ruling in the upcoming revision of the Machinery Directive, on which a political agreement between the Council and the European Parliament was reached in December 2022.¹⁸⁹ It might very well be that the compromise found in the Machinery Directive will set the benchmark in the upcoming finalisation of the AIA-P. However, the version to which the non-paper refers¹⁹⁰ focuses entirely on the conditions under 3a) and 3b) but does not provide guidance on the conditions under which the European Commission may mobilise fundamental rights in order to justify adoption of common specifications.

d) Common Specifications – Conflicts of Interest

Positions on the residual powers of the European Commission differ widely. The ESOs are quite critical because the requirements spelt out in the existing and envisaged legislation provide the European Commission with considerable discretion: 'Commissioner Breton is a control freak'.¹⁹¹ The only measurable exception is rejection of a standardisation request. Past experience demonstrates that the ESOs may delay elaboration of standards for decades without having to fear

¹⁸⁹ https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7741

¹⁹⁰ 3. The Commission is empowered to adopt implementing acts establishing common specifications to cover the essential health and safety requirements set out in Annex III where the following conditions have been fulfilled: (a) no reference to harmonised standards covering the relevant essential health and safety requirements set out in Annex III is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012; (b) the Commission has requested, pursuant to Article 10(1) of Regulation 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the essential health and safety requirements set out in Annex III (c) the request referred to in point (b) has not been accepted by any of the European standardisation organisations or the European standards or the European standardisation deliverables addressing that request is not delivered within the deadline set in accordance with article 10(1) of Regulation 1025/2012 or European standardisation deliverables does not comply with the request.

¹⁹¹ Interviews with representative from the ESOs.

implementing acts. The most problematic requirement seems to be the potential threat that the elaborated standard ‘does not satisfy the requirements of the relevant EU legislation’. The high rejection rate mentioned in the E&Y report does not clarify whether compliance with EU law or compliance with the mandate stood in the way. It seems fair to assume that all depends on the background of the HAS consultant: a lawyer will look into legal compliance with the mandate, and a computer scientist into technical compliance therewith. However, it seems that HAS consultants are mostly technical experts.

Here we are back to the responsibilities of the European Commission under Article 10 (6) Regulation 1025/2012 in assessing compliance prior to publication in the Official Journal. Integration of fundamental rights in the standardisation process enhances the legalisation and the judicialisation of technical standards far beyond health and safety issues. Legalisation and judicialisation, in sum juridification, takes autonomy away from the ESOs and strengthens the power of the European Commission. If, however, the European Commission opts for a common specification, it has to undergo the whole legislative procedure, including impact assessment and even public consultation.¹⁹² In the interviews, the ESOs expressed concern that DG GROW might set an end to co-regulation and co-operation between the European Commission and the ESOs and, instead, put standardisation under the tutelage of the European Commission as a whole, very much in line with the French approach.¹⁹³

On the other end of the spectrum are the civil society organisations, which are critical of stretching technical standards to fundamental rights, arguing that the decision over the degree to which technical standards comply with fundamental rights must be left to the democratic organs of the EU or the Member States. In a joint statement, BEUC and ANEC argue – and find support in legal scholarship – that a red line needs to be drawn between technicalities and political issues: the first might be delegated to self-regulatory bodies; the second should remain in the hands of democratic institutions.¹⁹⁴

Harmonised standards must not be used to define or apply fundamental rights, legal or ethical principles. Their use should be limited to implement technical aspects. In this regard, a standard should, for example, not be used to determine what types of biases are prohibited under Art. 10 (2) f) (and Art. 10 (4)).¹⁹⁵

Article 10 (2) f) and (4) serve as an example which underpins the problem:

We think that technical standards are not the right tool to define what type of biases are prohibited and how they should be mitigated under (Art. 10 (2) f)) or the determination of specific geographical, behavioural or functional setting of training data sets (art 10.4). Standards can be used and are used to determine the safety and performance requirements of a fridge or an oven in terms of surface temperature or energy use. The performance and outcome of an AI system depend not only on its technical components, but on decisions about who uses the technology

¹⁹² Interview with representative from the stakeholder organisations.

¹⁹³ Particularly outspoken ETSI, see on AFNOR under II 2 d) aa).

¹⁹⁴ BEUC, Regulating AI to Protect the Consumer, Position Paper on the AI Act, 7.10.2021 in particular under 9 at 25, co-authored with ANEC https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf

¹⁹⁵ ANEC Position Paper, ANEC amendments for the European Commission proposal for an Artificial Intelligence Act (Regulation laying down harmonised rules on artificial intelligence and amending certain Union legislative acts) COM(2021) 206 final, 2021/0106 (COD) at 7.

for what purpose, in what context. These decisions have the potential to involve and impact on fundamental rights.

The two position papers do not discuss the role and function of the common specifications in detail, and neither of them questions the usefulness of standardisation in general or of the ESOs in particular. The perception within the European Commission and the ESOs seems to be that they are in favour of having a strong stick behind the door.¹⁹⁶ Tensions between the ESOs and the European Commission are obvious. The more detailed the standardisation request, the lesser the preparedness of the ESOs to accept the proposal. The standardisation request on the Radio Equipment Directive is referred to as an example of where the European Commission has gone too far. In the words of an interviewee from business:¹⁹⁷ *‘they are so detailed that the Commission might as well have written the standard itself’.*

Consumer organisations insist on the need to strengthen the inclusiveness of stakeholder organisations in the standard-setting process through the introduction of two separate paragraphs in Article 40 AIA-P:¹⁹⁸

3. When requesting the drafting of European standards or European standardisation deliverables in accordance with Article 10 of Regulation (EU) 1025/2012, the European Commission shall request to the European Standardisation Organisations to provide evidence of the effective participation of civil society stakeholders, including consumer organisations, in the standardisation procedures both at the national and European levels.

4. Member States shall support the participation of public authorities and civil society stakeholders, including consumer organisations, in the standardisation procedures at the national level.

The proposal has found support in the EP committee on Legal Affairs and it remains to be seen what the final version of Article 40 AIA-P will look like. Inclusiveness would remain crucial even if the European Commission made use of its powers. Whether their chance of influencing the outcome is increased, and whether common specifications are ‘better’ than European harmonised standards would be the subject of research in each particular case. However, more ‘state’ does not automatically lead to increased consumer protection.

The elephant in the room – harmonised standards vs. common specifications – is not openly addressed. Has the European Commission the necessary resources and skills to develop common specifications independently and separately from the ESOs? The born candidate, mentioned in the interviews,¹⁹⁹ would be the Joint Research Centre, which claims on its website to provide *‘independent, evidence-based knowledge and science, supporting EU policies to positively impact society’*.²⁰⁰ The JRC was established in 1958 and operates as a separate entity of the European Commission with its own Commissioner and its own infrastructure, spread over several Member States. The 2021 report indicates that the JRC had 2752 staff members and a budget of EUR 131.4 million, of which 121 million came from European Commission

¹⁹⁶ Interviews with representatives from the European Commission and the ESOs.

¹⁹⁷ Interview with representative of the business sector.

¹⁹⁸ ANEC position paper (n 196), at 6.

¹⁹⁹ Interview with representative from the European Commission.

²⁰⁰ https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/joint-research-centre_en

services.²⁰¹ Two possible units could in theory undertake standardisation work – information society and standards. However, development of common specifications is hardly possible without a drastic budget increase and maybe establishment of a new unit in one of the EU Member States. Instead of mandating elaboration of harmonised standards and co-financing the ESOs, the European Commission would then have to conclude a contract with the JRC. A serious commitment by the European Commission to make use of its residual powers would therefore quite necessarily lead to a downgrading of the ESOs, in particular of CEN-CENELEC, which most benefit from EU subsidies. Whilst it might be that the European Commission will occasionally use its residual powers, it is hard to imagine that the European Commission is ready to take over production of AI standards.

e) Conformity Assessment, Self- and Third-party Certification

The AIA-P devotes particular attention to the conformity assessment procedure for high-risk AI systems in its two variations: self-certification and third-party certification. ‘Conformity assessment’ shows up 104 times in the document. The related rules (Article 43 AIA-P) are comprehensive and burdensome. They can be fulfilled by the big providers and users of AI systems, but render the lives of small companies and start-ups difficult.²⁰² In the language of the AIA-P, high-risk systems will have to comply with:

*a set of horizontal requirements for trustworthy AI. Predictable, proportionate and clear obligations are also placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems’ lifecycle.*²⁰³

Whether self-certification provides for consumer protection is subject of controversy.

When it comes to the distinction between self-certification and third-party certification, different rules apply to high-risk AI systems which are safety components of products or standalone AI systems. In the former group, the existing third-party certification is extended beyond product safety towards protection against physiological and psychological harm and respect for human rights.²⁰⁴ The notified bodies (Article 33 AIA-P) – the certification bodies – have to build competences far beyond product safety and enter into entirely new areas of skills to assess not only physiological harm – which comes close to protection against unsafe products – but also to handle psychological harm. Here, very different skills are needed. Are the notified bodies now required to hire psychologists and human rights lawyers who are familiar with the growing intricacies of the Charter of Fundamental Rights? Is this for the EU legislature to request? The AIA-P seems to take it for granted, although the European Commission is aware that additional resources are needed.²⁰⁵ In the latter group – the standalone AI systems where little to no experience exists – self-certification is the rule, Article 40 AIA-P. The only exceptions are remote biometric identification systems, Article 43 (1) Annex VII AIA-P. Recital 64 states:

²⁰¹ <https://publications.jrc.ec.europa.eu/repository/handle/JRC128620>

²⁰² On this aspect in particular P Palka, Algorithmic Central Planning: Between Efficiency and Freedom, Law and Contemporary Problems, Vol 83, No. 2, 125–149

²⁰³ Explanatory Memorandum at 4.

²⁰⁴ Explanatory Memorandum at 5 and rec 30, where the products are listed.

²⁰⁵ Explanatory Memorandum at 15 ‘The conformity assessment approach aims to minimise the burden for economic operators as well as for notified bodies, whose capacity needs to be progressively ramped up over time.’

Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for the remote biometric identification of persons, for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.

The design of the different conformity requirements for AI systems as safety components and standalone systems leads to a paradoxical result: third-party assessment might have a role to play in the ‘old’ industries, where technology is an ‘add-on’, whereas third-party assessment has practically no role in the world of the new risks – physiological and psychological harm and protection of fundamental rights. There is an obvious imbalance between the role of third-party assessment in product regulation and standalone technology. The rather liberal self-assessment, this is the idea, is to be compensated through appropriate enforcement mechanisms and establishment of a European Commission-run European ‘registry’ (Article 51):²⁰⁶

A comprehensive ex-ante conformity assessment through internal checks, combined with a strong ex-post enforcement, could be an effective and reasonable solution for those systems, given the early phase of the regulatory intervention and the fact the AI sector is very innovative and expertise for auditing is only now being accumulated. After the provider has performed the relevant conformity assessment, it should register those stand-alone high-risk AI systems in an EU database that will be managed by the Commission to increase public transparency and oversight and strengthen ex post supervision by competent authorities.

The AIA-P relies on strong – these are the words – public enforcement mechanisms. The Member States are in charge of providing the necessary resources. Regulation of enforcement and potential implementation in the Member States deserves a separate analysis.²⁰⁷ Experience with the GDPR demonstrates that common fully-harmonised rules in no way guarantee uniform enforcement.²⁰⁸ What matters, though, is that non-governmental organisations, such as consumer organisations, have no role to play in enforcing the AIA-P. The AIA-P is not added to the list of EU legislation under which they can take representative action.

Despite the rather limited importance of third-party conformity assessment, the AIA-P contains a comprehensive set of rules on notified bodies in Article 33 AIA-P for those located in the EU, and in Article 39 AIA-P for those outside the EU. Of the many detailed rules, three are of particular interest from a consumer perspective:

Article 33 Notified bodies

*5. Notified bodies shall be organised and operated so as to safeguard the **independence, objectivity and impartiality of their activities** (emphasis added). Notified bodies shall document*

²⁰⁶ Explanatory Memorandum at 15.

²⁰⁷ BEUC Strengthening the Coordinated Enforcement of Consumer Protection Rules, Revision of Consumer Protection Coordination (CPC) Regulation, December 2022, https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-135_Strengthening_the_coordinated_enforcement_of_consumer_protection_rules.pdf

²⁰⁸ U Pahl, Die Realität der Rechtsdurchsetzung im Datenschutz – bisher noch keine Erfolgsgeschichte für Verbraucher, Verbraucher und Recht 2020, 361.

and implement a structure and procedures to safeguard impartiality and to promote and apply the principles of impartiality throughout their organisation, personnel and assessment activities.

8. Notified bodies shall take out **appropriate liability insurance** (emphasis added) for their conformity assessment activities, unless liability is assumed by the Member State concerned in accordance with national law or that Member State is directly responsible for the conformity assessment.

10. Notified bodies shall have sufficient internal competences to be able to effectively evaluate the tasks conducted by external parties on their behalf. To that end, at all times and for each conformity assessment procedure and each type of high-risk AI system in relation to which they have been designated, the notified body shall have **permanent availability of sufficient administrative, technical and scientific personnel who possess experience and knowledge relating to the relevant artificial intelligence technologies**, (emphasis added) data and data computing and to the requirements set out in Chapter 2 of this Title.

There is a lot to say on ‘independence and impartiality’, let alone on responsibility and liability.²⁰⁹ The AIA-P uses similar language in terms of legal requirements of regulatory agencies that control and supervise so-called regulated markets. Does it make sense at all to expect from profit-run companies to be ‘impartial’? The AIA-P contributes to a further blurring of the limits between public and private responsibilities. A second even more important weakness results from the lack of mandatory liability insurance. The European Commission does not seem ready to learn the lessons from the PIP scandal,²¹⁰ let alone a debate on the insufficiencies of the Product Liability Directive, which does not cover certification bodies.²¹¹ The AIA-P, similarly to the New Approach directives, delegates the responsibility for the availability of appropriate insurance and liability rules to the Member States – with disastrous effects for all those who have been affected by the insufficient and light-handed shaping of the conformity obligations in the Medical Devices Directive 93/42/EC.

The AIA-P is more outspoken on the skills needed by certification bodies other than Regulation 1025/2012 on the ESOs. One might read into Article 33 AIA-P the requirement that the certification bodies need to have fundamental rights lawyers and psychologists.

2. CRA-P and Harmonised Standards

The CRA-P follows in large parts the regulatory rationale of NLF just as the AIA-P, in the choice of a risk-based approach, in the key role of harmonised standards and self and/or third-party certification to guarantee access to the Internal Market.

(38) In order to facilitate assessment of conformity with the requirements laid down by this Regulation, there should be a presumption of conformity for products with digital elements which are in conformity with harmonised standards, which translate the essential requirements of this Regulation into detailed technical specifications, and which are adopted in accordance with

²⁰⁹ C Glinski, Haftungsrechtlicher Rahmen von nachhaltiger Zertifizierung in textilen Lieferketten, Gutachten im Auftrag des VZBV, 2021.

²¹⁰ P Rott (ed) Certification – Trust, Accountability, Liability, Springer 2018.

²¹¹ H-W Micklitz/ N Reich/ L Boucon, L’Action de la victime contre l’assureur du producteur RIDE, 2015, 37–68.

Regulation (EU) No 1025/2012 of the European Parliament and of the Council. Regulation (EU) No 1025/2012 provides for a procedure for objections to harmonised standards where those standards do not entirely satisfy the requirements of this Regulation.

(45) As a general rule the conformity assessment of products with digital elements should be carried out by the manufacturer under its own responsibility following the procedure based on Module A of Decision 768/2008/EC. The manufacturer should retain flexibility to choose a stricter conformity assessment procedure involving a third-party. If the product is classified as a critical product of class I, additional assurance is required to demonstrate conformity with the essential requirements set out in this Regulation. The manufacturer should apply harmonised standards, common specifications or cybersecurity certification schemes under Regulation (EU) 2019/881 which have been identified by the Commission in an implementing act, if it wants to carry out the conformity assessment under its own responsibility (module A). If the manufacturer does not apply such harmonised standards, common specifications or cybersecurity certification schemes, the manufacturer should undergo conformity assessment involving a third party. Taking into account the administrative burden on manufacturers and the fact that cybersecurity plays an important role in the design and development phase of tangible and intangible products with digital elements, conformity assessment procedures respectively based on modules B+C or module H of Decision 768/2008/EC have been chosen as most appropriate for assessing the compliance of critical products with digital elements in a proportionate and effective manner. The manufacturer that carries out the third-party conformity assessment can choose the procedure that suits best its design and production process. Given the even greater cybersecurity risk linked with the use of products classified as critical class II products, the conformity assessment should always involve a third party.

The proposal distinguishes between ‘non-critical’, ‘critical’ and ‘highly critical’ products Article 3 (3) and (4). For each of them, the proposal lays down particular criteria in Article 6 (2) and 6 (5) CRA-P respectively. Similar to the AIA-P, the relevant product categories are transferred to an Annex which can be amended through implementing acts or, in the case of highly critical products, through delegated acts, Article 50 CRA-P. The category of ‘critical’ products is broken down into Class I and Class II, the latter representing a greater cybersecurity risk. This means there are three categories of risks, which remain under-defined – non-critical, critical and highly critical. Chapter II deals with the various economic operators, manufacturers, authorised representatives, importers, and distributors as well as their particular obligations, Chapter III with conformity of products with digital elements, with technical documentations Article 24 CRA-P and the conformity assessment procedure in Article 25 CRA-P. What is missing, though, are rules that clearly define the different risk categories and lay down criteria for a risk assessment methodology which takes the consumer concerns fully into account, such as:

the sensitivity of the data processed by these products, the risks entailed by their normal use, but also the potential dangers that these devices may represent in case of a successful cyberattack, including potential physical harm for consumers.²¹²

a) Consumer Protection – Missing

The major purpose of the CRA-P is to establish horizontal requirements ‘on products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect

²¹² BEUC 24.1.2023, The Cyber Resilience Act Proposal, BEUC position paper, https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-006_The_Cyber_Resilience_Act_Proposal.pdf, under 5.1. at 15

logical or physical data connection to a device or network' Article 2 (1) CRA-P.²¹³ The horizontal scope is meant to overcome deficits of the current piecemeal approach, which triggered strong criticism by ENISA²¹⁴ and by consumer associations.²¹⁵ The Proposal provides a broad definition, namely '*any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately*', Article 3 (1) CRA-P. The proposal covers consumer products.²¹⁶ Non-embedded software is included, against the resistance of DigitalEurope, but not (or not fully) software-as-a-service or websites (digital cloud services) despite BEUC's advocacy to do so.²¹⁷ The Proposal does not apply to products with digital elements which already fall within the scope of Regulation (EU) 2017/745 (Medical Devices Regulation), Regulation (EU) 2017/746 (Regulation on in vitro diagnostic medical devices) or Regulation (EU) 2019/2144 (Automotive type-approval general regulation), or products that have been certified in accordance with Regulation (EU) 2018/1139 (Common rules in civil aviation).

The scope of the CRA-P is defined through the category of products. The addressees are 'economic operators' as defined in Article 3 (17) CRA-P. Consumers are concerned but they are not addressed directly and that is why the CRA-P does not grant consumer rights. What matters is the *sedes materiae*. Going through Annex III is a déjà-vu. Consumer products are largely absent from the two risk classes. Just as in the AIA-P, consumer products are regarded as non-critical and are not subject to preventive risk management. The promising definition in Article 2 (1) CRA-P 'on the foreseeable misuse' comes to nothing. BEUC has come up with a list of products that should be put under Class II so as to ensure preventive protection, instead of waiting for incidents which could be remedied only through the market surveillance authorities:²¹⁸

Private security devices e.g. smart security alarms, smart smoke detectors or carbon monoxide alarms, digital door locks, security cameras and private surveillance equipment.

Smart home devices e.g. electricity control, heating or cooling appliances or ventilation in smart homes.

Connected toys and other devices intended to interact with children e.g. toys relying on active connection to function, baby monitors, educational devices and wearables for children.

Health appliances and wearables e.g. fitness trackers, smart watches, panic buttons, wearables for minors.

Currently, the four categories are not addressed: if anything, they have to be squeezed into the enumerated products by way of stretching their meaning.

²¹³ For an overview, P G Chiara, The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements, *Int Cybersec Law Rev.* (2022) 3:255–272.

²¹⁴ <https://www.enisa.europa.eu/about-enisa/structure-organisation/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019>

²¹⁵ Overview in BEUC 24.1.2023, The Cyber Resilience Act Proposal (n 213) under section 3.

²¹⁶ Rec 8.

²¹⁷ BEUC 24.1.2023, The Cyber Resilience Act Proposal (n 213) at 6 under reference to an impressive survey by the German Consumer Organisation, VZBV.

²¹⁸ BEUC 24.1.2023, The Cyber Resilience Act Proposal (n 213), under 5.4. at 18 where each of the four categories is explained and where evidence is presented.

b) Fundamental Rights – Less Prominent but Still Underdeveloped

All in all, fundamental rights rhetoric is much less developed than in the AIA-P. If anything, the CRA-P speaks of fundamental rights but without distinguishing between the various rights and principles (Article 38) granted in the CEUFR. This equally means that there is no space to introduce the economic interests of consumers. If anything, the position of consumers will be improved through enhancing protection against security risks, and against risks to health and safety. Conceptually speaking, the CRA-P is closer to product safety regulation with a particular emphasis on cybersecurity.

There is a difference between the Explanatory Memorandum and the text of the Proposal itself²¹⁹ in terms of fundamental rights. The Explanatory Memorandum mentions health, safety, and fundamental rights, though in a rather biased way, which goes along with the deficient consumer dimension. It suffices to contrast the statement on added value for consumers with added value for business:²²⁰

In the context of the various policy options, here option 4 advocating a regulation: Consumers and citizens would also benefit from better protection of their fundamental rights, such as privacy and data protection

*In the discussion of fundamental rights: All policy options are expected to enhance to a certain extent the protection of fundamental rights and freedoms such as privacy, protection of personal data, freedom to conduct business and protection of property or personal dignity and integrity. In particular the preferred policy option 4 ...would ...raise trust among users and the attractiveness of EU products with digital elements as a whole, **thus protecting the property and improving the conditions for economic operators to conduct business.** (emphasis added).*

The text of the CRA-P remains behind such language. Recitals 58 and 59 deal with the ex-post management of potential risks to fundamental rights. The CRA-P distinguishes between ‘products with digital elements’ and ‘products which present a significant cybersecurity risk’.²²¹ With regard to the former, the prime responsibility for monitoring the market and taking appropriate measures, like a product recall, lies with the Member States’ market surveillance authorities. If a Member State takes action, it has to notify the European Commission, which will then set coordination with the other Member States into motion. In the latter case:

the Commission may request ENISA to carry out an evaluation. Based on that evaluation, the Commission may adopt, through implementing acts, corrective or restrictive measures at Union level, including ordering withdrawal from the market, or recalling of the respective products, within a reasonable period, commensurate with the nature of the risk. The Commission may have recourse to such intervention only in exceptional circumstances that justify an immediate intervention to preserve the good functioning of the internal market, and only where no effective measures have been taken by surveillance authorities to remedy the situation. Such exceptional circumstances may be emergency situations where, for example, a non-compliant product is widely made available by the manufacturer throughout several Member States, used also in key sectors by entities under the scope of [Directive XXX / XXXX (NIS2)], while containing known vulnerabilities that are being exploited by malicious actors and for which the manufacturer does

²¹⁹ Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 Brussels, 15.9.2022, COM(2022) 454 final.

²²⁰ At 8.

²²¹ As defined in Art 3.

not provide available patches. The Commission may intervene in such emergency situations only for the duration of the exceptional circumstances and if the non-compliance with this Regulation or the important risks presented persist.

The various obligations imposed on economic operators do not refer to respect for fundamental rights, in contrast to respect for health and safety, which are explicitly mentioned, Article 10 (2) CRA-P. However, Article 46 CRA-P obliges the market surveillance authority to secure respect for fundamental rights.

c) Common Specifications – Without Compensating for Risks to Fundamental Rights

Just like the AIA-P, the CRA-P builds a safety net which empowers the European Commission to adopt implementing acts, subject to certain conditions.

Article 19 Common specifications

Where harmonised standards referred to in Article 18 do not exist or where the Commission considers that the relevant harmonised standards are insufficient to satisfy the requirements of this Regulation or to comply with the standardisation request of the Commission, or where there are undue delays in the standardisation procedure or where the request for harmonised standards by the Commission has not been accepted by the European standardisation organisations, the Commission is empowered, by means of implementing acts, to adopt common specifications in respect of the essential requirements set out in Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 51(2).

There is a difference with regard to the AIA-P, though. Article 19 CRA-P does not empower the European Commission to adopt implementing acts if fundamental rights are at risk.²²²

d) Conformity Assessment – Self-Assessment by the Back Door

Compliance with harmonised standards is the key to gaining access to the market. Within the scope of the CRA-P three different types of compliance must be distinguished – self-certification through the economic operator, third-party certification and European Cybersecurity Certification, called CSA certification.²²³ The latter provides for the highest standards of control as the laboratories in charge are not only obliged to check the functionality of the product but also to hack the device, so-called ‘penetration testing’. ENISA in co-operation with national cybersecurity authorities and stakeholders elaborates a common scheme that has to be applied whenever a CSA certification is required.²²⁴

The CRA-P in its current form understands consumer products mainly as being non-critical, so that self-certification suffices. But even if consumer products were to be upgraded to ‘critical’, there is no need for economic operators to mandate third-party certification bodies. Annex III distinguishes between Class I products (critical) and Class II (highly critical). Only if consumer products were to come under Class II, economic operators are required to use third-party

²²² BEUC 24.1.2023, The Cyber Resilience Act Proposal (n 213) under 4.3. (joint statement of BEUC and ANEC) The Role of Standards in ensuring cybersecurity for consumers at 14

²²³ P G Chiara (n 214) at 262.

²²⁴ <https://www.enisa.europa.eu/topics/incident-response/glossary/vulnerabilities-and-exploits>

assessment. Class I products remain subject to self-certification with harmonised standards, thereby establishing a presumption of conformity, Article 24 (2) CRA-P. This is what BEUC/ ANEC call ‘self-assessment by the backdoor’.²²⁵ CSA certification applies neither to Class I nor to Class II. However, Article 18 (4) CRA-P empowers the Commission:

by means of implementing acts, to specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts thereof as set out in Annex I.

Thereby certification schemes are put on equal footing with harmonised standards. Schemes can also provide a presumption of conformity, although the making of certification schemes is completely different and if certification is done at ‘high’ level it is fair to assume that the level of security is probably higher than what harmonised standards might offer.

The Impact Assessment of the CRA-P delivers insights on the conflicts running around the choice of the appropriate certification scheme and the potential costs of third-party assessment.²²⁶ BEUC argues in its position paper on the CRA-P that the European Commission estimates that 90 % of the products covered by the Proposal require self-assessment only. In light of the potential harm that cyber-attacks may cause to consumers, this statement does not sound reassuring, in particular as consumer products are not (or are but only to a limited extent) covered.²²⁷ BEUC calls for classification of certain consumer products as high-risk products with the consequence that third-party assessment would be mandatory. Even such an upgrade does not guarantee penetration testing. BEUC’s concerns equally affect products and services that come under the AIA-P.

3. DSA and Non-harmonised European Standards

The DSA was published in the OJ on the 22.10.22. In contrast to the AIA-P and the CRA-P, the DSA does not apply a risk-based approach, which classifies products/technologies according to the risks they produce to health, safety and fundamental rights. Therefore, the DSA does not follow the New Legislative Framework. The DSA mirrors the regulatory rationale of EU Digital Policy Legislation – harmonised European standards will guarantee an adequate level of protection against risks to health and safety, whereas voluntary standards (non-harmonised European standards) suffice when it comes to protection of economic interests in the framing of the market order. Non-harmonised European standards together with due diligence and self-regulatory mechanisms indicate a change in the design of consumer law and policy, a design which could be characterised through a certain tendency towards privatisation.

Conceptually the DSA comes closer to the DMA in its focus on regulating the rights and obligations of particular actors, which due to their size are claimed to legitimise legislative intervention. The DSA distinguishes between different types of intermediaries – SMEs, large online platforms (LOP) and very large online platforms (VLOP) – linking the scope and depth of obligations to the size of the company. EU legislation sets a precedent which has no counterpart in the consumer acquis. EU consumer rights and obligations do not differentiate between the addressees. But

²²⁵ Information from BEUC/ANEC.

²²⁶ <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment>

²²⁷ BEUC 24.1.2023, The Cyber Resilience Act Proposal (n 213) under 4.1. at 11.

even if a differentiation exists, as with the UCPD and the laws of the regulated market, rights and duties remain the same.²²⁸ In a more hidden form one might also detect risk-based thinking in the DSA. The VLOPs are qualified as potential producers of systemic risks. So far one might classify the DSA as risk-based, but here the reference point is not the category of product as in the AIA-P and the CRA-P but, rather, the size of the company.

a) Consumer Protection – Incomplete and Privatised

Recital (3) of the DSA expresses the spirit of the regulation and the aim to be achieved:

(3) Responsible and diligent behaviour by providers of intermediary services is essential for a safe, predictable and trustworthy online environment and for allowing Union citizens and other persons to exercise their fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union (the ‘Charter’), in particular the freedom of expression and of information, the freedom to conduct a business, the right to non-discrimination and the attainment of a high level of consumer protection.

Seen through the lenses of the distinction between safety-related and non-safety-related economic consumer policy issues, the DSA is to be situated on the economic side. Health, if it shows up at all, is mainly related to public health but without providing for a definition, and consumer safety is taken care of only randomly. Thus far one might understand the DSA as the economic complement to the health-and-safety-related AIA-P and CRA-P. In the field of economics – this is the message the DSA sends – there is no room:

- for health-and-safety-related harmonised standards;
- for strong involvement by the European Commission;
- for public finance or for public oversight.

The DSA leaves more space to ‘freedom to do business’ and therefore limits itself, either to imposing duties on the various addressees of the obligations, or to encouraging them to take voluntary measures and to establish and ensure self-compliance – towards ‘recipients’ and/or ‘consumers’, Article 3 (b) and c) DSA. Recipients are natural and legal persons who use an intermediary service. ‘Consumer’ is defined in line with the rather classic definition which dominates the core of European consumer law, namely a natural person who is acting outside their own business.

In order to understand the systemic positioning of technical standards in the DSA, it is necessary to put the rules into the context of Chapter II on liability and Chapter III on due diligence. The context tells the message and makes abundantly clear that the different rules read together draw a rather harsh line between risks to health and safety, which deserve much tighter public scrutiny, and risks to economic interests which are of less concern:

(102) To facilitate the effective and consistent application of the obligations in this Regulation that may require implementation through technological means, it is important to promote voluntary standards covering certain technical procedures, where the industry can help develop standardised means to support providers of intermediary services in complying with this Regulation, such

²²⁸ For an attempt to differentiate H-W Micklitz, *The Politics of Justice in European Private Law*, CUP 2018, at 281.

as allowing the submission of notices, including through application programming interfaces, or standards related to terms and conditions or standards relating to audits, or standards related to the interoperability of advertisement repositories. In addition, such standards could include standards related to online advertising, recommender systems, accessibility and the protection of minors online. Providers of intermediary services are free to adopt the standards, but their adoption does not presume compliance with this Regulation. At the same time, by providing best practices, such standards could in particular be useful for relatively small providers of intermediary services. The standards could distinguish between different types of illegal content or different types of intermediary services, as appropriate.

This is a large programme which interferes in each and every corner of the DSA. Chapter II on ‘the liability of providers of intermediary services’ puts potential illegal content at centre stage: conduit, caching, hosting, the scope of investigation duties, orders to act and to provide information. Illegal content – all this follows from the definition in Article 3 (h) in combination with Recital 12 and may result from infringement of consumer laws too. But what if the obligations under the DSA are concretised through non-harmonised European standards which impact consumers? Can a possible non-compliance infringement of a non-harmonised European standard be regarded as an infringement of the DSA? It should be recalled that compliance with non-harmonised European standards does not lead to a presumption of conformity.

Chapter III deals with ‘*due diligence obligations for a transparent and safe online environment*’. Setting aside Chapter IV on enforcement, Chapter III is by far the most relevant not only for consumers but also for business. It is broken down into six subsections, many (if not most of them) concerning consumers. The perspective is always the same: the EU legislature imposes obligations or encourages elaboration of non-binding self-regulation, while the addressees have to implement them through appropriate measures. The DSA does not define ‘due diligence’ but takes its meaning for granted. The DSA subsumes all sorts of obligations under that category:

- to deliver fair contract terms;
- not to mislead and deceive;
- to provide in-house complaint handling and ODR mechanisms, and
- to develop non-harmonised European standards.

Understanding non-harmonised European standards as being an integral part of due diligence obligations looks like a novelty in EU legislation. There is a tendency to privatise consumer law in the DSA. Getting to grips with the true meaning of all the due diligence obligations is rendered more difficult through the differentiation between the various addressees, SMEs – which are largely excluded – LOPs and VLOPs:

Subsection 1 one deals with ‘provisions to all providers of intermediary services (inter alia terms and conditions, Art. 14 DSA);

Subsection 2 ‘with provisions applicable to providers of hosting services, including online platforms’ (notice and action mechanism, inter alia of criminal offences);

Subsection 3 with ‘additional provisions to provide online platforms with the exclusion of SMEs (inter alia internal complaint handling Art. 20 DSA, out of court dispute settlement Art. 21 DSA, trusted flaggers Art 22 DSA, protection against misuse, Art. 23 DSA, transparency reporting Art 24 DSA, online interface design and organisation Art. 25 DSA, advertising, Art. 26 DSA, recommender system Art. 27 DSA, online protection for minors Art. 28 DSA);

Subsection 4 'additional provisions to providers of online platforms allowing consumers to conclude distance contracts' again under exclusion of SMEs, (traceability Art. 30 DSA, compliance by design Art. 31 DSA, right to information Art. 32 DSA);

Subsection 5 'additional obligations for very large online platforms and of very large online search engines to manage system risks', systemic risk assessment Art. 34 DSA (broken down into four categories, one of which is the risk to the infringement of fundamental rights, including those of the consumers, minors and the physical and mental well-being.²²⁹ Recital 83 refers to minors in particular, mitigation of risks Art. 35 DSA, crisis response mechanisms, Art. 36, independent audits, Art. 37 DSA, recommender systems Art. 38 DSA, additional online advertising transparency (repository), Art 39, data access and scrutiny, Art. 40 DSA, compliance Art. 41 DSA, transparency reporting obligations Art. 40 DSA);

Subsection 6 other provisions concerning due diligence, standards Art. 44 DSA, codes of conduct Art. 45 DSA, codes of conduct for advertising Art. 46 DSA, codes of conduct for accessibility Art. 47 DSA, crisis protocols Art. 48 DSA.

The DSA is not conceived as a piece of regulation of rights and duties in private relations, whether b2b or b2c. There are exceptions, though, such as the right to information in Article 32 DSA or the right to lodge a complaint in Article 53 DSA.²³⁰ However, consumers have no right to upload a text. This is all the more astonishing as the DSA focuses on management of 'illegal content'. Whether such a right exists is left to national law and the national courts. The horizontal dimension is by and large missing, which is one of the major flaws of the DSA.²³¹ Even more difficult, Article 25 DSA (dark patterns) seems to have the potential to increase protection of consumers, as:

providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.

However, Article 25 (2) DSA immediately takes away this opportunity by stating:

The prohibition in paragraph 1 shall not apply to practices covered by Directive 2005/29/EC or Regulation (EU) 2016/679.

This exemption or reduction met strong resistance from BEUC, but was nevertheless integrated in the final version of the DSA.²³²

²²⁹ (Art 34 (1) d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

²³⁰ Rec 118 and in more detail J-P Schneider, Das verwaltungsrechtliche Beschwerderecht für Plattformnutzer gem Art 53 DSA, CR 2023, at 45.

²³¹ G Spindler, Digital services act: Adapting commercial and civil law rules for commercial entities operating online: Legal assessment in N Lomba/T Evas European Parliament, Digital Services Act, European Added Value Assessment, Annex II, European Parliamentary Research Service, September 2020, 185 at 95.

²³² Interview with BEUC and informal position paper on file with the author.

b) Non-harmonised European Standards, Protection of Minors, Stakeholder Participation

Article 44 DSA in combination with Article 63 DSA lays down the operational framework. Article 44 DSA runs like this:

1. The Commission shall consult the Board, and shall support and promote the development and implementation of voluntary standards set by relevant European and international standardisation organisations, at least in respect of the following: (a) electronic submission of notices under Article 16; (b) templates, design and process standards for communicating with the recipients of the service in a user-friendly manner on restrictions resulting from terms and conditions and changes thereto; (c) electronic submission of notices by trusted flaggers under Article 22, including through application programming interfaces; (d) specific interfaces, including application programming interfaces, to facilitate compliance with the obligations set out in Articles 39 and 40; (e) auditing of very large online platforms and of very large online search engines pursuant to Article 37; (f) interoperability of the advertisement repositories referred to in Article 39(2); (g) transmission of data between advertising intermediaries in support of transparency obligations pursuant to Article 26(1), points (b), (c) and (d); (h) technical measures to enable compliance with obligations relating to advertising contained in this Regulation, including the obligations regarding prominent markings for advertisements and commercial communications referred to in Article 26; (i) choice interfaces and presentation of information on the main parameters of different types of recommender systems, in accordance with Articles 27 and 38; (j) standards for targeted measures to protect minors online.

The European Board of Digital Services Article 61 DSA is composed of the national digital service coordinators. It operates under the chairmanship of the European Commission and has the following tasks, Article 63 DSA:

1. Where necessary to meet the objectives set out in Article 61(2), the Board shall in particular: e) support and promote the development and implementation of European standards, guidelines, reports, templates and code of conducts in cooperation with relevant stakeholders as provided for in this Regulation.

Thereby the Board may cooperate with other Union bodies, offices, agencies, and advisory groups with responsibilities inter alia in consumer protection. What will this look like in practice? The problem of using non-harmonised European standards to solve consumer concerns may be illustrated by reference to the risk that minors face when using the internet. In recent years, consumer organisations have drawn the attention of national supervisory authorities to unlawful marketing strategies of TikTok.²³³ TikTok's clientele are by and large 'minors'. The DSA stresses the need to protect minors. Recital 46 addresses the comprehensibility of marketing strategies:

Providers of intermediary services that are primarily directed at minors, for example through the design or marketing of the service, or which are used predominantly by minors, should make particular efforts to render the explanation of their terms and conditions easily understandable to minors.

²³³ See the BEUC website on TikTok <https://www.beuc.eu/tiktok>, with a list of the actions, the demands and the documents, in this context see M Cantero Gamito/H-W Micklitz, Too much or too little? assessing the consumer protection cooperation (CPC) network in the protection of consumers and children on Tiktok, 16.2.2023 https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-018_Assessing_CPC_Network_in_the_protection_of_consumers_and_children_on_TikTok-Report.pdf

Recital 81 classifies an insufficient level of protection as a ‘systemic risk’ in the meaning of Article 34 DSA:

(81) A second category concerns...consumer protection. Such risks may arise, for example, in relation to the design of the algorithmic systems used by the very large online platform or by the very large online search engine or the misuse of their service through the submission of abusive notices or other methods for silencing speech or hampering competition. When assessing risks to the rights of the child, providers of very large online platforms and of very large online search engines should consider for example how easy it is for minors to understand the design and functioning of the service, as well as how minors can be exposed through their service to content that may impair minors’ health, physical, mental and moral development. Such risks may arise, for example, in relation to the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behaviour.

Article 34 (1) b) DSA requires respect for the rights of the child enshrined in Article 24 of the Charter, and to a high-level of consumer protection enshrined in Article 38 of the Charter. One could have expected that the EU legislature would have imposed clear obligations on what the VLOPs would have to do. However, all the European Commission – after having consulted the Board – will have to do is to promote adoption of non-harmonised European standards ‘for targeted measures to protection minors online’, Article 44 (1) j) DSA. In its own assessment, the European Commission regards the different safeguards enshrined in the DSA as a major success.²³⁴

The minimum that the DSA could have done is to refer to Regulation 1025/2012 so as to enable the European Commission to mandate elaboration of a *harmonised* standard. As the DSA stands, the ruling does not even require inclusion of stakeholder organisations. Here the DSA remains even behind what the VLOPs and LOPs are expected to do in their approach to risk assessment. Under Recital 90 providers

should, where appropriate, conduct their risk assessments and design their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations. They should seek to embed such consultations into their methodologies for assessing the risks and designing mitigation measures, including, as appropriate, surveys, focus groups, round tables, and other consultation and design methods. In the assessment on whether a measure is reasonable, proportionate and effective, special consideration should be given to the right to freedom of expression.

The inclusion requirement is partially reflected in Article 34 (1) g) DSA. They should put in place mitigation procedures which ‘may’ include inter alia initiating or adjusting cooperation with trusted flaggers in accordance with Article 22 DSA, and implementation of the decisions of out-of-court dispute settlement bodies pursuant to Article 21 DSA. In sum, Article 44 DSA remains behind other forms of due diligence mechanisms. Article 44 DSA does not require the inclusion of consumer organisations in elaborating non-harmonised European standards, which looks like a blatant contradiction in light of the EU Standardisation Strategy, which insists on the inclusion of stakeholder organisations in standard-setting. This might explain why BEUC

²³⁴ See the stocktaking in Brussels, 11.5.2022 COM(2022) 212 final A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212&from=EN>

advocated elimination of any rule which promotes development of non-harmonised European standards.²³⁵

c) Fundamental Rights – Reach and Uncertainties

An amazing contradiction exists in, on the one hand, the use of fundamental rights in the DSA, and, on the other hand, the AIA-P, CRA-P. These last two strongly focus on health and safety issues, in line with product safety regulation and elaboration of harmonised standards according to Regulation 1025/2012, whereas the former puts the emphasis on the economic implications of the platform economy. However, all three refer to fundamental rights, including consumer protection. EU Digital Policy Legislation understands the economic rights of consumers as an integral part of the Charter.

