Human Rights and ICT Standardisation: examples across diverse SDOs, current challenges and recommendations

Authors: *Shakira Bedoya, Gabriela Garnham, Christian Grafenauer, Veronique Lerch, Maria Grazia Porcedda, Monica Martinez Vargas and Charles Kiser Webb*

Editors and Contributors: *Maria Giuffrida, Silvana Muscella*

Acknowledgements

HSbooster.eu* and StandICT.eu** greatly acknowledge the dedicated work of the authors outlined below who have contributed to this document, released as an output of the workshop **"Human Rights and ICT Standardisation"** organised with the European Commission on 6th June 2024 .

This publication was prepared under the overall engagement and authorship of Shakira Bedoya, Gabriela Garnham, Christian Grafenauer, Veronique Lerch, Maria Grazia Porcedda, Monica Martinez Vargas and Charles Kiser Web. The authors are either standardisation or human rights experts, all part of the HSbooster.eu pool of consultants. Shakira Bedoya and Christian Grafenauer are additionally StandICT.eu and SEEBLOCKS.eu fellows.

We thank Lars Lünenburger for reviewing the final draft of this document.

We also extend our grateful appreciation to the European Commission DG CONNECT officers Emilio Davila Gonzalez, Carlos Lopez Rodriguez and Paul Killeen as well as extending our thanks to the other workshop speakers Jochen Friedrich, Olivier Alais, Arnaud Taddei, Viveka Bonde and all the participants who interacted with the speakers and moderators, exchanged views, shared ideas.

*HSbooster.eu has received funding from the EU's Horizon Europe research and innovation programme under Grant Agreement no. 101058391.

**StandICT.eu 2026 has received funding from the EU's Horizon Europe research and innovation programme under Grant Agreement no. 101091933.

Disclaimer

The views and opinions expressed in this publication are those of the authors alone and do not necessarily reflect the official policy or position of their employers, of HSbooster.eu, StandICT.eu projects, the European Commission or any of the organisations involved in the workshop. This document is intended for informational purposes only and is not meant to be an endorsement of any specific standards, technologies, or practices. While every effort has been made to ensure the accuracy of the information presented, the entities involved in the preparation of this publication cannot be held responsible for any errors or omissions or for any consequences from the use of the information contained herein.

Glossary of terms

Abbreviation / Term	Description
AHG	Ad-Hoc Group
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
DLT	Distributed Ledger Technologies
EC	European Commission
EEA	European Economic Area
EHRs	Electronic Health Records
ENISA	The European Union Agency for Cybersecurity
ESG	Environmental, Social and Governance
ETS	Emission Trading System
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GHG	Greenhouse Gases
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISO	International Organization for Standardisation
ITU	International Telecommunication Union
JTC	Joint Technical Committee
MDR	Medical Device Regulation
NLF	New Legislative Framework
OHCHR	Office of the High Commissioner for Human Rights
PET	Privacy Enhancing Technology
QARA	Quality, Regulatory, and Assurance
RRI	Responsible Research and Innovation
SBP	Strategic Business Plan
SDOs	Standards Development Organisations
WG	Working Group

Table of Content

Executive summary

The purpose of this report is to provide a summary of the key findings, takeaways and recommendations from the workshop **"Human Rights and ICT standardisation"** that took place online on the 6th June 2024. The workshop was organised by the **StandICT.eu2026** and **HSBooster.eu** EU funded projects.

The event brought together key experts working on human rights and standards to discuss the issue of how to ensure human rights are considered and dealt with when addressing technical specifications in ICT standardisation.

This report and supportive guide have been prepared to give an overview of existing examples of successful cases in which human rights were considered for the design, implementation or modification of ICT standards across different fields, SDOs and countries. The report also discusses still existing issues and challenges and provides recommendations for future actions, especially with reference to Research and Innovation projects working in the field and aiming to contribute to the advancement of this topic.