The DSA constantly refers to fundamental rights, often in connection with consumer protection (but without mentioning Article 38 EUCFR) – all in all, some 36 times. The overall credo is expressed in Recital 40, again dealing with the ‘online environment’:

(40) In order to achieve the objectives of this Regulation, and in particular to improve the functioning of the internal market and ensure a safe and transparent online environment, it is necessary to establish a clear, effective, predictable and balanced set of harmonised due diligence obligations for providers of intermediary services. Those obligations should aim in particular to guarantee different public policy objectives such as the safety and trust of the recipients of the service, including consumers, minors and users at particular risk of being subject to hate speech, sexual harassment or other discriminatory actions, the protection of relevant fundamental rights enshrined in the Charter, the meaningful accountability of those providers and the empowerment of recipients and other affected parties, whilst facilitating the necessary oversight by competent authorities.

The DSA is tying fundamental rights to hosting in Recital (41) and (52), to illegal content in Recital (63), systemic risks in (79), enforcement in Recital (109). All these references culminate in a general proviso (153) which is missing in the AIA-P and the CRA-P, and then reiterated in Article 1 (1) DSA:

(153) This Regulation respects the fundamental rights recognised by the Charter and the fundamental rights constituting general principles of Union law. Accordingly, this Regulation should be interpreted and applied in accordance with those fundamental rights, including the freedom of expression and of information, as well as the freedom and pluralism of the media. When exercising the powers set out in this Regulation, all public authorities involved should achieve, in situations where the relevant fundamental rights conflict, a fair balance between the rights concerned, in accordance with the principle of proportionality.

The reference to fundamental rights is less determined in the various due diligence obligations. The DSA mentions fundamental rights only twice explicitly, with regard to terms and conditions in Article 14 DSA:

4. Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients

²³⁵ BEUC The Digital Services Act Proposal, BEUC position paper, at 30. https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf

of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter.

and with regard to risk and crisis management in Articles 34, 36 and 48, 49 DSA. This again raises the question whether the EU legislature intends to rank the importance of fundamental rights, according to:

- whether they are mentioned in the recitals only;
- whether they are explicitly mentioned in the articles of the DSA, or
- whether they are only subject to the proviso or Article 1 DSA.

A more generous interpretation would be that the differences do not matter, because of the general proviso and Article 1 DSA. The question is legally relevant, as Article 44 DSA on non-harmonised European standards does not refer to fundamental rights. These come in with regard to protection of minors in Article 44 (1) j) DSA, implicitly through Recital 46 and Article 34 (1) b) DSA with regard to management of systemic risks. However, all other fields which are subject to non-harmonised European standards are only covered by the general proviso. This also includes the ‘Samaritan’ clause in Article 7 DSA, which reduces the critique voiced against the upgrade of ‘voluntary own initiative investigation and legal compliance’.²³⁶

d) Compliance – Institutional and Procedural Safeguards

Compliance with non-harmonised European standards:

- does not automatically grant access to the Internal Market,
- does not establish a presumption of conformity and
- does not free the addressees from liability under EU or national law.

This is explicitly stated in Recital 102 with regard to non-harmonised European standards and in Article 7 DSA with regard to all voluntary self-regulation. The DSA puts emphasis on SMEs, LOPs and VLOPs in order to ensure compliance with legally-binding requirements. In fact, compliance is omnipresent in the DSA, in particular with regard to due diligence duties, Chapter III.

From a public policy perspective, it is crucial to understand the kind of safeguards that addressees have to respect. Institutional safeguards interfere in the inner organisation of companies. The DSA obliges VLOPs – and these are the only ones in contrast to LOPs and SMEs – to:

establish a compliance function, which is independent from their operational functions and composed of one or more compliance officers, including the head of the compliance function. That compliance function shall have sufficient authority, stature and resources, as well as access to the management body of the provider of the very large online platform or of the very large online search engine to monitor the compliance of that provider with this Regulation’, Art. 41 DSA.

The very same VLOPs are also obliged to execute an independent audit which comprises all Chapter III obligations, in between all those that are related to consumer protection generally and more specifically, Article 37 (1) a) DSA. The broad scope includes Article 44 DSA which regulates compliance with non-harmonised European standards. It is the European Commission

²³⁶ Ibid.

which holds the exclusive power to supervise and enforce all obligations imposed on VLOPs. On top of all that, Article 37 (7) DSA grants the European Commission the power to adopt delegated acts which concretise:

the necessary rules on the procedural steps, auditing methodologies and reporting templates for the audits performed pursuant to this Article. Those delegated acts shall take into account any voluntary auditing standards referred to in Article 44(1), point (e).

All other rules address procedural arrangements. This includes the whole arsenal of requirements imposed by the legislator on the development of due diligence obligations, with or without the participation of consumers and other stakeholders; on access to the results of compliance, and on their dissemination and control (for example, by public supervisory bodies). The DSA puts much emphasis on reporting duties inter alia on due diligence obligations, and thereby distinguishes between different providers, SMEs, LOPs and VLOPs.

For the purpose of this Report, two of the due diligence obligations deserve particular scrutiny, namely:

- risk assessment due to the integration of the rights of minors and
- non-European harmonised standards.²³⁷

Article 42 (4) a) DSA requires VLOPs to report on risk assessment, that is, also on how they are weighing potential risks to minors in the design of mitigation of risks. There is no such obligation with regard to LOPs or SMEs. This is all the more amazing as Article 45 DSA Codes of Conduct addresses all providers independent of their size. Article 45 (5) DSA even obliges the Commission and the Board to regularly monitor and evaluate achievement of their objectives, having regard to key performance indicators, and to publish their conclusions. Why is there no such rule with regard to compliance with non-harmonised European standards? Why are SMEs and LOPs exempted?

Whether or not there is a reporting duty depends on the different categories of non-harmonised European standards. Article 44 Paragraph 2 provides a rather cryptic ruling which leaves space for interpretation:

2. The Commission shall support the update of the standards in the light of technological developments and the behaviour of the recipients of the services in question. The relevant information regarding the update of the standards shall be publicly available and easily accessible.

What does ‘the Commission shall support the update’ mean? What exactly is hidden behind ‘support’: financial support, moral support, legal support through safe harbour rules, or stand-still arrangements? Recital 102 is of limited help. As Paragraph 2 indicates, the DSA assumes that the new ‘technological environment’ requires an adjustment of non-harmonised European standards of whatever kind. All ‘relevant’ information on the update must be made public. However, non-harmonised European standards – just as harmonised European standards – are copyright-protected. This means, for instance, that the European Commission is not in a

²³⁷ Art 26 ‘Advertising of Online Platforms’ is also referring to Art 44 DSA. Art 26 (1) and (2) includes information on the reference to ‘voluntary standards in advertising’ – here a link could be built to Art 6 (2) UCPD. However, details are not relevant for the purpose of this Report.

position to publish an ‘updated voluntary standard’ on protection of minors. Similar to harmonised standards, the European Commission might publish the subject matter and maybe the reasons, but not the concrete requirements.²³⁸ It will have to be seen that AI standards on protection of minors already exist or are under way.²³⁹

4. Concept of Safety, Intended, Foreseeable Use or Misuse in the Digital Economy

The risk-based approach in the AIA-P, CRA-P and to some extent the DSA, suggests drawing a parallel to EU product safety regulation; to the definition of safety; to safe products, and to integration of the user perspective.²⁴⁰ It does not seem far-fetched that a similar conflict might arise on the wording in the three Acts, also in concretisation of the safety level through the ESOs. This begs the question of the interaction between them and the three Acts, and even more whether concepts of safety in the old and the new economy are comparable.

Unlike the General Product Safety Regulation (RGPS), the AIA-P does not contain a ‘general clause’ which submits all products within its scope to the same level of safety. The AIA-P breaks down the risks into three different categories. This means that the level of safety remains connected to the different risk categories. The explanatory memorandum to the AI is relatively outspoken with regard to high-risk AI, but no such statement was integrated into the text of the recitals of the AIA-P:²⁴¹

The classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation. Therefore, the classification as high-risk does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used.

There is no general proviso which ensures that the AIA-P does not affect rights and obligations under the RGPS. This makes it necessary to dismantle the rationale of ‘safety’ in connection to ‘usage’ with regard to the different risk categories.

The AIA-P operates with the pair of ‘intended and foreseeable misuse’ in Article 3 AIA-P

(12) ‘intended purpose’ means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

(13) ‘reasonably foreseeable misuse’ means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems

²³⁸ See II 1 d) cc)

²³⁹ See IV 3 a) bb) und IV 5 a).

²⁴⁰ See above under I. 1. e).

²⁴¹ Explanatory Memorandum 5.2.3. at 14.

The juxtaposition of ‘intended purpose’ vs ‘reasonably foreseeable misuse’ needs further reflection. The AIA-P introduces a layered approach – the counterpart to intended purpose (not use) is the reasonably foreseeable misuse, not by the consumer but by whoever is using an AI system, which of course implies a professional. The pair reappears in Article 9 AIA-P risk management, Article 13 AIA-P transparency, and Article 14 human oversight. Articles 9 and 13 AIA-P address the ‘user’ of an AI system, which is different from the consumer. Article 14 AIA-P instead addresses any ‘natural person’ who should be able to ‘effectively oversee’ high-risk AI systems ‘during the period in which the AI system is in use’. However, read in connection with Recital 48, the addressee of the obligation is not the consumer/user but the ‘natural person’ to whom human oversight has been assigned and this can only be a professional. In a second step, it is then for the user of the AI system to integrate reasonably foreseeable human behaviour, which seems to include the consumer. The definition in Article 3 (13) AIA-P is unfortunately not really helpful, as foreseeable human behaviour is not a self-standing criterion, but connected to foreseeable misuse by the user of the AI system. Neither the explanatory memorandum nor the recitals help to understand the interaction between intended purpose (of the AI system), foreseeable misuse (by the user of the AI system) and foreseeable human behaviour (those who are interacting with the AI system). In product safety regulation, the benchmark of ‘normal and reasonable foreseeable use’ was regarded as a kind of compromise between the different interests of manufacturers and users/consumers. The reason behind the opacity in the AIA-P has to be identified in the exclusion of the consumer perspective.

But even when the consumer appears, as in an AI system which contains ‘certain risks’, the AIA-P does not set a benchmark against which the advocated transparency can be measured. There is no reference to foreseeable misuse or foreseeable use, and there is no clear definition of the scope. The addressee is a ‘natural person’ just as in Chapter II High Risk AI Systems. This seems rather confusing as the addressee of Article 54 AIA-P is not only a professional but also a consumer. The temptation might be to use the average consumer and their capacities as a yardstick. Article 54 AIA-P remains silent. The question arises how far the scope of the transparency requirement reaches. If it is limited to health and safety, it is hard to remain behind ‘reasonably foreseeable use’ of the RGPS; if Article 54 also covers economic interest, the reference might be the average consumer and, depending on context, the vulnerable consumer.

In contrast to the AIA-P, Article 7 CRA-P together with Recital 28 deals explicitly with the relationship to the RGPS. The overall rationale of the rather complex paragraph is to secure that the RGPS remains applicable as a safety net if there are no other more specific Union acts.²⁴² Article 2 CRA-P provides a general clause which comes close to the RGPS:

This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.

Just as in the RGPS, whether or not consumers are affected depends on the type of products. Consumer products – this is the message – are regarded as ‘non-critical’.²⁴³ The problem discussed with regard to Article 54 AIA-P reappears. Consumer organisations advocate classification of a particular group of consumer products as critical.²⁴⁴

²⁴² Pier Giorgio Chiara (214) at 267.

²⁴³ Under III 2 a).

²⁴⁴ Under III 2 a).

The DSA does not focus on health and safety, but on economic interests. Therefore, the DSA does not deal with the concept of safety and how it could be defined. Nevertheless, foreseeable use plays a role, though in a very specific context, namely in assessing accessibility of codes of conduct with regard to disabilities, Article 47 DSA. One might turn the argument upside down and conclude that in all other fields covered by the DSA which concerns the consumer, the average consumer test applies. The DSA contradicts the universal, structural, and relational vulnerability of consumers in the digital economy, which main theme that underpins this Report.²⁴⁵

A more complex question refers to the comparability of a legal concept in two different economic environments. First of all, consumers are not users of AI systems, at least not in the meaning of ‘use’ and ‘AI system’ given to it by the AIA-P. Not much fantasy is needed to assume that consumers might very well think that they are using an AI system when they are working on a computer or communicating via the internet, just as they are users of consumer products. Foreseeability plays a role in terms of the accessibility requirements for IT products and services. Should they be designed so that they can be used by the elderly or the handicapped? The ETSI standard on accessibility requirements for IT products and services has met strong criticism from stakeholder organisations which represent the handicapped.²⁴⁶ However, accessibility requirements should not be confounded with foreseeable use of a computer for what it has *not* been designed for cannot be compared to a ladder when it comes to foreseeable use or even foreseeable misuse. The consumer might use household ladders in a rather risky way, neglecting precautionary measures and warnings affixed to the ladder itself, or might use the ladder as a plank to bridge a gap. Something similar is hard to imagine with a computer or a mobile. A comparable phenomenon would be that the consumer is using the computer software for purposes it was not designed for. However, only very few consumers might be able to manipulate and use software in a way that contradicts their intended purpose.

The problem around ‘foreseeable use’ seems to lie elsewhere. In the old economy, ‘foreseeable use’ or even ‘foreseeable misuse’ is by and large a matter of statistics, studying household accidents, or heuristics and fantasy – although in reality human behaviour is richer and more imaginative than desk research and statistics. In the digital economy, the problem turns around the potentially *unforeseeable* use of AI systems, Article 3 (1) AIA-P, in concrete circumstances which are nearly impossible to overlook.²⁴⁷ The regulatory tool – which is discussed mainly in the political, the academic, and the technical environment – is the use case, and whether and to what extent it is possible to typify or even standardise use cases so as to be able to make safer and better-grounded statements on what might nevertheless be called ‘foreseeable use’ or even ‘foreseeable misuse’. Use cases will be one of the key issues in the third part.

²⁴⁵ Helberger et al Consumer Protection 2.0. (n 8).

²⁴⁶ I am grateful to Alejandro Moleda from European Disability Forum (EDF) for the reference to the ICT standard EN 301 549 https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf and the position taken by EDF on Global Accessibility Awareness Day, <https://www.edf-feph.org/affordablestandards-eu-needs-to-make-accessibility-standards-affordable/>

²⁴⁷ DIN DKE Deutsche Normungsroadmap Künstliche Intelligenz Ausgabe 1 2020, p. 5 discussing possible scenarios of application <https://www.dke.de/resourc/blob/2008048/99bc6d952073ca88f52c0ae4a8c351a8/nr-ki-english---download-data.pdf>

5. Lessons to be Learned

Analysis of the role of voluntary and harmonised standards in the digital economy allows us to formulate clear-cut messages to the ESOs, which are supposed to concretise the regulatory framework. These messages are not at all reassuring from a consumer policy perspective. Harmonised standards cover only high-risk areas and only if health and safety are at issue. The bulk of consumer products and services are classified as non-risky. This equally means they are subject to non-harmonised European standards. If the ESOs engage in non-harmonised European standards, they have 'only' to respect the existing body of consumer law which, by now, is claimed to be fit for purpose – unless the pending digital fairness test demonstrates insufficiencies. This is even true with regard to protection of minors, although the TikTok saga has given rise to intensive litigation which has not overcome consumer concerns. The system of conformity assessment remains by and large untouched. Third-party certification will be the exception to the rule even in high-risk areas. If all these barriers are overcome, a blind spot remains which is not filled by the EU legislation under review – this is the role and importance of use cases in the development of technical standards that have to comply with fundamental rights. EU law does not offer guidance. One of my interviewees rightly asked why the law does not foresee establishment of a European data pool for training purposes, so as to avoid discrimination.²⁴⁸

One magic tool remains to which the EU and the EC constantly refer – namely, protection of core values to be equated with fundamental rights. However, none of the three acts under review provides guidance on how fundamental rights should be integrated into technical standards and by whom, let alone the question where to draw the red line between standardisable and non-standardisable standards and, last but not least, who bears the responsibility for compliance with technical standards.

Interviews revealed an amazing optimism which could be summed up in one sentence – the New Approach/NLF is so stable and so well-established that it will be able to handle 'uncharted territory':²⁴⁹ at least this seems to be true for the European Commission as the instigator but also for the European Parliament and the Member States, who did not object to transfer of the New Approach/NLF into the digital economy. The European standardisation organisations are more sceptical:

I do not know whether my organisation is able to handle fundamental rights. Engineers believe what they are doing is neutral

or

the political intentions of the European Commission clash with the technical experts who are sitting and the working committees and are wondering what to do.²⁵⁰

They may think so in light of the experience they gained with the Radio Equipment Directive, where the European Commission via a delegating act activated Article 3 (3) d) e) f) to increase

²⁴⁸ Interview with an expert from a standardisation organisation.

²⁴⁹ Interview with a representative from the European Commission.

²⁵⁰ Interview with an expert from standardisation organisations.

the level of cybersecurity, personal data protection, and privacy, all of which bear a human-rights touch.

The standardisation request found support despite the critique raised from industry circles that it is overly detailed. The Working Group is composed of 150 persons, of whom 80 are active. ANEC belongs to them. After nine months of work, the Group took the unusual decision to make the draft public and to ask for comments, due to the high degree of controversy. The WG received 700 comments, both technical and general, which now have to be integrated into the final draft. The pressure is high as the respective parts of the Directive will enter into force by 1 August 2024.²⁵¹ The outcome might very well be that the Group does not succeed in operationalising fundamental rights, which would mean that a fundamental rights check is only possible *ex post* through independent testing, or in the very end through courts faced with a case in which the claimant argues that the respective standard infringes fundamental rights.²⁵² The conflict provides a foretaste of the problems that will be encountered by all the actors involved in the development of AI harmonised standards. Once again, the problem of the lack of a red line that allows adequate weighting of fundamental rights according to the subject matter becomes apparent.

The sheer analysis of the law in the books, the lengthy drafts and regulations together with their explanatory memoranda, leads to a rather negative assessment. As the law stands, fundamental rights seem to function as a place holder, but a place holder for what? Consumer rights are part of the Charter, even economic rights recognised in the DSA which focuses on economic regulation. Therefore, the AIA-P, the CRA-P and the DSA have to respect consumer interests, independent of their character as risky or non-risky and independent of the type of risk – health/safety or economic interests. In light of all the uncertainties, which turn around the scope and reach of the Charter in consumer law, one would have expected more legislative guidance and more clarity, not only to the benefit of consumers, but also to the benefit of the standardisation organisations which need to implement ‘binding legal requirements’ – fundamental rights form an integral part of these – into the elaboration of technical standards. The unclear status of fundamental rights begs the question whether fundamental rights are a substitute for consumer protection and consumer law. Such an interpretation is enhanced by the ongoing privatisation of consumer law²⁵³ through an ever-denser net of due diligence obligations, codes of conduct, voluntary technical standards and even harmonised European standards, provided the ESOs are left alone with implementing fundamental rights into standardisation. Seen this way, one may wonder whether in the current battleground the various democratic organs are fighting over the right issues. The degree to which standardisation organisations are able to handle fundamental rights will be a central subject of the third part of this Report.

There is definitely more to say on the relationship between fundamental rights in the framework of the digital economy and consumer law. But this is not the place to study the issue in depth. It suffices to point to the consequences that result from neglecting consumer law and consumer protection. One might wonder whether the overall notion of the consumer is gradually dissolved, just like its counterpart ‘the trader’ or ‘supplier’ in the old economy. There is practically no consumer in the Digital Legislative Framework and if the consumer shows up,

²⁵¹ Interview with an expert from standardisation organisations.

²⁵² Interview with experts from standardisation organisations.

²⁵³ I borrow the term from Natali Helberger, who used the language first.

they are enshrined into other categories: users, natural persons, or individuals. Similar developments can be observed at the other end of the spectrum. There is no trader or supplier, but there are many more categories which are adjusted to the particular type of business they are undertaking. The DSA – and the DMA – define different rights and obligations of companies depending on their size. This could be understood as an invitation to link different types of rights to different types of consumers. This overall trend must be read in the light that digitisation blurs the boundaries between the market, politics, and society or in terms of addressees of EU digital legislation between the consumer as a market participant and the consumer as a citizen. The debate on the consumer citizen, the worker citizen, the supplier citizen, and so on, is not really new,²⁵⁴ but digitisation of the economy and society has substantially increased the speed in which well-established distinctions in the legal system are melting away.

The transfer from the old to the new economy has laid bare many open issues of the Regulation on European Standardisation, Regulation 1025/2012. Many have been addressed long before the CJEU entered the scene: the legitimacy of technical standardisation, the borderline between public and private law-making, the role of stakeholder organisations and their underrepresentation in the elaboration of technical standards. However, it needed the CJEU to push the European Commission into action and thereby also the ESOs. Open issues range from the reach of judicial review; the legitimacy of copyrights; deep into the distribution of responsibilities between and among the EC, the ESOs, the Member States and the stakeholders in formulation of the standardisation request; its monitoring during elaboration and review before it is published, not to mention the outstanding issue of *effective* consumer participation. In the aftermath of *James Elliott*, the European Commission took over from the ESOs the task and the responsibility to hire consultants who check compliance of a standard with an official request. The so-called HAS consultants remain a black box. Neither the accessible rules, nor the interviews could shed light on what exactly HAS consultants are doing; what kind of responsibilities they have; how tasks are divided with the European Commission, the European Parliament, and the Member States, and – last but not least – who they are. All we know is that *Ernst and Young*, one of the big four consultancy companies in the world, selects them and administers their tasks.

254 M Everson ‘The legacy of the market citizen’, in J Shaw and G More (eds), *New Legal Dynamics of European Union* (Oxford: Clarendon Press, 1995), 73–90; M Everson, and Ch Joerges, ‘Consumer Citizenship in Postnational Constellations?’ (2006) EUI Working Paper Law No. 47; N N Shuibhne, ‘The Resilience of EU Market Citizenship’ (2010) 47 *Common Market Law Review* 1597–1628.

IV. Acid Test: Secure, Trustworthy, and Ethical AI

‘Trustworthy AI’ is the banner that the OECD and the EU, along with international and European standardisation organisations carry before them, independent of the different legal status of OECD Guidelines as policy recommendations,²⁵⁵ binding EU Regulation on the Digital Market (adopted and in the making) or technical standards, elaborated or to be elaborated by international and European standardisation bodies. Chapter II offers a taste of the regulatory power which the EU sets into motion in a policy field where many actors and institutions compete with their different aims and perspectives. Chapter III uses the ‘*formula of secure, trustworthy and ethical AI*’ complemented by ‘human-centric’²⁵⁶ as an acid test for the feasibility of the New Approach/NLF in the digital economy at both levels – at the level of binding legal requirements and at the level of technical standardisation.

The EU is a latecomer in terms of concretising the formula at the conceptual level as well as in terms of concretising the concept through technical standards. The conceptual level starts with a second look at EU Digital Policy Legislation on what the formula means and could mean in light of the High Level Expert Group (HLEG) which the European Commission set up to develop guidelines and ethical principles. However, at the conceptual level the European Commission is already confronted with the activities of international standardisation organisations, the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronics Engineers (IEEE), all of which are trying to do exactly what the European Commission is aiming at. Here is also the place for OECD Recommendations, which could be understood as an equivalent to binding EU legal requirements. The picture becomes even more blurred when diving deep into the activities of the international standardisation organisations which are under way with a view to developing AI standards which concretise the concept of secure, trustworthy, and ethical AI.²⁵⁷ Fortunately, many of the AI Standards are publicly available, although copyright-protected.²⁵⁸ The story to tell is the one about the tortoise and the hare: wherever the European Commission is promoting the development of secure, trustworthy, and ethical AI through European ‘core values’²⁵⁹ there is already an ISO/IEC, IEEE standard in place or one under development. The time-gap creates all sorts of tensions.

The national standardisation organisations were and are involved in elaborating international standards. The European Commission has one powerful tool in its hands which puts pressure

²⁵⁵ On the OECD initiative on responsible business standards under II 4.

²⁵⁶ European Commission, Building Trust in Human-Centric Artificial Intelligence, COM(2019) 168.

²⁵⁷ M Ebers (n 27) at 8–9.

²⁵⁸ ISO <https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>, IEEE <https://standards.ieee.org/news/get-program-ai-ethics/>

²⁵⁹ EC Roadmap Standardisation Strategy 2021 (n 45), at 3 under (5).

on standardisation organisations to co-operate in their elaboration of European harmonised standards – the presumption of conformity. CEN-CENELEC and ETSI serve as the spearhead to implement EU standardisation policy, which should be understood as a kind of value-oriented upgrade in a twofold sense – upgrade through inclusion of stakeholders to increase democratic legitimacy, and upgrade through tying technical standards to Union law. On the other hand, CEN-CENELEC and ETSI are sandwiched between different dependencies and loyalties. Whenever they initiate elaboration of a European harmonised standard, they have to serve five masters: the national standardisation organisations, the international standardisation organisations, the European Commission, the EU Member States, and stakeholder organisations.

The argument will be unfolded in the following way. The *first* step is to provide a short overview of international standardisation bodies and their potential relationship with European and national standardisation bodies, the *second* to clarify the meaning of trustworthy AI which is floating around not only in EU political debates, EU legislation, standardisation policies, but also in international politics and international standardisation bodies. The meta discussion is mainly a *conceptual* exercise, linking the debate on AI ethics to human oversight, safety, security, and trustworthiness and trying to lend a rather vague catch-all category clearer normative contours which helps guide elaboration of particular AI standards across sectors or with regard to particular sectors, particular methodologies, or particular AI systems. The international standardisation organisations in particular have not only invested in the conceptual exercise, but have at the same time started to develop concrete AI standards which have to be understood as attempts to concretise what ‘trustworthy’ and ‘ethical’ could mean definitively. Against such an international scenario, which is undertaken in a *third* step, the *last and fourth* part of this section will turn to the EU Working Programme and Standardisation Requests, highlighting potential differences between the international and European levels in elaborating such definitive AI standards, as well as identifying open issues which still await a reply.

1. ISO/IEC, IEEE, and CEN-CENELEC

It will have to be shown that the key actors from the technical side are not national standardisation bodies but international ones. ISO is an association established under Swiss law. It has 167 members.²⁶⁰ The website speaks of ‘national standards bodies’. In fact, two-thirds of ISO members are national governments. Depending on whether national standardisation is public or private, national governments may mandate their national private standardisation organisations to represent national interests, like DIN on behalf of Germany or – though under the tutorship of the French government – AFNOR. IEC²⁶¹ has 89 members, out of which 27 are associate members. The organisational principles are the same. IEC is composed of national standards bodies and there is only one body per country with one vote.

In the European perspective, there is a kind of a hierarchy from national to international standardisation organisations, with CEN-CENELEC in between and ETSI as hybrid European/international due to its international membership from countries around the world.²⁶²

²⁶⁰ <https://www.iso.org/about-us.html>

²⁶¹ <https://www.iec.ch/national-committees>

²⁶² Interview with a representative from the European Commission; on ETSI more generally M Cantero Gamito, ‘The role of ETSI in the EU’s regulation and governance of artificial intelligence’ – ETSI Workshop (Tilburg, 23 November 2022) on file with the author.

International standardisation is associated with ISO/IEC. The assessment looks very different from the US perspective. Here ISO/IEC is just one body among ‘hundreds of others’ which play a certain role in the US market, uniting mainly European standardisation bodies.²⁶³ However, in terms of international trade, to the role and function of the WTO/TBT agreement, ISO/IEC moves into the spotlight, even more so after China decided to considerably increase its engagement within ISO/IEC.

The IEEE, the third international standardisation organisation, the Institute of Electrical and Electronic Engineers, was founded in 1884, prior to the BSI, DIN, and AFNOR. The current format results from a merger of two different American institutions – the American Institute of Electrical Engineers and the Institute of Radio Engineers. Covering more than 427.000 members in 160 countries and engaging more than 1000 employees according to its vision statement:²⁶⁴

IEEE’s core purpose is to foster technological innovation and excellence for the benefit of humanity’ ... IEEE will be essential to the global technical community and to technical professionals everywhere, and be universally recognised for the contributions of technology and of technical professionals in improving global conditions.

Professional membership is open to individuals whose experience gives evidence of competence in an IEEE-designated field. The designated fields are: Engineering, Computer Sciences and Information Technology, Physical Sciences, Biological and Medical Sciences, Mathematics, Technical Communications, Education, Management, and Law and Policy.²⁶⁵ The website does not state who the members are and where they come from, not even in an anonymised form. National standardisation organisations do not seem to be members. The website does not disclose the statutes, the conditions for becoming a member, the procedural rules for developing standards, or the voting mechanisms. This information is available only upon registration.²⁶⁶

IEEE and ISO/IEC are not connected through formal co-operation. Exchange is on an ad hoc basis, although it is rather biased: ISO grants access to its working document in concreto, whereas IEEC is not ready to do so.²⁶⁷ However, negotiations are under way to improve the situation. Nor is working co-operation formalised between IEEE and CEN-CENELEC, mirroring the two agreements between CEN and ISO or CENELEC and IEC. The recent JRC report highlights the importance of technical standards elaborated by the IEEE and advocates better co-operation between CEN-CENELEC and IEEC. CEN-CENELEC, IEEE, and other standardisers have set up working agreements. IEEE are coming together in ISO/IEC JT C1 SC42, which offers opportunities for cooperation with CEN and CENELEC.²⁶⁸

The relationship between the ESOs, ISO/IEC, and IEEE could be turned into a topic of its own. From the outside, it looks as if the ESOs are closer to ISO/IEC and this is particularly true of CEN-CENELEC, whereas IEEE leans to the United States, due to its origin in American electrical engineering and due to its very different membership. IEEE developed gradually from a body bringing together engineers to a body of software engineers, computer scientists, and mathematicians. Today, IEEE is pushing into the European market and seeking greater recognition,

²⁶³ Interview with a representative of an internationally operating tech company.

²⁶⁴ <https://www.ieee.org/about/at-a-glance.html> and Wikipedia.

²⁶⁵ https://www.ieee.org/membership/join/index.html?WT.mc_id=hc_join

²⁶⁶ <https://www.ieee.org/searchresults/index.html?q=bylaws#gsc.tab=0&gsc.q=bylaws&gsc.page=1>

²⁶⁷ Interview with a representative from a standardisation organisation.

²⁶⁸ JRC Technical Report AI Watch Artificial Intelligence Standardisation Landscape Update, An Analysis of IEEE Standards in the Context of EU AI Regulation, 2023 <https://publications.jrc.ec.europa.eu/repository/handle/JRC131155> at 29.

not least through the European Commission. Hence IEEE is a potential competitor to ISO/IEC and maybe in future to the ESOs.²⁶⁹

A notable difference exists between the three European standardisation organisations, not only in the way they are organised, but also and in particular how they approach the field of AI standardisation. CEN-CENELEC unites the national standardisation organisations and provides the framework for development of European (harmonised) standards. The focus is on Europe: on the EU, EFTA, the UK and thereby very much guided by interaction with the European Commission and the relationship between the EU legal order and technical standardisation. ETSI reflects direct participation and assembles not only the national standardisation organisations from Europe, but is open to membership from all around the world. This means that shareholder expectations are different. CEN-CENELEC are much more dependent on the EC than ETSI, even if ETSI was established by the telecom companies in the Member States (CEPT) on a proposal from the EC. This difference can be felt in all the documents which are to be analysed and which renders it problematic to speak of the ESOs as a triumvirate, thereby including ETSI.

2. Trustworthy AI in the EU, ISO/IEC, IEEE – Search for a Concept

Whether the regulatory bodies are private or public, they are tying trustworthiness to acceptability of risk. Establishing trustworthy AI – this is the mantra – helps to unlock the potential of the digital economy to the benefit of all citizens. All those public and private regulators may be accused of conflating trustworthiness as a genuine *normative* concept and acceptability of risk as a *descriptive/empirical* element.²⁷⁰ However, it is necessary to disentangle trustworthiness and acceptability of risk by looking deeper into the normative and empirical backgrounds to ethical trustworthy AI.

The *normative* dimension is difficult to grasp as trustworthiness is a kind of catch-all term. However, the EU is about to introduce trustworthiness into the EU legal order. This means in the very end that it will be for the CJEU to interpret its meaning. Analysis of the AIA-P and the CRA-P serves as a starter. EU Digital Policy Legislation is intermingling trustworthiness and ethics. This is certainly not the place to get into a definition of what ‘ethics’ is, how ethics is related to ‘core values’²⁷¹ and whether, if, and how a society may, should, and can decide on ethics meant to govern the digital economy and society.²⁷² Linking trustworthiness to ethics – and not only to values/morals – levels trustworthiness up to an even higher and even more abstract *normative* level. On the *descriptive/empirical* side, trustworthiness points to the question what exactly determines trust and how, by what means, and by whom trust can be built. The different public and private regulators are united in the belief that trust can be developed through law,

²⁶⁹ One interviewee argued that IEEE is struggling for survival, as electrical engineering has no or very little future.

²⁷⁰ J Laux, S Wachter and B Mittelstadt, ‘Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk’, *Regulation and Governance* February 2023 <https://onlinelibrary.wiley.com/doi/epdf/10.1111/rego.12512>

²⁷¹ On the interaction between ethics and values/morals see HLEG Guidelines (n 22) at 11 and in a similar vein IEEE P7000 <https://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=7000%20series> at 28, which both mirror the commonly agreed understanding of the relationship ethics vs values/morals.

²⁷² Deeper, S Nyholm, *This is Technology Ethics, An Introduction*, Wiley, 2023.

and that the technical standards which underpin the law are to be concretised by AI experts – computer scientists, physicists – under inclusion of stakeholders. This is evident through the rigour with which standardisation organisations promote their activities internationally and with which the EU defends extension of the New Approach/NLF to the digital economy.

There are serious theoretical and empirical concerns that the EU Digital Policy Legislation will not be apt to build up ‘trust’ via a regulatory tool which leaves the decision as to what trustworthy AI means to standardisation organisations and their experts. The belief in regulation to build trust – through a combination of binding legal requirements and (voluntary) harmonised technical standards and institutional interaction between the European Commission and the ESOs – is highly presuppositional and, in light of the available research on how people perceive AI, rather optimistic, if not naïve.²⁷³ The EC Standardisation Strategy seems to insinuate that the existing mechanism of trust-building, through inclusion of stakeholder organisations, does not suffice and that more is needed, at the normative level though. This is documented in the pressure the European Commission puts on CEN-CENELEC to revise its cooperation agreements with ISO and IEC. Here an additional problem appears. How should stakeholder participation be organised so that their input guarantees that they speak on behalf of laypersons, who are the ones who are supposed to signal trust to political institutions and to the economy? The debate on the legitimacy of stakeholder organisations in the legislative machinery fills libraries.²⁷⁴ Eurocentrism has added an additional layer. Can European stakeholder organisations speak up for the Global South in case the standard produces the Brussels effect? However, even if the ‘inclusion’ of possible stakeholders is designed in a ‘perfect way’ which finds common acceptability, the question remains whether the rules which are developed produce the *empirical* results they are designed for and means they manage to increase trust.

The connecting link between the *normative* and the *empirical* dimension of trustworthiness vs acceptability of risk is the degree to which the legal system connects the abstract world of ethical and trustworthy AI to its concrete application, first in the normative order and later in empirical monitoring and surveillance. The high-flying ideas of trustworthy ethical AI can be condensed into a simple question: who decides over the application – is it the provider/user of the AI system or the natural person which interacts with the AI system? Here we are back to the decade-old debate on the triad of intended use, foreseeable use, and foreseeable misuse – or now, intended purpose, foreseeable misuse, and foreseeable human behaviour. The triad enshrines the different ways to balance out the conflicting interests of the manufacturer vs. the user in the old economy, or the AI provider/user and the customer in the digital economy. It is no coincidence that consumer organisations ever since have promoted the need to rely on the consumer/customer perspective, on the way the product or service is applied *in concreto* – in the language of technical standards – on use cases. Here the normative and the empirical dimension of trustworthy ethical AI come together.

²⁷³ Helberger et al Consumer Protection 2.0 (n 8).

²⁷⁴ Lately M Eliantonio/C Cauffmann (eds) *The Legitimacy of Standardisation as a Regulatory Technique A Cross-disciplinary and Multi-level Analysis*, Elgar 2020; K Lee, *The Legitimacy and Responsiveness of Industry Rule-Making*, Hart, 2018.

a) Trustworthiness in the AIA-P, the CRA-P and the DSA

Trustworthiness in the three Acts focuses on the normative dimension, to a very different degree though. Detailed reconstruction will demonstrate a certain helplessness on the part of the EU legislature. Formulas are floating around, but they are not tied together in a legal concept. However, one overall trend is clear: the closer the moment comes where high-flying and fine-sounding ideas have to be condensed into legal rules, the more the economic – the market – dimension of AI gains impetus. One might link this observation to the legal basis, to Article 114 TFEU, although this seems to be a rather weak and insufficient explanation.

aa) Trustworthiness in the AIA-P

Trustworthy AI is omnipresent in the AIA-P. However, a gulf yawns between the Explanatory Memorandum to the AIA-P published in 2021, the Communication from the European Commission on ‘Building Trust in Human Centric Artificial Intelligence’ from 2019,²⁷⁵ and the text of the proposal for regulation, published together with the Explanatory Memorandum. The explanatory memorandum refers extensively to trustworthy AI and links it to the debate about ‘AI ethics’ and randomly to ‘human-centric’:²⁷⁶

*AI should be a tool for people and be a force for good in society with the ultimate aim of increasing human well-being. Rules for AI available in the Union market or otherwise affecting people in the Union should therefore be **human centric**, so that people can trust that the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights (emphasis added HWM).*

In order to understand the meaning of ‘human-centric’ one has to go back to the 2019 Communication, which points to the HLEG Guidelines on Human agency and oversight:²⁷⁷

*AI systems should support individuals in making better, more informed choices in accordance with their goals. They should act as enablers to a flourishing and equitable society by supporting human agency and **fundamental** rights, and not decrease, limit or misguide human autonomy.*

*The overall **wellbeing of the user** should be central to the system’s functionality. Human oversight helps ensuring that an AI system does not undermine human autonomy or causes other adverse effects. Depending on the specific AI-based system and its application area, the appropriate degrees of **control measures**, including the adaptability, accuracy and explainability of AI-based systems, should be ensured (Fn 12 with reference to the GDPR). **Oversight** may be achieved through governance mechanisms such as ensuring a human-in-the-loop, human on-the-loop, or human-in-command approach (Fn. 13 with a definition) It must be ensured that public authorities have the ability to exercise their oversight powers in line with their mandates. All other things being equal, the less oversight a human can exercise over an AI system, the more extensive testing and stricter governance is required. (bold letters in the original HWM)*

Footnote 13 provides – finally – a definition of oversight, which highlights a certain tension between AI serving the well-being of the user and human oversight through the user:

²⁷⁵ COM (2019) 168 final Building Trust in Human Centric Artificial Intelligence.

²⁷⁶ Explanatory Memorandum to EUI Proposal on AIA-P COM (2021) 206 final at 2 under reference to COM (2019) 168 final Building Trust in Human Centric Artificial Intelligence.

²⁷⁷ HLEG Guidelines (n 22) at 5.

*Human-in-the-loop (HITL) refers to the human intervention in every decision cycle of the system, which in many cases is neither possible nor desirable. Human-on-the-loop (HOTL) refers to the capability for human intervention during the design cycle of the system and monitoring the system's operation. Human-in command (HIC) refers to the capability to oversee the overall activity of the AI system (including its broader economic, societal, legal and ethical impact) and the ability to decide when and how to use the system in any particular situation. **This can include the decision not to use an AI system in a particular situation, to establish levels of human discretion during the use of the system, or to ensure the ability to override a decision made by the system.** (emphasis added HWM).*

Not much of this long-lasting and extensive debate made it into the recitals, in particular not the definition of HITL, HOTL, and HIC. However, such clarification would be needed in order to clarify the tension between well-being and human oversight. Instead, Recital 5, the internal market perspective, is put upfront and the complex question of human control is hidden in the reference to the resolutions:

*(5) A Union legal framework laying down harmonised rules on artificial intelligence is therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market and putting into service of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. By laying down those rules, this Regulation supports the objective of the Union of being **a global leader in the development of secure, trustworthy and ethical artificial intelligence**, as stated by the European Council (with reference in Fn. 33 to European Council, Special meeting of the European Council (1 and 2 October 2020)²⁷⁸ – Conclusions, EUCO 13/20, 2020, p. 6), and **it ensures the protection of ethical principles, as specifically requested by the European Parliament** (with reference in Fn. 34 to European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).²⁷⁹*

The lack is not at all compensated through Article 14 AIA-P, which refers to human oversight of high-risk AI:

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.

²⁷⁸ 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; and provide a clear, objective definition of high-risk Artificial Intelligence systems. <https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf>

²⁷⁹ Under H. whereas a common Union regulatory framework for development, deployment, and use of artificial intelligence, robotics, and related technologies ('regulatory framework for AI') should allow citizens to share the benefits drawn from their potential, while protecting citizens from the potential risks of such technologies and promoting the trustworthiness of such technologies in the Union and elsewhere; whereas that framework should be based on Union law and values and guided by the principles of transparency, explainability, fairness, accountability and responsibility https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html

The draft begs the question why human oversight is limited to high-risk AI only and why the AIA-P does not provide more general ruling which covers all sorts of AI risks and which clarifies the link between trustworthiness and human oversight and in particular how human oversight is to be exercised. Reconstructing what trustworthiness entails and means is like a puzzle, where the bits and pieces are disseminated over various documents. However, nowhere and in particular not in the AIA-P is there an attempt to define trustworthiness as a normative concept which links trustworthiness to human oversight, let alone the interaction between the normative and the descriptive/empirical dimension. Instead, trustworthy AI – without human oversight – seems to cover all sorts of AI systems, independent of their degree of risk, even with regard to non-high-risk AI Systems which require no more than a code of conduct:

*(81) The development of AI systems **other than high-risk** AI systems in accordance with the requirements of this Regulation may lead to a larger uptake of trustworthy artificial intelligence in the Union. Providers of non-high-risk AI systems should be encouraged to create codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk AI systems.*

The AIA-P establishes a kind of a two-layer model, one of trustworthiness linked to human oversight limited to high-risk AI and then trustworthiness as a catch-all term for all other risks.

bb) Background to Recital 5 AIA-P

A deeper look into Recital 5 reveals a tension between the European Council and the European Parliament, in particular on the role and importance of the HLEG Guidelines. The European Council to which Recital 5 refers does not even mention the HLEG Guidelines. However, the Resolution of the European Parliament includes the HLEG Guidelines in the list of documents on which the Resolution is based. In contrast, the Parliamentary Resolution is more outspoken and more demanding of the role and function of trustworthy AI, and on the need to protect consumers.²⁸⁰ Trust and trustworthiness appear many times throughout the Parliamentary Resolution, first in the ‘introduction’:

*K. whereas there are **concerns** that the current Union legal framework, **including the consumer law** and employment and social acquis, data protection legislation, product safety and market surveillance legislation, as well as antidiscrimination legislation, **may no longer be fit for purpose** to effectively tackle the risks created by artificial intelligence, robotics and related technologies;*

then under the heading of ‘human centred and human made technologies’:

*3. Emphasises **the asymmetry between those who employ AI technologies and those who interact and are subject to them**; in this context, stresses that citizens’ **trust in AI can only be built on an ethics-by-default and ethics-by-design regulatory framework** which ensures that any AI put into operation fully respects and complies with the Treaties, the Charter and secondary Union law; considers that building on such an approach should be in line with the precautionary principle that guides Union legislation and should be at the heart of any regulatory framework for AI; calls, in this regard, for a clear and coherent governance model that allows companies and innovators to further develop artificial intelligence, robotics and related technologies.*

²⁸⁰ https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html

No. 3 is worth highlighting as the Parliamentary Resolution adds a substantial component to trustworthy AI – ethics by default and ethics by design, a component which is centre-stage in terms of building a choice architecture which takes universal and structural vulnerability seriously.²⁸¹ The Parliamentary Resolution is reaching beyond the AIA-P in an attempt to concretise the requirements to be fulfilled ‘With regard to safety features, transparency and accountability’, thereby stressing the need to include the consumer perspective in EU Digital Policy Legislation:

*18. Underlines that **consumers’ trust is essential for the development and implementation of these technologies**, which can carry inherent risks when they are based on opaque algorithms and biased data sets; believes that **consumers should have the right to be adequately informed** in an understandable, timely, standardised, accurate and accessible manner about the existence, reasoning, possible outcome and impacts for consumers of algorithmic systems, about how to reach a human with decision-making powers, and about how the system’s decisions can be checked, meaningfully contested and corrected; underlines, in this regard, the need to consider and respect the principles of information and disclosure on which the consumer law acquis has been built; considers it necessary to provide detailed information to end-users regarding the operation of transport systems and AI-supported vehicles.*

*23. Underlines that regulation and guidelines concerning **explainability, auditability, traceability and transparency**, as well as, where so required by a risk assessment and strictly necessary and while fully respecting Union law such as that concerning data protection, privacy, intellectual property rights and trade secrets, access by public authorities to technology, data and computing systems underlying such technologies, are essential to ensuring citizens’ trust in those technologies, even if the degree of explainability is relative to the complexity of the technologies; points out that it is not always possible to explain why a model has led to a particular result or decision, black box algorithms being a case in point; considers, therefore, that the respect of these principles is a precondition to guarantee accountability.*

The limits of the information model which dominates European Consumer law are highlighted ‘Under Consumers and the Internal Market’:

*81. Stresses the need to effectively address the challenges created by artificial intelligence, robotics and related technologies and to **ensure that consumers are empowered and properly protected**; underlines the need **to look beyond the traditional principles of information and disclosure** on which the consumer law acquis has been built, as stronger consumer rights and clear limitations regarding the development, deployment and use of artificial intelligence, robotics and related technologies will be necessary to ensure such technology contributes to making consumers’ lives better and evolves in a way that respects fundamental and consumer rights and Union values;*

Unfortunately, though, despite its rather promising outlook, the Resolution of the European Parliament is not very helpful in clarifying what exactly trustworthy AI might mean. The Resolution, perhaps even more than the AIA-P, resembles a hodgepodge of demands grouped together under a long list of high-level principles, resolutions, and precepts, which however, in theory could have been taken up by the European Commission in drafting the AIA-P. At the time of writing the European Parliament is trying to integrate its concerns into a revised version which inter alia aims at strengthening the importance of human oversight. These proposed amendments would then have to be agreed upon in the interinstitutional negotiations between the European Parliament, the Council, and the European Commission.

²⁸¹ Helberger et al. Consumer Law 2.0. (n 8)

cc) Trustworthy AI and Generally Acknowledged State of the Art

The lack of clarity insinuates that trustworthy AI is a place holder for something different or that it is just an empty shell which needs to be filled by the CJEU in the years to come. Part of the solution can be found in Recital 49:

*High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity **in accordance with the generally acknowledged state of the art**. The level of accuracy and accuracy metrics should be communicated to the users. (emphasis added HWM).*

The formula is reiterated in Chapter II Requirement for High Risk AI Systems in Article 9 (3) on risk management systems

The risk management measures referred to in paragraph 2, point (d) shall give due consideration to the effects and possible interactions resulting from the combined application of the requirements set out in this Chapter 2. They shall take into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications.

The European Commission borrows this language from the law on technical standards. The suggested applicability of the New Approach/NLF to product safety triggered a debate on the adequate level of protection against potential risks. The debate must be seen in the wider context of risk regulation, protection against risks resulting from chemicals and pesticides, from pharmaceuticals, and last but not least from nuclear power plants.²⁸² In a long interdisciplinary debate involving sociologists, philosophers, economists, natural scientists, and lawyers, a graded concept of risk emerged, tailored to the intensity and scope of risk.²⁸³

On the one hand stands established technical knowledge, for example about the safety of children's toys or household appliances. These are typically summarised in the formula also used by the EU Commission 'generally acknowledged state of the art'. Emphasis has to be put on 'generally acknowledged', which means the lowest common denominator in the technical community. The opposite pole is formed by the reference to pure *scientific findings/science/scientific knowledge*, that is, to those that have not yet become established and generally acknowledged and might not have yet found their way into technology. In between the poles are two different layers – the '*state of science and technology*' on the one hand and the '*state of the art*'. The former leans towards the highest conceivable category, the latter to the lowest category. Pharmaceuticals, which have to be based on the '*state of the science/scientific knowledge and technology*', have been used again and again as an example of a sound compromise between scientific knowledge and technology. Risk regulation in the fields of inherently dangerous products such as pharmaceuticals, chemicals, and pesticides will pave the way for the development of products which may cause harm but where the potential gain outweighs the remaining risk. Below '*state of scientific knowledge and technology*' are ranking those product categories that cannot be definitively assigned. Here, the '*state of the science of scientific knowledge*' seems to be too high, but the reference to the merely '*generally acknowledged*

²⁸² U Beck, *Risk Society, Towards a New Modernity*, English Version Published in 1992.

²⁸³ There is an abundant literature on risks, risk regulation and the different layers in law. For the sake of this Report it might suffice to refer to our analysis of the New Approach in connection with product safety regulation, see Ch. Joerges et al (Fn. 58)

state of the art' seems insufficient. A simple reference to '*the state of the art*' has become the formula used in risk regulation.

The wording chosen in the AIA-P indicates that the European Commission sees no need to include the latest state of scientific knowledge in assessment of high-risk AI systems; moreover, it does not even require respect for the '*state of the art*'. It thus places AI technology on a level with old technologies and risks, known from the industrial economy, widely-known, and well accepted. Such thinking explains the lean transfer of the New Approach/NLF from the industrial economy to the digital economy. The European Commission is thus diametrically opposed to the findings that underpin the Guidelines of the High Level Expert Group on AI, which are widely shared internationally.²⁸⁴

dd) Trustworthiness in the CRA-P and the DSA

The CRA-P does not speak of trustworthy AI or trustworthy ethical AI.²⁸⁵ Trust appears only in terms of the interaction among different users and in Article 6 CRA-P with regard to 'certain risks', without reference to ethics. On the other hand, ethics is only referred to as potential boundaries that set limits '*to reap(ing) all the benefits of the digital age and to strengthen its industry and innovation capacity.*'²⁸⁶

Amazingly enough the DSA contains quite forceful language on trustworthiness in Recital 3, despite its reliance on non-harmonised European standards, due diligence obligations and codes of conduct:

*Responsible and diligent behaviour by providers of intermediary services is essential for a **safe, predictable and trustworthy online environment** and for allowing Union citizens and other persons to exercise their fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union (the 'Charter'), in particular the freedom of expression and of information, the freedom to conduct a business, the right to non-discrimination and the attainment of a high level of consumer protection (emphasis added HWM).*

Thereby the DSA underpins the need to develop a normative concept which is able to cope with all sorts of AI risks, both economic and non-economic.

b) HLEG Guidelines and Ethical Principles

In 2018 the European Commission established the High-Level Expert Group of Experts (HLEG) with the aim of elaborating ethical guidelines.²⁸⁷ The HLEG Guidelines²⁸⁸ were made operational in an Assessment List for Trustworthy Artificial Intelligence (ALTAI)²⁸⁹ with over 350

²⁸⁴ See under IV 2 b).

²⁸⁵ There is no mentioning of trustworthiness, only of trust and not in connection to AI.

²⁸⁶ At 4.

²⁸⁷ Under 3.2. 'The proposal builds on two years of analysis and close involvement of stakeholders, including academics, businesses, social partners, non-governmental organisations, Member States and citizens...The key requirements reflect a widespread and common approach, as evidenced by a plethora of ethical codes and principles developed by many private and public organisations in Europe and beyond, that AI development and use should be guided by certain essential value-oriented principles.'

²⁸⁸ HLEG, Ethics Guidelines for Trustworthy AI (n 22).

²⁸⁹ HLEG, Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, 2020.

organisations and complemented through the AI Alliance platform,²⁹⁰ the White Paper on AI, and the Inception Impact Assessment.²⁹¹ First and foremost, the HLEG Guidelines define how they use ‘ethics’ and how they use ‘trustworthy AI’. What they reproduce seems to be common sense. Ethics is broken down into (i) meta-ethics; (ii) normative ethics, that is, determining a moral course of action by examining the standards for right and wrong action; (iii) descriptive ethics, that is, empirical investigation of people’s moral behaviour and beliefs; and (iv) applied ethics, concerning what we are obligated (or permitted) to do in a specific (often historically new) situation.²⁹² The HLEG Guidelines mostly deal with normative and applied ethics.²⁹³

aa) Four Components of Trustworthy AI

The HLEG Guidelines provide a circumscription²⁹⁴ and a definition of trustworthy AI, thereby indicating how the two are interlinked. Here is the definition:²⁹⁵

*Trustworthy AI has three components: (1) it should be **lawful**, ensuring compliance with all applicable laws and regulations (2) it should be **ethical**, demonstrating respect for, and ensure adherence to, ethical principles and values and (3) it should be **robust**, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm. Trustworthy AI concerns not only the trustworthiness of the AI system itself but also comprises the trustworthiness of **all processes and actors** that are part of the system’s **lifecycle**.*

The circumscription and the definition read together deliver a kind of programme that has to be respected in terms of assessing whether AI is trustworthy. Four elements are decisive – the three enumerated *lawfulness*, *ethical principles*, *robustness* and – in addition according to my understanding there is a fourth separate element mentioned but not mentioned as the fourth component – *holism*. The latter fourth element is crucial as it stresses the need to integrate in ethics how the AI system is applied and by whom. Respecting the ‘entire lifecycle’ cannot exclude the customer/consumer from a legal system that has to be respected in order for an AI system to be qualified as ‘lawful’. The European Commission has condensed the ethical principles into seven requirements.²⁹⁶

²⁹⁰ AI Alliance <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>

²⁹¹ European Commission, Inception Impact Assessment for a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence.

²⁹² (n 22) at 39.

²⁹³ Clarification: applied ethics may also transport normative values, for the sake of the argument built the normative dimension of applied ethics can be set aside.

²⁹⁴ (n 22) at 6 ‘Trustworthy AI Trustworthiness is a prerequisite for people and societies to develop, deploy and use AI systems. Without AI systems – and the human beings behind them – being demonstrably worthy of trust, unwanted consequences may ensue, and their uptake might be hindered, preventing the realisation of the potentially vast social and economic benefits that they can bring. To help Europe realise those benefits, our vision is to ensure and scale Trustworthy AI. Trust in the development, deployment and use of AI systems concerns not only the technology’s inherent properties, but also the qualities of the socio-technical systems involving AI applications. Analogous to questions of (loss of) trust in aviation, nuclear power or food safety, it is not simply components of the AI system but the system in its overall context that may or may not engender trust. Striving towards Trustworthy AI hence concerns not only the trustworthiness of the AI system itself, but requires a holistic and systemic approach, encompassing the trustworthiness of all actors and processes that are part of the system’s socio-technical context throughout its entire lifecycle.’

²⁹⁵ (n 22) at 40.

²⁹⁶ At 4 under II. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1893

Human agency and oversight: AI systems should enable equitable societies by supporting human agency and fundamental rights, and not decrease, limit or misguide human autonomy.

Robustness and safety: Trustworthy AI requires algorithms to be secure, reliable and robust enough to deal with errors or inconsistencies during all lifecycle phases of AI systems.

Privacy and data governance: Citizens should have full control over their own data, while data concerning them will not be used to harm or discriminate against them.

Transparency: The traceability of AI systems should be ensured.

Diversity, non-discrimination and fairness: AI systems should consider the whole range of human abilities, skills and requirements, and ensure accessibility.

Societal and environmental well-being: AI systems should be used to enhance positive social change and enhance sustainability and ecological responsibility.

Accountability: Mechanisms should be put in place to ensure responsibility and accountability

bb) Giving Shape to Human Agency and Oversight

The first principle needs to be further investigated due to the importance of ‘human agency and oversight’ for the development of a normative understanding of trustworthy AI. Article 14 AIA-P only deals with human oversight but not human agency. The HLEG invests in clarification of ‘human-centric AI’, first with regard to fundamental rights:²⁹⁷

*These rights are described in the EU Charter by reference to dignity, freedoms, equality and solidarity, citizens’ rights and justice. The common foundation that unites these rights can be understood as rooted in respect for human dignity – thereby reflecting what we describe as a **“human-centric approach” in which the human being enjoys a unique and inalienable moral status of primacy in the civil, political, economic and social fields** (Fn 17 specifies: It should be noted that a commitment to human-centric AI and its anchoring in fundamental rights **requires collective societal and constitutional foundations** in which individual freedom and respect for human dignity is both practically possible and meaningful, rather than implying an unduly individualistic account of the human) (emphasis added HWM).*

Later with regard to one of the four ethical principles in the context of AI systems:²⁹⁸

The principle of respect for human autonomy

*The fundamental rights upon which the EU is founded are directed towards ensuring respect for the freedom and autonomy of human beings. **Humans interacting with AI systems must be able to keep full and effective self-determination over themselves**, and be able to partake in the democratic process. AI systems should not unjustifiably subordinate, coerce, deceive, manipulate, condition or herd humans. Instead, they should be designed to augment, complement and empower human cognitive, social and cultural skills. The allocation of functions between humans and AI systems should follow human-centric design principles and leave meaningful opportunity for human choice. This means securing human oversight (Fn. 28) over work processes in AI*

²⁹⁷ HLEG Guidelines (n 22) at 12.

²⁹⁸ HLEG Guidelines (n 22) at 14.

systems. AI systems may also fundamentally change the work sphere. It should support humans in the working environment, and aim for the creation of meaningful work (emphasis added HWM).

The Glossary provides a definition of human-centric:²⁹⁹

Human-Centric AI

*The human-centric approach to AI strives to ensure that human values are central to the way in which AI systems are developed, deployed, used and monitored, by ensuring respect for fundamental rights, including those set out in the Treaties of the European Union and Charter of Fundamental Rights of the European Union, **all of which are united by reference to a common foundation rooted in respect for human dignity, in which the human being enjoy a unique and inalienable moral status.** This also entails consideration of the natural environment and of other living beings that are part of the human ecosystem, as well as a sustainable approach enabling the flourishing of future generations to come. (emphasis added).*

The whole exercise culminates in the first principle on ‘human agency and oversight’ broken down into fundamental rights, human agency, and human oversight.³⁰⁰ Interestingly, what the European Commission condenses into a principle on human agency and oversight appears in the HLEG as a series of questions to which answers have to be found. Thereby the HLEG Guidelines go far beyond mere principles; the listed questions could be understood as a checklist that the AI provider/user (the professional) has to have an answer to. The questions could be used in developing minimum testing requirements to which I will come back when it comes to possible solutions in the improvement of the governance structure.³⁰¹

Human agency and oversight

Fundamental rights:

Did you carry out a fundamental rights impact assessment where there could be a negative impact on fundamental rights? Did you identify and document potential trade-offs made between the different principles and rights?

Does the AI system interact with decisions by human (end) users (e.g. recommended actions or decisions to take, presenting of options)? Could the AI system affect human autonomy by interfering with the (end) user’s decision-making process in an unintended way? Did you consider whether the AI system should communicate to (end) users that a decision, content, advice or outcome is the result of an algorithmic decision? In case of a chat bot or other conversational system, are the human end users made aware that they are interacting with a non-human agent?

Human agency:

Is the AI system implemented in work and labour process? If so, did you consider the task allocation between the AI system and humans for meaningful interactions and appropriate human oversight and control? Does the AI system enhance or augment human capabilities? Did you take safeguards to prevent overconfidence in or overreliance on the AI system for work processes?

²⁹⁹ HLEG Guidelines (n 22) at 39.

³⁰⁰ HLEG Guidelines (n 22) at 28.

³⁰¹ On minimum testing requirements, under V. 2 b).

Human oversight:

Did you consider the appropriate level of human control for the particular AI system and use case? Can you describe the level of human control or involvement? Who is the “human in control” and what are the moments or tools for human intervention? Did you put in place mechanisms and measures to ensure human control or oversight? Did you take any measures to enable audit and to remedy issues related to governing AI autonomy?

Is there is a self-learning or autonomous AI system or use case? If so, did you put in place more specific mechanisms of control and oversight? Which detection and response mechanisms did you establish to assess whether something could go wrong? Did you ensure a stop button or procedure to safely abort an operation where needed? Does this procedure abort the process entirely, in part, or delegate control to a human?

The seven principles have met both support and strong criticism. One of the members of the HLEG, L Floridi,³⁰² concedes that the guidelines are ‘not very original and innovative’, but defends their usefulness for guiding EU politics and EU policies. Critique has been raised against the non-binding character and the often vague and unspecific language in the seven principles.³⁰³ What is all the more amazing is that the HLEG Guidelines do not define red lines, although it is exactly these red lines that are subject of intense debate in AI.³⁰⁴ Seen through the lenses of a risk-based approach and the crucial importance of applied AI, the seven EU principles suffer from a twofold downgrading: first, the European Commission does not explicitly refer to lawfulness, which is of limited importance due to the dominating role of the law in the EU anyway; secondly, but more importantly, the European Commission does not integrate the fourth key element – the holistic perspective, which explicitly includes users. True, the lifecycle shows up in the principle of transparency, and the applicable AI system in societal and environmental well-being. However, in light of the experience gained in product safety regulation, and in view of the risk-based approach in the AIA-P and the CRA-P – which both lean on product safety regulation – it would have been necessary to give applicable AI/applied ethics a much more prominent position. The lack of such an explicit positioning of descriptive and applied AI is mirrored in the way in which the AIA-P deals with the triad of intended, foreseeable use and foreseeable misuse.³⁰⁵

One might therefore feel tempted to look into the overwhelming number of ethical principles around the world. In one way or the other, they are all connected to ‘trustworthy AI’. There are equally many attempts to compare the different principles and to find a common denominator.³⁰⁶ In the transnational environment, the following ethical principles have been identified which carry the normative undertone of the Berkman Klein Centre:³⁰⁷

302 Establishing the rules for building trustworthy AI, <https://philpapers.org/archive/FLOETR.pdf>

303 e.g., T Greene, ‘A critical review of the EU’s ‘Ethics Guidelines for Trustworthy AI’ Every silver lining has a raincloud’ August 19, 2022 <https://thenextweb.com/news/critical-review-eus-ethics-guidelines-for-trustworthy-ai>

304 For a strong plea, R Brownsword, ‘From Erehon to AlphaGo: For the sake of human dignity, should we destroy the machines?’ *Law, Innovation and Technology* 2017, 117 https://kclpure.kcl.ac.uk/portal/files/137551177/From_Erehon_to_AlphaGo_BROWNSWORD_Acc12Feb2017Epub22Mar2017_GREEN_AAM.pdf

305 See under II 1) e).

306 See references and summaries in S Fukuda-Parr and E Gibbons, ‘Emerging Consensus on ‘Ethical AI’: Human Rights Critique of Stakeholder Guidelines’, First published: 19 June 2021 <https://doi.org/10.1111/1758-5899.12965> Vol12, Issue56 Special Issue: ‘Digital technology and the political determinants of health inequities’ July 2021, 32–44, <https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12965>

307 J Fjeld, N Achten, H Hilligoss, A Nagy, and M Srikumar (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>.

(1) human rights incl. privacy, (2) promotion of human values (beneficial to the society), (3) professional responsibility (human control of technology, accountability), (4) fairness and non-discrimination, (5) transparency and explainability, (6) safety and security.

There is clearly not much difference between the seven European principles and the six identified as the common transnational core. Despite the high degree of compliance, they do not help to overcome the twofold lacunae with regard to descriptive and applied ethics. The principles are open to interpretation and there is room to stretch their meaning, in particular the one on promotion of human values. However, in contrast to the HLEG Guidelines and despite the normative undertone, the six transnational principles do not require that trustworthy AI must be 'lawful'. The Policy Recommendations of the HLEG adopted in June 2019³⁰⁸ stress the need to establish a horizontal risk-based regulatory approach to promote the Internal Market. Thereby the Policy Recommendations might have contributed to elaboration of the AIA-P.

c) ISO/IEC and IEEE's Search for a Concept

ISO/IEC and IEEE have elaborated a kind of umbrella standard which aims at concretising trustworthy AI. CEN and CENELEC are in the process of doing so. The European and International standardisation organisations are not the only ones involved in the debate around trustworthiness. There is extensive debate in the DIN and in AFNOR. Both institutions have set up a roadmap and both are deeply engaged in shaping their input.³⁰⁹ The focus in this report will nevertheless be put on the European perspective in its interaction with ISO/IEC and IEEE, where national standardisation organisations, national governments, and companies are involved. The websites of ISO/IEC and IEEE allow relatively easily to identify all standards that are classified as AI and filter out those related to trustworthiness and ethical principles. Thereby it was possible to determine ISO/IEC TR (Technical Report) 24028:2020 on trustworthiness; ISO/IEC FDIS (Final Draft International Standard) 22989 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology; and ISO/IEC TR (Technical Report) 24368:2022(MAIN) on ethical and societal concerns; as well as the IEEE-SA P 7000 series, which are the result of the Global Initiative of Autonomous and Intelligent Systems.³¹⁰

The AI standards of the three standardisation organisations are copyright-protected. ISO has published a list of open access AI standards.³¹¹ Those dealing with trustworthiness are not open access. However, ISO allows a preview of copyright-protected AI standards in parts but reproducing them is not allowed. As the table of contents is available, it is possible to at least understand the potential content. IEEE grants free access to some of the IEEE-SA P 7000 series – after registration. BEUC/ANEC bought the IEEE-SA P 7000, 7001, 7002, 7010.³¹² ISO rejected my request to grant free access for research purposes.³¹³

[InstRepos:42160420](#)

308 'Policy and Investment Recommendations for Trustworthy AI' High-Level Expert Group on Artificial Intelligence political recommendations under G.

309 DIN DKE Deutsche Normungsroadmap Künstliche Intelligenz Ausgabe 1 2020 <https://www.dke.de/resource/blob/2008048/99bc6d952073ca88f52c0ae4a8c351a8/nr-ki-english---download-data.pdf> und Ausgabe 2, 2022; <https://www.dke.de/resource/blob/2008010/776dd87a4b9ec18d4ab295025ccbb722/nr-ki-deutsch---download-data.pdf> in AFNOR the discussion runs under the heading of 'Confiance Numérique <https://www.afnor.org/numerique/>

310 <https://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=7000%20series>

311 <https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

312 On file with the author.

313 Email from copyright@iso.org dated 20.3.2023.

The three different standards, including the CEN-CENELEC project, are presented in the following way: abstract, trustworthy AI, HLEG ethical principles. The benchmark is the twofold definition in the HLEG – the definition of trustworthy AI (the four elements) and concretisation in the seven principles. Taking the HLEG as a benchmark results from its prominent importance in the preparation of EU digital policy legislation and its indirect inclusion in the AIA-P in Recital 5.³¹⁴ The three documents are hardly comparable. The designated ISO/IEC document, the TR 24028:2020, is 40 pages long, of which 15 pages are freely accessible; ISO/IEC 298298 FDIS is 71 pages long. The IEEE standards come to 82 pages. So far, CEN-CENELEC text is only a draft. The interviews taken allow me to complement the picture. In order to respect the copyright, the reader is invited to consult the respective links to the standards. The information provided in the following is therefore reduced to the absolute minimum.

| Organisation | Abstract and Purpose | Trustworthy AI | Seven HLEG Principles |
|---|--|--|---|
| ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence ³¹⁵ | | 3.4.2. ³¹⁶ provides a definition | Incomplete list: reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability – each of which is then further defined ³¹⁷ |
| ISO/IEC FDIS (First Draft International Standard) 22989 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology ³¹⁸ | | Ability to meet stakeholder (3.5.13) expectations in a verifiable way Note 1 Depending on the context or sector, and also on the specific product or service, data and technology used, different characteristics apply and need verification to ensure stakeholder (3.5.13) expectations are met | Note 2 includes, e.g., reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, and usability |
| ISO/IEC TR 24368:2022(MAIN) Information technology — Artificial intelligence — Overview of ethical and societal concerns ³¹⁹ The standard provides a list of definitions | Overview of AI ethical and societal concerns | With regard to trustworthiness the standard refers to ISO/IEC TR 24028:2020 above | Definitions of equity, fairness treatment, overview for an ethical framework (virtue ethics, utilitarianism and deontology), deals with human rights practices discussed in ISO/IEC 38507 |
| IEEE P7000™ Standard Model Process for Addressing Ethical Concerns during System Design | Processes by which organisations can include consideration of ethical values throughout the stages of concept exploration and development ³²⁰ | Trust is classified as one of 11 typical ethical values ³²¹ | Ethical Concerns are broken down into 8 categories (4) |
| CEN-CENELEC ³²² prEN XXX (pr=JT021008) Artificial Intelligence trustworthiness characterisation | Provides a horizontal framework for specifying assessable criteria and controls in relation to AI services and products trustworthiness | | |

The dissimilarities between the different documents are striking. A prominent example might be how they deal with autonomy. The HLEG are deeply engaging with what they call ‘respect for human autonomy’; ISO/IEC mention autonomy once in the introduction, whereas IEEE understands autonomy as one of the core issues of ethical AI and tries to define it by reference

³¹⁴ Under IV 2 a).

³¹⁵ <https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24028:ed-1:v1:en>

³¹⁶ <https://cdn.standards.iteh.ai/samples/77608/c7169c6c89ab48f09ac82cbf27f2f2f/ISO-IEC-TR-24028-2020.pdf>

³¹⁷ Under 3.4.2. of ISO/IEC TR 24028 at 12

³¹⁸ <https://www.iso.org/obp/ui/#iso:std:iso-iec:22989:ed-1:v1:en>

³¹⁹ <https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24368:ed-1:v1:en>

³²⁰ Taken from the P7000 Standard.

³²¹ At 72.

³²² Downloaded from the CEN website https://standards.cencenelec.eu/dyn/www/f?p=305:22:0:::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1E7E2C95DEE9A536E535BC6BAE2D4C821

to ‘Related values: Moral agency, dignity, independence, freedom, liberty, mobility, self-direction, power, self-actualisation, ownership’.³²³ However, even IEEE remains far behind the sophisticated analysis of human agency and oversight in the HLEG.³²⁴

Timewise ISO/IEC were first, adopted in 2020 and then 2022; IEEC in June 2021, with CEN-CENELEC pending. ISO/IEC 24368 and ISO/IEC 22989 are mainly composed of definitions with a different degree of explanatory text. The IEEC standard is a fully-fledged document that not only contains definitions but also offers guidance on different steps in design:

- definitions which underpin the standard;
- the responsibilities of the team in charge;
- how a system is expected to operate from users’ perspective and its context of use, its stakeholders, and its potential for ethical benefit or harm;
- how to obtain and rank values and value demonstrators for approval by management and other stakeholders as a basis for the requirements and the design of the SOI (System of Interest= whose lifecycle is under consideration);
- how prioritised core values and their value demonstrators are reflected in the SOI;
- how to realise ethical values and required functionality through an ‘ethical risk-based design’, and last but not least,
- how to ensure transparency of the management process by sharing information with internal and external, short-term, and long-term stakeholders about how the developer should address ethical concerns during SOI design.

The IEEE standard is a kind of business administration guidebook for organisations which develop AI systems. In the language of governance, one may find institutional, procedural, and substantive safeguards. The institutional safeguards are laid down in chapter 6 of IEEE 7000 in particular. But there are no rules which come even close to what the DSA requires from the VLOPs.³²⁵ The chapter focuses on individual competences and the division of responsibilities but does not require Chinese walls in the company when it comes to the question how and by whom compliance of a software programme with ethical values is to be tested. The IEEE 7000 is more outspoken on inclusiveness. Stakeholders include inter alia consumer organisations. Inclusiveness is even upgraded to one of the ‘typical ethical values’.³²⁶

Inclusiveness in a system means that it is accessible to differently abled users, unbiased in its decisions, and fair to the broadest range of characteristics (especially human characteristics) it may encounter. On a project, inclusiveness involves respect and consideration for the judgment of internal stakeholders and other participants who provide information and participate in decision making. Inclusiveness encompasses suggested improvements to the design and product and alerts regarding risks and harms arising during the product lifecycle.

Inclusiveness will be guaranteed through the design process, within the various steps of drafting the software, of processing the software, and of making sure that the output complies with ethical values and is sufficiently transparent. However, this promising language is somewhat toned down in terms of specifying what companies should do to realise ‘inclusiveness’. 5.4. deals with the concept of stakeholders – their rights and duties so to say, which are inter alia users,

³²³ HLEG (n 22) at 14, ISO Introduction, IEEE at 69.

³²⁴ Under IV 2 b) and IV 2 c).

³²⁵ Under III 3 d).

³²⁶ At 72.

both professional and non-professional. Thereby the IEEE standard includes the descriptive and the applied dimension of ethical concerns, focusing on risks which result from biases that:

unjustly favour or select users in certain geographic areas, or of certain biometric or demographic characteristics, or based on unvalidated reports, or unfairly target or exclude other classes of users.³²⁷

The IEEE standard does not define values, on the basis that they are very different depending on the cultural context. Concretising values lies in the hands of the developers of an AI system. As to how to ensure – through stakeholders – the necessary input about potentially missing information, the IEEE standard becomes vague:

*Because it can be difficult to interact directly with the broad scope of user stakeholders, development organisations **may** include user advocates or create personas that act as proxy stakeholders. However, just including a stick-figure user in a use case is unlikely to capture the variety of ethical concerns and values that the actual users **may** bring to the transaction and how it is handled by the system. (emphasis added HWM).*

d) Evaluation and Consumer Concerns

The content of trustworthiness is by and large shaped by ethical principles or ethical values. A brief overview demonstrates that both the ISO/IEC and the IEEE standard – the latter despite its high intellectual ambitions, leaves the reader puzzled. The selection seems rather arbitrary and hard to bring into line with deeper reflections on what ‘ethics’ in ‘AI might mean. Here is a comparison of the ISO/IEC with the IEEE standard in contrast to the HLEG Guidelines, focusing on common denominators and potential overlap:

| HLEG Guidelines | ISO/IEC | IEEE |
|--|---|--|
| Human agency and oversight | Reliability and availability | Autonomy and care |
| Robustness and safety | Resilience and security | Control and fairness |
| Privacy and data governance | Privacy and safety | Inclusiveness and innovation |
| Transparency | Accountability and transparency | Perfection and privacy |
| Societal and environmental well-being | Integrity and authenticity | Respect, sustainability , transparency , values not treated as ethical: aesthetics, health, safety , security (confidentiality, integrity, availability, accuracy) |
| Accountability | Quality and usability | |

The terms in bold letters are those cutting across all three. Overall, a higher degree of overlap exists between the HLEG Principles and ISO/IEC than between the HLEG Principles and IEEE. Only three of the ethical values appear in all documents: privacy, transparency, and safety (although the IEEE does not regard safety as a primary ethical value). One might certainly engage in closer analysis and stretch the meaning of the various categories so as to increase mutuality between them. Nevertheless, what remains are substantial differences, the under-performance of human agency and oversight (human-centric), and the insight that – despite all the intellectual investment from the various regulators – the ‘ethical values’ seem of limited relevance as clear, definitive language is missing.

What is even more striking is that all attempts by regulators to get to grips with trustworthiness and ethical values end up in highly *normative* assessments without taking law as a constitutive element of trustworthy ethical AI seriously. The IEEE deliberately stays away from using a particular legal system as a reference point. The content of the standard should be open to each and every legal system and can and should be adjusted to particular cultures and traditions in case of need.³²⁸ This, however, does not exclude making ‘law’ one of the central elements in the development of trustworthy ethical AI. Law is more or less absent in the ISO/IEC and IEEE standard. Human rights are regarded as being part of ethical value systems, but only in the overview and when it comes to ethical value elicitation and context exploration processes. Here human rights are mentioned as one of the four non-exhaustive input elements.³²⁹

The envisaged CEN-CENELEC standard aims at complementing the AIA-P, but only with regard to conformity assessment. Therefore, the major contribution of any attempt by the European Commission to upgrade international standards through harmonised European standards or even only through European standards would be their juridification. EU law – this is the essence of the debate about ethical principles and values to give shape to trustworthiness – ends up in giving all EU guiding principles a normative outlook. EU law will set the benchmark and will define what, for instance, privacy, transparency, and safety means, just to name the three which all international standards are sharing.

3. ISO/IEC, IEEE – Concretising Trustworthy AI through Technical Standards

Outside and beyond attempts by international – and to some extent European – standardisation organisations to conceptualise trustworthiness, they have developed or they are preparing AI standards dealing with all sorts of AI-related issues which are meant to move trustworthiness from the abstract conceptual level to the highly concrete challenges which result from methodological questions or sector-related risks

a) ISO/IEC JTC 1/SC 42 on Artificial Intelligence

ISO/IEC JTC 1/SC 42 Artificial Intelligence serves as the focus and proponent for JTC 1’s standardisation programme on Artificial Intelligence, and offers guidance to JTC 1, IEC/ISO committees developing Artificial Intelligence applications. The structure is built around 11 working groups. Some 17 Standards were adopted, 27 are under development, 36 countries are participating, the USA (ANSI) holds the secretariat, and 18 further countries are observers.³³⁰ Here are the working groups

1. ISO/IEC JTC 1/SC 42/AG 3 AI standardisation roadmapping,
2. ISO/IEC JTC 1/SC 42/AHG 4, Liaison with SC 2,
3. ISO/IEC JTC 1/SC 42/AHG 6 Comment resolutions – CD/DIS ballots,

³²⁸ At 26: ‘This standard also does not address how to determine the legal feasibility of designing a system nor how to effect changes in ethical values and cultures on a national level or changes in the legal environment’

³²⁹ Under 1.4. and later under 8.4. at 14, 42.

³³⁰ <https://www.iso.org/committee/6794475.html>

4. ISO/IEC JTC 1/SC 42/AHG 7 JTC1 joint development review,
5. ISO/IEC JTC 1/SC 42/JWG 2, Joint Working Group ISO/IEC JTC1/SC 42 – ISO/IEC JTC1/SC 7: Testing of AI-based systems, I,
6. ISO/IEC JTC 1/SC 42/JWG 3 Joint Working Group ISO/IEC JTC1/SC42 – ISO/TC 215 WG: AI enabled health informatics,
7. ISO/IEC JTC 1/SC 42/WG 1 Foundational standards;
8. ISO/IEC JTC 1/SC 42/WG 2 Data,
9. ISO/IEC JTC 1/SC 42/WG 3, **Trustworthiness**,
10. ISO/IEC JTC 1/SC 42/WG 4 Use cases and applications
11. ISO/IEC JTC 1/SC 42/WG 5 Computational approaches and computational characteristics of AI systems.

So far, ISO/IEC have published 17 AI standards.³³¹ ISO distinguishes between five different deliverables, each of which is defined:

- ISO standards,
- ISO/TS Technical Specifications,
- ISO/TR Technical Reports,
- ISO/PAS Publicly Available Specifications,
- ISO/IWA International Workshop Agreements and ISO Guides.³³²

IEC does not feature the IWA. IEC does have the Systems Reference Deliverable (SRD) intended to address standardisation immediately at the systems level rather than at the product level.³³³

ISO/IEC standards are broadly defined:

An International Standard provides rules, guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context. It can take many forms. Apart from product standards, other examples include: test methods, codes of practice, guideline standards and management systems standards.

Technical Specifications are supposed to be turned into fully-fledged ISO/IEC standards, given experience.³³⁴ A Technical Report is different from ISO/IEC standards or Technical Specifications: based on surveys or available information, it provides a kind of situation report.³³⁵ International Workshop Agreements are prepared outside of ISO/IEC committee structures, following a procedure that ‘ensures the broadest range of relevant interested parties worldwide have the opportunity to participate, and are approved by consensus amongst the individual participants in the workshops’.³³⁶ The following list documents that there are few ISO/IEC standards, many more Technical Specifications and Technical Reports:

³³¹ <https://www.iso.org/committee/6794475/x/catalogue/p/1/u/0/w/0/d/0>

³³² <https://www.iso.org/deliverables-all.html>

³³³ https://www.iec.ch/dyn/www/f?p=103:48:0:::FSP_ORG_ID,FSP_LANG_ID:3228,25#3

³³⁴ Definition: A Technical Specification addresses work still under technical development, or where it is believed that there will be a future, but not immediate, possibility of agreement on an International Standard. A Technical Specification is published for immediate use, but it also provides a means to obtain feedback. The aim is that it will eventually be transformed and republished as an International Standard.

³³⁵ Definition: A Technical Report contains information of a different kind from that of the previous two publications. It may include data obtained from a survey, for example, or from an informative report, or information of the perceived ‘state of the art’.

³³⁶ Definition from ISO website.

1. ISO/IEC TS 4213:2022 *Information technology — Artificial intelligence — Assessment of machine learning classification performance*;
2. ISO/IEC 20546:2019; *Information technology — Big data — Overview and vocabulary*;
3. ISO/IEC TR 20547-1:2020 *Information technology — Big data reference architecture — Part 1: Framework and application process*;
4. ISO/IEC TR 20547-2:2018 *Information technology — Big data reference architecture — Part 2: **Use cases and derived requirements***;
5. ISO/IEC 20547-3:2020 *Information technology — Big data reference architecture — Part 3: Reference architecture*;
6. ISO/IEC TR 20547-5:2018 *Information technology — Big data reference architecture — Part 5: Standards roadmap*;
7. ISO/IEC 22989:2022 *Information technology — Artificial intelligence — **Artificial intelligence concepts and terminology***;³³⁷
8. ISO/IEC 23053:2022 *Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)*;
9. ISO/IEC 23894:2023 *Information technology — Artificial intelligence — Guidance on risk management*;
10. ISO/IEC TR 24027:2021 *Information technology — Artificial intelligence (AI) — **Bias in AI systems and AI aided decision making***;
11. ISO/IEC TR 24028:2020 *Information technology — Artificial intelligence — Overview of **trustworthiness** in artificial intelligence*;
12. ISO/IEC TR 24029-1:2021 *Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview*;
13. ISO/IEC TR 24030:2021 *Information technology — Artificial intelligence (AI) — **Use cases***;
14. ISO/IEC TR 24368:2022 *Information technology — Artificial intelligence — **Overview of ethical and societal concerns***;
15. ISO/IEC TR 24372:2021 *Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems*;
16. ISO/IEC 24668:2022 *Information technology — Artificial intelligence — Process management framework for big data analytics*;
17. ISO/IEC 38507:2022 *Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organisations*.

aa) Seven AI Standards Shaping Trustworthiness

The table below builds on the AI standards which operate under the flag of trustworthiness³³⁸ on the ISO website, seven in all. Two of them – the umbrella standards ISO/IEC TR 24028:2020 and ISO/IEC TR 24368:2022(MAIN) – have already been analysed.³³⁹ Those listed below deal with particular aspects of trustworthiness. The table distinguishes between the subject matter, the content and purpose, overlap with the EU Digital Policy Framework and, last not least, the suggested impact on the consumer in light of the HLEG Guidelines and Principles.