Key Takeaways

Based on the discussions held during the workshop and the research conducted to produce this report, a selection of key takeaways regarding ICT standardisation and human rights is presented below. Please note that this is not an exhaustive list; additional insights and findings can be found within the full report:

- **Strengthened International Cooperation**
  International cooperation is vital for developing common standards that promote privacy, security, and ethical technology use globally. The collaborative efforts among various international bodies are important to create comprehensive standards that protect human rights within the ICT landscape. This is especially crucial in areas such as cybersecurity, where enhancing security measures must be balanced with protecting individual rights.
- **Ongoing collaboration and continued dialogue**
  The integration of human rights into ICT standardisation requires a continuous and collaborative approach involving all stakeholders, including governments, private sector companies, international organisations, academic institutions, and civil society. This ongoing dialogue promotes innovation and facilitates the possibility that human rights considerations are embedded at every stage of the standardisation process.
- **Importance of ethical leadership**
  Ethical leadership is key in driving responsible ICT development. Leaders in both the public and private sectors must promote ethical behaviour, establish clear values, and ensure accountability within their organisations. Ethical leadership is crucial for fostering a culture where human rights are respected and prioritised in technological advancements.
- **Consumer-centric standards**
  There is a need for more **consumer-centric standards in ICT.** Technical standards must consider the impact on end-users, particularly vulnerable groups like children and the elderly. By integrating consumer concerns such as privacy, safety, and trustworthiness into the standardisation process, ICT can better serve and protect users, ensuring that technology advances in a way that is beneficial and safe for all members of society.

1.Introduction

In the modern digital age, Information and Communication Technology (ICT) is integral to societal progress, economic development, and the functionality of everyday life. The rapid pace of technological advancements presents both opportunities and challenges, particularly concerning human rights. As technologies become increasingly embedded in our lives, it is essential to ensure that their development, implementation, usage and maintenance align with human rights principles.

Establishing robust policies is the first critical step towards achieving this balance. Policies that ensure technology serves humanity, respects privacy, and upholds ethical standards are essential. Such policies must be designed to promote technological advancements while safeguarding human rights, reflecting a committed effort to embed these considerations into ICT standardisation. This approach supports innovation while also placing human rights at the core of technological development.

International cooperation plays a crucial role in developing standards that safeguard human rights globally. The collaborative efforts among various international bodies aim to create harmonised standards that promote privacy, security, and ethical use of technology. Without such cooperation, developing comprehensive standards that adequately protect human rights in the global ICT landscape would be challenging, especially in key ICT areas like cybersecurity where the balance between enhancing cybersecurity measures and protecting individual rights is particularly delicate as cybersecurity efforts often involve surveillance and data collection practices that can infringe on privacy and freedom of expression.

Integrating human rights into ICT standardisation is not a one-time effort but should be considered a continuous effort aimed at embedding human rights considerations into every stage of the standardisation process. This requires an ongoing dialogue and collaboration among all stakeholders. Governments, private sector companies, international organisations, universities and academic institutions as well as civil society must work together to develop and implement standards that are both technologically sound and human rights-centric. This collective effort promotes that as technology advances, it does so in a manner that is inclusive, ethical, and respectful of the rights and dignity of all individuals.

The European Commission, specifically through DG CONNECT, is leading efforts to create a framework that integrates human rights considerations into ICT standardisation. Among these efforts, an online workshop was organised on the 6th June 2024 facilitated by the European-funded projects **StandICT.eu 2026** and **HSbooster.eu** to provide preliminary reflections and the opportunity for discussions around these themes.

This report summarises the evidence discussed during the event. More precisely, while this introduction has highlighted some of the key messages stemming from introductory overviews on high-level aspects, chapter two dives deeper into the topics discussed in a panel discussion by key stakeholders from various sectors, who are also the main authors, each of a specific section of this report containing also dedicated recommendations whenever possible.