³³⁷ Analysed above under concepts, IV 2 c).

³³⁸ <https://standards.iteh.ai/catalog/tc/iso/2554a560-8d3b-4560-b9ba-ecd985ed1c64/iso-iec-jtc-1-sc-42-wg-3>

³³⁹ Under IV 2 c).

| Subject matter | Abstract/Content/Purpose | Overlap with AIA-P, CRA-P, DSA and ESO and IEEE | Consumer impact in light of the HLEG Guidelines |
|--|---|---|--|
| ISO/IEC 23894:2023(MAIN) Information technology — Artificial intelligence — Guidance on risk management ³⁴⁰ | 4 Principles of Risk Management | Art 9 AIA-P Risk assessment DSA Art 34 Risk assessment Overlap EC WP 2.1. Risk assessment | HLEG Safety, security + the standard includes descriptive and applied AI, as well as stakeholder participation |
| ISO/IEC TR 24029-1:2021(MAIN) Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview ³⁴¹ | 3.6 Robustness – ability of an AI system to maintain its level of performance under any circumstances | Art 15 AIA-P Accuracy and robustness Art 3 CRA-P Art 47 DSA Overlap with WP EC 2.6. and 2.7. Accuracy and robustness specifications | HLEG Robustness Focus on neural networks, of general importance for any form of risk management |
| ISO/IEC FDIS 24029-2(MAIN) Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for use of formal methods ³⁴² | 9 formal methods to assess the robustness of neural networks during their lifecycle | Art 15 AIA-P Accuracy and robustness Art 3 CRA-P Art 47 DSA Overlap with WP EC 2.6. and 2.7. Accuracy and robustness specifications ISO/IEC TR 24029-1:2021 beyond the formal methods used by this document | HLEG Robustness Lifecycle – the fourth component |
| ISO/IEC TR 24027:2021(MAIN) Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making ³⁴³ | The standard distinguishes between (i.e. desired bias), unintended unwanted biases | Art 10 AIA-P Data governance Overlap with WP EC 2.2. Data governance | HLEG, Non-discrimination, fairness Robustness and safety ISO/IEC suggest that unwanted biases can be overcome through defining the intended use Does not deal with the problem of foreseeable use in AI ³⁴⁴ |
| ISO/IEC PRF 25059(MAIN) Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems ³⁴⁵ | Quality models, quality requirements, quality measurement, and quality evaluation | Art 10 AIA-P Data governance Overlap with WP EC 2.2. Data governance Meant to complement existing ISO/IEC standards, inter alia: ISO/IEC TR 24028:2020, specifying emergent properties of a system ISO/IEC 25010:2011 ISO/IEC TR 24028:2020 specifying the testing and evaluation of AI systems (see also ISO/IEC TR 29119-11:2020) ISO/IEC 25010:2011 by specifying quality requirements with evaluation measures | HLEG Privacy, Data, Governance and Accountability |

Risk management, accuracy, and robustness and data governance should be understood as integral components of the common core of ethical AI. Only the two standards on accuracy and robustness deal with a particular aspect of AI – neuronal networks. All other standards break down the different components, thereby strongly overlapping with key concepts of the AIA-P.

³⁴⁰ <https://cdn.standards.iteh.ai/samples/77304/cb803ee4e9624430a5db177459158b24/ISO-IEC-23894-2023.pdf>

³⁴¹ <https://cdn.standards.iteh.ai/samples/77609/973220c049a74afaa24822b5a46cf957/ISO-IEC-TR-24029-1-2021.pdf>

³⁴² <https://cdn.standards.iteh.ai/samples/79804/7068cd0ffd814b49b8977ce2be993514/ISO-IEC-FDIS-24029-2.pdf>

³⁴³ <https://cdn.standards.iteh.ai/samples/77607/c0664994eace4bd597db80bb10c18dec/ISO-IEC-TR-24027-2021.pdf>

³⁴⁴ Under III 4.

³⁴⁵ <https://cdn.standards.iteh.ai/samples/80655/f8bda40b1f7845218aa0ef5121e1ed5c/ISO-IEC-PRF-25059.pdf>

bb) AI Draft Proposals on Shaping Trustworthiness

The information is taken from the ISO website.³⁴⁶ Some 27 AI standards are under preparation.³⁴⁷

1. ISO/IEC CD 5259-1 Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology, and examples
2. ISO/IEC CD 5259-2 Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures
3. ISO/IEC CD 5259-3 Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines
4. ISO/IEC CD 5259-4 Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 4: Data quality process framework
5. ISO/IEC AWI 5259-5 Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 5: Data quality governance;
6. ISO/IEC CD TR 5259-6 Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 6: Visualisation framework for data quality;
7. ISO/IEC DIS 5338 Information technology — Artificial intelligence — **AI system lifecycle processes;**
8. ISO/IEC DIS 5339 Information technology — Artificial intelligence — **Guidance for AI applications**
9. ISO/IEC DIS 5392 Information technology — Artificial intelligence — Reference architecture of knowledge engineering;
10. ISO/IEC CD TR 5469 Artificial intelligence — **Functional safety and AI systems;**
11. ISO/IEC AWI TS 6254 Information technology — Artificial intelligence — Objectives and approaches for **explainability** of ML models and AI systems;
12. ISO/IEC FDIS 8183 Information technology — Artificial intelligence — **Data lifecycle framework;**
13. ISO/IEC WD TS 8200 Information technology — Artificial intelligence — **Controllability of automated artificial intelligence systems;**
14. ISO/IEC CD TS 12791 Information technology — Artificial intelligence — **Treatment of unwanted bias in classification and regression machine learning tasks**
15. ISO/IEC AWI 12792 Information technology — Artificial intelligence — **Transparency taxonomy of AI systems**
16. ISO/IEC AWI TS 17847 Information technology — Artificial intelligence — Verification and validation analysis of AI systems
17. ISO/IEC AWI TR 17903 Information technology — Artificial intelligence — Overview of machine learning computing devices;
18. ISO/IEC AWI TR 20226 Information technology — Artificial intelligence — Environmental sustainability aspects of AI systems
19. ISO/IEC AWI TR 21221 Information technology – Artificial intelligence – **Beneficial AI systems**
20. ISO/IEC FDIS 24029-2 Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods
21. ISO/IEC CD TR 24030 Information technology — Artificial intelligence (AI) — **Use cases**

³⁴⁶ <https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0>

³⁴⁷ <https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0>

22. ISO/IEC WD TS 25058 Software and systems engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of AI systems
23. ISO/IEC PRF 25059 Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems
24. ISO/IEC AWI TS 29119-11 Software and systems engineering — Software testing — Part 11: **Testing of AI systems**
25. ISO/IEC DIS 42001 Information technology — Artificial intelligence — Management system
26. ISO/IEC AWI 42005 Information technology — Artificial intelligence — **AI system impact assessment**
27. ISO/IEC CD 42006 Information technology — Artificial intelligence — Requirements for bodies providing **audit and certification** of artificial intelligence management systems

Analysis of the 27 projects running is limited to those overlapping with different EU legislation impacting the consumer interest. A number of abbreviations are connected to the procedural steps:

- AWI= Approved Work Item Proposal (the majority of the national mirror committees supports the proposal since November 2022);
- CD=Committee Draft (which has not yet reached the stage at which the public comment takes place);
- DIS = Draft International Standard,
- FDIS=Final Draft International Standard.

The website reports on the stage of affairs in percentage categories. From an outsider perspective, it is not comprehensible at what stage a preview or part of the project is made publicly available, or where this is not the case. The list documents how important stakeholder participation at an early stage would be in the various international projects. As things stand, stakeholder participation at the European level comes in only if an EC working programme has been adopted and a standardisation request implemented. However, it should not be forgotten that ISO/IEC standards might benefit from the input which consumer organisations provide at the national level, for instance via DIN or AFNOR. Consumer input into ISO/IEC depends to a large extent on the degree to which consumers and their representatives have a say in the national standardisation organisations.³⁴⁸

The overlap between ISO/IEC standards and the EC working programme is strong, as will be shown,³⁴⁹ and underpins the need for coordination. Participation would at least allow stakeholders to get access to ongoing work. Although ANEC is active in ISO/IEC, its small resources do not allow it to contribute to all ISO/IEC work of interest to the consumer. The resources of Consumers International for standardisation, which equally enjoys observer status, are even smaller (much smaller). Publicly available information on ISO/IEC is hardly appropriate to undertake a fully-fledged analysis. That is why assessment is much more guesswork than evaluation, perhaps a kind of qualified guesswork as integration of conceptual (umbrella) standards on trustworthiness allows one to get an idea of the issues which are of major consumer concern. The following highlights the problem of the tortoise and the hare in a twofold sense – both

³⁴⁸ Germany is playing an active role in standardisation of AI, in particular terminology and concepts, framework for machine learning, and more recently impact assessment (information from a representative of a German standardisation organisation).

³⁴⁹ Under III 4.

the ESOs, perhaps ETSI to a somewhat lesser degree, and the EC are lagging behind ISO/IEC activities, which are run – this should not be forgotten – by national standardisation organisations, private organisations, and public ministries. The analysis follows the same structure as the table on conceptualising trustworthiness, whilst under consumer impact already including potential overlap with the EC Working Programme.³⁵⁰

| Subject matter | Content/Abstract/Purpose | Overlap with AIA-P, CRA-P, DSA and CENELEC/ETSI and IEEE | Consumer impact in light of the HLEG Guidelines |
|---|--|---|---|
| ISO/IEC DIS 5338 Information technology — Artificial intelligence — AI system lifecycle processes ³⁵¹ | Preview provides only the table of contents, no further information (draft comprises 40 pages) | Art 9 AIA-P (Risk assessment) Overlap with WPEC 2.1. Risk management deals with the lifecycle | HLEG robustness and safety in the entire lifecycle EC WP does not take a holistic perspective as required by the HLEG |
| ISO/IEC DIS 5339 Information technology — Artificial intelligence — Guidance for AI applications ³⁵² | Preview provides only the table of contents, no further information | | |
| ISO/IEC CD TR 5469 Artificial intelligence — Functional safety and AI systems ³⁵³ Under development | No information | | |
| ISO/IEC AWI TS 6254 Information technology — Artificial intelligence — Objectives and approaches for explainability of ML models and AI systems ³⁵⁴ Under development, only abstract | Approaches and methods that can be used to achieve explainability objectives | Art 15 AIA-P (Transparency) Arts 15 and 32 DSA Reference to ISO/IEC 22989 of lifecycle WP EC 2.4. Transparency and information for users refers to transparency but not to explainability | HLEG Transparency EC WP does not deal with explainability, but leaves it to the ESOs to cover or not to cover explainability |
| ISO/IEC FDIS 8183 Information technology — Artificial intelligence — Data lifecycle framework ³⁵⁵ Abstract but no further information | Provides an overarching data lifecycle framework | Art 9 AIA-P (Risk assessment) Overlap with WP EC 2.1. Risk assessment deals with the lifecycle | HLEG – the fourth element No equivalent in the EC WP, important gap as only covered through the lenses of risk assessment |
| ISO/IEC WD TS 8200 Information technology — Artificial intelligence — Controllability of automated artificial intelligence systems ³⁵⁶ | Basic framework with principles, characteristics and approaches for controllability | At. 17 Quality management EC WD 2.9. Quality management, including post marketing | HLEG Human oversight and agency, Accountability HLEG fourth element descriptive and applicable AI |
| ISO/IEC AWI 12792 Information technology — Artificial intelligence — Transparency taxonomy of AI systems ³⁵⁷ Under development | Horizontal taxonomy of information elements | Art 15 AIA-P (Transparency) Arts 15 and 32 DSA Reference to ISO/IEC 22989 of lifecycle WP EC 2.4. Transparency and information for users | HLEG Transparency and the fourth element |
| ISO/IEC FDIS 24029-2 Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods ³⁵⁸ | No information | Related to Art A5 AIA-P Accuracy and robustness EC WP 2.6. and 2.7. robustness and accuracy | HLEG fourth element, Crucial gap in the EC WP |

³⁵⁰ With regard to the table on conceptualising trustworthiness see IV 2 c) and with regard to the EC WP below IV 4 a) and b).

³⁵¹ <https://www.iso.org/obp/ui/#iso:std:iso-iec:5338:dis:ed-1:vl:en>

³⁵² <https://www.iso.org/obp/ui/#iso:std:iso-iec:5339:dis:ed-1:vl:en>

³⁵³ <https://www.iso.org/standard/81283.html?browse=tc>

³⁵⁴ <https://www.iso.org/standard/82148.html?browse=tc>

³⁵⁵ <https://www.iso.org/standard/83002.html?browse=tc>

³⁵⁶ <https://www.iso.org/standard/83012.html?browse=tc>

³⁵⁷ <https://www.iso.org/standard/84111.html?browse=tc>

³⁵⁸ <https://www.iso.org/standard/79804.html?browse=tc>

| Subject matter | Content/Abstract/Purpose | Overlap with AIA-P, CRA-P, DSA and CENELEC/ETSI and IEEE | Consumer impact in light of the HLEG Guidelines |
|---|--|--|--|
| ISO/IEC CD TR 24030 Information technology — Artificial intelligence (AI) — Use cases ³⁵⁹ | Provides a collection of representative use cases of AI applications in a variety of domains | Totally underdeveloped in the EU legislation and non-existent in the EC WP | HLEG stresses the descriptive and applied dimension of ethics |
| ISO/IEC WD TS 25058 Software and systems engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of AI systems ³⁶⁰ | No information | Art 17 AIA-P Quality management | HLEG Privacy and data governance |
| ISO/IEC AWI TS 29119-11 Software and systems engineering — Software testing — Part 11: Testing of AI systems ³⁶¹ | Describes testing techniques applicable for AI and ML systems | Art 3 (31) AIA-P provides for definition Art 9 AIA-P risk management system , Art 10 data governance deals with testing , Art 53 sandboxes deal with testing Art 4 CRA-P (free movement) EC WP mentions testing as an integral part of the 10 projects, but does not offer more specific guidance Reference to testing methods ISO/IEC/IEEE 29119-2 +4), to lifecycle model stages defined in ISO/IEC 22989 | Important gap – the type of testing and the perspective of testing is crucial for consumer protection purposes |
| ISO/IEC AWI 42005 Information technology — Artificial intelligence — AI system impact assessment ³⁶² | Guidance for organisations performing AI system impact assessments | Overlap with EU methodology on better regulation , here the concept of impact assessments | HLEG related to holistic perspective and to descriptive and normative ethics ISO/IEC Impact assessment project integrates foreseeable use |
| ISO/IEC CD 42006 Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems ³⁶³ | Enables accredited and/or peer-assessed certification bodies to reliably audit the management system | Art 19 Conformity Assessment and Art 43 AIA-P Conformity Assessment Art 24 CRA-P EC WP 2.10 additional requirements for ISO/IEC 17021-1 and | HLEG Accountability But no direct equivalent Of utmost importance, self and third-party certification, kind of testing methods etc. |

ISO/IEC are systematically filling the different components of the common core of AI ethical principles, such as transparency and safety, as well as deepening and further specifying those where standards are already under preparation – such as risk management, accuracy, and robustness – thereby often insinuating a normative consensus which on closer inspection proves to be futile.³⁶⁴ However, what might be more important, in particular with regard to consumer impact, is the move in the standardisation exercise towards lifecycle, testing requirements and impact assessment. Here ISO/IEC are reaching deeply into potential use cases and the requirements which a local user of an AI system has to meet to establish trust.

³⁵⁹ <https://www.iso.org/standard/84144.html?browse=tc>

³⁶⁰ <https://www.iso.org/standard/82570.html?browse=tc>

³⁶¹ <https://www.iso.org/standard/84127.html?browse=tc>

³⁶² <https://www.iso.org/standard/44545.html?browse=tc>

³⁶³ <https://www.iso.org/standard/44546.html?browse=tc>

³⁶⁴ J Laux, S Wachter and B Mittelstadt, 'Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act' (February 20, 2023). Available at SSRN: <https://ssrn.com/abstract=4365079> or <http://dx.doi.org/10.2139/ssrn.4365079> at 13.

b) IEEE Global Initiative

IEEE is particularly active in the standardisation of trustworthy AI. The current IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems Industry Connections Activity Initiation Document (ICAID)³⁶⁵ dates from February 2023, building on earlier initiatives. The initiative does not claim to be unique:

We do wish to note, however, that the organisations listed below all contain representatives who are members of The Initiative. We are not, in any way, trying to say, “The Initiative is ‘better’” than any of these fine organisations, but rather the unique need and niche we fill. Partner/ Related Organisations beyond IEEE focusing on similar work: The Partnership on AI – The Future of Life Institute – The British Standards Institute – ISO – Harvard Berkman Klein (Harvard University) – The Alan Turing Institute

The list is telling. All institutions are US or UK based, CEN-CENELEC is not mentioned, nor are national standardisation institutions (like AFNOR or DIN). Of particular interest are the so-called IEEE-SA’s P7000 Series, which are listed below. After registration, some of the IEEE-SA’s P7000 Series (7000, 7001, 7002, 7005, 7007, 7010) can be downloaded. A request to allow access to the whole 7000er series with the right to use them remained unanswered.³⁶⁶ That is why there is an uneven spread and depth of analysis: 7003, 7004, 7006, 7008, 7009 and those beyond 7010 are not accessible in full. The basic information is taken from the website. The focus of analysis is on the degree to which there is an overlap with EU law and with ESO and ISO/IEC standards.

The list of projects might reach beyond even the envisaged EU regulatory framework on the digital economy. However, in light of the broad definition of AI in the AIA-P, it seems useful to demonstrate how IEEE is occupying the field ahead of the ESOs and in competition with ISO/IEC. One disclaimer has to be made. IEEE only occasionally refers to particular laws, in general or to EU law in particular. If this is the case, EU law is enumerated and mentioned in line with laws from other countries. Overall, IEEE makes clear that it is for the professional user of the standard to make sure that transposition of the standard into business practice complies with relevant laws, which are the laws where the company is located. The analysis of the various AI standards follows the same categories applied for analysis of ISO/IEC AI standards. Again, the fourth column integrates the upcoming findings of the European Commission Working Programme on AI standards.³⁶⁷

³⁶⁵ https://standards.ieee.org/wp-content/uploads/import/governance/iccom/IC16-002-Global_Initiative_for_Ethical_Considerations_in_the_Design_of_Autonomous_Systems.pdf

³⁶⁶ Email 18.3.2023 on file with the author.

³⁶⁷ Under IV. 4.

| Subject matter | Content/Abstract/Purpose | Overlap with AIA-P, CRA-P, DSA and standardisation projects of CEN-CENELEC and ISO/IEC | Consumer impact in light of the HLEG Guidelines |
|---|---|--|--|
| IEEE P7001™ – Transparency of Autonomous Systems ³⁶⁸ | Definitions on transparency and explainability | Art 13 AIA-P (Transparency) Art.9 AIA-P Risk Assessment Overlap with EC W 2.1. | HLEG Transparency, governance Reference to ethical risk assessment, ethical governance, ethical audit trail |
| IEEE 2089™-2021 establishes a framework that can help organisations recognise and respond to the needs of children and young people ³⁶⁹ | | Overlap with DSA Art 44 voluntary standards (non harmonised European standards) , including protection of minors Overlap with EU policy initiative euConsent ³⁷⁰ Topic 12 SMP-STAND-2023-ESOS-01-IBA Age verification online | HLEG human agency and oversight |
| IEEE P7002™ – Data Privacy Process ³⁷¹ | Defines requirements for a systems-engineering process for privacy-oriented considerations | Art 10 AIA-P (Data Governance) Overlap with EC WP 2.2. GDPR is mentioned in particular to highlight the differences between data privacy laws and data protection law. However, the GDPR is in no way taken as the benchmark | HLEG Governance Lifecycle Definition of data privacy |
| IEEE P7003™ – Algorithmic Bias Considerations ³⁷² No public access | Describes specific methodologies to help users certify how they worked to address and eliminate issues of negative bias in the creation of their algorithms | Art 10 AIA-P Data governance Overlap with WP EC 2.2. Data governance ISO/IEC TR 24027:2021 Bias in AI systems | HLEG Non-discrimination and fairness, robustness and safety |
| IEEE P7004™ – Standard on Child and Student Data Governance ³⁷³ No public access | Provides stakeholders with certifiable and responsible child and student data governance methodologies | Overlap with DSA Art 44 voluntary standards (non-harmonised European standards) , including protection of minors Overlap with EU policy initiative euConsent Topic 12 SMP-STAND-2023-ESOS-01-IBA Age verification online | Very short publicly available summary |
| IEEE 7005™- 2021 – Standard on Employer Data Governance ³⁷⁴ | Designed to provide organisations with a set of clear requirements and guidelines for data governance | Reference to the GDPR, definition of informed consent In parts highly technical | HLEG Privacy and Data Governance Explainability |
| IEEE P7006™ – Standard on Personal Data AI Agent Working Group ³⁷⁵ | Means to influence and determine the values, rules and inputs that guide the development of personalised algorithms and Artificial Intelligence | Art 14 AIA-P Human oversight ECWP 2.5. | HLEG Human Agency and Oversight |
| IEEE P7007™ – Ontological Standard for Ethically-driven Robotics and Automation Systems ³⁷⁶ | | Based on IEEE P7000, abundant references to ethics and ethical standards, but no reference to HLEG Principles, Technical mathematical | |

368 <https://www.frontiersin.org/articles/10.3389/frobt.2021.665729/full>

369 <https://standards.ieee.org/news/ieee-2089/>

370 <https://euconsent.eu/>

371 <https://standards.ieee.org/ieee/7002/6898/>

372 https://standards.ieee.org/news/ieee_p7003/

373 <https://site.ieee.org/sagroups-7004/>

374 <https://ieeexplore.ieee.org/document/9618905>

375 <https://www.standict.eu/standards-repository/ieee-p7006-standard-personal-data-artificial-intelligence-ai-agent>

376 https://www.ieee-ras.org/images/IEEE_Ethics_Efforts_7000_series_Sandro_Fiorini.pdf

| Subject matter | Content/Abstract/Purpose | Overlap with AIA-P, CRA-P, DSA and standardisation projects of CEN-CENELEC and ISO/IEC | Consumer impact in light of the HLEG Guidelines |
|---|--|---|---|
| IEEE7008™-2021 – Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems ³⁷⁷ | This standard establishes a delineation of typical nudges | No direct discussion in AIA-P, CRA-P, to some extent in the DSA dark patterns prEN ISO/IEC 23053 (pr=JT021005) Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (ISO/IEC 23053:2022) ³⁷⁸ | HLEG Human agency and oversight Digital architecture may affect autonomy |
| IEEE P7009™ – Standard for Fail-Safe Design of Autonomous and Semi- Autonomous Systems ³⁷⁹ | | Very limited publicly accessible information | Consumer impact through development of testing methodologies |
| IEEE 7010™ -2020- Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems ³⁸⁰ On file with the author | | EU Charter of Fundamental Rights AIA-P references to fundamental rights Reference to human rights (18 times) and discrimination with reference to UN and UNESCO documents | HLEG principles in particular the fourth element descriptive and applied ethics HLEG Societal and Environmental Well-being |
| IEEE P7011™ – Standard for the Process of Identifying and Rating the Trustworthiness of News Sources ³⁸¹ | | Overlap with the DSA in particular | |
| IEEE P7012™ – Standard for Machine Readable Personal Privacy Terms ³⁸² Unclear to what extent the work is still ongoing ³⁸³ | David Reed, Department of Aerospace Engineering, University of Michigan will serve as chair of the IEEE Working Group on Machine Readable Privacy Terms ³⁸³ | | Building countervailing power through AI, similarities to www.claudette.eui.eu ³⁸⁴ |
| IEEE P7014™ – Standard for Emulated Empathy in Autonomous and Intelligent Systems ³⁸⁵ | | Art1 c) scope; Art 3 (34) definition of emotion recognition systems Art 52 para 2 (AIA-P) Transparency of Certain AI risks | HLEG Human agency and oversight |
| Pending IEEE P2863 – Recommended Practice for Organisational Governance of Artificial Intelligence ³⁸⁶ | Specifies governance criteria of artificial intelligence within organisations | Art 10 AIA-P Data Governance ECWP 2.2. | HLEG Privacy and data governance |

377 https://standards.ieee.org/ieee/7008/7095/?utm_source=beyondstandards&utm_medium=post&utm_campaign=working-group-2022

378 https://standards.cenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:76617,25&cs=175908B3693FAE6F804270BDF8CF8BC0A

379 <https://standards.ieee.org/ieee/7009/7096/>

380 <https://ieeexplore.ieee.org/document/9084219>

381 <https://standards.ieee.org/ieee/7011/7191/>

382 https://standards.ieee.org/news/p7011_p7012/; there were only two meetings and it is unclear whether the group is still active, information from a member of IEEE.

383 David Reed, Department of Aerospace Engineering, University of Michigan will serve as chair. According to Searls, ‘It is only because standard-form “contracts of adhesion” became the norm in the industrial age, and were borrowed for use in client-server settings starting with dial-up, that they continue to be the box outside of which developers have a hard time thinking. But a simple fact remains: we need a way for machines to hear and agree to terms proffered by individuals, in a way that accords with freedom-of-contract as it has been understood and practiced throughout the history of civilisation. I expect this working group to provide the standard required for that new norm.’

384 <http://claudette.eui.eu/>; on Claudette see F Lagioia, A Jablonowska, R Liepina, K Drazewski, ‘AI in Search of Unfairness in Consumer Contracts: The Terms of Service Landscape’, *Journal of Consumer Policy*, 2022, 1–56.

385 <https://standards.ieee.org/ieee/7014/7648/>

386 <https://sagroups.ieee.org/2863/>

| Subject matter | Content/Abstract/Purpose | Overlap with AIA-P, CRA-P, DSA and standardisation projects of CEN-CENELEC and ISO/IEC | Consumer impact in light of the HLEG Guidelines |
|--|--|--|--|
| PARS accepted: IEEE P7030: Recommended Practice for Ethical Assessment of Extended Reality (XR) Technologies (Potential new series of standards) ³⁸⁷ | Technical challenges to the metaverse ³⁸⁸ | AIA-P depending on the scope, probably covered, not categorised as high risk | There is a general description on what the objective is. More detailed information is coming from the report |
| PARS accepted IEEE P7010.1: Recommended Practice for Environmental Social Governance (ESG) and Social Development Goal (SDG) Action Implementation and Advancing Corporate Social Responsibility ³⁸⁹ | | Art 10 AIA-P Data governance EC WP 2.2. | HLEG Societal and environmental well-being |

The double comparison between ISO/IEC and IEEE on the one hand and, on the other, between ISO/IEC/IEEC vs the AIA-P offers telling insights. IEEE mainly deals with AI issues, which are not taken up by ISO/IEC. Either they are filling gaps like the various initiatives dealing with data privacy and data governance, or they are focusing on future uses of AI technologies such as robots and autonomous systems or addressing typical issues such as the needs of children and young people or trustworthiness of new sources. Some of these issues seem to be driven by particular developments in the USA, which underpins the assessment that IEEE is mainly following developments of AI in the USA. An overlap exists between the IEEE and the AIA-P. In terms of transparency requirements, IEEE has a full standard on this one, as well as a quality management system (IEEE 7000 2021). If we take into account IEEE draft standards, they cover nearly all the AIA-P requirements – which does not mean that they comply with the AIA-P.³⁹⁰ The more recent IEEE initiative IEEE P7012™ – Standard for Machine Readable Personal Privacy Terms – picks up a number of bottom-up initiatives around the globe to use AI for enabling consumers and citizens to exercise countervailing power.³⁹¹

c) Evaluation and Consumer Concerns

The tortoise and the hare story continues. Whilst ISO/IEC are ahead of the EU working programme and the ESOs, IEEE is ahead of ISO/IEC – in many domains which are of relevance to consumers. This is particularly true with regard to the fourth element of the HLEG principles – descriptive and applied ethics – the degree to which the perspective of the consumer takes into account the concrete use of AI systems. The difference between ISO/IEC and IEEE might be due to the membership structure. IEEE is in principle open to everybody who believes themselves able to contribute to standardisation of ethical AI, whereas ISO/IEC is dominated by private national standardisation organisations and their counterparts in ministries and public agencies.

³⁸⁷ <https://standards.ieee.org/beyond-standards/industry/technology-industry/why-are-standards-important-for-the-metaverse/>

³⁸⁸ <https://standards.ieee.org/beyond-standards/industry/technology-industry/why-are-standards-important-for-the-metaverse/>

³⁸⁹ <https://standards.ieee.org/ieee/7010.1/10756/>

³⁹⁰ See JRC Technical Report AI Watch Artificial Intelligence Standardisation Landscape Update, An Analysis of IEEE Standards in the Context of EU AI Regulation, 2023 <https://publications.jrc.ec.europa.eu/repository/handle/JRC131155>.

³⁹¹ Giovanni Sartor, Francesca Lagioia and Hans-W. Micklitz organised a workshop on 29 and 30 May 2023 at the European University Institute in Florence which aims to bring together the various initiatives using AI in the field of data privacy and standard terms.

One striking difference deserves to be equally highlighted – the style of writing. ISO/IEC are very much bound to clear-cut definitions: the documents are much shorter and seem more suitable for those who are drafting software. IEEE is much more expansive, much more academic, so to say. Throughout, the documents analysed contain many references to academic journals and even to books, mainly from the US and UK contexts, though, and only those written in English. The style of conceptualising IEEE standards makes them more easily accessible not only for academics but also for stakeholders. A notable difference also exists between the ESOs and the international organisations. The ESOs, as will be shown, are much more law-focused, whereas ISO/IEC and IEEE stay away from engaging too much in legal references, for obvious reasons. If they do so, however, they refer to international rules and conventions, human rights instead of fundamental rights. However, a single European legal document is more or less omnipresent in the different documents: the General Data Protection Regulation, sometimes downgraded to a single legal set of rules among many others from the USA or the UK, for instance; sometimes, however, used implicitly as a benchmark.

4. European Commission Working Programme on Trustworthy AI Standards

The European Commission adopted and published two working programmes which indicate the areas where the European Commission wants CEN-CENELEC and ETSI to step in. The European Commission proceeds in three steps – a working programme to be adopted in line with Article 8 Regulation 1025/2012, a call for proposals, a standardisation request, Article 10 Regulation 2015/2012. The various documents are screened under three different criteria – fundamental rights as place holder for core European values, ethical guidelines (in particular the HLEG), and references to trustworthiness. The guiding research question is to find out what remains of the high-flying vocabulary of fundamental rights and trustworthy, ethical AI, when it comes down to concrete standardisation projects. Such a perspective equally allows a better understanding of how the European Commission – often more implicitly than explicitly – is giving shape to ‘trustworthy ethical AI’ and what kind of guidance it is giving to handle the fundamental rights issue.

a) 2023 Working Programme, Call for Proposals

Under Article 8 Regulation 1025/2012, the European Commission is obliged to publish its annual working programme for European standardisation. A top-level EC working programme is also published annually. Overall, the EC working programme is operating below the radar of categories such as human-centric, secure and ethical trustworthiness, or foreseeable use. There are elements which point in that direction, but seen through consumer lenses, it is exactly these elements that need to be made much more specific.

aa) Working Programme

The 2023 programme³⁹² defines implementation of policy priorities, such as: the European Green Deal, Europe's Digital Decade, the Commission's new industrial strategy, and a stronger Europe in the world. The 2023 programme pursues a strategic approach to strengthening 'the EU's voice as a leader in global standardisation.' In line with the standardisation strategy of 2 February 2022, the Commission identified standardisation actions on hydrogen, solar electricity for energy systems, the digital product passport, critical raw materials, cybersecurity, quantum, and the recently adopted Digital Services Act as policy priorities. There is NO mention of fundamental rights in the 2023 working programme. The key information is found in the Annex. The working programme refers only occasionally to trustworthiness; references to the HLEG Guidelines and fundamental/human rights are missing.

Action 9 of the Annex 2023 points to revision of 'existing European standards and develop new ones supporting the topics listed in Article 44 DSA'. The 2023 working programme still refers to the Article 34 DSA proposal, although the DSA had been adopted and published in the meanwhile. Out of the four policy priorities, actions on digital transition aim to support the following: *Security, safety, and accessibility: Safety and trustworthiness of AI* (Action 59) *Online verification of age* (Action 60), *Deployment of new ICT technologies: Interoperability of the internet of things in edge and swarm computing* (Action 61), *Deployment of electronic ledgers and of the European blockchain services infrastructure* (Actions 62–63), *interoperability of data spaces used in EU smart cities – digital twins* (Action 64). In our context, actions 59 and 60 seem of major relevance. The explanations in the document remain rather vague. The deliverable of action 59, namely 'trustworthy AI', refers to the AI proposal and defines the deliverable in the following way:

Laying down technical specifications for the placing on the market, putting into service and use of artificial intelligence systems in the EU, addressing specifications related to their safety and trustworthiness, including risk management, data quality, transparency, human oversight, accuracy, robustness and cybersecurity.

The 'including' covers more or less the AIA-P requirements, which are enshrined in the HLEG Principles, but without mentioning them explicitly. In a separate rubric the deliverable is connected to the objective:

Ensuring that artificial intelligence systems can be safe and trustworthy, are monitored appropriately throughout their lifecycle, respect fundamental values and human rights recognised in the EU, and strengthen European competitiveness

Is this sloppy language or political intention: instead of fundamental rights 'fundamental values' – like core European values and then human rights? Or does the wording result from the fact that the ESOs are not well-placed to deal with fundamental rights? In the end, technical standardisation is not a fundamental rights free space. That is why clarification on the inter-relationship between fundamental rights and technical standardisation is so urgently needed. One cannot get rid of the impression that these documents are all over the place. Terms are interspersed arbitrarily and the possible consequences are not clearly stated.

³⁹² Commission Notice, The 2023 annual Union working programme for European standardisation, Brussels, 27.2.2023 C(2023) 1210 final and the Annex Brussels, 27.2.2023, C(2023) 1210 final ANNEX

In light of the TikTok case, the political decision to seek a solution through non-harmonised European standards along the line of the requirements laid down in Article 44 DSA and the existence of a similar standard developed by IEEE,³⁹³ it seems worth highlighting that the European Commission takes up Age Verification as a subject matter of standardisation. The working programme connects the initiative to two EC proposals ‘Digital Decade for Children and Youth’³⁹⁴ and ‘Proposal for a Regulation on Personal Identity’ which will amend Regulation (EU) 910/2014.³⁹⁵ The deliverable of action 60 ‘age verification’ is defined in the following way:

BIK+) COM(2021)281 final – Proposal for a Regulation establishing a framework for a European Digital Identity Development of new European standards for online age assurance/age verification, in the context of the proposal for a European identity framework (eID) proposal.

with the objective:

...to improve child safety online through secure, certified and interoperable age verification (systems to access online services across the EU). The aim is to build trust and confidence in AV mechanisms and in particular to minimise the risk of children accessing age-inappropriate content.

There is a difference between verification and assurance.³⁹⁶ In the first case, the match is 100% as the software matches the screened face with a photo the person has themselves put on the net or produced at the border, where the customs authorities compare the photo in the passport with the photo in their internal computer system. Age identification requires a face recognition system which is able to assess whether the minor in front of the screen is 14 or 16 years old. There is much uncertainty about how the problem of age verification/age assurance will be resolved. With the future European digital identity wallet, there will be technical means to disclose age or even just information saying “this wallet holder is over 18 years old” without resorting to face recognition. How the digital wallet will go together with the ‘policy request’ – it is not yet a standardisation request as the AIA is not yet adopted – remains unclear. Once the AIA is adopted the European Commission will send out another request, now a standardisation request, probably for elaboration of harmonised standards. However, such a future standardisation would have to be brought into line with the respective rules on protection of minors in the DSA.

bb) Call for Proposals

The following information is taken from the Call, which is addressed to the ESOs.³⁹⁷ The Call contains references to trustworthy AI particularly in the context of the AIA-P and the CRA-P, to ethical standards, though without mentioning the HLEG Guidelines directly, only referring indirectly to the two references in Recital 5 AIA-P to the Council and the European Parliament and also extensively to fundamental rights. Particularly noteworthy is the intention of the European Commission to initiate better interaction between the ESOs and ISO/IEC (see topic 11). The

³⁹³ See below IV 3 b).

³⁹⁴ Brussels, 11.5.2022 COM(2022) 212 final A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212&from=EN>

³⁹⁵ <https://www.european-digital-identity-regulation.com/>

³⁹⁶ Interview with representatives from stakeholder organisations.

³⁹⁷ Single Market Programme (Standardisation) Call for proposals – Invitation to submit a proposal Support to Standardisation activities performed by CEN, CENELEC and ETSI SMP-STAND-2023-ESOS-01-IBA Version 1.0 March 2023 on file with the author

Call for proposals leaves it to CEN-CENELEC to identify policy gaps in the existing set of international standards elaborated by ISO/IEC and by IEEE. The call does not contain a gap analysis. The following distinguishes between the issues, the themes and priorities, and the impact the European Commission expects. The comment clarifies where the gaps are, seen through the lenses of the foregoing analysis, in particular of the four components of the HLEG Guidelines.³⁹⁸

| Issue | Themes and priorities | Expected impact | Comment |
|--|---|--|--|
| <p>Topic 5 SMP-STAND-2023-ESOS-01-IBA Pre-standardisation work related to the proposed REGULATION on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act, proposal COM/2022/454 final) by CEN-CENELEC</p> | <p>The Cyber Resilience Act (CRA-P) sets out essential cybersecurity requirements, including processes that manufacturers must put in place to comply with certain essential requirements, for which <i>harmonised standards</i> could provide a presumption of conformity, Article 18(1) CRA-P</p> <p>.. activities relevant for developing harmonised standards ETSI, CEN and CENELEC, ISO/IEC JTC1 and ITU-T. Action should be taken within a short timeframe (approx. five months after signature of the grant) in order to meet the timeline of the CRA-P proposal</p> <p>For fulfilment of these tasks, CEN-CENELEC are expected to cooperate with each other and pro-actively liaise with the EU Agency for Cybersecurity (ENISA) and the EU Joint Research Centre (JRC)</p> | <p>A gap analysis against existing standards, technical specifications, technical reports or other relevant guidelines that could adequately address needs resulting from the objectives of the CRA-P proposal will prepare and facilitate upcoming work on harmonised European standardisation deliverables, which are necessary and suitable to support implementation of the Cyber Resilience Act</p> | <p>There is no stocktaking of where the gap is, what kind of standards exist already and in what way they are insufficient</p> <p>High time pressure – what about stakeholder participation?</p> |
| <p>Topic 11 SMP-STAND-2023-ESOS-01-IBA Support to standardisation work on artificial intelligence (AI) – engagement with international Standards Development Organisations</p> <p>This action will aim to support the work of European standardisation body(ies) responsible for preparing standards in support of the AI Act, by facilitating their Call: Support to Standardisation activities performed by CEN, CENELEC and ETSI – SMP-STAND-2023- ESOS-01-IBA 38 discussion and interaction with Standards Development Organisations, such as ISO/IEC, IEEE, ITU in the field of AI standardisation</p> | <p>Risk management systems, governance, and quality of datasets used to build AI systems, record keeping through built-in logging capabilities, transparency and information to users, <i>human oversight</i>, accuracy specifications, robustness specifications, cybersecurity specifications, quality management system for providers, including post-market, monitoring process, conformity assessment</p> <p>Contributions in these technical areas should be produced as a result of workshop agreements or other forms of cooperation between the ESOs and other international standard development organisations in a manner consistent with the objectives of a future standardisation request in support of <i>safe and trustworthy AI</i></p> | <p>Gap analysis against existing standards, technical specifications, technical reports or other relevant guidelines that could adequately address needs resulting from the objectives of the CRA-P proposal will prepare and facilitate upcoming work on harmonised European standardisation deliverables, which are necessary and suitable to support implementation of the Cyber Resilience Act</p> | <p>So far there is no stocktaking of where the gaps are, what kind of standards exist already and in what way they are insufficient</p> <p>The long list of activities complies with what the European Commission equates with trustworthy AI without digging deeper into human-centric AI and without emphasis on applied AI (use cases)</p> <p>What about stakeholder participation in workshops and the other forms of co-operation between the ESOs and ISO/IEEE</p> |

³⁹⁸ See under IV. 2 b).

| Issue | Themes and priorities | Expected impact | Comment |
|--|--|---|--|
| <p>Topic 12 SMP-STAND-2023-ESOS-01-IBA Age verification online</p> | <p>The project will support implementation of the DSA, be in line with the AVMSD and GDPR and respond to the Commission’s commitment under BIK+ Strategy... This framework could gain ETSI or ISO/IEC standard status during the post-project implementation phase...collaboration with ETSI on this work is highly desirable</p> <p>This project is also <i>complementary</i> to the ongoing work of CEN-CENELEC. CENCENELEC ..The work is based on the IEEE Standard for Age -Appropriate Digital Services Framework (IEEE 2089-2021) which builds on the 5 Rights Principles for Children</p> | <p>The project is expected to support development of a European standard for online age assurance / age verification, in the context of the eID proposal as well as the euConsent project.³⁹⁹ Overall, it is expected to contribute to a safer and better internet for children and young people by offering a standard which can be used by industry including online platforms to deploy effective and privacy-preserving age verification solutions on their services</p> | <p>There is no stocktaking of where the gap is, what kind of standards exist already and in what way the IEEE standard, to which the call refers, is insufficient</p> <p>Would it not be necessary to explicitly include children as potential stakeholders?</p> <p>The euConsent provided evidence that age verification is possible through biometric recognition systems.⁴⁰⁰ Co-ordination with the digital wallet is needed</p> |
| <p>Topic 15 SMP-STAND-2023-ESOS-01-IBA Making harmonised standards inclusive/gender-responsive</p> <p>So far, in many standards the male body (often 176cm tall, weighing 70kg) is taken for reference, including European harmonised standards</p> <p>The Commission has contracted a consultant to carry out a study to screen more than 3,500 harmonised standards supporting almost two dozen pieces of legislation.⁴⁰¹ (available end of 2023)</p> <p>This work contributes to implementation of the UNECE’s Declaration for Gender Responsive Standards. The study is expected to identify 200-300 harmonised standards whose anthropometric provisions need to be updated</p> | <p>From the outset, equality and diversity have been identified as important topics in President von der Leyen’s mandate. The ‘Union of Equality’ was one of the themes in the Political Guidelines for the next Commission 2019-2024. In the meantime, the Commission Gender Equality Strategy has announced several measures to complement existing infrastructure, such as the European network of experts on gender equality. Similarly, DG GROW adopted an Equality Mainstreaming Work Plan</p> <p>The AUWP’S main objective is to move away from working with anthropometric averages to start working with ranges, so that products are safe for people with all body dimensions...The standards should consider more body dimensions i.e. not just height but also the shapes of the spine and the hip bones. Standards should be developed to account for gender differences but also differences among humans more generally</p> | <p>The immediate impact of this project would be preparation of systematic collection of the anthropometric parameters necessary to develop inclusive European standards, so that a comprehensive, up-to-date body of anthropometric data is available for standardisers</p> <p>The ultimate expected impact is that all existing harmonised standards that have inadequate anthropometric provisions are updated on the basis of the collected anthropometric data</p> | <p>Most probably no proposal will be submitted (copied from the call for proposals at 2)</p> |

The 2023 working programme continues to set the standardisation machinery into motion long before the EU legislative act – here the CRA-P – is adopted. This is a meaningful exercise as the ESOs are overlooking ongoing developments in international standardisation better than the European Commission. But questions remain as to how the responsibilities should be shared between the European Commission, the ESOs, and the stakeholder organisations. One might wonder whether more clarity is needed. The key role of the four components laid

399 <https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-consent>: see : S Smirnova, S Livingstone and M Stoilova, ‘Understanding of user needs and problems: A rapid evidence review of age assurance and parental controls WP2: Existing Methods, User Needs and Requirements’ Date: September 2021 http://eprints.lse.ac.uk/112559/1/Stoilova_understanding_of_user_needs_and_problems_published.pdf

400 euConsent set out to prove that it is possible to make online age checks, and the process of securing parental consent for sharing personal data from younger children, simple and convenient while guaranteeing user privacy. Through two pilots, involving over 2,000 children and adults across five European countries, we demonstrated this was not only achievable but was also well-received by users. We also learnt a number of other valuable lessons and made several key recommendations for EU policymakers. As the first phase of the project completes, this is a short summary of our achievements and a look forward to what happens next; <https://euconsent.eu/a-summary-of-the-achievements-and-lessons-learned-of-the-euconsent-project-and-what-comes-next/>

401 However, no particular information is available.

down in the HLEG Guidelines insinuates that it is for the European Commission to provide much clearer guidance on human-centric AI, for instance, and on use cases, which in turn brings in applied ethics. It is then for the ESOS to screen the ISO/IEC and IEEE standards and to point to potential gaps. The openness of the call offers opportunities in upcoming debates for stakeholder organisations to influence the content of the standardisation request and the concrete mandates assigned to the ESOS. It looks as if the stakeholder organisations will have a crucial role to play in identifying gaps and pushing for appropriate solutions. All depends on the participatory rights of the stakeholder organisations and the remedies they have available to enforce their position. So far these rights have been underdeveloped and are hardly sufficient to fulfil such a prominent role.⁴⁰²

b) 2022 Working Programme, Call for Proposals

The 2022 Working Programme looks relatively similar. In between, it aims to promote standardisation in the digital economy.⁴⁰³ It is composed of the main document, which defines the policy fields in broad language, and a detailed Annex. The Annex uses language identical to the 2023 Working Programme, namely safe and trustworthy AI as well as fundamental values and human rights equally without reference to ethics, though, under action 63. The two calls based on the 2022 Working Programme provide further insight into how the European Commission intends to operationalise AI standardisation.

The June 2022 Call⁴⁰⁴ mentioned as Top 12 ‘Standards for Artificial Intelligence’ reiterating the language of the AI proposal:

High-risk” AI systems, those that pose significant risks to the health and safety or fundamental rights of persons, will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the market or put into service in the Union.

The call then specifies in some more detail what kind of standards are needed to achieve the very same objective (emphasis added HWM):

*“Themes and priorities (scope) AI systems – **especially AI systems posing a high-risk to consumer safety or fundamental rights** – should meet specific requirements that ensure those systems can be placed on the market or put into service in the Union.*

*The scope of the activities to be carried out for this action concerns the following technical areas for high-risk AI systems: **risk management system, governance and quality of datasets used to build AI systems, record keeping through built-in logging capabilities, transparency and information to users, human oversight, accuracy specifications, robustness specification, cybersecurity specifications, quality management system for providers, including post-market monitoring process, conformity assessment.** This scope reflects the set of technical areas underpinning the relevant requirements for high-risk AI systems set out in the Commission’s proposal for a horizontal regulatory framework on AI (COM/2021/206).*

⁴⁰² See under II 2 b) bb) on the deficient participation.

⁴⁰³ Brussels, 2.2.2022 C(2022) 546 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022XC0208%2801%29>

⁴⁰⁴ Single Market Programme (SMP Standardisation) Call for proposals – Invitation to submit a proposal Support to Standardisation activities performed by CEN, CENELEC and ETSI SMP-STAND-2022-ESOS-02-IBA Version 1.0 June 2022 at 21.

All activities done should build on previous efforts carried out both at European and International levels. Actions should be defined strategically, considering the need to balance the desirability of achieving international standards, with the necessity to provide standards to cover the needs of the European market and the need to ensure European values are respected, while also taking into consideration the applicability of possible future rules. Additionally, a mapping exercise should be carried out in order to identify what deliverables are needed to respond to the above needs (as also presented in the standardisation request) and how concretely the activities (to be) performed and resulting deliverables respond to those needs.

In addition, considering the specificities of European legislation and the needs of European market players, **the work should be carried out with strong assurances of unbiased technical capacity and inclusiveness of all relevant stakeholders.** The standardisation activities described are supported by a forthcoming Standardisation Request (for European Standards and European Standardisation deliverables) to European Standardisation Organisations in support of safe and trustworthy AI systems, to be adopted in accordance with Regulation 1025/2012. The availability of funding will be linked to the acceptance and execution of that request. The activities should be carried out with reference to the same timing considered for the standardisation request. Moreover, this activity could also focus on other, non-high risk, new technology products in particular virtual reality and augmented reality products.

Activities that can be funded (scope)

The following activities can be funded under this action: I. the **development and revision of European standards or European standardisation deliverables which is necessary and suitable for the support of Union legislation and policies;** II. the **performance of preliminary or ancillary work in connection with European standardisation,** including studies, cooperation activities, including international cooperation, seminars, evaluations, comparative analyses, research work, laboratory work, inter-laboratory tests, conformity evaluation work and measures to ensure that the periods for the development and the revision of European standards or European standardisation deliverables are shortened without prejudice to the founding principles, especially the principles of openness, quality, transparency and consensus among all stakeholders.

In November 2022, the European Commission started a third call for proposals. Three of the topics are of major relevance to the role and function of harmonised standards Topic 10 – Enhancing the involvement of under-represented stakeholders in the standardisation activities of ETSI; Topic 12 – Mapping of standards related with the Cyber Resilience Act proposal by CEN-CENELEC (CEN-CENELEC); Topic 13 – Mapping of standards related with the Cyber Resilience Act proposal by ETSI (ETSI).⁴⁰⁵

c) Implementing Decision on a Standardisation Request

A first version bore the promising title ‘*standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence on trustworthy AI*’.⁴⁰⁶ The revised version has considerably toned down the language to a rather meaningless message: ‘*standardisation request to the European Committee for Standardisation (i.e. CEN)*’

⁴⁰⁵ The third ESOs call for proposals for 2022 will support the Standardisation activities performed by CEN, CENELEC and ETSI https://eisma.ec.europa.eu/news/third-esos-call-proposals-2022-will-support-standardisation-activities-performed-cen-cenelec-and-2022-11-08_en

⁴⁰⁶ COMMISSION IMPLEMENTING DECISION of C(2023)3215 COMMISSION IMPLEMENTING DECISION of 22 May 2023 on a standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence (on file with the author).

and the European Committee for Electrotechnical Standardisation (i.e. CENELEC) in support of Union policy on artificial intelligence'. The implementing decision provides a 'definition' of what should be understood by 'trustworthy AI' by simply reiterating the ten issues mentioned already in the Working Programme:

risk management system, governance and quality of datasets used to build AI systems, record keeping through built-in logging capabilities, transparency and information to users, human oversight, accuracy specifications, robustness specification, cybersecurity specifications, quality management system for providers, including post-market monitoring process, conformity assessment.

Fundamental rights are mentioned 14 times, ethical principles not at all. The Annex to the Implementation Request is supposed to deliver more concrete information – at least, this was what an unbiased reader would expect. However, the implementing decision together with the Annex is *nothing less than an attempt to break down the legal requirements under Chapter II and Chapter III AIA-P and to give them a new heading 'trustworthy AI'*. This consequence may be concluded from Rec. 1 'make the Union a global hub for trustworthy AI'. In contrast to a previous draft, Article 1 of the final draft no longer refers to 'safe and trustworthy AI' but to 'Union Policy on Artificial Intelligence'. Whilst this change might not make such a difference in practice, due to the reference in the recitals to safe and trustworthy AI, nevertheless extraction of the language indicates a kind of downgrading.

aa) Trustworthy AI and Generally Acknowledged State of the Art

The overall message remains the same, though. Compliance with Chapter II and Chapter III of the AIA-P indicates trustworthiness. References to fundamental rights abound, whereas ethical standards vanish in the haze. The number of references to fundamental rights has even increased in the final decision, from 5 to 14. However, not much has been added in substance, perhaps with one exception, that is, under the final version of Article 2 (1) (b) the ESOs are requested to set up a working programme:

to ensure that European standards and European standardisation deliverables are in conformity with Union law on fundamental rights and Union data protection law, in accordance with Annex II.

Annex II 1. Requirements for all European standards and European standardisation deliverables provides for much more striking findings:

*European standards and European standardisation deliverables shall reflect **the generally acknowledged state of the art** in order to minimise risks to the health and safety and fundamental rights of persons as guaranteed in the Charter of Fundamental Rights of the European Union as well as in applicable EU law aiming to protect fundamental rights that arise from the design and development of AI systems in view of their intended purpose. State-of-the-art should be understood as a developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience and which is accepted as good practice in technology. **The state of the art does not necessarily imply the latest scientific research still in an experimental stage or with insufficient technological maturity.** To the purpose of ensuring that European standards and European standardisation deliverables are in line with Union law on **fundamental rights and Union data protection law, CEN and CENELEC shall gather relevant expertise in those areas** (emphasis added).*

The European Commission is launching the standardisation request prior to adoption of the AIA and prior to any agreement on the appropriate level of protection against risks resulting from AI systems. In light of the speed and the difficulties – if not the impossibility of foreseeing the potential impact of AI on society, downgrading the level of scrutiny to the ‘*generally acknowledged state of the art*’ is miles away from the benchmark the HLEG Guidelines have set on ‘*human-centric, secure, ethical and trustworthy AI*’.⁴⁰⁷ The formula sounds like a *carte blanche* for using society as a test field for experimenting with technologies that are not yet the ‘state of the art’, let alone ‘state of science and technology’.⁴⁰⁸ CEN-CENELEC are requested to make sure that the necessary *legal* expertise is available. The last sentence of Annex II delegates the responsibility for compliance with fundamental rights to the ESOs. Astonishingly, data protection law is explicitly mentioned – but not consumer law. In light of ISO/IEC and IEEE activities, what remains to be highlighted is the degree of legalisation and juridification. One might wonder, though, whether the broad language in the AIA-P provides sufficient guidance in ‘upgrading’ ISO/IEC and IEEE standards, let alone the question whether the ESOs are willing and are in a position to combine technical with legal expertise.

Moreover, there are a couple of remarkable further shortcomings and these are not to the benefit of consumers. Technical documentation under Article 11 AIA-P does not form part of the implementing decision. However, technical documentation, the degree of scrutiny and its accessibility are absolutely crucial for any consumer action aiming at defence of consumer interests with regard to all the topics mentioned in Chapter II. There is equally no reference to foreseeable use or foreseeable misuse. Instead, the Annex refers eight times to the intended use – which means that the European Commission empowers all those who set up the AI system to define the potential use, but without taking foreseeable use or foreseeable misuse into account. This in turn means that the whole dimension of descriptive and applied ethics is set aside, specifically, those who are the addressees of AI systems, those who may benefit or suffer, their perspectives and their way of looking at AI systems does not appear on the radar of the European Commission. This is a severe flaw in comparison to the HLEG Guidelines, because thereby the European Commission reduces the potential input of stakeholder participation. The wonderful words of the European Commission on strengthening inclusiveness do not go beyond Article 5 Reg. 1025/2012 with the exception of Article 3 Implementing Decision, which imposes reporting duties on CENELEC and besides pressure on ETSI to revise its voting procedure, resulting from the amendment to Reg. 1025/2012 through Regulation 2022/2480. As the EU is a latecomer, it would be crucial to integrate into the Standardisation Request how potential conflicts with ISO/IEC and IEEE should be handled, and what the place for stakeholders might be in resolving conflicts. These implications will be taken up in the proposed revision of Regulation 1025/2012.⁴⁰⁹

In sum, the specifications in the Annex to the Standardisation Request are an incomplete version of the more detailed and more specific legal requirements in Chapter III of the AIA-P. Only occasionally is the Standardisation Request more specific than the AIA-P. One obvious argument might be the need to draw a distinction between what is technical and what is legal. This is particularly clear with regard to Chapter III AIA-P, which differentiates between the various operators and their duties. However, if one looks into the Chapter II AIA-P rules and compares them with the Standardisation Request, it is hardly understandable why the text of

⁴⁰⁷ Under IV 2 b).

⁴⁰⁸ H-W Micklitz, in Ch Joerges et al. (58) at 61 and 84.

⁴⁰⁹ Under VI.

the corresponding articles is not fully reiterated in the request. Does concretisation through a standardisation request mean reduction and adaptation of legal requirements to the feasibility of standardisation?

bb) Ten Mandated Standards

The following chart:

- reproduces the ten projects which the European Commission intended to initiate to develop ‘European standards or European standardisation deliverables’,
- sums up the specification,
- highlights references to respective provisions in the AIA-P, the CRA-P and the DSA and
- offers an initial analysis of the consumer impact in light of the HLEG Guidelines, which are taken as a benchmark.⁴¹⁰

Regulation 1025/2012 does not define what a ‘European standardisation deliverable’ is. In practice it could be everything other than a European (harmonised) standard, means which do not justify a presumption of conformity. CEN-CENELEC distinguish between

- a European Standard (EN),
- Technical Specification (CEN/TS), that serves as a normative document in areas where the actual state of the art is not yet sufficiently stable for a European Standard;
- Technical Report (CEN/TR), for information and transfer of knowledge;
- CEN Workshop Agreement (CWA), which aims at bringing about consensual agreements based on deliberations of open Workshops with unrestricted direct representation of interested parties;
- Guides (CEN Guide), with information about standardisation principles and policies and guidance to standards writers.⁴¹¹

The following information is taken from the Standardisation Request, adopted on the 22.5.2023.⁴¹² In line with the overall approach taken on the scope of EU Digital Policy Legislation, it deliberately includes the CRA-P and the DSA, so as to demonstrate potential overlaps.

⁴¹⁰ The analysis includes ANEC’s comments to the implementing decision which are on file with the author.

⁴¹¹ <https://boss.cen.eu/reference-material/guidancedoc/pages/del/>

⁴¹² Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, Brussels, 22.5.2023, C(2023) 3215 final

| Components | Content/Abstract of Annex II (emphasis added HWM) | Juridification through AIA-P, CRA-P, DSA | Impact on consumers in light of the HLEG Guidelines |
|--|---|---|--|
| 2.1. Risk management systems | <p>Risk management shall be intended as a continuous iterative process run throughout the <i>entire lifecycle of the AI system</i> which is aimed at preventing or minimising the relevant risks to health, safety or fundamental rights</p> <p>Specifications shall be drafted in such a way that, for AI systems which are safety components of products, risk management system aspects related to the AI system may be integrated into the risk management system for the overall product</p> | <p>Art 9 AIA-P Risk Management Systems (AIA-P rules are more specific)</p> <p>Harmonised standards explicitly mentioned in Art 9 (3)</p> <p>CRA-P (-)</p> <p>DSA Art 34 Risk Assessment</p> | <p>HLEG 2 robustness and safety</p> <p>Entire lifecycle, a remainder of the fourth element in HLEG guidelines aiming at descriptive and applied AI, which enables bringing in the consumer perspective (foreseeable use)</p> <p>Potential overlap of the envisaged HS with the rules in the DSA on risk assessment. Should minors not be given the same importance in Art 9 AIA-P?</p> |
| 2.2. Governance and quality of datasets used to build AI systems | <p>(a) include specifications for adequate data governance and data management procedures to be implemented by providers of AI systems (with specific focus on data generation and collection, data preparation operations, <i>design choices</i>, procedures for detecting and addressing biases or any other relevant shortcomings in data)</p> <p>(b) include specifications on <i>quality aspects</i> of datasets used to train, validate and test AI systems (including representativeness, relevance, completeness, correctness)</p> | <p>Art 10 AIA-P Data Governance (AIA-P rules are more specific)</p> <p>CRA-P (-)</p> <p>DSA nothing on datasets, instead databases</p> | <p>HLEG 3 privacy and data governance</p> <p>No guidance on differentiating between institutional, procedural, and substantive governance</p> <p>HLEG 5 Non-discrimination and fairness</p> <p>Design choices and regulation by design</p> <p>Requirements on training sets without mentioning biases and the risk of discrimination</p> <p>The requirements of Articles 10 (2) f) and 10 (4) should not be included⁴¹³</p> |
| 2.3. Record keeping through logging capabilities | <p>Automatic logging of events for AI systems. Those specifications will enable <i>traceability</i> of those systems throughout <i>their lifecycle</i> as well as monitoring of their operations and will facilitate post-market monitoring of AI systems by providers</p> | <p>Art 12 AIA-P Record keeping (ditto)</p> <p>CRA-P (-)</p> <p>DSA Art 30 Traceability of Traders</p> | <p>HLEG 4 Transparency</p> <p>Record keeping and traceability will be crucial in case consumers are harmed and seeking compensation</p> |
| 2.4. Transparency and information for users | <p>Specifications related to:</p> <p>(a) <i>design</i> and development solutions which ensure transparency of the operation of the AI system to enable <i>users</i> to understand the system's output and use it appropriately</p> <p>(b) instructions for use accompanying AI systems, including information on the system's capabilities and limitations as well as on maintenance and care measures, taking into particular account:</p> <p>(i) The need to identify and appropriately distinguish information which is relevant and comprehensible for different professional user profiles and non professional users⁴¹⁴</p> <p>(ii) Without prejudice to point (i), the need to ensure that identified information is sufficient to enable users to interpret the system's output and use it appropriately in a way that mitigates risks</p> | <p>Art 13 Transparency and provision of information of users (using an AIA-P system under its authority)-with regard to content less specific</p> <p>CRA-P only with regard to the financial statement</p> <p>DSA Art 15 Transparency reporting obligations for providers of intermediary services and Art 24 for providers of platforms, Art 27 Recommended System Transparency, Art 34 Online advertising transparency, Art 42 Transparency reporting obligations for VLOPs</p> <p>DSA Art 32 Right to information</p> | <p>HLEG 4 Transparency</p> <p>Design, user, but in contrast to Art 13 AIA-P also lay user (the sole example where the IA reaches beyond the AIA-P)</p> <p>Applicability of the envisaged HS to certain risk Art 52 AIA-P? If yes, stakeholder participation would be even more important</p> <p>However, transparency is a purely legal concept – can interpretation of what transparency means be left to the ESOs? Raising the question provides the answer. Concretisation and to what extent transparency enshrines or even requires explainability is a legal question, which does not exclude that a potential standard goes beyond the law</p> <p>Last version amended to the detriment of the consumer</p> |

⁴¹³ For the reasons see under III 1 d).

⁴¹⁴ In the previous version laypersons.

| Components | Content/Abstract of Annex II (emphasis added HWM) | Juridification through AIA-P, CRA-P, DSA | Impact on consumers in light of the HLEG Guidelines |
|--|--|--|---|
| 2.5. Human oversight | <p>Measures and procedures for human oversight of AI systems which are:</p> <p>(a) identified and built, <i>when technically feasible</i>, into the AI system by the provider before it is placed on the market or put into service</p> <p>(b) identified by the provider before placing the AI system on the market or putting it into service and that are appropriate to be implemented by the user</p> <p>These shall include measures <i>enabling users to understand, monitor, interpret, assess and influence relevant aspects of the operation of AI systems</i></p> <p>Shall also establish, <i>where justified</i>, appropriate oversight measures which are specific to certain AI systems <i>in consideration of their intended purpose</i>. With respect to AI systems intended for remote biometric identification of persons, human oversight measures provide for the possibility⁴¹⁵ that <i>no action or decision is taken by the user on the basis of identification resulting from the system unless this has been separately verified and confirmed by at least two natural persons</i></p> | <p>Art 14 AIA-P Human Oversight (ditto)</p> <p>CRA-P (-)</p> <p>DSA (-)</p> | <p>HLEG 1 Human agency and human oversight</p> <p>No clarification as to what is meant by ‘protection against risks’ or ‘maintaining human control’,⁴¹⁶ with the exception of biometric identification</p> <p>Proviso – technically feasible</p> <p>Art 14 (4) speaks of individuals, but means user of the AI system</p> <p>Comprehensibility and explainability</p> <p>Last version amended to the detriment of the consumer: ‘must inter alia ensure’</p> |
| 2.6. Accuracy specifications for AI systems | <p>“accuracy” shall be understood as referring to the capability of the AI system to perform the task for which it has been designed. This should not be confused with the narrower definition of statistical accuracy, which is one of several possible metrics for evaluating the performance of AI systems</p> <p>..specifications for ensuring an appropriate level of accuracy of AI systems and for allowing providers to declare the relevant accuracy metrics and levels. This (these) European standard(s) or European standardisation deliverable(s) must also define, where justified, a set of appropriate and relevant tools and <i>metrics to measure accuracy against suitably defined levels</i>, which are specific to certain AI systems in consideration of their <i>intended purpose</i></p> | <p>Art 15 AIA-P Accuracy, robustness and cybersecurity – here robustness only</p> <p>Slightly more specific</p> <p>CRA-P Art 8 High Risk Systems</p> <p>DSA in connection with transparency and reporting obligations</p> | <p>HLEG 2 Robustness and safety</p> <p>Intended (not foreseeable use)</p> |

⁴¹⁵ In the former version ‘must inter alia ensure’.

⁴¹⁶ See under IV. 2) b)

| Components | Content/Abstract of Annex II (emphasis added HWM) | Juridification through AIA-P, CRA-P, DSA | Impact on consumers in light of the HLEG Guidelines |
|--|---|--|---|
| 2.7 Robustness specifications for AI systems | Specifications for the robustness of AI systems, <i>taking into consideration relevant sources of errors, faults and inconsistencies</i> , as well as interactions of the AI system with the environment | Art 15 AIA-P Accuracy, robustness and cybersecurity – here robustness only Identical, other systems in (3) replaced through environment CRA-P Art 3 High Risk Systems Art 47 (2) a) Codes of Conducts for Accessibility) | HLEG Robustness and safety Errors, faults and inconsistencies (but not foreseeable misuse) Last version amended to the detriment of the consumer, deleted after environment: ‘including those AI systems which continue to learn after being placed on the market or put into service, notably in respect to feedback loops’ |
| 2.8. Cybersecurity specifications | Suitable organisational and technical solutions, to ensure that AI systems <i>are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the AI systems’</i> vulnerabilities. Organisational and technical solutions should thus include, where appropriate, measures to prevent and control for cyberattacks trying to manipulate AI-specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial examples), or trying to exploit vulnerabilities in an AI system’s digital assets or the underlying ICT infrastructure. These technical solutions should be appropriate to the relevant circumstances and risks | Art 15 AIA-P Accuracy, robustness and cybersecurity here robustness only Identical CRA-P omnipresent, distinction between cybersecurity risks and signification cybersecurity risks, Art 3 (35) and (36) | HLEG Robustness and safety The requirements need to be much more specific, ⁴¹⁷ and cover suitable organisational and technical solutions such as secure authentication, security updates, incident management and abuse alerts, encryption and organisational requirements such as information on product security status and support, and expected product lifetime Concretise penetration testing |
| 2.9. Quality management systems for providers, including post-marketing monitoring process | Specification for a quality management system to be implemented by providers of AI systems within their organisations. These systems must ensure <i>inter alia continuous compliance</i> of an AI system with the aspects described under points 2.2. 2.3, 2.4, 2.5, 2.6, 2.7 and 2.8. Appropriate consideration should be given to implementation of quality management system measures by medium and small size organisations Specifications shall be drafted such that the quality management system aspects related to the AI system may be integrated in the overall management system of the provider | Art 17 Quality management systems (less specific and less comprehensive) HS explicitly mentioned Art 17 (1) e) CRA-P (-) DSA compliance omnipresent, in connection with transparency and reporting obligations, with regard to VLOP institutional requirements | HLEG 3 Privacy and data governance Post-marketing – continuous monitoring is absolutely crucial under the aspect of the lifecycle, of accessibility of data with regard to possible action No distinction between institutional, procedural, and substantive governance Quality management systems should also include robust consumer relationship management and systems for dispute resolution, complaints, customer redress, objection, accessibility, recall of harmful products and a post-marketing monitoring system. A vulnerability disclosure policy should be implemented ⁴¹⁸ |

417 Taken from ANEC’s comments.

418 Taken from ANEC’s comments.

| Components | Content/Abstract of Annex II (emphasis added HWM) | Juridification through AIA-P, CRA-P, DSA | Impact on consumers in light of the HLEG Guidelines |
|------------------------------------|--|--|--|
| 2.10. Conformity assessment | <p>shall provide procedures and processes for conformity assessment activities related to AI systems and quality management systems of AI providers</p> <p>This (these) European standard(s) or European standardisation deliverable(s) shall also provide criteria for assessing the competence of persons tasked with the conformity assessment activities</p> <p>This (these) European standard(s) or European standardisation deliverable(s) shall consider both the scenarios whereby the conformity assessment is carried out by the provider itself or with the involvement of a professional external third-party organisation</p> | <p>Art 19 in combination with Art 43 Conformity assessment and the respective annexes</p> <p>CRA-P Art 24</p> <p>DSA nothing on conformity, compliance instead, with different obligations according to the size of providers</p> | <p>Requirements on self and third-party certification</p> <p>Self-certification no requirements on the governance structure – institutional safeguards for instance</p> <p>Testing part of self- and third-party certification</p> <p>But what kind of testing – penetration testing/red teaming?</p> <p>What exactly should be tested – compliance with ‘fundamental values and human rights’?</p> <p>Last version much less specific than the former one⁴¹⁹</p> |

c) Evaluation and Consumer Concerns

The Standardisation Request sets the course for the future as it is for the ESOs to concretise binding legal requirements. Harmonised European standards will turn into the benchmark for:

- the feasibility of transferring the New Approach/NLF into the digital economy,
- interaction between binding legal requirements and harmonised technical standards,
- extending standardisation into the field of fundamental rights;
- giving shape to trustworthy AI and ethical AI;
- the role and function of stakeholders in standards-making and
- surveillance of technical standards.

Moreover, a number of legal concepts will have to be upgraded to the digital economy, such as ‘digital governance’, ‘traceability’, ‘human oversight’, ‘transparency’, ‘accuracy’, ‘robustness’, ‘intended use’, ‘foreseeable use’, ‘foreseeable misuse’ and on so on and so on. The overlap of many of these concepts with the consumer acquis is striking, but the EU documents here under scrutiny lack any reference whatsoever.

Seen through the lenses of the consumer and their organisations, the Standardisation Request suffers from serious deficits:

- missing topics such as technical documentation and its accessibility,
- missing dimension of applied ethics, there is no holistic perspective and there is no mandate to standardise use cases

⁴¹⁹ Verification and validation procedures and methodologies to assess whether: (a) an AI system that is placed on the market or put into service is fit-for-purpose, notably with regard to aspects described under points 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7 and 2.8. This (these) European standard(s) or European standardisation deliverable(s) should contain objectively verifiable criteria and should indicate not only the risks that they cover, but also the major risks that they do not cover; (b) quality management system measures and processes, as described under point 2.9, are appropriately implemented by the provider of an AI system ...deliverable(s) should consider both scenarios where conformity assessment is carried out by the provider itself or with the involvement of a professional external third-party organisation.... should include specifications for testing AI systems in the context of conformity assessment

- missing concretisation of what lifecycle means with regard to consumers
- missing mandate on laying down testing requirements,
- very limited elements of strengthening participation by stakeholders in development of AI standards (Recital 14: ‘European Standardisation Organisations are then expected to take all steps to ensure the involvement of civil society organisations in the standardisation processes and in the consensus-building exercise’),
- no guidance on how and by whom fundamental rights will be integrated into standardisation work,
- no reference to the role and function of the consumer acquis with regard to legal concepts, such as transparency, traceability, explainability, governance,
- no discussion on the impact of ethics on the AI profession, on software designers and software engineers.⁴²⁰

It is in no way clear from the various regulatory activities of the European Commission – be it the AIA-P, the working programme, the call, the Standardisation Request or any other policy document – how the ESOs should deal with the fundamental rights issue once they have build the necessary skills, whether this sensitive field should and could be left to the HAS consultant, to either self-certification or third-party certification, or whether the European Commission should ensure compliance with fundamental rights before a harmonised standards is published.

5. CEN-CENELEC, ETSI on Trustworthy AI Standards

Whilst the three ESOs are all addressed in Regulation 1025/2012, they have developed very different activities in the field of AI standards, not least due to their different profile and policy intentions.

a) CEN-CENELEC Initiatives in the Field of AI

CEN-CENELEC have set up a working group on AI CEN/CLC/JTC 21. The purpose is ‘to produce standardisation deliverables to address European market and societal needs and to underpin primarily EU legislation, policies, principles, and values’. There is no mention of trustworthiness of AI, nor of safety, of ethical values, of fundamental rights, at least not in the general description.⁴²¹ The field is therefore much broader than just focusing on ‘safe, ethical trustworthy AI’, which is the objective of EU digital market policy. CEN-CENELEC set up four working groups – WG 1 Strategic Advisory Group, WG 2 Operational Aspects, WG 3 Engineering Aspects, WG 4 Foundational and Societal Aspects. So far, concrete activities cannot be associated with the different working groups. The relevant information has to be taken from the working programme. The website⁴²² informs the reader on the status and the next steps. None of the projects listed have yet led to adoption of a European standard. However, it seems that the work is partly

⁴²⁰ U Gasser and C Schmitt, The Role of Professional Norms in the Governance of Artificial Intelligence (April 25, 2019). Forthcoming in: M D Dubber, F Pasquale, and S Das (eds), The Oxford Handbook of Ethics of AI, Oxford University Press, Available at SSRN: <https://ssrn.com/abstract=3378267> or <http://dx.doi.org/10.2139/ssrn.3378267>

⁴²¹ https://standards.cencenelec.eu/dyn/www/f?p=305:22:0:::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1E7E2C95DEE9A536E535BC6BAE2D4C821

⁴²² https://standards.cencenelec.eu/dyn/www/f?p=305:22:0:::FSP_ORG_ID,FSP_LANG_ID:2916257,25&cs=1E7E2C95DEE9A536E535BC6BAE2D4C821

more advanced than the website demonstrates, as I learnt from interviews with experts taking part in standardisation work.⁴²³

The following table lists the activities started, independent of the WG with which it might be associated. The table is built around the name of the project, the abstract made available on the website, potential overlap with the respective articles of the pending EU legislation as well as the Standardisation Request, ISO/IEC and IEEE standards, whether already adopted or under development. The last column points to the consumer impact in light of the HLEG principles and the EU understanding of ‘trustworthy AI’ as being equated with Chapters II and III of the AIA-P. CEN-CENELEC’s position on the concept of ‘trustworthiness’ has already been analysed in comparison to the HLEG guidelines and the ISO/IEC and IEEE standards.⁴²⁴

| Project | Content/Abstract | Overlap with AIA-P, CRA-P, DSA, the implementing decision and ISO/IEEE standards | Consumer impact in light of the HLEG Guidelines |
|--|--|--|--|
| prCEN/TR XXX ⁴²⁵ (pr=JT021009) AI Risks – Checklist for AI Risk Management preliminary | Checklist of risk criteria for assessment guidance as well as risk events and their assessment for any system using AI | Overlap with Art 9 AIA-P and Art 34 DSA Implementing Decision 2.1. Risk management | HLEG Robustness and safety |
| prCEN/TR XXX (pr=JT021010) Information Technology – Artificial Intelligence – Green and Sustainable AI ⁴²⁶ under drafting | Framework for quantifying the environmental impact of AI and its long-term sustainability during life cycle and use | Overlap with Art 9 AIA-P (2) The risk management system will consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating (with a set of criteria in the AIA-P) Art 12 CRA-P Record keeping and Art 15 Accuracy, robustness and cybersecurity Not covered by the implementing decision | HLEG Societal and environmental well-being |
| prCEN/TR XXX (pr=JT021007) Data Governance and data quality for AI in the European context ⁴²⁷ preliminary | Guideline for implementing AI systems, aligned with EU Regulation | Mentions AIA-P and the Data Governance Act Overlap with Art 10 AI. Implementing Decision – nearly congruent with 2.2. Governance | HLEG privacy and data governance Fourth element – the holistic perspective Question: lifecycle in risk management and data lifecycle in the project? |
| prCEN/CLC/TR XXXX (pr=JT021002) Artificial Intelligence – Overview of AI tasks and functionalities related to natural language processing under drafting committee stage | No abstract | Not part of the EU working programme | |

⁴²³ Interview with experts from the standardisation organisations.

⁴²⁴ Under IV 2 c).

⁴²⁵ https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:76987,25&cs=1142318F59535D0D20B2BE9063981FAE6

⁴²⁶ https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:77083,25&cs=197A5B7DE5AF67591683D893C2D99E9D2

⁴²⁷ https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:76985,25&cs=1B86307C96416BF6C255E61A6B4097187

| Project | Content/Abstract | Overlap with AIA-P, CRA-P, DSA, the implementing decision and ISO/IEEE standards | Consumer impact in light of the HLEG Guidelines |
|---|---|--|---|
| prCEN ISO/IEC/TS 12791 (pr=JT021013) ⁴²⁸ Information technology – Artificial intelligence – Treatment of unwanted bias in classification and regression machine learning tasks preliminary | Deals with mitigation techniques that can be applied throughout the AI system lifecycle in order to treat unwanted bias | Art 10 AIA-P Data governance Overlap with WP EC 2.2. Data governance EC WP 2.2. Data Governance Reference document ISO/IEC TS 12791 (EQV) IEC Technical Body ISO/IEC JTC 1 | HLEG Robustness and safety ISO/IEC TR 24027:2021 suggests that unwanted bias can be overcome through defining the intended use. Contradiction to use cases and to a holistic perspective on lifecycle |
| prCEN/CLC/TR 17894 (pr=JT021001) Artificial Intelligence Conformity Assessment ⁴²⁹ under drafting | Sets out a review of current methods and practices (including tools, assets, and conditions of acceptability) for conformity assessment | Mentions EU AI strategy Overlap with Art 17 AIA-P Quality management systems (less specific and less comprehensive) Art 19 AIA-P in combination with Art 43 EC WP 2.10 2.10 | HLEG Accountability |
| prEN ISO/IEC 22989 (pr=JT021004) Information technology – Artificial intelligence – Artificial intelligence concepts and terminology (ISO/IEC 22989:2022) ⁴³⁰ enquiry stage | Establishes terminology for AI and describes concepts in the field of AI which can be used in development of other standards and in support of interested parties or stakeholders is applicable to all types of organisations | Overlap with the definition of AI in AIA-P Reference document ISO/IEC 22989:2022 (EQV) IEC Technical Body ISO/IEC JTC 1 ICS 01.040.35 – Information technology (Vocabularies) 35.020 – Information technology (IT) in general | |
| prEN ISO/IEC 23053 (pr=JT021005) Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (ISO/IEC 23053:2022) ⁴³¹ enquiry stage | Framework for describing a generic AI system using ML technology | Not part of the EU working programme Reference document ISO/IEC 23053:2022 (EQV) ICS 35.020 – Information technology (IT) in general | |
| prEN XXXXX (pr=JT021006) AI-enhanced nudging ⁴³² under drafting | Definitions, concepts, and guidelines to address specifically AI-enhanced nudging mechanisms by organisations | Not part of AIA-P, CRA-P IEEE P7008™-2021 – Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems ⁴³³ Project mentions GDPR and UCPD as reference points of regulations without capturing the subtleties Not part of the EU working programme | HLEG Human agency and oversight Digital architecture may affect autonomy |
| prEN ISO/IEC 23894 (pr=JT021016) Information technology – Artificial Intelligence – Guidance on risk management ⁴³⁴ under drafting | This document provides guidance on how organisations that develop, produce, deploy or use products, systems and services that utilise artificial intelligence (AI) can manage risk specifically related to AI | Art 9 AIA-P Risk management Art 34 DSA EC WP 2.1. Risk Management Reference document ISO/IEC 23894:2023 (EQV) Technical Body ISO/IEC JTC 1 | HLEG Robustness and safety |

428 https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:77584,25&cs=158BAC287B70CAF2AAF9C919B528EA2C1

429 https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:75934,25&cs=170463965A18711F2A19536751DBEBA84

430 https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:76616,25&cs=19D5CC537D829476F1B42C2C7C7105832

431 https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:76617,25&cs=175908B3693FAE6F804270BDF8CF8BC0A

432 https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:76794,25&cs=1473286A1FA8DA98C9EBA0377F8C67CCD

433 See under IV 3 a) bb).

434 https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:77587,25&cs=135C3DE21AAF5EDE3D270EB3C0A230933

| Project | Content/Abstract | Overlap with AIA-P, CRA-P, DSA, the implementing decision and ISO/IEEE standards | Consumer impact in light of the HLEG Guidelines |
|--|--|---|--|
| prCEN/CLC ISO/IEC/TR 24029-1 (pr=JT021018) Artificial Intelligence (AI) – Assessment of the robustness of neural networks – Part 1: Overview ⁴³⁵ under drafting | Provides background about existing methods to assess robustness of neural networks | Art 15 AIA-P Accuracy, robustness, cybersecurity Art 8 CRA-P EC WP 2.6 and 2.7. | HLEG Robustness and safety |
| prEN ISO/IEC 42001 (pr=JT021011) Information technology – Artificial intelligence – Management system ⁴³⁶ proposal stage | No abstract | Art 17 AIA-P Quality management EC WP 2.9 Quality management Reference document ISO/IEC 42001 (EQV) IEC Technical Body ISO/IEC JTC 1 | HLEG privacy and data governance |
| CEN-CENELEC Workshop on 'Age-Appropriate Digital Services Framework' ⁴³⁷ | Framework for developing age-appropriate digital services for situations where users are children, and by doing so, tailors the services provided so that they are age-appropriate | Overlap with DSA Art 44 voluntary standards (non-harmonised European standards), including protection of minors Overlap with EU policy initiative on euConsent Overlap with working programme 23 Topic 12 SMP-STAND-2023-ESOS-01-IBA Age verification online | HLEG Human agency and oversight |
| CEN-CENELEC Workshop on Digital sovereignty – European perspective, general approach and implications on standardisation ⁴³⁸ | Defines digital sovereignty is as a concept based on a set of common principles, applicable equally to individuals, organisations, and states ⁴³⁹ | | HLEG Human Agency and oversight Joint initiative by CN/CENELEC, AFNOR and VDE |

The various initiatives can be divided in two groups: those where CEN-CENELEC are in a way forestalling the agenda of the European Commission, now concretised in the Standardisation Request; and those where CEN-CENELEC are moving beyond the agenda of the European Commission. The first set of projects is more or less determined by the AIA-P, the second by potential competition between CEN-CENELEC and ISO/IEC or IEEE, provided the projects are comparable. More telling is the horizontal comparison between the ISO/IEC, IEEE, CEN-CENELEC and ETSI activities. This will be done after having completed the review of ETSI.⁴⁴⁰

b) ETSI initiatives in the field of AI

The ETSI Industry Specification Group on Securing Artificial Intelligence (ISG SAI) was established in 2019.⁴⁴¹ The group focuses on three key areas: enhancing security, mitigating against attacks that leverage AI, and securing AI itself from attack.⁴⁴² Five Active Work Items are under way:

● Security Testing of AI

⁴³⁵ https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:77589,25&cs=1B03DCBF986E06FC606CCB85FA379742E

⁴³⁶ https://standards.cencenelec.eu/dyn/www/f?p=305:110:0:::FSP_PROJECT,FSP_LANG_ID:77581,25&cs=1B229400423DCBB41B64CBD21E2AD4473

⁴³⁷ <https://www.cencenelec.eu/news-and-events/news/2022/workshop/2022-03-28-digital-services/>

⁴³⁸ <https://www.cencenelec.eu/news-and-events/news/2023/workshop/2023-01-23-digital-sovereignty/>

⁴³⁹ The CAW working agreement is 28 pages long and sets out the framework in which the current standardisation initiative should be embedded: https://www.cencenelec.eu/media/CEN-CENELEC/News/Workshops/2023/draftcwa_forpublicconsultation.pdf

⁴⁴⁰ Under IV.6.