By linking various topics, the report offers, in chapter 2, a comprehensive view of how human rights considerations can be integrated into ICT standards across different domains and regions. Some sub-chapters provide a broad overview, while others focus on specific types of human rights, and some extend beyond Europe to include perspectives from Latin America. This structure ensures a diverse and well-rounded discussion on the subject.

Chapter 3 concludes with a set of more comprehensive and general combined recommendations, directed to specific stakeholder categories including research projects, standardisation experts and policy makers.

Based on their interests and needs, readers can either consult the individual sub-chapters or the entire report.

2. Human Rights Considerations in ICT standardisation

2.1. Rights and Technical Standards in EU Law (authored by Dr Maria Grazia Porcedda[1])

Human rights and technical standards have historically travelled on separate tracks

Historically, international technical standardisation precedes and is a separate process from the international recognition of human rights as we understand them today. [1] Technical standards and human rights have historically travelled on separate tracks. International standards are governed by private international/global administrative law; [2] they are drafted by permanent Standards Development Organisations (SDOs) and are usually not legally binding, but if they are widely adopted can have significant legal weight. Rights are governed by public international and specifically human rights law; they are drafted by *ad hoc* conventions and are meant to be legally binding, but their enforcement requires significant investment of public resources and personnel, legislation and a court system to uphold them.

The same is true for the European Union: standards and rights travel on separate tracks. Product and technical standardisation was embraced quite early in the history of the EU as a mechanism to build the Common/Single Market and the freedoms attached to it. The new approach, now called new legislative framework (NLF), created a procedure to draw up harmonised standards against which the conformity of products could be assessed. [4]
Due to political choices, the predecessors of the European Union had no explicit mandate (conferred powers) in the sphere of human rights, a task that was left to a separate intergovernmental organisation, the Council of Europe, until the early 2000s. Thanks to the Charter and the Lisbon Treaty, the EU has defined powers in the sphere of fundamental rights [5] (leading to, e.g, the GDPR implementing the fundamental right to data protection [6]).

Digital technologies are however forcing the separate tracks of technical standards and human rights to meet. Digital technologies affect the fundamental right to privacy, to data protection and with it many connected rights, such as freedom of information. Standardisation is closely related to the design of technology and therefore the practical safeguard or violation of rights.

[1] Writing in a private capacity.

Legislation within the EU Digital Single Market shows an appreciation of both standardisation processes and rights, but does not yet possess the mechanisms to connect the two organically. Let us take data protection and cybersecurity as examples.

In the GDPR there are mentions of technical standards and related technical developments, but otherwise there are no mechanisms to enforce its 'by design' aspirations. [7] A privacy and data protection by design standard drawn up by CEN/CENELEC in 2022 upon request by the European Commission does not have the same legal force as harmonised standards do. [8] Cybersecurity legislation, such as the NIS Directives and the Cybersecurity Act, [9] focus heavily on technical standardisation but do not enforce rights. The first cybersecurity certification scheme adopted on the basis of the Cybersecurity Act, Common Criteria for Information Technology Security Evaluation, [10] is based on ISO standard ISO/IEC 15408, which was not drawn up with rights in mind.

Cybersecurity standards miss the fundamental rights dimension, while data protection standards lack 'teeth', which reflects the broader issue of the disconnect between legislation enforcing rights based on principles and technology development (see below). The upcoming Cyber Resilience Act [11] is part of the New Legislative Framework and the adoption of related standards will offer an opportunity to consider the rights dimension, but before we can do so we need to appreciate some crucial differences.

Any integration between technical standards and human rights must acknowledge their differences

Standards and rights differ not only as to the mechanism of their adoption, but also in terms of form, level of prescriptiveness and jurisdiction. These differences must be taken into account as part of any attempts to connect the tracks of human rights and technical standards.

Standards are longer than a couple of lines, but are often non-prescriptive, leaving it to designers and developers to adjust them to their processes. [12] There are often multiple international standards for any given process, with the market determining the winner.
Rights are often defined in one or a handful of lines, and even when there is a law to give them authority, like the GDPR with data protection, much of the text is open to interpretation, which is for courts to give. In the EU, national and EU courts (and to an extent the European Court of Human Rights) feed into the interpretation of fundamental rights. As a result, the meaning of rights is not carved in stone, which results from the desire to adjust such meaning to evolving societal norms.

Unlike technical standards, rights are a close expression of the values and culture of a given society and are therefore jurisdiction-specific. If we wanted to connect rights and standards internationally, we could only find agreement on a diluted notion of rights, due to scant United Nations Human Rights Committee material and significant international disagreement on digital rights. As a result, technical standards would only reflect a minimum threshold of protection of rights, which begs the question of the utility of such an exercise. A threshold of protection above the bare minimum could only be achieved within a single jurisdiction.

The challenge rests in reconciling processes that were born for different purposes and follow different logics. In particular, technical standardisation cannot interpret rights, but rather needs to account for the latest interpretation of rights, which is for the judiciary to determine.

Rights, standardisation and tech development cohabit in a 'stair-less' house: let's build the staircase!

Any attempt to connect standards and rights must first consider their existing relationship and the ecosystem they create together with tech development, which is the ultimate goal of (rights-infused) standards. As highlighted previously, EU law lacks the mechanisms to meaningfully connect the three: a useful analogy is that of a three-floor house. [13] The top floor is occupied by lofty formulation of rights and laws such as the GDPR, the middle floor by standards and the bottom floor by tech development. Any desire for fundamental rights law to directly communicate with - and direct - standards and technology development is frustrated by the absence of a staircase connecting the floors.

Building the staircase is no mundane job: it requires rethinking the relationship between law, standardisation and tech development. This not only requires the involvement of independent ethical and legal experts in SDOs to come up with common vocabularies, but quite literally to connect the building blocks of engineering and rights. In my own work on cybersecurity, privacy and data protection I have suggested a method to connect design strategies, principles and attributes of rights, which takes inspiration from work by the OHCHR on rights indicators and privacy engineering (Table 1). [14] Irrespective of the method, we need to address how standards and technology development can incorporate the dynamic conception of rights.

Law			**Engineering**		
Rights (EU Charter)	Essence of rights (Courts)	Regulatory principles (e.g. GDPR)	Protection goals (e.g. ENISA, LINDDUN)	Design strategies (e.g. Hoepman)	Information security properties (CEN/CENELEC, ITU, ISO etc)

Table 1 Connection between law and engineering to inform standards (Porcedda, 2023, 2018)

2.2. Climate Change and the AHG3 Fintech in Carbon Markets (authored by Dr. Shakira Bedoya)

Climate change is considered "one of the greatest threats to human rights" [15]. For long it has been recognised "that a clean, healthy and functional environment is integral to the enjoyment of human rights, such as the rights to life, health, food and an adequate standard of living."[16] The following chapter highlights the role of the newly established *AHG3 FinTech in Carbon Markets* under the technical Committee ISO/TC322 (Sustainable Finance) in addressing climate action.

The international organisation for Standardization (ISO) and Climate Action

For some time, ISO has been producing standards addressing core topics in climate action, like climate mitigation, adaptation and resilience. (For example, ISO 14001 on environmental management systems was initially published in 1996). Most recently, to foster its commitment to combat climate change, in September 2021, ISO approved the London Declaration, the document reads *"ISO hereby commits to work with its members, stakeholders and partners to ensure that (…) International Standards and publications accelerate the successful achievement of the Paris Agreement, the UN Sustainable Development Goals and the UN Call for Action on Adaptation and Resilience."* [17]Other efforts include the *Net Zero Guidelines* (IWA 42:2022) and the forthcoming *Net Zero Aligned Organizations* (ISO/AWI 14060).

In February 2024, ISO published a joint statement with the international Accreditation Forum to include a climate change amendment applicable to all type A ISO management system standards "to ensure that Climate Change issues are considered by the organisation in the context of the effectiveness of the management system"[18]. The list included – among others – specific standards on information security and information technology (ISO/IEC 200000-1:2028 and ISO/IEC 19770-1:2017).