⁴⁴¹ With regard to the working programme, ETSI White Paper No. #34 Artificial Intelligence and future directions for ETSI 1st edition – June 2020 https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp34_Artificial_Intelligence_and_future_directions_for_ETSI.pdf

⁴⁴² <https://www.etsi.org/committee/sai>

- Explainability and Transparency of AI Processing
- Privacy aspects of AI/ML Systems
- Artificial Intelligence Computing Platform Security Framework
- Traceability of AI Models

Searching for ‘trustworthiness’ on the ETSI website leads to five major documents:⁴⁴³

- the 2023 Report on Explainability and transparency of AI processing,⁴⁴⁴
- the 2022 Study into the challenges of developing harmonised standards in the context of future changes to the environment,⁴⁴⁵
- the 2021 Report on Data Supply Chain Security,⁴⁴⁶
- the 2020 Report on Securing Artificial Intelligence (SAI) Problem Statement⁴⁴⁷ and
- the 2019 Report User Group – User centric approach in Digital Ecosystem.⁴⁴⁸

All reports can be downloaded for free. However, they are all copyright-protected and can therefore not be reproduced.

ETSI is not directly involved in the overall debate on how to conceptualise trustworthy and ethical AI.⁴⁴⁹ Instead, ETSI focuses on areas which are of particular interest for its stakeholders. This might be hardware much more than software.⁴⁵⁰ That is why ETSI’s approach looks more focused. In order to ensure compatibility, the same key words are used in screening ETSI’s five reports – trustworthiness, trustworthy AI, ethical principles, and fundamental rights. On its website ETSI uses the language of safe and trustworthy AI – without ‘ethical’ though and obviously taken from the first call of the European Commission.⁴⁵¹ The five reports use the terms to a very different degree.

⁴⁴³ <https://www.etsi.org/standards#page=6&search=artificial%20intelligence&title=1&etsiNumber=1&content=1&version=1&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=2023-03-24&harmonised=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1>

⁴⁴⁴ https://www.etsi.org/deliver/etsi_gr/SAI/001_099/007/01.01.01_60/gr_SAI007v010101p.pdf

⁴⁴⁵ https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63987&curlItemNr=33&totalNrItems=198&optDisplay=100000&qSORT=TB&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qEND_CURRENT_STATUS_CODE=11+WI%3BM58&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qCLUSTER_BOOLEAN=OR&qFREQUENCIES_BOOLEAN=OR&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=TUBE

⁴⁴⁶ https://www.etsi.org/deliver/etsi_gr/SAI/001_099/002/01.01.01_60/gr_SAI002v010101p.pdf

⁴⁴⁷ https://www.etsi.org/deliver/etsi_gr/SAI/001_099/004/01.01.01_60/gr_SAI004v010101p.pdf

⁴⁴⁸ https://www.etsi.org/deliver/etsi_tr/103400_103499/103438/01.01.01_60/tr_103438v010101p.pdf

⁴⁴⁹ Under IV. 2 c).

⁴⁵⁰ Interview with representatives from the business environment.

⁴⁵¹ <https://www.etsi.org/technologies/artificial-intelligence>

| | Abstract/content/purpose | Overlap with AIA-P, CRA-P, DSA, the implementing decision and ISO/IEEE standards | Consumer impact in light of the HLEG Guidelines |
|---|---|--|--|
| 2019 Report User Group – User-centric approach in Digital Ecosystem | The user is at the heart of the architecture | References to ETSI documents, to ISO 000 20000-1: ‘Service management system requirements’ and to the GDPR No reference to the key words | Report complies with the fourth element of the HLEG guidelines – descriptive and applied AI Use cases: smart meters, interaction within smart city, travel management, video on demand, surveillance of pets, and a generic model Report does not discuss foreseeable use but provides a definition of misuse of AI (under 7.) |
| 2020 Report on Securing Artificial Intelligence (SAI) Problem Statement | The document describes the problem of securing AI-based systems and solutions at each stage of the machine learning including bias, ethics and explainability | References inter alia to the HLEG Guidelines, Organisation for Economic Co-operation and Development (OECD) Council recommendation on Artificial Intelligence and mainly to academic writings Explicit discussion on business ethics, with reference to lawful, ethical, and robust AI systems (but only after a general proviso on their relevance) ⁴⁵² | The categories are by and large in line with the seven principles Missing: safety, non-discrimination and fairness, accountability |
| 2021 Report on Data Supply Chain Security | The document focuses on security, data integrity and techniques for assessing and understanding data quality for performance, transparency, or ethics purposes are applicable to security assurance too | Long list of references to legislation and standards from around the world Explicit reference to the GDPR and data protection laws in the world (under 6.2. policy and legal frameworks) | Data manipulation not defined Trustworthiness not defined, instead referred to ISO/IEC JTC 1 (6.3.) |
| 2022 Study into the challenges of developing harmonised standards in the context of future changes to the environment in which products are being developed and operated | The document examines the background to citation of harmonised standards and explore recommendations made to alter ETSI working practices | Long list of references to EU legislation inter alia, AIA-P and CRA-P (under 2.2.), the <i>Elliott</i> judgment and its implementation in Reg 1025/2012 | The study lays down the position of ETSI in the current procedure on elaboration of harmonised European standards, the critique voiced by the European Commission on ETSI, and the possible ways out ⁴⁵³ |
| 2023 Report on Explainability and transparency of AI processing | The document identifies steps that give assurance of the explainability and transparency of AI processing | Reference to AIA-P and to ETSI documents: Problem Statement Definitions taken from ETSI GR SAI 004 (Report on Problem Statement): on explainability, transparency and trust | |

c) Evaluation and Consumer Concerns

It is near impossible to provide a deeper evaluation of the different initiatives of CEN-CENELEC and ETSI. This is not only due to copyright issues but also due to the very much infant stage of the initiatives. Many of these are overlapping with the Standardisation Request of the European Commission. One might therefore understand the setting up of CEN-CENELEC JTC 21 working groups as a kind of place holder for the now adopted Standardisation Request. Initiation of setting up the groups might then facilitate the next steps, official acceptance or rejection of the Standardisation Request, and taking up the work. Getting a deeper insight on what is behind the various working groups, how advanced the projects are, and where the team would like to go, would require more comprehensive research – unfortunately hindered by the copyright issue, though.

⁴⁵² T Hagendorff, ‘The Ethics of AI Ethics: An Evaluation of Guidelines’. *Minds & Machines* 30, 99–120 (2020) who criticises its marketing nature https://uni-tuebingen.de/fileadmin/Uni_Tuebingen/Forschung/Exzellenzinit/Cluster/Machine_Learning/news/Hagendorff-2020-Minds_and_Machines.pdf

⁴⁵³ See for a more detailed discussion ETSI Technical Report, Study into the challenges of developing harmonised standards in the context of future changes to the environment in which products are being developed and operated, 2022 with a detailed critique of the consequences, in particular with regard to ‘subjective testing’ at 26 with regard to the RED

Formally the European Commission may adopt an implementing decision based on Regulation 1025/2012 in order to speed up standardisation and put the ESOs into a more prominent, legally, and financially secure position. Politically it might not be wise to get the standardisation work started before – in particular – the AIA-P has been adopted. It should be recalled that the harmonised standards that the European Commission is calling for need to be in compliance with binding legal requirements – which are, however, not yet binding because the AIA-P has not yet been adopted. Even if adopted, the AIA-P will not enter into force in the near future. The time lag that European standardisation suffers from speaks in favour of speeding up the process; democratic credentials indicate the opposite.

Two observations deserve to be highlighted: ETSI pursues a different approach and a different language. When reports and studies discuss ethics, trust, and to some extent fundamental rights, they always relate high-flying abstract categories to concrete examples and provide a specific context. Perhaps more importantly, fundamental rights are nearly absent in the reports, whereas both trust (not necessarily trustworthiness) and ethics form an integral part of the debates. The language is also different. ETSI tries to balance out potential risks against gains and keeps a certain distance from abstract categories. This does not mean that they do not see the necessity to engage with trust and ethics – when it comes to it. The overall attitude is nicely expressed in the summary to the ‘problem statement’:⁴⁵⁴

While ethical concerns do not have a direct bearing on the traditional security characteristics of confidentiality, integrity and availability, they can have a significant effect on an individual’s perception of whether a system can be trusted. It is therefore essential that AI system designers and implementers consider the ethical challenges and seek to create robust ethical systems that can build trust among users.

However, one of the most important gaps is missing clarity on use cases and the degree to which they should be integrated. In the use case, business and consumer interests clash. At the same time, there are differences between CEN-CENELEC and ETSI. ETSI seems to be more use-case focused due to their profile, whereas CEN-CENELEC is not addressed in the Standardisation Request due to its voting structure, which is said to allow too much non-European/non-EU influence. Experience gained in implementation of the adopted Radio Equipment Directive (RED) points to the core of the problem on concretising the use case. The Directive covers thousands of products, including consumer products. The challenge is how to find a common denominator for all products, which is the purpose of standardisation. In theory, it might be possible to provide the same level of data protection for all products, independent of their use. However, the counterargument is that the same level of data protection is not needed and that there might be products where a lower standard suffices. The RED example points to the difficulty of how to build categories of potential use case which allow for differentiation. One might very well assume that this kind of conflict considerably delayed the process in the respective WG.⁴⁵⁵

The still infant stage of AI standardisation provides limited evidence on potential conflicts which arise between business and consumers. However, one such example for controversy is ICT standard EN 301 549 ‘Accessibility requirements for ICT products and services’, where Europe is ahead of the international standardisation organisations.⁴⁵⁶ ETSI supported its transforma-

⁴⁵⁴ Problem Statement under 5.3.2.4. p. 17.

⁴⁵⁵ Interview with representative from the standardisation organisations.

⁴⁵⁶ https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf

tion into an ISO/IEC JTC 42 standard, while CEN-CENELEC did not – and EN 301 549 carries the logos of all 3 ESOs. The standard was criticised by stakeholder organisations, ANEC, and EDF due to insufficient safeguards to protect the interests of people with disabilities and insufficient respect for the European Accessibility Act. After its adoption, interested business circles pushed for transformation of the European standard into an international standard. Some countries even started using EN 301 549 for their national accessibility policies (Mexico, Kenya, Japan, India, Canada). The conflict is still unresolved, but might serve as an example where the European Commission could demonstrate that it takes core European values seriously, and that it is ready to fulfil the role of a global standard setter, in order not only to protect European citizens and but to use its regulatory power to the benefit of all persons with disabilities around the world.⁴⁵⁷

6. Comparison ISO/IEC, IEEE, CEN-CENELEC Trustworthy AI Standards with EC WP

The third part provided for an overview of the various standardisation activities at the international level through ISO/IEC and IEEE as well as through CEN and CENELEC, either self-standing activities or those initiated by the European Commission in order to implement Digital Policy Legislation. A comparison between the various activities might help to understand not only the differences in the regulatory approaches of the international organisations, the ESOs, and the EU, but also what it means for the EU to want to become a ‘*global standard setter*’ and to promote ‘*core European values*’ in standardisation of AI. The comparison is meant to set details aside and to lay bare the key messages.

ISO/IEC benefit from the first mover advantage. ISO/IEC and IEEE have been occupying the field since about 2018 and are systematically filling out the broad rhetoric of ethical principles with international standards. The focus is necessarily put on the interest of the AI business, which does not exclude the consumer dimension, but which explains why ISO/IEC standards are developed through industry lenses. This may be highlighted in the way ISO/IEC approaches the lifecycle. ISO/IEC is not dealing with ‘*lifecycle through the eyes of the consumer*’, which would have meant opening up the complicated issue of use cases.⁴⁵⁸ IEEE is picking up forthcoming technical developments more outspokenly, sometimes driven by recent developments and events in the United States.⁴⁵⁹ At the same time, IEEE is engaging eagerly in the societal and political dimension of AI, thereby coming closer to the empirical dimension of applied AI. The agenda of the European Commission is determined by the Digital Legislative Framework, in particular by the AIA-P (harmonised standards), the CRA-P (harmonised standards) and the DSA (voluntary industry standards=non-harmonised European standards). CEN-CENELEC have set up their own agenda, which reflects the political needs of the EU, as well as the attempt to find a self-standing position in a highly crowded field of ongoing and pending international activities.

⁴⁵⁷ Information made available from a representative of European stakeholder organisations.

⁴⁵⁸ Interview with a representative from stakeholder organisations.

⁴⁵⁹ For comparison of ISO and IEEE in AI standardisation, JRC Technical Report AI Watch Artificial Intelligence Standardisation Landscape Update, An Analysis of IEEE Standards in the Context of EU AI Regulation, 2023 <https://publications.jrc.ec.europa.eu/repository/handle/JRC131155> focusing on bias, transparency/explainability and risk management, at 29.

Seen through consumer lenses, waiting for the European Commission and CEN-CENELEC to build a ‘*human-centric, secure, trustworthy, ethical and lawful AI*’ (HLEG and fundamental rights), one might divide the ISO/IEC and IEEE standards into three groups – those where ISO/IEC and IEEE are filling obvious gaps in the EC working programme,⁴⁶⁰ those where they are competing in between them and the EC working programme and, last but not least, those where the ISO/IEC and IEEE are looking far beyond the EC working programme into future challenges of AI. Double entries are possible. A disclaimer is needed, though. Classification is based on publicly available information, which might not be complete. Many projects are pending at the international level and at the European level. European lenses are directed to the Standardisation Request which covers ten rather broad categories, meant to implement mainly the AIA-P, to which neither the ESOs nor stakeholder organisations have yet had the opportunity to respond. At the time of writing the European Parliament is heavily promoting major revisions of the structure of the AIA-P, which might affect the legal framework in which AI standards are embedded – provided they survive the interinstitutional agreements between the European Parliament, the Council, and the European Commission.

Independent from the legislative level, in practice much depends on what kind of project the ESOs will take on board, where they set their priorities, and how they coordinate with ISO/IEC and maybe even with IEEC. It seems highly likely that the ESOs, in line with the Vienna Agreement, will be inclined to take over existing ISO/IEC standards and transform them into European standards, wherever there is compliance between the ten EC categories and existing ISO/IEC standards.⁴⁶¹ The Vienna Agreement leaves space for European standards only when there are gaps to be filled. Here we are back to one of the key consumer concerns – the very limited consumer participation at the international level, which can only partly be compensated through input from national standardisation bodies with strong consumer participation and the observer status of ANEC and CI within ISO/IEC. Can the lack of adequate participation by stakeholders in elaborating international standards at ISO/IEC be identified as ‘a core value’ in the language of the EC Strategy on a New Standardisation Strategy, or can participation even be upgraded to fundamental rights status under the EU Charter of Fundamental Rights? If yes, it would allow reopening of the standardisation procedure, so as to enable Annex III stakeholder participations to be involved in the screening process. The other option would be to allow the existence of substantive gaps, not only in the missing or underdeveloped empirical dimension – use cases – but also with regard to a detailed analysis of existing ISO/IEEE standards and projects in comparison to the ten mandated projects? Neither the European Commission nor ISO/IEC, nor CEN-CENELEC have institutionalised co-operation with IEEE, although attempts are under way to establish a liaison with CEN-CENELEC.

| | Gap filling | Competition | Future proof |
|---------|--|---|------------------|
| ISO/IEC | Lifecycle (also on data) Guidance for application and use case Explainability AI impact assessment Children and young people | Risk management Robustness (neural networks) Bias Quality evaluation Transparency Testing Conformity assessment | Machine learning |

⁴⁶⁰ See under IV 4 and 5.

⁴⁶¹ This was mentioned by a number of interviewees from the standardisation organisations.

| | Gap filling | Competition | Future proof |
|------|---|--|---|
| IEEE | Explainability Well-being metrics Environmental and social governance | Transparency Data privacy Bias Nudging Organisational governance | Ethically driven robots Rating of trustworthy news sources Machine Readable personal privacy terms Emotion recognition Extended reality |
| ETSI | Ethical ecosystems Problem stating (use case) Explainability | Transparency | Supply chains |

The classification is admittedly rather crude and subject to revision, if the perspective is broadened beyond the search for AI standardisation on human-centric, secure, ethical, and trustworthy AI. ISO/IEC have developed standards on the AI lifecycle, which are not fully taken care of in this report, but which are supposed to integrate the consumer.⁴⁶² Nevertheless, the overview helps to identify important gaps in the EC working group as well as strong competition over key concepts such as risk management, governance, transparency, or conformity assessment.

However, none of the grand components or concepts mentioned are self-explanatory and none of them is without ambiguities. This is true for transparency⁴⁶³ and it is equally true for human oversight. The EC working programme wants human oversight to be transformed into a harmonised European standard, thereby maybe filling a gap left by ISO/IEC and IEEE, who are not explicitly dealing with the topic. However, the EC working programme does not provide guidance on how human oversight should be understood, in particular whether human-centric means that humans should remain in control. The sympathetic idea behind promotion of human oversight in the EC working programme is that human oversight helps to build trust. However empirical research demonstrates that humans fail and that ‘institutional distrust’ might be required.⁴⁶⁴ Similar questions arise with regard to explainability, which seems to attract more attention by the international standardisation organisations ISO/IEC and IEEE than by the EC. Explainability immediately enters the normative arena and opens the battlefield to disagreement about what it comprises and what the yardstick might be. Explainability even made it to a separate entry in Wikipedia.⁴⁶⁵ The same uncertainty exists with regard to the 4th element of HLEG guidelines. Here, the international standardisation organisations dominate the debate and have brought strong initiatives under way – related to use, to impact assessment and even to well-being – which have no counterpart in the EC Working Programme, in the Standardisation Request or in self-standing CEN-CENELEC activities. Whilst these international initiatives have to be applauded, the devil is in the detail. Each of the initiatives raises a bunch of questions, for instance on the validity of impact assessments and how impact assessment should

⁴⁶² DIN DKE Deutsche Normungsroadmap Künstliche Intelligenz Ausgabe 2, 2022, 87, 133 and 159 on the socio-technical lifecycle, Artificial Intelligence; Overview of the AI Standards Program and Novel Ecosystem Approach, OCEANIS Steering Committee, March 2023.

⁴⁶³ I Koivisto, *The Transparency Paradox*, OUP 2022.

⁴⁶⁴ J Laux *Institutionalised Distrust and Human Oversight of Artificial Intelligence: Toward a Democratic Design of AI Governance under the European Union AI Act* (March 3, 2023). Available at SSRN: <https://ssrn.com/abstract=4377481> or <http://dx.doi.org/10.2139/ssrn.4377481>

⁴⁶⁵ https://en.wikipedia.org/wiki/Explainable_artificial_intelligence

look like to serve the consumer interest⁴⁶⁶ or when AI-augmented nudge shall be introduced into human-computer interactions.⁴⁶⁷

466 See the contributions in E van Schagen/ St Weatherill (eds.), *Better Regulation in EU Contract Law: The Fitness Check and the New Deal for Consumers*, Hart Publishing, 2019

467 E. Panai and L. Devillers, *How AI-augmented nudges may impact EU consumer in a moral situation?*, (ed.) M Ho-Dac and C Pellegrini, *Governance of Artificial Intelligence in the European Union – What Place for Consumer Protection?*, Brussels, Bruylant, 2023 [forthcoming]

V. Lessons to be Learned and Conclusions to be Drawn



Seen through the lenses of the European Commission, the success story of Internal Market regulation started in 1985 with adoption of the New Approach/NLF. This very same success story – invented and promoted in the industrial economy – is now to be continued in the digital economy. Seen through the lenses of consumer advocacy, the New Approach/NLF suffered right from the beginning from serious deficiencies, which the CJEU is now gradually bringing to the limelight. The unquestioned transfer of the New Approach/NLF from the industrial to the digital economy, from combining product safety with mass production to squeezing fundamental rights into the co-regulatory approach in the digital economy, has added a long list of unanswered questions to the existing deficits, which in turn requires a rethink of the governance structure of the interaction between binding legal requirements and voluntary harmonised standards.

The time has come to sum up and systematise analysis of the deficiencies in order to prepare the ground for possible counterstrategies. Therefore, the following should be understood as a kind of interim conclusion which highlights the major findings, built around catchwords, which dominate discussion of the New Approach/NLF in the industrial economy and now in EU Digital Policy Legislation. The chapter concludes with discussing possible options for action.

1. Legacy of the New Approach/NLF Designed Made for the Industrial Economy

The arguments in favour of change differ according to the affected economy – the industrial and the digital economy.

a) Participation by Stakeholders – Consumer Organisations and ANEC

Until 1985 EU technical standardisation was widely regarded as a matter which lay in the hands of industry itself. Reliance on technical standardisation to cope with potential risks to health and safety of consumers triggered a search for appropriate mechanisms to integrate consumer concerns into elaboration of technical standards. Amazingly enough there was little to no attempt to link the debate on consumer participation in technical standardisation to much broader political implications resulting from the rise of the consumer society. At the EU level the debate was narrowed down to ‘the right to be heard’, born in the Kennedy Declaration of 1962, translated into a ‘right to participate’ in the political processes around the two consumer

programmes of 1975 and 1981.⁴⁶⁸ The national consumer policy programmes which preceded the European Programmes led to the birth of consumer organisations which were expected to initiate and to comment on political initiatives, in particular on the emerging development of consumer laws.⁴⁶⁹ Similar developments took place at the EU level, both in civil society and in the political arena. The national consumer organisations founded BEUC in 1962,⁴⁷⁰ whereas consumer policy was not seriously integrated into the administrative structure of the European Commission before 1973.⁴⁷¹

Consumer policy became relatively quickly integrated into the political systems at national and European levels. The debate around a true ‘consumer movement’, grounded in civil society – being understood as a counterpart to the ‘worker movement’ at the beginning of the 20th century – remained by and large an academic exercise, just as attempts to build conceptual and theoretical links between labour and consumer law.⁴⁷² To the best of my knowledge France is the only country where a merger between trade unions and consumer associations gained some importance in the aftermath of the 1968 events, which in French intellectual history are understood as a revolution. It is far-fetched even to think of the rise of consumer policy in the late 1970s and early 1980s in categories of a ‘social movement’, driven bottom-up by consumers around Europe, self-organising themselves and advocating for political change. Right from the beginning there was a strong connection between politics and civil society organisations.

The overall scenario is important in order to understand why the debate about consumer participation in the ESOs never got off the ground and why it remained a rather eclectic discourse within the technical standardisation community. Technical standardisation, not even in combination with product safety, triggered much attention in consumer organisations or in political bodies dealing with consumer policy at the national or European level. Looking back, one might recognise a divide between consumer policy built around consumer rights and consumer policy in technical standardisation. The first led to legalisation of consumer policy and thereby of consumer organisations. Law and lawyers became ever more important and gained ever more ground in the institutions, inside and outside civil society. The second required technical expertise, which was urgently needed to counterbalance business-driven elaboration even of product safety standards. The scissor between law-driven consumer organisations and technically-driven standardisation bodies opened ever further over the years, as lawyers gained prominence in consumer organisations and consumer agencies.

The result is well known. ANEC was established by the European Commission in response to a long lasting pressure from national consumer organisations and BEUC, articulated through the European Consumer Consultative Committee, in order for its members and experts to provide legitimacy to the elaboration of harmonised European standards in the field of product safety. The insecure position of ANEC is obvious, despite Regulation 1025/2012 citing its political recognition and funding in such an instrument for the first time. CEN-CENELEC and ETSI are giving a secure status, they are named as the European Standardisation Organisations

468 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.

469 H-W Micklitz (ed), *The Making of Consumer Law and Policy in Europe*, Bloomsbury Publishing, 2021

470 K Doctor, ‘The Early Years of the European Consumer Organisation BEUC, 1962–1985’, in H-W Micklitz (n 470), at 31.

471 L Krämer, ‘The Origins of Consumer Law and Policy in Europe’, H.-W. Micklitz (n 471), 13 pp at 15.

472 Michel Mialle, *Une introduction critique au droit*, Paris, Éditions Maspéro, 1976.

with which the European Commission co-operates.. ANEC, however, is not given status on a level playing field. Regulation 1025/2012 provides categories and criteria for stakeholder participation, consumers being one out of four. The decision as to who complies with the criteria and who receives funding lies in the hands of the European Commission alone. The European Commission is entitled to deny ANEC the status of a stakeholder organisation in the next upcoming round in which ANEC seeks funding from the European Commission to continue its work. Whilst it might be politically unlikely that the European Commission will take such a step, ANEC's shaky status affects the role and function that it can play in the technical standardisation process. The current state of affairs must be seen in the light of growing pressure from industry circles to reduce participation by stakeholder organisations. Such arguments point in the wrong direction and in no way do justice in the debate on the role of civil society in evaluation of risks.⁴⁷³

The New Approach was adopted in 1985, ANEC was established in 1995, the Regulation dates from 2012. Seen through the lenses of consumer participation, nothing has changed since 2012. Nearly forty years after the invention of the New Approach and despite its prominent and successful role in building the Internal Market, participation by stakeholders looks more like a fig leaf than a structural pillar of EU technical standardisation policy. A wide gap exists between the legal position granted to stakeholder organisations in the EU legal order and the social significance of consumer representation in technical standardisation.

b) Conformity Assessment, Presumption of Conformity, and Certification

The established co-operation between the ESOs and the European Commission rests on the premise that harmonised European standards must comply with binding legal requirements. The 'co' in the regulation requires that law – the legal implication – and technology – the technical implication – have to come together. 'Someone' has to ensure that technical standards comply with the law. Article 10 (5) Regulation 1025/2012 is deliberately vague – *'the Commission together with European standardisation organisations'* – are in charge of the compliance test. The rule has to be read in light of the experience which the EU legislature gained in the aftermath of the 1969 Programme on Standardisation.⁴⁷⁴ Via the 1985 New Approach, the EU legislature intended to overcome the deadlock resulting from a policy which put the final decision on technicalities into the hands of the European Commission, the European Parliament, and the Council. The many detailed reports and guiding documents which accompany the New Approach, the NLF, and later the Better Regulation Approach never clarified what exactly had to happen and what exactly happened *prior to James Elliott*, when ESOs monitored and surveyed the HAS consultants in charge of the compliance test. The European Commission took away the responsibility from the ESOs *after James Elliott*, but what exactly the HAS consultants are doing and how the tasks and responsibilities between the European Commission, the ESOs, and the HAS consultants are shared remains is shielded through a strict confidentiality regime. Interestingly, the insiders, which means all those who are involved in elaborating technical standards, in particular industry representatives, might very well know not only what

⁴⁷³ J Baron/ P Larouche, 'European Standardisation System at a Crossroads', Centre on Regulation In Europe, 2023 https://cerre.eu/wp-content/uploads/2023/05/CERRE_The-European-Standardisation-System-at-a-Crossroads.pdf

⁴⁷⁴ J Pelkmans, 1987. 'The new approach to technical harmonization and standardization'. *Journal of Common Market Studies*, 25 (3), 223.

the HAS consultants are doing, let alone who they are, they also have an insight on how the ESOs and the European Commission are exercising their responsibilities.

The crucial point, namely where legal and technical expertise come together, remains a black box. The knowledge gap is particularly problematic due to the legal effects that harmonised standards produce. Somewhat hidden in the New Approach/NLF, EU legislation inserted a mechanism which explains why industry is keen to develop harmonised European standards, why co-operation between the ESOs and the European Commission is successful, and why the number of harmonised European standards is steadily increasing. The magic formula is ‘presumption of conformity’. Compliance with harmonised European standards ensures access to the Internal Market. One might wonder what would happen if the presumption of conformity were to be abolished. Indeed, some voices are considering such a decisive step.⁴⁷⁵ Thinking the alternatives through, the EU legislature would have to reconceptualise the overall role of harmonised European standards and the distinction between harmonised and non-harmonised European standards.

It is to be recalled that EU law does not oblige business to make use of harmonised European standards. They are voluntary. Business is free to develop their own technical standard provided it complies with binding legal requirements. In practice business saves a lot of money, time, and resources in using the pre-fabricated harmonised European standards in their industrial production. As the CJEU made clear in *Fra.bo*, the voluntary character might quickly get lost if the harmonised European standard is de facto the only option which grants access to the market of a particular Member State.⁴⁷⁶ Tension is inbuilt into the New Approach/NLF between the rather broad *binding* legal requirements and the *non-binding voluntary* character of harmonised European standards. This tension is unresolvable unless there is political will to put an end to the co-operation mechanism, for instance by deciding that technical standardisation should be put into the hands of the legislature – which would be a return to the failed 1969 programme.

Consumer advocacy immediately identified the weak point in the construction of the presumption of conformity: who will be in charge of demonstrating that a particular producer complies with harmonised European standards? EU law has distinguished ever since between self-certification and third-party certification. The conflicting parties take clear positions – consumer advocates argue in favour of third-party certification in order to ensure an impartial and competent investigation, whereas industry opts for self-certification, for the responsibility to execute the compliance test themselves. This is not the place to delve deeper into self- vs third-party certification, in particular what exactly industry is doing when it self-certifies, what kind of documents are produced and who has access to these documents in case of conflict. Similar questions arise when it comes to third party certification, as to who the certification bodies are that are allowed to certify and under what conditions they are accredited and by whom. The PIP scandal demonstrated that the scope and reach of what exactly the certification bodies have to investigate depends on the requirements in the respective EU laws. This is true with regard to the first compliance test but also with regard to monitoring duties which may be imposed on the certification body via secondary EU law. In PIP⁴⁷⁷ one of the key issues was whether the certification bodies are obliged to make unexpected inspections without

⁴⁷⁵ Interview with a representative from a stakeholder organisation.

⁴⁷⁶ ECJ Case C-171/11 *Fra.bo* ECLI:EU:C:2012:453.

⁴⁷⁷ Under II 3.

prior notification to the company. The Medical Device Directive was only amended after the PIP scandal and the claimants largely failed in seeking compensation from the certification body, except those domiciled in France, who benefited from a mandatory insurance scheme. The uncertainties and lack of knowledge on the inner mechanics of self- and third-party certification, the availability of appropriate remedies, and the scope of liability deserves further investigation but reaches beyond the purpose of this Report.

2. Unquestioned Transfer of the New Approach/NLF to the Digital Economy

The unquestioned transfer raises a number of questions which have to be analysed one by one, from the 'passing the buck' policy and the lack of descriptive/applied ethics to the new AI category of socio-economic AI standards, from there to the missing red lines and the missing respect for the consumer acquis, to the redesign of the compliance procedure and participation by stakeholder organisations and last but not least to the geopolitics of the New Approach/NLF in AI standardisation.

a) Passing the Buck, Normative and Descriptive/Applied Ethics, Use Cases

Integration of fundamental rights into EU Digital Policy Legislation challenges the feasibility of the New Approach/NLF in the digital economy. The analysis so far has amply demonstrated that on a closer look the three pieces of legislation under scrutiny, namely AIA-P, CRA-P, and the DSA, pursue a 'pass the buck' policy, which remains true notwithstanding that the DSA does not call for harmonised European standards and therefore does not follow the NLF. EU legislation requires the integration of fundamental rights into technical standards. It is for the ESOs to make sure that the standards comply with fundamental rights. Delegation to the ESOs implies the involvement of stakeholder organisations. If the ESOs are not doing what is requested from them – they have legitimate reasons to claim that they are ill-equipped to do so – the stakeholder organisations remain the last resort for realising the ambitious aim of a '*human-centric, secure, ethical and trustworthy AI*' through '*fundamental rights.*' Passing the bucket does not end here, though. The potential risks of AI systems materialise only under concrete circumstances due to the difficulty – if not impossibility – of foreseeing the potential risks which result from their application. The risk assessment, even if made at the moment when AI standards are developed, is of limited relevance for the local AI provider or AI user (in the terminology of the AIA-P, the CRA-P, and the DSA), who needs to test the potential impact on fundamental rights under real life conditions. If the local AI provider or AI user – who might often be an SME or a start-up – does not undertake the attempt to assess the risk locally, then the consumer or the citizen ends up as the one bearing the risk.

Handing over the hot potato of 'fundamental rights' from the EU, to the ESOs, to stakeholder organisations, to the local AI provider or AI user, to the final consumer or citizen is accompanied by a gradual thinning out of high claims of 'trustworthy AI' down the road or perhaps more precisely together with the shift of responsibilities from one institution to the next. The EU started with ethical guidelines elaborated by the High Level Expert Group, which identified four major components (lawfulness, ethical guidelines, robustness, and lifecycle (applied ethics)) and which devoted particular attention to human oversight in shaping the ethical

guidelines.⁴⁷⁸ ANEC is proposing a concept of lifecycle, which integrates the consumer and breaks down a business perspective.⁴⁷⁹ The European Commission has stressed the normative dimension of ethics through abundant references to fundamental rights, but reduced the crucial importance of the empirical/applied dimension to a degree where it is nearly invisible.

Within the normative dimension, one key element remains under-specified – *human-centric* – AI in the meaning of humans remaining in control over and of AI. What might be remedied at the legislative level through interpretative means, at least to some extent, becomes much more dramatic when it comes to elaboration of technical standards through standardisation requests from the European Commission. EU digital policy legislation lacks guidance on how, by whom, and under what responsibility compliance with fundamental rights has to be assured. The unintended result of the unquestioned transfer to the digital economy might therefore lead to a situation where real life serves as a field of experimentation. What looks like a strong ex-ante approach in the tradition of health and safety regulation turns de facto into an ex-post approach, where all depends on control of AI through national and European market surveillance authorities and the efficiency of product liability and tort law claims. Sad to say, this very much recalls the PIP experience, where the EU succeeded in opening up the market for medical devices through harmonised European standards, but where effective safeguards in EU law were missing in terms of monitoring and surveying the potential risks and adequately compensating the victims. Again, closer analysis of the market surveillance mechanism and the potential impact of the PLD-P and the AIL-P reaches beyond the scope of this Report.

Passing the buck leads to deficiencies which have to be remedied – through clearer guidance on how compliance with fundamental rights must be ensured through red lines, through building safeguards to the benefit of the last holder of the buck – the ESOs together with the stakeholder organisations – in elaborating technical standards; the local AI provider or AI user in assessing the impact of the AI system on the concretely envisaged field of application; and the consumer/citizen as the one confronted with the concrete risks of an AI system. As a direct consequence, the envisaged Revision of Regulation 1025/2021 has to put emphasis on descriptive/applied ethics, on use cases, on their standardisation as well as on development of testing requirements which support the local AI provider and AI user.

b) Technical Standards, Deliverables, and Socio-technical Standards

The role and function of technical standards is constantly changing. This goes hand in hand with ever new categories of technical standards. ISO/IEC and CEN-CENELEC are not using the same terminology. The EU perspective is guided by one crucial question, namely whether the standard is certifiable and apt to trigger the presumption of conformity.

ISO distinguishes between six different deliverables, each of which is defined:

- ISO standards,
- ISO/TS Technical Specifications,
- ISO/TR Technical Reports,

⁴⁷⁸ Under IV 2 b).

⁴⁷⁹ ANEC Basic Consumer Product Lifecycle, on file with the author.

- ISO/PAS Publicly Available Specifications,
- ISO/IWA International Workshop Agreements and
- ISO Guides.

IEC does not feature IWA but does have the Systems Reference Deliverable (SRD) intended to address standardisation immediately at the systems level, rather than at the product level. ISO/IEC standards are:

guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context. It can take many forms. Apart from product standards, other examples include: test methods, codes of practice, guideline standards and management systems standards.

Technical Specifications can be turned into fully fledged ISO/IEC standards, given experience. A Technical Report is different from ISO/IEC standards or Technical Specifications: based on surveys or available information, it provides a kind of situation report. International Workshop Agreements are prepared outside of ISO/IEC committee structures, following a procedure that:

ensures the broadest range of relevant interested parties worldwide have the opportunity to participate, and are approved by consensus amongst the individual participants in the workshops.

Regulation 1025/2012 does not define what a ‘European standardisation deliverable’ is. In practice it could be everything other than a European (harmonised) standard and thus a means which does not justify the presumption of conformity. CEN-CENELEC distinguish between:

- a European Standard (EN), Technical Specification (CEN/TS), that serves as a normative document in areas where the actual state of the art is not yet sufficiently stable for a European Standard;
- a Technical Report (CEN/TR), for information and transfer of knowledge;
- a CEN Workshop Agreement (CWA), which aims at bringing about consensual agreements based on deliberations of open Workshops with unrestricted direct representation of interested parties;
- Guides (CEN Guide), which gives information about standardisation principles and policies and guidance to standards writers.

The engagement of ISO/IEC and IEEE has led to a new category of technical standards – termed ‘socio-technical’. Socio-technical terms combine the technical dimension with the societal dimension of AI. The search for concepts to give shape to trustworthiness provides ample character for the characteristics of those standards. They are broadly worded and link policy objectives and ambitious language derived from the debate around ethical AI into a formula which can provide guidance to software developers – and not only to them but also to policymakers. They take an intermediate position between legal requirements – such as binding EU requirements – and certifiable technical AI standards. The VDE report from ‘Principles to Practices’⁴⁸⁰ recognises exactly what is at stake and intends to give shape to socio-technical-standards. There is a need to introduce a new category into the EU Regulation – a category which needs to be defined and which needs to be separated from certifiable harmonised Euro-

⁴⁸⁰ AI Ethics Impact Group led by VDE and Bertelsmann Stiftung, From Principles to Practice An interdisciplinary framework to operationalise AI ethic, 2020 <https://www.ai-ethics-impact.org/resource/blob/1961130/66db9894ee73aefa489d6249f5ee2b9f/aiieg---report---download-hb-data.pdf>

pean standards which in any case have yet to be developed. The very same report comes up with a set of criteria on how to operationalise AI ethics and make them fit for development of AI standards.⁴⁸¹ The VDE report is not directed to the European standardisation community but, rather, to the international and European community.

c) Red Lines on Standardisability in both the Industrial and the Digital Economy

This Report subscribes to the HLEG Guidelines and in particular to making sure that AI is human-centric and that it does not impinge on human dignity. Human-centric AI is not limited to ensuring that humans are protected against risks of whatever kind but, rather, human-centric AI requires that the humans remain in control of the AI system. EU digital policy legislation is not very clear on what human oversight might mean, in particular whether human oversight necessarily implies human control. In light of the HLEG Guidelines but also in light of the abundant literature on AI risks in general and on the key role of human dignity in particular,⁴⁸² safeguards are needed that make sure that AI technical standards do not cross that line. There is a limit to what is standardisable – a limit enshrined in the formula of human dignity and human control. This limit is certainly not the ‘*generally acknowledged state of the art*,’ as proclaimed by the European Commission in the AIA-P and already set into stone in the Implementing Decision on the AI Standardisation Request.⁴⁸³ The EU Directive on Biodiversity may, together with the *Brüstle* judgment,⁴⁸⁴ serve as a source of inspiration which does justice to the importance of the protection of human dignity.

Whilst there might be agreement on preserving human dignity and on drawing a red line over which AI technical standardisation may never trespass, no such agreement is supposed to exist when it comes to respect for fundamental rights in technical standards of whatever kind, independent of whether technical standards are produced for the industrial economy and/or the digital economy. The declaration of fundamental rights goes back to the year 2000, the EU Charter of Fundamental Rights became effective in 2009, and Regulation 1025/2012 entered into force on 20 January 2013. However, not even the recitals of Regulation 1025/2012 refer to fundamental rights, although the Regulation itself deals with health and safety, which are stable fundamental rights, let alone interference with fundamental rights which protect the economic interests of both businesses and consumers. Integration of fundamental rights into Regulation 1025/2012 is long overdue. Technical regulation – like all other secondary EU law – has to comply with the Charter and this has to be made explicit in the revised Regulation 1025/2012. What should be the yardstick of care to be provided? From product safety regulation we know the established distinction between the ‘*generally acknowledged state of art*’ the ‘*state of the art*,’ and ‘*the state of science and technology*’.⁴⁸⁵ The Commission Implementing Decision on

⁴⁸¹ From Principles to Practices (472) at 8. We present the so-called VCIO (Values, Criteria, Indicators, Observables) model, an approach for specification and operationalisation of values. This is necessary to make ethical principles practicable, comparable, and measurable. We also demonstrate different ways of dealing with conflicts between values.

⁴⁸² R Brownsword, ‘From Erehwon to AlphaGo: For the sake of human dignity, should we destroy the machines?’ *Law, Innovation and Technology* 2017, 117 https://kclpure.kcl.ac.uk/portal/files/137551177/From_Erehwon_to_AlphaGo_BROWNSWORD_Acc12Feb2017Epub22Mar2017_GREEN_AAM.pdf

⁴⁸³ See the analysis of the AIA-P under IV 2 a) cc) and of the Implementing Decision on the AI Standardisation Request under IV 4 b) bb).

⁴⁸⁴ CJEU Case C-34/10 *Brüstle* ECLI:EU:C:2011:138

⁴⁸⁵ Ch Joerges/ J Falke/ H-W Micklitz/ G Brüggemeier, *Die Sicherheit von Konsumgütern und die Entwicklung der Europäischen Gemeinschaft*, Band 2, ZERP Schriftenreihe, 1988; Joerges, Ch, Falke, J, Micklitz, H-W and Brüggemeier,

a Standardisation request has opted for the lowest level ‘the generally acknowledged state of the art’, thereby putting technology in both the industrial economy and the digital economy on an equal footing. This Report takes a different position, insisting on the particularities of the digital economy and calling for the urgent need to include scientific knowledge into risk assessment.