AHG3 FinTech in Carbon Markets under the technical Committee TC322 (Sustainable Finance)

The Sustainable finance Committee established in 2018 aims to integrate sustainability considerations including environmental, social and governance (ESG) practices in all aspects of financing economic activities. The work programme covers three sets of standardisation activities: First, harmonisation, second, setting principles and framework standards to guide the operations of financial institutions, and to give a structure for the development and role of specific standards, and third, developing technical standards that contribute to sustainable finance taxonomies, impact assessment and disclosure requirements, verification, and stewardship.[19]

In October last year, The Sustainable Finance committee approved the creation of an *Ad-Hoc Group* (AHG) namely, 'FinTech in Carbon Markets' with specific goals such as [20]:

- Study material relevant to the various aspects of carbon markets involving FinTech, for example the use of blockchain.
- Make recommendations on future standard work
- And review relevant standards from related fields (i.e. the ISO 14 000 family of standards for environmental management, quantification of greenhouse gases and climate mitigation and adaptation.)

Fintech in Carbon Markets: Blockchain

As a result of climate change there is an increased – and in some cases irreversible – change to rainfall patterns, oceans, and winds in all regions of the world. This results in "huge costs for the EU's economy and impact countries' ability to produce food"[21]. By 2050, EU countries will have to drastically reduce their greenhouse gas emissions and find ways of compensating for the remaining and unavoidable emissions to reach a net-zero emissions balance.

A current challenge is that decarbonisation through limiting energy consumption of fossil fuels will cause significant economic disruptions without an established (global) energy infrastructure [22]. Carbon Markets present an opportunity to cut down on carbon emissions while fostering economic growth and technological developments through the trading of carbon credits. A carbon market is an emission trading system (ETS) where carbon is transformed into a commodity in which carbon credits are sold and bought. The establishment of ETS and Carbon Markets has several difficulties related to four areas: effectiveness, accountability, transparency, and operability of these mechanisms. One of the most pressing challenges is the lack of standardisation in carbon calculation standards, lack of transparency in carbon market methodologies and therefore inadequate quality assurance of the ETS.[23]

Carbon markets allow participants to trade, purchase or sell carbon credits for this purpose. A carbon credit is a market-based mechanism that allows to reduce or remove GHG from the atmosphere through 'carbon sequestration'. It aids climate change mitigation by connecting "those who can efficiently create the carbon deficit, with those needing to add a carbon deficit to their organisational balance sheet. They are usually generated through adherence to accepted carbon standards, which are overseen by either voluntary or regulated carbon registries and standards-setting bodies" [24].

Blockchain offers an excellent solution to regulate carbon credits transactions and their allocation, and improve carbon offset projects management. There are two areas where blockchain is especially beneficial: 1) Blockchain can promote the digitalisation of the measuring, reporting, and verification processes during climate mitigation activities. 2) The implementation of blockchain in carbon markets could combine heterogeneous national emission accounting systems in one meta- registry (e.g., "The Climate Warehouse" proposed by the World Bank) [25] A blockchain technology is a back-end database that maintains a distributed ledger (DLT). From a business and legal perspective, a blockchain is considered an "exchange network for moving

transactions, value, assets between peers, without the assistance of intermediaries" that "validates transactions"[26]

What differentiates blockchain from a conventional database is how the data is structured, stored and linked to participants in a particular ecosystem: Blockchain rest on a consensus mechanism that ensures that "1) the network is distributed and not controlled by any single party; 2) the validator nodes are incentivised to behave honestly; and 3) blocks, once verified, can no longer be tampered with or changed"[27]. It allows for the use of 'smart contracts' where metadata (on i.e., carbon credits/climate positive activities) can be fused with tradable units simplifying processes by using digital signatures.