The question remains how can an adequate level of protection be achieved outside and beyond mere rhetorical references to fundamental rights in the recitals, which would lead to questions similar to those which have been identified in the AIA-P, the CRA-P, and the DSA?⁴⁸⁶ Two possible options spring to mind. The *first* is the definition of a red line which applies to all sorts of technical standards, not only to AI standards and which could be understood as a second layer, complementing the benchmark of human dignity. This could be a kind of general clause which hammers out that it is ultimately for the political authorities to decide if technical standardisation might be used at all. Such a general clause would affect the relationship between the European Commission and the ESOs, as it gives shape to the ultimate responsibility which *James Elliott* requires. It would be for the European Commission to decide whether a particular standard in a particular field of the economy and society could be mandated at all or whether it is for the EU legislature to hold back the responsibility and to lay down the respective rules in secondary EU law. This should not be confounded with the compliance test, which in effect means the question whether an already mandated harmonised European standard complies with EU law. The general clause requires an ex-ante investigation prior to elaboration of a call for proposals, a standardisation request, and later a compliance test.

The *second* option – though the two are not mutually exclusive, but complement each other – results from making a fundamental rights impact assessment mandatory. The European Parliament seems to be in favour of amending the AIA-P accordingly.⁴⁸⁷ It is by far not clear whether such a requirement will pass interinstitutional negotiations with the European Commission and the Council. However, even if the AIA in its final version provides for such an impact assessment, the question remains: how can such a test can be operationalised and at what level will be executed, that is, at the level of the ESOs which develop the standard or at the local level? Here the differences between the industrial and the digital economy matter. In the industrial economy it might suffice to submit harmonised European standards to a fundamental rights impact assessment as part of the compliance procedure. Then the question arises: who should be in charge of the test? This brings us back to the role of the HAS consultants, the division of responsibilities between the European Commission and the ESOs, and the gap between Article 10 (5) Regulation 1025/2012 and the current practice of the European Commission in the aftermath of *James Elliott*. Closely related to the ‘who’ is the ‘how’. By what means will the impact assessment be executed? The subject matter consists in technical standards in combination with binding legal requirements. This is also uncharted territory for the established practice of fundamental rights impact assessment.⁴⁸⁸ In order to operationalise the fundamental rights impact assessment, testing requirements need to be developed for the industrial economy and the digital economy, taking due regard of differences in the foreseeability of potential

G ‘European Product Safety, Internal Market Policy and the New Approach to Technical Harmonisation and Standards’ (1991) EUI Working Paper Law No. 10–14 = with a new foreword reprinted in (2010) 6 *Hanse Law Review* 109.

486 Under III 1 -3. Under the respective headings.

487 At the time of writing the EP is in the middle of internal negotiations to formulate a position. Information from BEUC.

488 On fundamental rights impact assessment Kosta, V *Fundamental Rights in EU Internal Market Legislation* (Oxford: Hart Publishing, 2015).

risks. Testing requirements could be developed in the form of technical standards by the ESOs, initiated by the European Commission through a standardisation request. However – and the ‘however’ needs to be written in bold letters – these testing requirements need to be freely accessible, at least whenever the potential risks materialise at the local level. Otherwise, SMEs and start-ups might shy away from using them, which could lead to transferring the ultimate risk to the consumer citizen.

d) Technical Standards, Fundamental Rights and the Consumer Acquis

The New Approach/NLF in the industrial economy led to the explicit integration of consumer policy into technical standardisation guided by the idea that health and safety issues can and should be integrated into elaboration of technical standards. Right from the beginning, protection of the economic interests of consumers remained outside the scope of harmonised European standards. The EU did not use harmonised European standards to interfere in the quality of products. In a market society, quality is supposed to be left to competition between producers and therefore it is not for the EU to mandate the ESOs with elaborating them, even if harmonised European standards remain voluntary in nature. However, EU policy is currently breaking down the distinction between safety-based standards, which could be mandated, and quality-based standards, which remain outside the New Approach/NLF in the intended replacement of the rather narrow eco-design Directive to the much more comprehensive eco-design Regulation. Whenever and wherever technical standardisation engages with sustainability and the greening of the economy, harmonised European standards serve as a tool for change. Here the New Approach/NLF is crossing a line which would have been unthinkable in 1985, but which today is becoming ever more relevant not only for the economy as such but also for the consumer in particular.⁴⁸⁹ The currently proposed ‘right to repair’ in its interaction with the eco-design regulation bears witness to the prominence of harmonised European standards as an objective benchmark which might trigger consumer rights in case of non-conformity under Directive 771/2019 on Consumer Sales.⁴⁹⁰ The integration of sustainability into the New Approach/NLF demonstrates that protection of economic interests is becoming ever more important in technical standardisation.

Strangely enough, EU Digital Policy Legislation mirrors the distinction between safety vs quality through its reliance on the risk-based approach. The AIA-P and the CRA-P insinuate that relevance can be maintained despite the integration of fundamental rights in the New Approach/NLF. However, the very same draft regulations refer to particular fundamental rights which enshrine protection of the economic interests of consumers as well as to Article 38 EUCFR either explicitly or implicitly through a reference to ‘fundamental rights’ or even to a ‘general proviso’, such as in the DSA, which to some extent covers protection of consumers’ economic interests. However, the draft regulations do not engage with the consumer acquis. They do not even clearly state that the consumer acquis remains unaffected by the draft regulations, let alone refer to consumer issues more broadly – for instance, by pointing to the ongoing

⁴⁸⁹ H-W Micklitz, *European Transnational Private Law in Regulated Markets* (n 43).

⁴⁹⁰ Proposal for a Directive of the European Parliament and of the Council on Common Rules Promoting the Repair of goods and amending Regulation (EU) 2017/2394, Directives (EU) 2019/771 and (EU) 2020/1828 COM/2023/155 final; Feedback of the European Law Institute on the European Commission’s Proposal for a Directive on Common Rules Promoting the Repair of Goods (COM(2023) 155 final) (Final Word version – the final publication will be available on the ELI website in due course) Drafters: S Augenhofer, Y M Atamer, K Południak Gierz, with the support of R Küter. Advisory Committee: A De Franceschi, P Gautier, M J Sørensen, H Micklitz, A Perzanowski, Project Number: RC-2023-8 Approved by the ELI Council on 24 May 2023. Published on 25 May 2023.

negotiations on the ‘Digital Fairness Check’ –⁴⁹¹ which might lead to an adjustment of the consumer acquis. As they stand, the draft regulations look as if the economic interests of consumers can only be inserted into harmonised European standards, as far as they enjoy ‘constitutional relevance’ via fundamental rights.

Thereby they leave it in the end to the EU judiciary to concretise the consumer relevance of fundamental rights. The ESOs lack guidance on what to do exactly and how to take care of a legal dimension for which they are ill-equipped. As long as such guidance is missing, the standardisation bodies will struggle in what to do in terms of elaborating AI standards. The ESOs and, more broadly speaking, also the international standardisation bodies could at least in theory take into account ‘*the technical standards consumer acquis*’ which has been developed in recent decades outside the ISO/IEC JTC 1 SC 42 AI committee and which has to be developed and condensed. These non-SC 42 standards show that there are well established good practices in current standards that have not been included in the SC 42 standards, with the consequence that such content could be included in the AI Trustworthiness standard which should ‘set the scene’ for all other European AI standards.⁴⁹² Legally speaking, these practices might not reach the level of ‘constitutionalised consumer rights’ under the Charter of Fundamental Rights, but they might in a very practical way help to fill gaps. The difficulties and uncertainties around the consumer acquis and the ‘technical standards consumer acquis’ could be overcome if the finally adopted versions of the AIA-P and the CRA-P were to deal with protection of consumers’ economic interests outside and beyond consumer rights as fundamental rights.

e) HAS Consultants, Standardisation Scrutiny Board, Accessibility

The deficiencies already enshrined in the role of HAS consultants in the industrial economy are severely aggravated in the digital economy. In the old economy the HAS consultants have to ensure ‘only’ compliance of a technical standard with a particular piece of secondary EU law. What might in theory be possible in the industrial economy is close to impossible in the digital economy in light of the inclusion of fundamental rights. The tasks imposed on HAS consultants require unique capabilities both in technology and in law. The HAS consultant should be able to communicate in both worlds and should be in a position to translate technical concerns into legal questions and vice-versa. However, looking into the intellectual capacities the perfect HAS consultant should bring in is only half the battle.

Regulation 1025/2012 carries a heavy burden of unresolved issues, in particular with regard to what exactly is happening between the ESOs, the European Commission, and the HAS consultants. This black box needs to be opened. Harmonised European standards are treated by the CJEU as ‘law’, even if it is law of a very particular kind. Since the time of *Hammurabi*,⁴⁹³ law should be publicly accessible so as to enable citizens to learn what the law is. In a democratic society, this equally implies that citizens have access to how the law is built, by whom, and at

⁴⁹¹ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

⁴⁹² An ANEC expert is currently preparing such a list which covers inter alia product safety, children’s protection, age checking, vulnerable consumers and inclusiveness, product market monitoring and reporting, complaints handling, product recall, redress, product privacy and security that differs from the SC 27–27000 series which protects the organisation, consumer high-risk activities with human supervision and incident and emergency plans

⁴⁹³ [https://de.wikipedia.org/wiki/Hammurabi_I._\(Babylon\)](https://de.wikipedia.org/wiki/Hammurabi_I._(Babylon))

what stage, and why drafts underwent changes. The current compliance mechanism is miles away from such transparency. The CJEU has not yet clarified the consequences of treating harmonised European standards as 'law', in particular not what this means with regard to distribution of responsibilities and with regard to their accessibility. However, there is no reason to wait for the CJEU to clarify the open issues, let alone the fact that the CJEU can only deal with harmonised European standards in the old economy as neither has the AIA been adopted nor are harmonised European AI standards already in place.

Taking together the deficiencies resulting from the industrial economy and the new challenges resulting from the unquestioned transfer of the New Approach/NLF, the compliance procedure calls for a new regulatory design, one where the responsibilities are clearly defined, one where the burden is not on the shoulders of the HAS consultants alone, one which establishes greater transparency of the inner mechanics and one where appropriate safeguards are in place to guarantee access to harmonised European standards, which themselves have to comply with fundamental rights and which, in case of compliance, justify the presumption of conformity. The Better Regulation approach led to establishment of the Regulatory Scrutiny Board, which has to examine whether proposed secondary EU legislation meets the five requirements of transparency, consistency, proportionality, targeting, and accountability.⁴⁹⁴ As harmonised European standards are to be treated as 'law', it seems then only logical to submit harmonised European standards to a similar test. This is all the truer as such a Standardisation Scrutiny Board would have to combine the five requirements with a sixth – the fundamental rights test, put on an equal footing with the other five. A Standardisation Scrutiny Board should assemble the necessary technical and legal expertise and the results of assessment should be made public.

What remains to be clarified are the conditions under which harmonised European standards are accessible. Harmonised European standards as well as non-harmonised technical standards are copyright-protected. Elaborating one single standard has been estimated to cost one million Euro – and this was 20 years ago. It is hard to imagine that industry will continue to bring in their expertise for free if copyright protection were to be lifted. Harmonised European standards are a collaborative exercise. The public legislature relies on private expertise in order to fulfil its constitutional mandate. Therefore, the only available option seems to be that the EU legislator pays for making harmonised European standards accessible. The question remains what accessibility implies – should harmonised European standards be made public in the OJ or should they only be only accessible. In the first case the full text of the harmonised European standard would have to be published in the Official Journal L, in the second case the harmonised European standard would not be published in the Official Journal L in full, but nevertheless made freely accessible by other means, such as through information points or through platforms. If access is monitored by the European Commission and the ESOs, the additional question arises whether interested parties may go to court if access is denied or if a particular harmonised European standard is not fully accessible. A couple of these questions might indeed be clarified by the CJEU in *Public.Resource.Org*.⁴⁹⁵ In the very end the decision to be made should not be one between yes or no but between the standards which should be made freely accessible and those where mere notice in the Official Journal suffices. There might be technical standards which *must* be made public. Obvious candidates are standards on use cases and testing requirements. However, there is large grey area where a decision has

⁴⁹⁴ https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation_en

⁴⁹⁵ Case T-185/19 *Public.Resource.Org* ECLI:EU:T:2021:445, Appeal Case before the Court of Justice C-588/21 P

to be made on a case-by-case basis. The final decision should be left to negotiations between the European Commission, the ESOs – and the stakeholder organisations.

f) Civil Society Participation as Core Values

The transfer of the New Approach/NLF from the industrial economy to the digital economy allows final accomplishment of a project which started in 1985, but which has not yet provided stakeholder organisations with the status they need to enjoy in a co-regulatory process which is worthy of its name. Co-regulation is becoming more and more widespread, in more and more areas of the economy. This changes communication structures – not only in the economy but also in the interaction between the economy, the state, and society.⁴⁹⁶ Digitisation sets an end to the dividing line between economy, state, and society. Integration of product (consumer) safety opened the door for stakeholder organisations to apply their expertise in terms of developing technical standards which include foreseeable risks of potential (mis-) use of consumer products. In foreseeability, both legal and technical expertise merge. Digitisation has dramatically altered the scenario due to the potential impossibility of foreseeing risks. This cognisance, widely agreed between technical experts of whatever kind, means that society at large is submitted to a technology whose implications nobody can overlook. There are voices who call for a stronger positioning of the state in monitoring and surveying the societal implications of AI. This would lead in the end to the question whether the state should take over technical standardisation. Such a call is based on the assumption that the state – in our case the EU – is better suited to deal with transformation of the economy and society. This would mean turning the clock back, not only prior to 1969 and adoption of the programme on technical standardisation, but to the late 19th century. The relocation of knowledge from the administration to industry is the result of a process which dates back to the late 19th century and begins with industrialisation.⁴⁹⁷ Today, the relevant AI expert knowledge is only partly represented in the national and European parliaments, or in the executive institutions of the EU and the Member States. In the present era, the digital industry holds most of the AI expert knowledge in its hands. This Report starts from the premise that there is no alternative to co-regulation, simply because technical expertise is needed. The overarching effect of digitisation in society provides the opportunity to remedy one of the structural deficits in the New Approach/NLF – namely, the role of stakeholder participation. What might be true for all four groups of stakeholder organisations in Annex III is to be exemplified by studying consumer organisations.

The – so far – bilateral relationship between the European Commission and the ESOs has to be turned into a fully-fledged trilateral relationship, where the stakeholder organisations are regarded as equal partners and where they enjoy a status similar if not equal to that granted to the ESOs.⁴⁹⁸ In its resolution from the 9th May the European Parliament is equally stressing the need for a more balanced approach to ensure inclusiveness.⁴⁹⁹ Such an extension has

⁴⁹⁶ In a deeper sense on the transformation of social relations one might refer to N Elias, *Über den Prozess der Zivilisation*, Suhrkamp 1976

⁴⁹⁷ K-H Ladeur, 'The Evolution of General Administrative Law and the Emergence of Postmodern Administrative Law' (2011) Comparative Research in Law & Political Economy. Research Paper No 16

⁴⁹⁸ In the same direction Lovelace Institute Discussion Paper, Inclusive AI governance, Civil Society participation in standards development, March 2023 <https://www.adalovelaceinstitute.org/report/inclusive-ai-governance/>

⁴⁹⁹ 8. Calls for improved representation within the standardisation system and for balanced representation among designated experts, in order to guarantee fair outcomes in respect of the Union's accessibility legislation and standards, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0136_EN.pdf

been forestalled to some extent by the OECD paper on ‘responsible governance’.⁵⁰⁰ The decisive step would be:

- to free ANEC from its shaky status,
- to name ANEC explicitly as the authority representing consumer input,
- to equip ANEC with the sets of rights needed to influence the standardisation process and
- to provide ANEC with solid funding apt to complete the responsibility imposed on it through the transfer of the New Approach/NLF from the industrial to the digital economy.

However, such an upgrade of ANEC, urgently needed anyway, does not solve all the problems which result from the impact of digitisation on society. ANEC grew up and developed in the industrial economy, where independent technical expertise is available in consumer organisations and if not in consumer organisations then in publicly-funded research institutions. On top, consumer councils in national standardisation bodies may involve technical experts on an individual basis, a policy which seems widespread within national standardisation bodies and ANEC. However, the necessary independent and impartial technical knowledge of AI is to a much larger degree located outside consumer organisations and consumer agencies and therefore also outside ANEC, which relies on input from consumer organisations, from consumer councils integrated into the national standardisation organisations, and from independent experts who raise their voice on behalf of ANEC. New ways of funding independent experts seem to render the rise of input from the civil society more realistic.⁵⁰¹

The expert knowledge that exists in and outside the EU at the nation-state level needs to be mobilised and needs to be integrated into the co-regulatory process. The envisaged revision provides the opportunity to systematically integrate expert knowledge available outside the consumer organisations into the standardisation process. So far, representation of consumers in Annex III is bound to institutional requirements, a mandate by two-thirds of Member States’ consumer organisations. The institutional requirement would lose importance if ANEC is given a status similar to that of the ESOs and named explicitly. However, the very same institutional requirements might help to leave the door open to new developments in the organisation of consumer protection through civil society organisations. The two-thirds quorum makes sense as long as the legislature focuses on policy input, which stakeholder organisations are expected to provide. In terms of technical expertise such a quorum is counterproductive. All that counts is the quality of the expertise and the independence and impartiality of the non-governmental organisation concerned.

Such a strengthening of civil society, be it through ANEC and/or through independent and impartial knowledge-based NGOs, could be convincingly connected to the ‘core European values’ that the European Commission intends to promote in its New Standardisation Strategy.⁵⁰² So far, all the rhetoric on ‘*human-centric, secure, ethical and trustworthy AI*’ is focusing – too much – on fundamental rights. The European Commission seems to equate core values with fundamental rights, at least in the AIA-P, CRA-P and the DSA. Reliance on co-regulation

⁵⁰⁰ OECD Working Party on Artificial Intelligence Governance, Common guideposts to promote interoperability in AI risk management – comparing AI risk management frameworks, work in progress not yet available.

⁵⁰¹ StandCt Programme to finance standardization experts <https://www.standict.eu/> and the last call for funding www.standict.eu/standicteu-2026-1st-open-call; see also Lovelace (fn 500) throughout the paper.

⁵⁰² Roadmap for a European Standardisation Strategy May 2021 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy_en

offers the opportunity to send a signal to the standardisation community around the world that stakeholder participation and civil society participation belongs to the values which the EU would like to see promoted. It would equally pave the way for a broader discussion on how to include voices from the Global South in the standardisation process. Such an extension of core values would enable the European Commission, if not the European Union, to call for the involvement of civil society at both the national and the international level as well as to legitimate a potential upgrade of ISO/IEC standards, which are elaborated with limited stakeholder participation, if any at all.

g) Geopolitics

The bold language of the European Commission in the New Standardisation Strategy that the EU should become ‘a global leader in the development of secure trustworthy and ethical AI’⁵⁰³ clashes with the reality, where the EU has to convince ISO/IEC and IEEE that existing international standards have to be upgraded to meet ‘core European values’ and to the same extent with the interests of the national standardisation bodies of the EU Member States, which participated in elaborating them and which must implement harmonised European standards as national standards in the member countries of CEN-CENELEC and withdraw conflicting national standards.

There is a strong overlap between the ten mandated standards and the ISO/IEC and IEEE standards. The ISO/IEC standards – this cannot be reiterated often enough – have been elaborated with the support and participation of EU national standardisation organisations. In practice, the same people who elaborated the ISO/IEC standard⁵⁰⁴ will come together again within CEN-CENELEC once the current Standardisation Request has led to concrete mandates to develop harmonised European standards.⁵⁰⁵ The European call for ‘upgrading’ existing international standards will meet resistance, not only from ISO/IEC – who will insist on the Vienna and Frankfurt Agreement – but also from the national standardisation bodies. As things stand, national representatives of the standardisation organisations might tend to defend the international standard they had developed as being trustworthy and ethical, and promote their transformation into a European standard in order to benefit from the presumption of conformity. In light of the broad fundamental rights rhetoric which is not so far transformed into concrete measures which the ESOs have to take, the members of the working group will insist on the technical character of their work and reject responsibility for engaging in a fundamental rights compliance test. For good reasons, standardisation organisations are ill-equipped to answer hard normative questions. The envisaged co-operation between the EU and the USA on the development of AI standards, which is a product of the EU-US Trade and Technology Council (TTC),⁵⁰⁶ might lead to further complications to the integration of ‘core values’.⁵⁰⁷

What will happen? Key figures in AI standardisation proposed relabelling international standards as harmonised European standards, together with minor rewording and – eventually

⁵⁰³ New Standardisation Strategy (n 490).

⁵⁰⁴ DIN for instance is the leader in development of the ISO standard on impact assessments.

⁵⁰⁵ Interviews with experts from standardisation organisations and representatives from IT companies.

⁵⁰⁶ https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en

⁵⁰⁷ <https://spectrum.ieee.org/ai-standards>

– garnering the ‘EN ISO/IEC standard’ with fundamental rights rhetoric.⁵⁰⁸ A possible way out might be the need to juridify international standards, which implies – now – involving lawyers in the working groups and asking them to check compliance. Here the proposed Regulatory Scrutiny Board comes in. This should replace the HAS consultants and should be composed of lawyers and technical experts. Eventual compliance with fundamental rights cannot be achieved without having standardised the potential use cases and without submitting the envisaged standards to minimum testing requirements apt to test local impact. Both use cases and testing requirements are by and large non-existent in EU Digital Policy Legislation and the EC working programme. Developing use cases and standardising them is a necessary requisite for developing testing schemes. Not to forget that developing such methods, as well as testing itself, is not only time-consuming but also highly expensive.

3. Options for Change

The foundations for today’s governance structure which will manage digital policy legislation were laid down in 1985. The following decades were characterised by gradually developing institutional governance, first through the establishment of ANEC and in 2012 through Regulation 2015/2012, which conferred status on the ESOs and the stakeholders, operationalising co-operation through procedural requirements on elaboration of technical standards broken down into:

- working programme,
- call for proposals,
- standardisation request and
- publication in the Official Journal.

The substance equally changed over time, but remained in essence the same in that it is built around the distinction between non-harmonised and harmonised European standards. The attempt to stretch the scope of technical standardisation to services failed. To the best of my knowledge, the proposed extension was never seen as a potential reason to put the then existing governance structure into question. Setting aside the debacle with service standards, one may understand the years between 1985 and 2018 as a rather smooth period where the key actors – the European Commission, the ESOs, and stakeholders – quietly put flesh on the bones of the New Approach/NLF through gradual extension of European technical standards in quantity and in the applied fields. This impression does not alter if one takes comitology into account, or even the distinction between delegated acts and implementing acts in the Treaty, or the gradual fine-tuning of regulatory projects which are suited to become subject to technical standardisation. All these various amendments and adjustments are rooted in the 1985 New Approach. To put the process into a metaphor, the plan for the house was there but the house itself took decades to build – step by step, governed by the same corporate spirit – the 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.

⁵⁰⁸ Interviews with experts from standardisation organisations and representatives from IT companies.

The first major change resulted from outside intervention, from the appearance of the CJEU, not only in *James Elliott and Stichting Rookprevenite*, but also in *Fra.bo* and *Schmitt*. It is hard to predict how far the Court will go, certainly not in submitting harmonised standards to full judicial review. However, it might very well be that the CJEU increases pressure on the governance structure, interfering with the institutional setting and in the procedural requirements laid down in Regulation 2015/2012 through facilitating the conditions of access to European harmonised standards. The outcome of the pending appeal against *Public.Resource.Org* will be crucial.⁵⁰⁹

The next game changer results from universalised structural, architectural, and relational digital vulnerability, which challenges the foundations of the consumer acquis.⁵¹⁰ This shattering makes it all the more important to identify intermediaries – stakeholder organisations, who can speak of the behalf of citizens when it comes to elaboration of AI standards and to the mediation of technicality and its relevance for the practical use of whatever software. The search for a more balanced governance structure within the EU, meant to build ‘*human-centric, secure, trustworthy and ethical AI*’, must start from the following premises:

- the final responsibility of statutory actors in developed democracies;
- their limited AI expertise;
- the concentration of technical knowledge in the hands of the digital industry; and
- the legitimate expectation of civil society to rely on trustworthy and ethical AI.

A more balanced governance structure requires the full inclusion of civil society through its legal, political, and technical-digital representatives in elaborating a new generation of AI standards which harnesses the huge potential that AI could bring to the people.⁵¹¹ The required governance structure should turn into a joint exercise where the Member States, the EU, business – big and small – and civil society – political and technical – are all integrated.

The following considerations focus on harmonised European standards alone. The arguments do not extend to non-harmonised standards. Where there are deficiencies, as in protection of minors in the DSA,⁵¹² the solution is not to submit non-harmonised standards to the same requirements but to correct the deficit and to turn these standards into harmonised European standards. The strong hand of the EU is limited to harmonised European standards, as only these can be required to be certifiable and as only these establish the presumption of conformity, independent of the field where they are applied.

a) First Option – No Change

The current regulatory framework – the AIA-P, CRA-P together with Regulation 1025/2012 as revised in 2022 – seems to suggest that there is no substantial difference between using technical standards in product safety regulation in the industrial economy, on the one hand, and using technical standards to guarantee compliance with fundamental rights in the new economy. The rationale behind this is based on the assumption that safety is a fundamental right

⁵⁰⁹ Case T-185/19 ECLI:EU:T:2021:445, Appeal Case before the Court of Justice C-588/21 P

⁵¹⁰ Helberger et al Consumer Law 2.0 (n 8).

⁵¹¹ O Lobel, *The Equality Machine: Harnessing Digital Technology for a Brighter, More Inclusive Future*, 2022.

⁵¹² See under III 3 b).

too, and that therefore standardisation organisations are well equipped to handle fundamental rights on a much broader scale. Interviewees from the European Commission openly admitted that the AIA-P and the CRA-P, in their reliance on harmonised standards, are breaking new ground and that Regulation 1025/2012 might need to be adjusted to the new task. However, at the time of writing the European Commission aims to come up with more concrete proposals by the end of 2023.⁵¹³

The deficiencies so far identified of the current design of the New Approach/NLF would already suffice to justify revision, due to incomplete and insufficient regulation of participation by stakeholders, the – as yet unimplemented – consequences of CJEU involvement in judicial control of harmonised European standards and the long overdue integration of fundamental rights into the New Approach/NLF, which allows a new benchmark to be set for fundamental rights-compatible harmonised European standards.

However, the transfer of the New Approach/NLF to the digital economy has laid bare four major reasons why a ‘no change’ is no viable option and why the need for action is urgent:

- The *first* reason results from incomplete implementation of the HLEG Guidelines which advocate the necessity to draw a red line which ensures human control over AI.
- The *second* reason result from the incomparability of health and safety-related risks in the industrial economy to those from non-trustworthy and unethical AI. Health and safety-related risks in the industrial economy are legally and empirically manageable by and large via the principle of foreseeable use, and the possibility to build appropriate use cases which must be integrated into the design of a product, whereas AI risks lay bare the limits of the law to reach into the technicalities of rule production as well as the limits of even AI experts to build a serious set of potential use cases which allow supervision the potential effects. One of the major finding of the Report is the need to test the feasibility of drafting use cases.
- The *third* reason is that fundamental rights form part of the EU constitutional order, reaching from product safety to non-discrimination and protection of consumers’ economic interests. Whilst the right to safety is relatively well established, not least through extensive EU regulation on product safety, the same cannot be said of the broad range of fundamental rights which are enumerated in the AIA-P and mentioned in the CRA-P and the DSA more broadly.
- The *fourth* reason is the risk that certified compliance with a future harmonised European AI standard of the type so far developed by ISO/IEC and IEEE might lull the final user of an AI system into a false sense of security that they are protected from possible liability risks. AI systems are highly unpredictable in their potential effects. This means that effective safeguards are needed to reduce the liability risk as far as possible. This requires integrating foreseeable uses into the elaboration process as far as possible, and to equip the final user of an AI system with the necessary tools to test and to document what they have done to keep the potential detrimental effects as far as possible under control.

In the light of such gaps, a ‘no change’ policy is not a responsible option, either under the Treaty or in light of the New Standardisation Strategy of the European Commission, which launched

⁵¹³ The sole reference can be found in the Standardisation Strategy document. It gives no other context or specific driver for the review than whether the Reg is fit for purpose. It is also there where the date of Q2/2023 is mentioned, which is now postponed to Q4/2023.

the willingness of the EU to become a global leader in ‘human-centric, secure, trustworthy and ethical AI’, which respects fundamental rights as ‘core European values’.

b) Second Option – Amendment of Regulation 1025/2012

At the time of writing, it seems difficult to imagine that there is political preparedness in the Council, in the European Parliament, and in the European Commission to reopen the debate over the feasibility of the New Approach/NLF to fill out the regulatory framework of the AIA-P but also of the CRA-P. The European Parliament is pushing for amendments to increase and sharpen the role and function of fundamental rights through promotion of a fundamental rights impact assessment, which in turn increases the necessity to focus on Regulation 1025/2012 as the prime target for change – for overcoming the existing deficiencies of the New Approach/NLF and for adapting the co-regulatory mechanism which was built in 1985 to the needs of the 21st century – the digital economy and the digital society. This Report puts the emphasis on the consumer perspective, although there are good reasons to rethink the New Approach/NLF in a much wider context which also addresses the – here left out – dimension of the legitimacy of private rule-production.⁵¹⁴

A revised name must express the overall political message to the standardisation organisations and to civil society. Regulation 1025/2012 is called ‘*Regulation on European Standardisation*’. In order to express the new spirit, Regulation 1025/2012 should be termed ‘*Standardisation Governance Act*’ (SGA). The overall aim of the revision is to develop technical standards which respect human dignity and comply with fundamental rights *ex ante* and which enable the potential addressee of technical standards – in the case of AI the local provider – to keep under control the potential risk which results from a particular AI system. This is an extremely ambitious undertaking. Subjecting technical standardisation to a fundamental rights test requires revision of the governance structure, to be broken down into institutional, procedural, and substantive governance. Such a new governance structure should make the New Approach/NLF fit for developing standards in the changing economic, political, and societal environment of the industrial and the digital economy. The required – and here proposed – design of a new governance structure should breathe a new spirit, one where EU law explicitly recognises that technical standardisation rests on three pillars:

- the European Commission – the political;
- the ESOs – industrial expertise; and
- stakeholder organisations – societal expertise.

Clear political guidance is all the more needed as there are strong voices which are pushing in the opposite direction – reduction if not elimination of stakeholder organisations.⁵¹⁵

⁵¹⁴ R van Gestel/P van Lochem, ‘Private Standards as a replacement for public policy making?’ In M Cantero Gamito/ H-W Micklitz (eds.), *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes*, Edward Elgar Publishing, 2020, at 45 proposes three models: the Agency Model, the Public Private Partnership Model, and the Disentangle Model

⁵¹⁵ J Baron/P Larouche, European Standardisation System at a Crossroads, Centre on Regulation In Europe, 2023 https://cerre.eu/wp-content/uploads/2023/05/CERRE_The-European-Standardisation-System-at-a-Crossroads.pdf

aa) Red Lines on Standardisability

Two reasons explain why there is a need to set limits to the standardisability of harmonised European standards, limits which result from the co-regulatory approach based on the ultimate responsibility of the EU legislator to guarantee that technical standards comply with EU law:

- the first is connected to the necessity to bind development of technical standards to respect for fundamental rights, independent of whether they are related to the industrial or the digital economy, and
- the second is tied to ensuring human-centric control over AI.

The Charter of Fundamental Rights dates back to the year 2000 before it became part of EU law in 2009. Since then, the EU has gradually made sure that secondary EU law complies with fundamental rights, either in the recitals or in the text of directives or regulations. Regulation 1025/2012 lags behind as there is currently no reference to the EUCFR. Neither the New Approach nor the NLF is exempted from the grip of fundamental rights. Delegating rule-making to the standardisation organisations does not free the EU legislator from the need to take measures to ensure that technical standards have to comply with fundamental rights. That is why a benchmark is needed and written into law which guarantees that technical standardisation – even in the form of harmonised European standards – is not crossing a red line which excludes standardisability because of the risk that elaboration of a technical standard might infringe fundamental rights.

Setting a benchmark in the form of a general clause sets limits to a standardisation request. It is for the European Commission to make sure that the red line is respected. What might be highly conflictual in the industrial economy might meet much more support in the digital economy. There is overall agreement that AI can be human-centric and respect human dignity. Human-centric AI might mean two different things though:

- it might mean that AI systems must not infringe human dignity or
- it might mean that humans should have the ultimate word over the use of an AI system.

The HLEG Guidelines are built around this distinction and promote an understanding where control over AI will remain in the human hands. EU digital policy legislation is less outspoken and open for interpretation. Regulation 1025/2012 has to give shape to the new mandate of elaborating trustworthy and ethical AI standards. This has to be done by a general clause which sets human dignity in a prominent position and which bars the European Commission from mandating technical standards which are apt to undermine ultimate human control of an AI system.

bb) Institutional Governance

In order to put the ESOs and the stakeholder organisations on an equal footing, they need to be treated equally before the law. In our context, this implies integrating ANEC into Annex I and enlisting ANEC in line with the three ESOs: CEN-CENELEC and ETSI. Which of the other three stakeholder organisations currently financed by the European Commission should be given the same status is not analysed. However, there are good reasons to assume that ECOS, ETUC and SBS should be given the same status. Such a step is more than symbolic. It would

deprive the stakeholder organisations of the risk inbuilt into the current governance structure that their role and function is entirely dependent on the discretion of the European Commission. In theory, the European Commission could substitute them via similar organisations which meet the Annex III requirements. However, formal upgrading does not overcome the necessity to provide adequate funding for ANEC. Safeguards have to be inbuilt into the governance structure as well as new forms of financing of the work of stakeholder organisations, for instance through the respective industries, provided financing does not prejudice their independent status.

Formalising the status of the current stakeholder organisations does not overcome the gap identified in opening up pathways for integrating into the governance structure independent expertise located outside the four stakeholder organisations. Independent experts may already take part in standardisation working groups if they go through their national standardisation body.⁵¹⁶ This possibility should be institutionalised in Annex III in order to increase the breadth and depth of independent technical expertise in elaborating harmonised European standards. Such a broadening is long overdue. The digital economy has revealed the need to broaden independent technical resources on which societal input into AI has to be built. The rise of the digital economy has led to a multitude of non-governmental organisations around Europe and the world which aim at providing independent critical expert knowledge into the potential risks which result from AI. Such knowledge, however, is not bound to the criteria set out in Annex III 2). Potential organisations must neither represent consumer interests in their statutes nor be mandated by two-thirds of the national consumer organisations. AI expertise in civil society organisations usually reaches beyond consumer interests and is certainly not bound to a certain degree of representativeness in the Member States. This means that existing criteria need to be fine-tuned so as to allow for integration of independent AI technical expertise outside and beyond the four established societal stakeholder organisations. Their status should not be tied to European Commission financing. They may apply for financing, but their input into elaboration of harmonised technical standards has to be uncoupled from financing.

Institutionalisation of co-operation between the three different actors, that is, the European Commission, the ESOs, and stakeholder organisations (the current four and the newly proposed independent ones) requires bringing a problem upfront, which goes back to the establishment of the New Approach/NLF in 1985 – co-operation between technical experts and lawyers, independent of whether their expertise leans to one side of the three actors they represent. Technicians and lawyers belong to two types of communities and speak different languages. The phenomenon that two communities, coming from different professional backgrounds, are talking at cross purposes is known as the ‘Not Invented Here Syndrome’ (NIH).⁵¹⁷ The problem is structurally inbuilt into the New Approach/NLF and cuts across all the different steps of co-operation mechanisms – the level of law-making, the call for proposals, the standardisation request, the compliance procedure, and last but not least assessment of whether non-compliance is in potential litigation before national and European courts. Going down the line from law-making to elaboration and compliance assessment demonstrates that co-operation becomes ever more important the more concrete the questions arising are. There are two breaking points in the whole procedure which are of utmost practical relevance – the first is the compliance test in Regulation 1025/2012, the second is local use of technical standards or an AI

⁵¹⁶ E.g., in CEN-CENELEC JTC 21, information provided by a representative of a stakeholder organisation.

⁵¹⁷ https://en.wikipedia.org/wiki/Not_invented_here I would like to thank one of my interviewees from the stakeholder organisations who pointed me to NIH.

system. In a perfect world those in charge of assessing compliance and/or the impact of local use on society should have a double qualification, similar to patent lawyers, who in many legal systems are not only qualified lawyers but also qualified technician – in the industrial economy, most often an engineer. Seen from the outside⁵¹⁸ it looks as if the HAS consultants are currently de facto in charge of merging law and technical expertise throughout the process of elaboration from the very beginning until the compliance test. The software developers who have to translate AI standards into local use face a similar challenge. These are the ones who have to bring together normative ethics and descriptive/applied ethics. In theory they should be in a position when designing software to take into account their impact on human dignity and fundamental rights. Regulation 1025/2012 in its current form does not deal with the tasks and responsibilities of HAS consultants, let alone with software developers who were not on the radar when the Regulation was drafted. Whilst it might be a separate issue to discuss whether there should be EU law requirements on the qualification of a software developer, the revision has to tackle the compliance mechanism and the ‘who is doing what’ upfront.

The necessity to clarify the role and function currently in the hands of the HAS consultants who operate under the auspices of the European Commission results from *James Elliott*. The European Commission has taken responsibility for selection and monitoring of HAS. Legally speaking, the rules that follow from the Regulation in line with *James Elliott* overlap with the EU Commission’s contractual relationship with Ernst and Young. The black box has to be opened and submitted to a procedure which does justice to the tripartite co-operation between the European Commission, the ESOs, and the stakeholder organisations. The proposal is to replace the HAS consultants with a Regulatory Scrutiny Board which analyses compliance in both directions – law and technical expertise – and which under due consideration by the ESOs and the stakeholder organisation issues opinions and recommendations to the European Commission. The model to be followed is the one from the Better Regulation Approach, although the five principles have to be complemented through a sixth – integration of fundamental rights. A Regulatory Scrutiny Board should be composed of technical experts and lawyers in equal numbers. The composition does not overcome the NIH syndrome, but it seems the best possible solution to entice exchange and the need to come to a technical-normative assessment of compliance. The Regulatory Scrutiny Board does not predetermine the decision of the European Commission. There is no doubt that the European Commission is ultimately responsible – and maybe even ultimately liable – for compliance of binding legal requirements with harmonised European standards. The need for reform provides an opportunity to implement *James Elliott*, and to amend Article 10 (5) and (6) accordingly.

But there is more to do to adjust the institutional governance structure to move from bilateral to a triangular co-operation. The whole process of elaborating harmonised European standards – set into motion through the work programme; moving from there to the call for proposals; to the standardisation request and the final approval procedure, prior to publication in the Official Journal – has to be rethought and reconceptualised. The guiding idea should be that stakeholder participation – resulting from the need for independent expertise and the legitimate societal interests of trade unions, environmental and consumer organisations – is to be guaranteed at each and every stage throughout production of harmonised European standards.⁵¹⁹ This claim has two implications – participation by the ESOs and stakeholder organisations

⁵¹⁸ Due to missing information from the HAS consultants themselves.

⁵¹⁹ See the table under II 2 b)cc) above.

should be put on an equal footing within the various steps of the European decision-making process. Analysis of the recently adopted Standardisation Request has demonstrated how crucial is involvement of stakeholder organisations prior to the start of work in the technical committees. The Standardisation Request is the bottleneck, the last chance for stakeholder organisations to give the mandate a political direction, in order to point to the gaps which result, for instance, from under-specification of use cases and minimum testing requirements. The second crucial moment is the compliance test, where the technical and legal implications come together and where it is to be decided whether the technical standard may enjoy the status of a harmonised European standard justifying the presumption of conformity. The third decisive moment of the decision-making process is the objection procedure. The proposed new spirit of tripartite co-operation requires not only to upgrade stakeholder organisations to the status of ESOs but also to treat the ESOs and the stakeholder organisations equally. They need to enjoy the same rights. Only equal rights guarantee co-operation in a level playing field. Equal treatment means that the rights of both the ESOs and the stakeholder organisations will have to be extended whenever there is a bias in the existing set of rules.

The stakeholder organisations should be involved in the decision on the standardisation request and no longer be obliged to leave the committee when it comes to a vote; they should participate in the compliance test together with the ESOs so far regulated in Article 10 (5) Regulation 1025/2012, and they should be entitled in their own right – just like the Member States and the European Parliament – to initiate the objection procedure and not only be consulted by the European Commission, Article 12 c) Regulation 1025/2012. Such an extension would underpin that the final decision on compliance, which might not be solved in the extended cooperation mechanism, should be decided politically through the assigned democratic institutions.

cc) *Procedural Governance*

Institutional restructuring concerns the role and function of stakeholders on the statutory side of the governance structure. However, the statutory side needs to be mirrored within the processes that determine the role of the stakeholders within the standardisation organisations.

Regulation 1025/2012 calls for including stakeholders into elaboration of technical standards, but stays away from laying down binding requirements on what participation should look like, thereby leaving it to the ESOs to decide. The current state of affairs is unsatisfactory and does not do justice to the role that societal actors play *de facto* and should play *de jure* in the industrial economy and in the digital economy, though for different reasons. In the industrial economy, stakeholder organisations should finally be given the status they deserve. The digital economy is dependent on the input of stakeholder organisations if the formula of human-centric, secure, trustworthy and ethical AI is not to remain an empty shell. Stakeholder organisations have to contribute to bringing in and insisting on the descriptive/empirical part of ethics – condensed in the importance of use cases.

The list of what the four stakeholder organisations are not entitled to do might be more telling than the one that says what they are allowed to do⁵²⁰ – they have no voting rights in

⁵²⁰ See the Joint Statement by the four stakeholder organisations ANEC, ECOS, ETUC (European Trade Union Confederation), SBS (Small Business Standards), CEN and CENELEC's governance review in support of inclusiveness Proposal of the Annex III organisations, December 2022,

CEN-CENELEC in contrast to ETSI where Annex III organisations are full members, although they can easily be outvoted (subject to change), they have no right to take over the secretariat; they have no right to require the ESOs to either comply with their claims or to receive a written explanation why the ESOs do not comply; they have no right to appeal independent from participation in a technical committee. Their status is that of an observer which may offer comments and opinions, but it depends on industry, on the HAS consultant, and on the European Commission whether their arguments are heard. To put it differently, the only power they have is knowledge and argument, but they have been given no tools to turn knowledge and argument into action in case they are outvoted or in case their comments are not respected. This needs to be changed.

It is plain that EU law cannot impose on the ESOs how they draft their statutes; how they rank and classify their members, including potential outsiders, let alone what kind of rights they should be granted. However, what the European Commission can do is to accept as Annex I institutions only those which meet the requirements laid down in a revised regulation. It has to be recalled that the degree to which the Regulation should specify participation rights came already up in the legislative process of Regulation 1025/2012 and led to major discussions between the European Parliament and the European Commission. In the end the Regulation did not include voting rights, but left it for the ESOs to grant such rights in their statutes (Recital 23). The required new spirit calls for putting the stakeholder organisations on an equal footing, turning them from observers into full members, equipped with the right to take over the secretariat, with voting rights up to a right to veto – at least in the meaning of ‘comply or explain’. Their role as partners requires going one step further to exclude the possibility that stakeholders can be outvoted by industry. In the case of conflict between the ESOs and the European Commission which cannot be resolved, the statutes should foresee an independent dispute resolution mechanism along the lines of Article 21 (3) DSA.

Technical standards are copyright-protected, although it might well be that the CJEU will limit copyright in the near future. In *Stichting Rookpreventie*⁵²¹ the CJEU opened the door to a legal discourse which will reach European harmonised standards sooner or later. Copyright protection goes back to the idea that technical standards enshrine a particular technical competence which guides the manufacture of products and therefore carries a particular ‘value’. Extension of technical standards to product safety issues added a new layer to technical standards. Whether or not safety-related harmonised European standards must be freely available became a subject matter long before the CJEU held them to be ‘law’. The transformation of the New Approach/NLF to the digital economy, thereby combining technicity with ethics and fundamental rights, makes it even more complicated to find arguments why rules – which are loaded with constitutional values – deserve copyright protection. Analysis of existing ISO/IEC and IEEE AI technical standards demonstrates that they are not very technical in nature, but normative-political – in the new language *socio-technical* – enshrining a heavy load of normativity without openly admitting it. The most radical solution would be to make European harmonised standards per se freely available. This, however, would imply that the European Commission is compensating the ESOs for their work, not in part but in full. An alternative could be that the European Commission buys open access. Both variants would imply that co-operation between the European Commission and the ESOs is put on a very different financial basis. The barriers are not insurmountable, though. There are possibilities to disclose standards, but

521 22.2.22 Case C-160/20 *Stichting* (n 4).

to monitor free access to standards through mandatory requirements to be fulfilled by potential applicants. Accessibility might also be made dependent on the type of standard elaborated – a matter to which we will come back below. However, here too procedural safeguards are needed which make the decision-making procedure transparent and which ensure adequate participation by stakeholder organisations.

The upgrading of stakeholder participation to co-operation partners in elaborating technical standards, through the necessary institutional safeguards which secure compliance with fundamental rights anchored in a revised Regulation 1025/2012, helps to overcome a key problem – lack of stakeholder participation within ISO/IEC. Juridification of the standardisation process through promotion of core values, inter alia of fundamental rights, empowers the European Commission to identify lack of participation by stakeholders as a gap which justifies and legitimates that the EU sets a review procedure into motion, one which aims at investigating whether international standards comply with the two dimensions of trustworthy and ethical AI – the normative implications and the empirical implications of the trust-building exercise. ISO/IEC and IEEC standards stress the need to take into consideration different understandings of ethics, of culture, and of different legal frameworks. It suffices to recall the different understandings of the role of privacy and equality/non-discrimination. However, the role and function that nation states grant to society in the development of technical standards vary considerably. Upgrading inclusiveness of all stakeholders from an ‘add-on’ to partnership provides the EU with the necessary argument that ISO/IEC standards need to be tested not only from a fundamental rights perspective: the normative side; but also from societal acceptance and acceptability: the empirical side. Therefore, the understanding of stakeholders as co-operating partners empowers the European Commission to argue that ISO/IEC and IEEE standards need to be submitted to an acceptability test – which will in essence be a test whether and to what extent use cases have been taken into consideration, and who was involved in drafting the use cases. Stakeholder participation is an acid test for the relationship between CEN-CENELEC and ISO/IEC. One might call the pressure the EU exercises on CEN-CENELEC and therefore on ISO/IEC as another variant of the Brussels effect. However, both the ESOs and ISO/IEC have a long-term interest in stabilising the relationship with the EU. Therefore, there is a good chance that ISO/IEC will change their rules and take participation of societal players seriously, not only from the Global North but also and in particular from the Global South, thereby facing the critique of EU/US-centrism.

dd) Substantive Governance

The major change in the substantive governance structure results from the need to integrate fundamental rights, not only in the industrial economy consequent to a long overdue adaptation with a general policy change in EU legislation, but also and in particular through the formula of human-centric, secure, trustworthy and ethical AI. Technical standards in the field of AI must fulfil two conditions – they must comply with EU law – fundamental rights, and they must be appropriate to build trust in society, which cannot be achieved through law alone but which requires that AI standards serve the needs of society at large, and that compliance does not trigger potential risks to those confronted with the use and the user of AI systems. The direct consequence is that the working programme, as well as the standardisation request, should insist on the need to develop standards – which are fit for purpose – to borrow that language from the European Commission itself – but fit in a twofold sense – complying with both normative and descriptive/applied ethics. Existing ISO/IEC and IEEE AI standards demonstrate

insufficiencies at both levels. It does not suffice that the AIA-P and the CRA-P require normative compliance with EU law, though. The European Commission needs to explicitly call for standards which meet the twofold dimensions, both in the working programme and in the standardisation request. The ESOs should develop a set of standardised use cases which could be widely applied for whatever user of AI systems. This would allow *ex ante* determination of the potential effects in the relevant sector of the economy and society. Use cases are a typical example of a socio-technical standard which stands in between binding legal requirements and certifiable AI standards, which still need to be developed – at least this is the major finding of the stocktaking of the various initiatives to standardise trustworthy AI.⁵²²

In AI, more needs to be done to solve the problem that the local user of an AI system – often an SME – needs help and support, which allows them to test their application. Here certifiable technical standards are needed which equip the user of an AI system – who can be a start-up company or a regulator, an enforcement authority or even a court – with a tool box which allows them to test biases, discrimination, and fairness. Such a tool box is even more important as it is not clear whether and to what extent it is possible to develop a standardised set of use cases. The standards the European Commission should call for should enable the user of the AI system to test their system prior to entering the internal market, so as to be able to eliminate potential risks. The concrete circumstances of application of AI in a use case can never be standardised, let alone automated. Values such as fundamental rights – which enshrine categories like fairness, transparency, explainability – may be standardisable up to a certain point (even automated), but only with regard to providing a test kit to identify biases, unfairness, and discrimination, but they cannot replace the value judgment when a risk materialises.⁵²³ Due to their crucial importance, such minimum standards should be freely available in particular for all SMEs as users of AI systems. Whether the EU pays for the mandate, or for open access, might be left to the European Commission and the ESOs. They should be designed in a way so that compliance triggers the presumption of conformity, otherwise they are more or less useless for the local AI provider. *Laux/Wachter/Mittelstadt* have proposed the following tools as examples, providing explanations and justifications for each of them:⁵²⁴

- *bias tests and de-biasing methods, including pre-, in-, and postprocessing methods;*
- *fairness measures and enforcement methods including individual, group, unawareness, and counterfactual measures, as well as open-source toolkits;*
- *transparency and explainability methods including local and global model and outcome explanations, model inspection methods, interpretable models, post hoc explanations;*
- *model and data standardised documentation such as datasheets for datasets, model cards, nutrition labels;*

⁵²² Under IV. 6.

⁵²³ S Wachter, B Mittelstadt and Ch Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (March 3, 2020). *Computer Law & Security Review* 41 (2021): 105567., available at SSRN: <https://ssrn.com/abstract=3547922> or <http://dx.doi.org/10.2139/ssrn.3547922>

⁵²⁴ J Laux, S Wachter, B Mittelstadt, 'Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act' (February 20, 2023). Available at SSRN: <https://ssrn.com/abstract=4365079> or <http://dx.doi.org/10.2139/ssrn.4365079> at p. 23; see in this context ETSI Technical Report, Study into the challenges of developing harmonised standards in the context of future changes to the environment in which products are being developed and operated, 2022 with a detailed critique of the consequences, in particular with regard to 'subjective testing' at pp. 26 with regard to the RED.

- *impact assessments such privacy impact assessments, Algorithmic Impact Assessments, equality impact assessments;*
- *any other documentation describing ethical decisions made by providers or procedures used to make such decisions such as internal or external ethics review committees, content moderation policies, model selection criteria, relevant elements of design specifications*

This list obviously overlaps with existing AI standards or AI standard projects under way and to some extent with Annex IV of the AIA-P. Once the AIA will be adopted, there is a need for a stronger comparison as well as the formulation of appropriate standardisation requests. However, it seems that the Standardisation Request already integrates partly the references in Annex IV to testing requirements.⁵²⁵ Worth mentioning is the French-German initiative to develop an AI label composed of five elements – transparency, accountability, privacy, fairness, reliability – which resembles in design and colour the Nutriscore. Each element ranks from A to G, from green to yellow to red.⁵²⁶ All these attempts, proposed by academics and/or by AI experts to give more weight to the concrete circumstances in which an AI system is applied, should take into account sandboxing, a strategy which is rather developed in the financial services, but which is also foreseen in the AIA-P.

The proposed set of certifiable minimum standards contributes to a fair share of responsibilities. Their elaboration and their availability avoid a situation where the final user of the AI system ends up with the incalculable risk of harming society, which could arise in the absence of such a toolkit or if they falsely believe that reliance on existing meta standards will protect them against liability claims. Only such minimum standards could break down the vicious circle that responsibility ('the buck') is passed from one instance to the next, with the potential outcome that – at the end of the day – nobody can be held liable any more as has been the case in PIP. Minimum standards enable the user of an AI system to apply the toolbox and to test the potential impact of their AI systems in the very concrete circumstances in which the AI system might gain importance. The duty to do so could be understood as a due-diligence obligation which should include the necessity to involve a local public which has a basic understanding of statistics, without being AI experts. However, in light of the fact that the AIA-P will probably not undergo major revisions any more, the minimum toolkit needs to integrate guidance on what the local user of an AI system has to do in order to increase the acceptability of their system in the very concrete local environment. This includes integration of those who are affected by the AI system. It would be on the local public to comment on the trade-offs: for instance, between accuracy and robustness; between transparency and explainability. The need for local acceptability is triggering actions by business circles which are in the limelight of consumer attention. It looks as if the credit bureaus, which will be affected by the AIA-P once adopted, are ready to move in the direction here proposed.⁵²⁷

⁵²⁵ Under IV 4 c) bb).

⁵²⁶ Information provided by S Hallensleben, How Standardisation brings AI ethics into practice, 6.10.2022, on file with the author, which is based on VDE/Bertelsmann Stiftung, From Principles to Practice, An interdisciplinary framework to operationalize AI ethics, 2020, <https://www.ai-ethics-impact.org/resource/blob/1961130/c6db9894ee73aefa489d6249f5ee2b9f/aieig---report---download-hb-data.pdf>

⁵²⁷ The German Schufa has developed a test kit which allows consumers to understand how the credit score operates in practice. It is built as a game, where the consumer can play around and see the impact if one of the mentioned score indicators changes.

c) Third Option – Amending the AIA-P, the CRA-P and the DSA

The third option would be to re-open the negotiation on the AIA-P and to integrate deficits identified in a revised version. The list of potential amendments is long:

1. introducing red lines;
2. operationalising the introduction of fundamental rights into the elaboration of technical standards;
3. thereby sharpening the dividing line between binding legal requirements on the one hand and technical standards on the other;
4. clarifying and defining human-centric, secure, trustworthy, and ethical AI;
5. stressing the twofold dimension of AI ethics – the normative and the empirical dimension;
6. integrating the local user of an AI system into the regulatory design and identifying their particular needs;
7. clarifying the relationship between foreseeable use/misuse and the potential use cases;
8. addressing the liability of standardisation and certification bodies.

The identified deficits in the DSA could easily be added to the list. These concern in particular protection of minors which cannot be guaranteed through non-harmonised standards, but (if any) should be subject to harmonised European standards and could therefore be integrated in a revised AIA-P.

However, in light of the advanced process in interinstitutional agreement, the third option does not seem to be a politically promising avenue. That is why the focus will be put on revision of Regulation 1025/2012.

VI. Proposal for a Standardisation Governance Act



PROPOSAL FOR REVISING REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 on European Standardisation

1. Recitals

1. Regulation 1025/2012 is more than ten years old. In the meantime **the importance of harmonised European standards for building the internal market at a high level of consumer protection has steadily increased**. Harmonised European standards are used not only to establish an adequate level of product safety but also and ever more strongly to adapt the economy to sustainability requirements. In European Digital Policy Legislation, harmonised European standards are meant to concretise the upcoming rules on Artificial Intelligence and Cyber Resilience. Last but not least, the Court of Justice of the European Union has taken far-reaching decisions on the legal character of harmonised standards, on the reach of the potential copyrights of technical standards, and on the liability of certification bodies.

2. In light of the crucial role of harmonised European standards in the European legal order, the proposed revision aims at adapting the rules governing elaboration of harmonised European standards, where the EU bears a particular responsibility with regard to protection of public policy interests, consumer and environmental protection, as well as fundamental rights in both the industrial and the digital economy. **The proposed revisions affect only harmonised European standards and socio-technical standards**. They are not applicable to non-harmonised standards.

3. The New Approach/NLF **contributed considerably to building the internal market** in the aftermath of adoption of the Single European Act in 1985. Co-operation between the European Commission and the European Standardisation Organisations (ESOs) paved the way for integrating and promoting product safety into technical standardisation. This was possible because production of technical standards was framed by the Product Liability Directive 85/374 and the Product Safety Directive 92/59, today's Regulation on General Product Safety 2023/998 (RGPS). These legislative measures were complemented through Regulation 1025/2012, which formalised the institutional and procedural requirements on elaboration of technical standards through co-operation between the European Commission and the European Standardisation Organisations on participation by the stakeholders mentioned in Article 5, and not least those categories of stakeholder mentioned in Annex III.

4. Ever since adoption of Regulation 1025/2012, there have been concerns that **the New Approach/NLF goes too far in submitting whole policy fields to technical standardisation**, in particular without questioning:

- whether standardisation is always the best option or
- whether it is necessary to keep particular problematic issues in the hands of the EU or national legislatures,

and additionally without taking into account that:

- existing mechanisms of participation fail to allow sufficient influence of societal interests in developing product safety-related harmonised European standards, and
- stakeholder organisations have to be turned into full partners with corresponding rights and remedies in elaborating harmonised European standards from the working programme over the standardisation request up to the compliance test and publication in the Official Journal.

The current revision aims at remedying these deficits. The current position of stakeholder organisations has to be upgraded and rules are needed to ensure that there are limits to the feasibility of the New Approach/NLF in covering all conceivable risks in the field of consumer and environmental protection.

5. EU Digital Policy Legislation, intended to establish a new legal framework for the Digital Economy, relies on the New Approach/NLF to complement binding legal requirements through harmonised European standards in the AIA and the CRA. **The Digital Economy poses two new types of challenges to the New Approach/NLF:**

- The first challenge is the need to respect the **red lines** which will be introduced in EU Digital Policy Legislation through prohibition of certain particularly risky potential applications of AI, which in turn means that safeguards have to be introduced which guarantee that potential mandates of the European Commission to elaborate harmonised European standards do not cross the red line.
- The second challenge results from the **impact of AI on society**. The New Approach/NLF was designed to deal with the potential risks of unsafe products to the health and safety of consumers and citizens. AI affects society at large and poses particular risks to humanity – risks which should be captured by reference to fundamental rights. Here, technical standardisation enters a new dimension which reaches far beyond established experience in the field of product safety and environmental regulation.

6. The cross-cutting character of technology – and its interference in the economy and society – brings technical standardisation ever closer to the consumer and the environmental acquis. Existing ISO/IEC and IEEE AI standards as well as the first Standardisation Request⁵²⁸ touches upon key concepts of the consumer acquis such as transparency. Here, ethical principles, individual fundamental rights, fundamental rights principles, and the consumer acquis overlap. **The long overdue integration of fundamental rights into elaboration of industrial**

⁵²⁸ Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, Brussels, 22.5.2023, C(2023) 3215 final

technical standards accentuates the need to seek enhanced compliance of individual fundamental rights and fundamental principles – in particular Article 38 EUCFR – with technical standardisation in the industrial and digital economy which takes due regard of the existing body of consumer and environmental law.

7. European industry benefits from European harmonised standards through their market-opening effects. Compliance with harmonised European standards establishes a presumption of conformity and grants access to the internal market, provided the standards comply with EU law. The New Approach/NLF established a type of co-regulation, where the EU legislature uses and relies on the technical expertise of the three European Standardisation Organisations (CEN-CENELEC and ETSI – the ESOs) to transform binding legal requirements under due participation of stakeholder organisations into technical rules. The EU legislation in the **industrial economy** connects the development of harmonised European standards to product safety and more recently ever more strongly to environmental protection. Here the ESOs enjoy a long **experience** in integrating societal concerns into technical rules. Stakeholder participation has turned into a necessary condition for elaborating such harmonised European standards.

8. The Charter of Fundamental Rights dates back to the year 2000 before it became part of EU law in 2009. Since then the EU has gradually made sure that secondary EU law complies with fundamental rights, either in the recitals or in the text of the respective directive or regulation. Regulation 1025/2012 lags behind as there is currently no reference to the EUCFR. **Neither the New Approach nor the NLF are exempted from the grip of fundamental rights.** Delegation of rule-making to the standardisation organisations does not free the EU legislator from the need to take measures to ensure that technical standards comply with fundamental rights. That is why a benchmark is needed and written into law which guarantees that technical standardisation even in the form of harmonised European standards do not cross **a benchmark which excludes standardisability** because of the risk that elaboration of a technical standard might infringe fundamental rights.

9. EU Digital Policy Legislation aims at establishing a digital market for **human-centric, secure, trustworthy, ethical, and lawful AI**. This formula is key for the legal framework in which elaboration of harmonised standards needs to be embedded. EU Digital Policy Legislation – as documented in the Explanatory Memorandum to the AIA:

is based on EU values and fundamental rights and aims to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them. AI should be a tool for people and be a force for good in society with the ultimate aim of increasing human well-being. Rules for AI available in the Union market or otherwise affecting people in the Union should therefore be human centric, so that people can trust that the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights.

10. Human-centric, sustainable, secure, inclusive, and trustworthy AI may either indicate a human-protective approach, with the emphasis on increasing human well-being as well as the take-up of AI, or may suggest an approach where humans continue to rely on rules and remain in control. The first brings EU digital policy legislation closer to other protective policies such as safety and the environment. Whilst AI should definitely serve human well-being, it is equally necessary to ensure that humans remain in control of the development and use of AI systems. This second strand, the **call for human control** is inspired by respect for human dignity and highlights the major concerns which stand behind the prohibition of certain AI applications

and which govern all sorts of AI risks, including those where EU harmonised standards are to be elaborated under the AIA-P and the CRA-P. The ultimate control of humans over AI is not negotiable: the responsibility must remain in the hands of the EU legislature and cannot be delegated to the ESOs. In order to ensure respect for human-centric AI through respect for human dignity in the development of technical standards, the revised New Approach/NLF needs to introduce **a general clause** which serves as a fall-back mechanism in terms of respect for human-centric control over AI. The EU Directive on Biodiversity may, together with *Brüstle* judgment,⁵²⁹ serve as a source of inspiration.⁵³⁰

11. EU Digital Policy Legislation calls for realisation of a **more balanced approach**, an approach which was already discussed during the legislative process of Regulation 1025/2012, now called for in the Resolution of the European Parliament on the Standardisation Strategy.⁵³¹ A more balanced approach enables remedying a long-standing deficiency in the existing co-regulatory mechanism. The more balanced approach should be implemented with regard to all harmonised standards as well as socio-technical standards notwithstanding the policy objective behind – health and safety, environmental protection, or fundamental rights in the digital environment. It thereby allows compensating for long-standing **institutional deficits in the governance structure**, levelling up the role and importance of stakeholder organisations and bringing the existing body of law into line with their societal relevance.

12. Article 10 (5) Regulation 1025/2012 leaves it to the European Commission, together with the ESOs, to assess compliance of documents drafted by the European standardisation organisations with its initial request. In *James Elliott*, the CJEU held that harmonised European standards have to be regarded as ‘law,’ which in turn led the European Commission to re-organise the compliance procedure through the involvement of Harmonised Standards (HAS) Consultants who operate under their responsibility, and through adoption of an implementing decision to publish the essentials of harmonised European standards in the Official Journal under the ‘L’ series, as part of EU law. The European Commission bears the ultimate responsibility for compliance with EU law and, even more so, with regard to fundamental rights. This responsibility cannot be delegated to the ESOs, which are ill equipped to deal with hard normative questions.

13. The **ultimate responsibility** of the European Commission for guaranteeing compliance of a harmonised standard with EU law does not eliminate the voluntary character of EU harmonised standards. As a result, the professional user or provider of AI – the equivalent to the manufacturer in the industrial economy – may still remain liable under the Product Liability Directive, even if they comply with the harmonised European standard if it turns out that harmonised European standards did not meet the legitimate expectations of all those entitled to launch a product liability claim.

14. The **potential effects of qualifying harmonised European standards as ‘law’ are not fully exhausted** with a revision of responsibilities of the European Commission and AI users/providers. They affect the potential rights of consumer organisations as well as the role of the HAS Consultants. Under Directive 1828/2020, qualified entities such as consumer agencies and/or consumer organisations are entitled to take representative actions against practices which potentially infringe consumer rights. Annex I enumerates all legislative acts which aim at

⁵²⁹ CJEU Case C-34/10 *Brüstle* ECLI:EU:C:2011:138

⁵³⁰ See explanatory memorandum AIA p. 2.

⁵³¹ 9.5.2023 https://www.europarl.europa.eu/doceo/document/TA-9-2023-0136_EN.pdf

protecting the collective interests of consumers. Harmonised European standards published in the Official Journal under the 'L' series have to be put on an equal footing with EU legislative acts against which qualified entities may take legal action, if they are meant to protect the collective interests of consumers. This means that **published harmonised European standards aiming at protection of collective interests have to be added to Annex I of the Directive**. Whether or not a particular harmonised European standard meets these requirements has to be decided together with the implementing decision on whether the European harmonised standard complies with EU law.

15. Restructuring of responsibilities in Article 10 (5) in light of *James Elliott* implies a need to **reconsider the role and function of the HAS Consultants**. Additional measures are needed to ensure that mandated harmonised standards comply not only with technical requirements but also with legal requirements, in particular the consumer acquis and fundamental rights. Such a compliance test cannot and should not be exercised by the HAS Consultants. These should be replaced by a regulatory scrutiny board, which may be inspired by the better regulation approach. The **regulatory scrutiny board** should bring together not only technical and legal expertise but also societal expertise, from both the current stakeholder organisations in Annex III and from civil society organisations which bring to bear the necessary independent technical expertise, independent of their representativeness in the Member States. The opinions of the regulatory scrutiny board should be made public.

16. The **role and function of stakeholder organisations** throughout the institutional structure that governs elaboration of harmonised technical standards **needs to be redesigned**. Foreseeable use, or even foreseeable misuse, is the formula which enshrines the concerns of society resulting from risks to health and safety, to the standardisation of products, and which found its way into product safety regulation that underpins the New Approach/NLF in the industrial economy. Stakeholder organisations under Annex III are supposed to supply the necessary input so as to guarantee an adequate level of health and safety protection in the elaboration of harmonised European standards. **The concept of foreseeable use**, or even foreseeable misuse, cannot be transferred to the digital economy, though. It needs to be adapted.

17. There is common agreement between technical experts, independent of their origin and their belongingness to the digital economy or digital society, that **foreseeability in the digital economy is limited**, not only due to the speed of technological development, but also and in particular due to the gap between the development of a particular AI standard and its potential effects on society. The potential impact of AI systems on fundamental rights materialises in concrete circumstances only. It suffices to think of ChatGPT, which is about to make its way from general purpose AI to commercial use. The potential risks and impact depend on the commercial sector in which ChatGPT is applied. The Guidelines of the High Level Expert Group⁵³² highlight à in full compliance with world-wide efforts to give shape to ethical AI – the necessity to **complement normative ethics with applied ethics**. The instrumentalisation of the New Approach/NLF has not come to an end with elaboration of AI standards which set its potential use aside. If it were otherwise, society would turn into guinea pigs and local users of the AI systems would have to bear the risk that they may be held liable for an infringement of

⁵³² HLEG, Ethics Guidelines for Trustworthy AI, 2019. [file:///C:/Users/Mi-PC-SFF/Downloads/ai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419%20\(1\).pdf](file:///C:/Users/Mi-PC-SFF/Downloads/ai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419%20(1).pdf)

fundamental rights, even though the AI system complies with the harmonised EU standard and even though it is self- or third-party certified.

18. The urgent necessity to integrate the potential future application of an AI harmonised standard into its design highlights the need to grant civil society – in the language of Regulation 1025/2012, the stakeholder organisations – a much more prominent role. So far, these stakeholder organisations are an add-on which lend the standardisation process a certain degree of legitimacy whenever the standards concerned enter the area of public interests. Stakeholder organisations have to become full co-operating partners in the standardisation process, not only in the digital economy but also in the industrial economy, and not only in terms of fundamental rights, but also when product safety and environmental concerns are involved. **The bilateral relation between the European Commission and the ESOs has to be turned into a fully-fledged trilateral relation**, one where the stakeholder organisations enjoy secure status and a say which cannot be simply outvoted in practice. That is why they have to be **named in Annex I**. What is needed is a new spirit of tripartite co-operation in mutual trust.

19. **Annex III** Regulation 1025/2012 distinguishes between consumer, environmental, and labour organisations and ties their participation to particular requirements based on the idea of independence from industry and representativeness to be able to speak on behalf of European consumers, workers, and citizens as a whole. These requirements should be left unchanged so as to provide **leeway for future development of non-governmental organisations**.

20. The **scope of stakeholder organisations at the European level should be broadened** so as to enable participation by non-governmental organisations which specialise in building independent knowledge and which represent societal interests, but which are not represented in at least two-thirds of the Member States. Representativeness of technical expertise, both in the industrial and in the digital economy, should be made a necessary requirement for the status of a stakeholder organisation. Representativeness matters when it comes to the political dimension of assessing safety, environmental protection, and the impact of AI on society. However, representativeness spread over the Member States does not matter in terms of the pure technical dimension of old and new technologies. Here all that counts is independent knowledge and expertise, which is of particular relevance in the field of AI. **Therefore technical expertise should not bound to a particular Member State or to the degree to which the knowledge is spread** over the majority or even two-thirds of the Member States. The representative stakeholder organisations under the current Annex III and the newly introduced non-representative stakeholder organisations should complement each other in their input to elaboration of harmonised European standards. They are both eligible for funding but their potential participation is not dependent on being funded.

21. The status of the stakeholder organisations in elaborating harmonised European standards needs be upgraded with regard to **their involvement in the formal decision-making procedure of the European Commission, and with regard to their role at each stage in elaboration of technical standards**. They should be involved in the mandating process, the compliance procedure and, together with the ESOs, they should also have the right to initiate the objection procedure. The mirror image to their enhanced role in formal decision-making should be their enhanced role in elaborating technical standards. They need to have the following rights to be anchored in Regulation 1025/2012, the right to take over the chair of a particular ESO working group, voting rights, and a right to veto which could not be outvoted in the decision-making procedure of the ESOs. In the case of conflict between the ESOs and

the stakeholder organisations, a dispute settlement procedure must be in place which meets minimum requirements of independence and procedural fairness, similar to Article 21 (3) DSA.

22. Elaboration of technical standards which interfere in ever more policy areas not only requires a very different role for the stakeholder organisations at the European level. In order to increase input from civil society, input from consumer organisations into the standard-making process should **also be considerably strengthened at the national level. So far, national standardisation bodies**, whether public or private, differ considerably in the degree to which stakeholder organisations are integrated into the governance structure, let alone the procedural rights they enjoy in concrete working activities. What is true for the Annex III organisations in Regulation 1025/2012 also applies broadly to the national standardisation bodies. These bodies should grant stakeholder organisations status in the governance structure and equip them with appropriate rights, thereby looking for new ways of experimental financing.

23. Development of technical standards in product safety, environmental protection and AI has led to development of a new category of technical standards which do not fit into the established categories of the ESOs. This new type of standards, **'socio-technical standards', stand in between binding legal requirements and harmonised European standards.** Harmonised European standards define concrete technical requirements and justify the presumption of conformity in case of compliance. Socio-technical standards have gained particular ground in AI and they dominate current efforts to give shape to human-centric, secure, trustworthy, and ethical AI. These socio-technical standards are useful in that they explain and concretise the different parameters of trustworthy and ethical AI. The existing socio-technical standards elaborated by ISO/IEC and IEEE suffer from a notable gap in that they focus too much on the normative dimension – but somewhat neglect the applied dimension – of human-centric, secure, trustworthy, and ethical AI. This means that socio-technical standards can only unfold their potential as guidance for interpretation if they include standardisation of use cases. Such an extension would allow systemisation of potential fields of application and allocate particular risks to the potential fields. An obvious example would be elaboration of use cases in the field of financial services and health-related AI.

24. The limited foreseeability of the potential risks of AI applications to the economy and society which might jeopardise establishment of human-centric, secure, trustworthy, and ethical AI requires the introduction of **minimum testing requirements** in order to enable the local AI provider to monitor and survey potential fundamental rights infringements. Here is the place for **a fundamental rights impact assessment.** These risks cannot be defined and standardised at a rather abstract level. The fundamental rights impact assessment needs to be exercised in concreto when it comes to application of a particular AI by a local provider. However, the local provider might be more often than not a start-up, an SME which lacks the resources and the skills to develop a design for a fundamental rights impact assessment and to organise its proper execution. The fundamental rights impact assessment can only contribute to establishing human-centric, secure, trustworthy, and ethical AI **if local AI providers receive the necessary support through development of certifiable minimum testing requirements.** These should be understood as a toolbox to test biases, discrimination, and fairness. AI providers are not the only potential beneficiaries of such minimum testing standards. Enforcement authorities, whether public or private as well as courts, might also belong to potential addressees.

25. Use cases and on minimum testing standards should be elaborated in the triangular relationship between the European Commission, the ESOs, and the enlarged group of stakeholder

organisations. Establishing human-centric, secure, trustworthy, and ethical AI requires **opening the consultation procedure on socio-technical standards to the public at large, in the EU and beyond**. Such open consultation is not without precedent. For example, elaboration of ISO standards 26000 on Social Responsibility was accompanied by a broad consultation process. The standard is freely accessible, but not freely available.⁵³³ Such an opening-up forms a first building-block in offering the opportunity to establish human-centric, secure, trustworthy, and ethical AI.⁵³⁴ **Open-ended consultation and free accessibility is a major prerequisite for building trust**. Trust cannot be built if these socio-technical standards remain confidential or accessible only to those who participated in their elaboration or who paid for accessing them.

26. Socio-technical standards serve as a necessary bridge between technical, legal, and societal expertise. They lay down the ground rules on which concrete technical standards can be elaborated, which in case of compliance justifies a presumption of conformity with binding EU law. **Compliance with broad interpretative socio-technical standards does not suffice to insinuate compliance with binding legal requirements, let alone with the Charter of Fundamental Rights**. This is particularly true with regard to standardisation of use cases. Socio-technical standards, such as those elaborated by ISO/IEC and IEEE, cannot be translated into harmonised European standards without major changes which result from the need to ensure compliance with EU law in general, and fundamental rights in particular. However, with regard to minimum testing standards, the situation is different. These should be designed to be certifiable. That is why they should be developed as harmonised European standards.

27. CEN-CENELEC are dependent on income resulting from **copyright**. Socio-technical standards – for instance, the standard on use cases as well as the harmonised standard on minimum testing standards – are of utmost importance in order to ensure that AI serves society and that AI is accepted in society. For these reasons, they must be freely accessible in full. The decision whether the EU pays for the mandated standard or whether the EU pays for free accessibility could be left to the European Commission and the ESOs. **The AI standard on use cases and AI minimum testing standards should be published in the Official Journal under the ‘L’ series. With regard to all other harmonised standards, a differentiation is needed**. It seems unrealistic to assume, not least due to the costs of paying for free accessibility, that all harmonised standards must be publicly available. The three partners, the European Commission, the ESOs and the stakeholder organisations, should agree on those where free access is indispensable.

28. The increased importance of stakeholder participation for development of trustworthy and ethical AI standards calls for a **revision of the agreements which CEN/CENELEC have concluded with ISO/IEC**. CEN/CENELEC should use their position within Europe to exercise their influence to integrate stakeholder participation into ISO/IEC standards in an appropriate way, so as to increase the acceptability of technical standardisation which touches upon the various policy fields in both the industrial and the digital economy, alternatively it would be for the Committee on Standards to decide in approving a standardisation request whether the standard should be developed at European level or passed to the international level.

⁵³³ <https://iso26000sgn.org/iso-26000/free-iso26000-downloads/>

⁵³⁴ AI and standards, IEC, ISO, and ITU respond to FLI open letter: International Standards can help ensure safe and responsible AI development, <https://www.worldstandardscooperation.org/ai-and-standards/>

32. Regulation 1025/2012 on European Standardisation has to **be renamed as the European Standardisation Governance Act**. Such a renaming indicates the policy shift and the new spirit which will govern elaboration of harmonised European standards

2. Text of the Proposed Amendment

Recital 23 will be deleted

Article 1 Subject Matter will be amended:

(1) This Regulation establishes rules with regard to the cooperation between European standardisation organisations, national standardisation organisations, *stakeholder organisations*, Member States and the European Commission. They shall co-operate in mutual trust and respect on a level playing field.

(2) This Regulation, wherever applicable, aims at establishing a high level of product safety and a human-centric, secure, trustworthy, and ethical AI in compliance with EU law and with the European Charter of Fundamental Rights.

(3) The rules on the participation of stakeholder organisations apply only to harmonised European standards and Socio-Technical Standards. They do not affect the elaboration of non-harmonised European standards.

Article 2 Definitions

(6 new) socio-technical standards combine technicity with policy objectives, such as product safety, environmental protection and Artificial Intelligence, and bridge the gap between binding legal requirements and technical standards. Socio-technical standards are not certifiable.

(7 new) ‘use cases’ means socio-technical standards which aim at the standardisation of potential uses of AI systems in the economy and society,

(8 new) ‘minimum testing requirements’ means technical standards which enable the local user of an AI system to test compliance with fundamental rights prior to entering the internal market,

(9 new) ‘local user of an AI system’ means a company, a regulatory body’ or a court which intends to set up an AI system which directly affects the public at large.

Letters 6–10 become 9–13

Article 2 a) Harmonised European Standards and Fundamental Rights

1. Harmonised European standards and socio-technical standards have to comply with the Charter of Fundamental Rights.

2. Harmonised European standards and socio-technical standards have to respect the state of the art in science and technology.

3. Binding legal requirements for AI systems shall be considered non standardisable where placing them on the market or putting them into service would be contrary to fundamental rights, in particular to human dignity; and placing them on the market or putting them into service shall not be deemed NOT to be so contrary merely because it is permitted by law or regulation

Article 4 (a) Free Accessibility

(1) Socio-technical standards on use cases, and socio-technical standards laying down minimum testing requirements for local users of AI systems shall be discussed not only with the stakeholder organisations but also with the public at large, and their agreed texts shall always be published in full in the Official Journal, as opposed to simple citation of the references of harmonised standards.

(2) Socio-technical standards shall be freely accessible. It is for the European Commission and the European Standardisation Organisations to decide whether the European Commission pays for the mandated standards or whether the European Commission covers the costs for free accessibility.

(2) All other harmonised European standards shall also in principle be freely accessible. However, the European Commission, the ESOs, and the enlarged group of stakeholder organisations shall agree on those harmonised standards for which free accessibility is indispensable in order to ensure the safety of products, a sustainable environment, and to build a human-centric, secure, trustworthy, and ethical AI.

Article 5 Stakeholder Participation in European and National Standardisation

The title needs to be amended so as to indicate that National Standardisation Bodies are also included.

Article 5 (1) Sentence 2 shall be replaced:

They shall in particular encourage and facilitate such representation and participation through European stakeholder organisations, in particular but not only those receiving Union financing in accordance with this Regulation, at the policy development level and at all stages in the development and approval of European standards or European standardisation deliverables through appropriate procedural rights. They shall be entitled

Article 5 (1) (a) to (e) shall be replaced through (a) to (k).

- (a) to propose and accept new working items
- (b) to unimpeded and free access to standardisation activities
- (c) to free access to draft standards
- (d) to take over the chair of a technical committee and a working group
- (e) to discuss and comment on proposals at their choice

- (f) to submit drafts and comments, to which the ESOs are obliged to reply
- (g) to vote on drafts
- (h) to veto all drafts which come under the statute of the respective stakeholder, in particular with regard to socio-technical standards and minimum testing requirements
- (i) to call for dispute settlement in the case of disagreement between ESOs and stakeholders
- (j) to ask for revision of existing European standards or European standardisation deliverables
- (k) to disseminate and to build awareness of adopted European standards and European standardisation deliverables.

A new para (2) shall be inserted and the former para (2) will become para (3).

(2) National standardisation bodies shall establish stakeholder organisations which need to enjoy independence whether internally or externally. National standardisation bodies should create consumer councils or provide funding for national consumer experts to participate at the national level either unilaterally or in partnership with the public authorities in charge. These consumer councils should have similar rights as those set out in Article 5 (1) (a) to (h).

Article 10 Standardisation Requests to European Standardisation Organisations

Para (1), (5) and (6) shall be replaced.

(para 1) revised sentence 1: The European Commission may within the limitations of the competences laid down in the Treaties *and concretised in Articles 2 a*), request one or several European standardisation organisations to draft a European standard or European standardisation deliverable within a set deadline.

(para1) new sentence 2. The European Commission may request one or several stakeholder organisations, in particular to draft socio-technical standards such as use cases and/or on AI minimum testing requirements in the meaning of Article 2 6) and 7) new.

(para 1) sentence 2 old shall be replaced through sentence 3 new:

European standards and European standardisation deliverables shall strive for a fair balance between economic efficiency, effectiveness, and public interests, in particular the consumer and environmental acquis, the European Charter of Fundamental Rights, and the policy objectives stated in the Commission's request and based on consensus.

(para 5) amendment of sentence 2 old:

The European Commission together with the European Standardisation Organisations and the stakeholder organisations shall investigate compliance of documents drafted by the European Standardisation Organisations with its initial request. They shall be supported by a standardisation scrutiny board composed of technical and legal experts. The final responsibility for

compliance with European Union law and the European Charter of Fundamental Rights lies with the European Commission.

(para 6) Where a harmonised standard satisfies the requirements which it aims to cover and which are set out in the corresponding Union harmonisation legislation, the European Commission *shall take an implementing decision* to publish a reference of such harmonised standard without delay in the Official Journal of the European Commission (the last part of the sentence will be deleted). *The texts of socio-technical standards, in particular those on use cases and on minimum testing requirements, are to be fully and freely accessible.*

Art. 11 Formal Objections to Harmonised Standards

Para (1) will be amended as follows:

When a Member State, the European Parliament, *the European Standardisation Organisations, or the stakeholder organisations* consider that a harmonised standard does not entirely satisfy the Requirements which it aims to cover...

Art. 12 Notification of Stakeholder Organisations

Art. 12 c) shall be deleted.

Art. 16 Financing of other European Organisations by the Union

(lit c) should be amended as follows:

The *elaboration* and participation in the technical work with respect to development and revision of European standards and European standardisation deliverables, which is necessary and suitable for the support of Union legislation and policies, *in particular with regard to socio-technical standards on use cases and on minimum testing requirements.*

At the bottom a new para should be introduced.

The European Commission shall ensure an adequate level of funding so that stakeholder organisations can effectively fulfil their role and function as co-operating partners in elaboration of harmonised technical standards. The European Commission and the European Standardisation Organisations shall encourage national standardisation bodies to look for innovative financing mechanisms, including mechanisms whereby industries contribute to the financing of civil society participation without exercising influence on the statutes and the work programme of these civil society organisations.

Article 24 Report on AI Standards

The European Commission shall report on a biannual basis on development of AI standards, and on how and by what means the elaborated standards implement fundamental rights.

Annex I European Standardisation Organisations and European Stakeholder Organisations

The title needs to be amended so as to make sure that European Stakeholder Organisations enjoy the same standing as the ESOs.

Under 4. Shall be inserted

4. ANEC – The European Voice in Standardisation

Annex III European Stakeholder Organisations eligible for Union Financing

Will be complemented

(5) An organisation representing societal interests in building a European society which

(a) is non-governmental, non-profit-making, and independent of industry, commercial, and business or other conflicting interests

(b) has as its statutory objectives and activities representation of societal interests in the development and use of technology

(c) provides for independent technological expertise which is representative for European Society

Amendment of Annex I Directive 1828/2020 on Representative Action

Socio-technical standards and harmonised European standards which are freely accessible should be added to the list in Annex I together with their publication in the Official Journal.



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