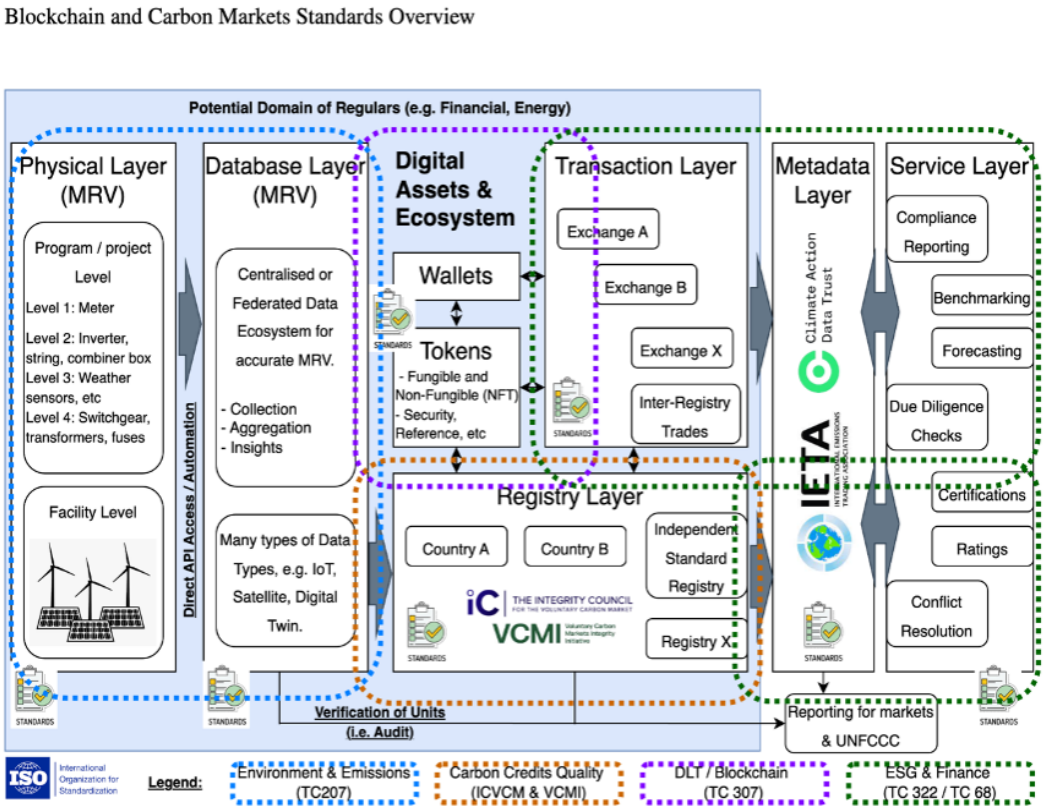

Figure 1End-to-End Ecosystem of DLT Carbon Markets [28]

The establishment of the new *AHG3 FinTech in Carbon Markets* under TC322 (Sustainable Finance) originated from feedback gathered from the group in TC307 (Blockchain), which *"considered many aspects (e.g. carbon knowledge) not suitable to their domain of expertise and therefore it should not be developed there".* The mandate of TC322 AHG3 is to take "ownership of environmental and other financial aspects while TC307 will remain the home of DLT/Blockchain aspects"[29]

As Baiz has discussed, the physical layer is dependent on the emissions of the specific economic sectors and standards of specific importance include: A. Carbon accounting (Co2) GHG Protocol and ISO 1406 x series B. Energy (ISO 5000) B.Other GHG emissions and C. Hardware and Software.[30]

2.3. Holistic strategy to achieve effective fundamental right protection across all consumer relevant standards (authored by Christian Grafenauer)

Current Situation and Developments

As consumer markets become increasingly complex and intertwined with technological advancements, the protection of fundamental rights for consumers has never been more critical. ISO has recently introduced new guidelines aimed at integrating consumer-centric and environmental considerations into the Technical Committees' (TC) Strategic Business Plans (SBP). These guidelines encourage Technical Committees (TCs) to address a broad spectrum of consumer matters, including privacy, safety, and the protection of vulnerable consumers such as children and the elderly, wherever appropriate. This development highlights the significant potential to advocate for the integration of fundamental right protection into every aspect of consumer standards.

Moreover, existing standards such as ISO 10377, which focuses on consumer product safety, have set a precedent for integrating consumer concerns into standardisation processes. On a European level, there has been ongoing work to develop general guidelines for privacy, safety, and trustworthiness that align with European values and levels of protection. These consumer-centric guidelines are a good foundation to build further towards harmonised European horizontal standards. Ensuring they are referenced and properly applied to technical standards is the way to go to protect fundamental rights effectively.

As we look to enhance consumer protection, it becomes increasingly evident that there is a pressing need to develop more standards focused on fundamental right performance metrics. This necessity is particularly pronounced in areas such as privacy and trustworthiness. ISO 10377, which introduces a lifecycle-oriented approach to safety by considering harms and their severity, provides an excellent foundation. However, there is a notable disconnect between this approach and existing risk management standards like ISO 31000. The current state-of-the-art risk management systems often exclude considerations of hazards and hazardous situations, except in the healthcare sector in Europe, which employs ISO 14971. This gap indicates a significant opportunity to align safety considerations with broader risk management frameworks, ensuring that fundamental rights like privacy and trustworthiness are consistently upheld across all sectors.

There is a pronounced lack of experts who specialise in fundamental rights and practical safety within the ICT domains of technical standardisation. While technical experts possess a perceived

awareness of safety and consumer protection, their understanding is often limited to the technical aspects of these terms. This gap in understanding frequently results in resistance when fundamental rights experts and consumer representatives attempt to introduce concepts such as safety, hazards, and the severity of harms into ICT standardisation. Technical experts often deem these aspects as "out of scope," highlighting a critical disconnect. The reality we must confront is that both technical experts and fundamental rights experts may be overwhelmed by the complexities and the differing paradigms of each other's domains. Bridging this gap requires fostering a mutual understanding and collaboration between these experts to ensure comprehensive and effective consumer protection standards.

Proposed Holistic Strategy and Necessary Steps

To capitalise on the current developments and achieve comprehensive fundamental right protection across all consumer-relevant standards, a holistic horizontal approach is essential. This approach necessitates the involvement of dedicated consumer rights experts who can collaborate closely with technical experts at the TC level. The following steps outline the proposed strategy to implement this approach effectively:

1. **Expert Collaboration and Integration:**
    i. **Dedicated Consumer Rights Experts:** Establish a team of consumer rights experts within ISO and CEN/CENELEC who can work in tandem with technical experts to build interdisciplinary expertise. These experts will ensure that consumer needs and rights are integrated during the development and revision of standards. It is obvious that having all stakeholder groups represented in the relevant technical committees is not enough.
    ii. **Cross-functional Teams:** Encourage the formation of cross-functional teams that include consumer rights experts, technical experts, and other stakeholders. This will facilitate the seamless integration of consumer concerns into technical standards.
    iii. **Interdisciplinary approach to standardisation:** The Code of Conduct and willingness of experts allow and welcome the integration of fundamental rights into technical standards. But the main problem today is the lack of a methodology allowing these two fundamentally different fields to harmonise. There needs to be an initiative of interdisciplinary thought leaders creating a prime example of how the integration of fundamental rights with technical standards can be implemented. The work currently done in CEN JTC21 WG2 on “EN AI Risk Management System” is taking impactful steps in that direction.

2. **Guidance and Actionable Recommendations:**
    i. **Strategy and Working Plan:** Civil Society Representatives should actively participate in the development of the strategy and working plans for new technical experts. This plan should provide clear guidance on consumer needs and outline how experts can make actionable suggestions to TC members, leading to the creation of consumer-friendly standards with robust fundamental rights protection. This important strategic aspect is not always covered by civil society stakeholder groups.
    ii. **Training and Resources:** In order to help technical and human rights experts to deepen their understanding in the relevant domains in standards development, there needs to be clear and concrete guidance on consumer as well as technical standards that should be referenced. Most technical experts are not aware which consumer standards are relevant and how they can be included effectively as human rights experts often lack the sufficient technical expertise to interface the two domains with each other in order to achieve a sufficient and effective level of protection of human rights.
3. **Leveraging Existing Standards and Developing New Guidelines:**
    i. **Continuation of Existing Work:** We recommend building on the work done in existing standards, such as ISO 10377. Extend these efforts to develop general guidelines for privacy, safety, and trustworthiness that align with European values and protection levels. These standards are covering the basics in regards to fundamental rights, but need a lot more work to become effective and sufficient. There is also a desperate need for guidelines and methodologies on how to integrate these consumer-centric standards into more technical ones, since they are simply speaking a different language and follow two different approaches, which are not compatible in their current design. **Particular recommendations to focus on:** Harmonise ongoing developments of the risk management standards with the risk relevant definitions used in consumer product standards especially the product safety standard **ISO 10377**. Privacy by design consumer goods and service **ISO 31700**, inclusive service and vulnerable consumers **ISO 22485** and standards defining specific good practices in the software lifecycle standards like **ISO/IEC 12207** should be taken into account.
    ii. **Harmonised European Horizontal Standards:** The Standardisation request in relation to the AI Act, which led to the development of harmonised European horizontal standards have been the silver bullet for consumer representatives to ensure the sufficient level of protection of fundamental rights. We hope to see much more of those standardisation requests, since it allows Legal Tech experts

in standardisation to translate legal requirements directly into technical specifications, just for them to never make into the final standard. Without the argument of harmonisation, consensus is rarely reached and fundamental right considerations are pushed out of scope.

4. **International Adaptation and Participation:**
   i. **Adaptation of Standards:** Propose the adaptation of these guidelines and standards on an international level to maintain high levels of consumer protection globally.
   ii. **Active Consumer Representation:** Most consumer organisations are spread so thin in their resources, that they can barely keep up with the amount and speed that ICT standardisation is progressing right now. Most consumer organisations have to rely on independent funding from foundations, which may or may not be granted. If the hard work of fundraising pays off the resources are often barely enough to participate as active observers and do comprehensive reporting.
   iii. **Active Participation and Contributions:** In order to have an actual impact on behalf of consumers in regards to fundamental right protection consumer organisations need to actively participate in standardisation. This is only possible if the resources are made available to draft contributions, defend their positions consistently and fill strategic positions as editors, conveners and other key positions. Most critical contributions today are made by volunteers, who work on their own time. This leads to a rather low retention of qualified experts in consumer organisations, which reduces effectiveness significantly.
   iv. **Expertise required in "the new era of standardisation":** Particularly ICT standardisation has been operating in its own bubble for the past decades, since the requirements until now were focused on purely technical aspects, like protocols, processes. The new trend we see in standardisation to include fundamental rights requires a wider set of expertise. **Professionals like lawyers, fundamental right experts and interdisciplinary generalists** need to participate in the development of those new kinds of standards to interface these different fields with each other.
   v. **Provide additional financial resources to civil society organisations to enable effective and proactive participation.** Many civil society organisations are struggling to keep up with the flood of new standards being developed. The reality is that many organisations have to restrict themselves to simple reporting and providing comments and feedback - they are forced to be observers. Additional resources would allow **ANNEX III organisations** to actively participate in standardisation by providing contributions to standards and actively drive the inclusion of safety, trustworthiness and sustainability standards as normative

references. This would ultimately increase the level of protection of fundamental rights significantly

5. **Legislative Alignment and Requests:**
   i. **Standardisation Requests:** Continue the strategy of launching Standardisation Requests (SReqs) for European laws such as the General Data Protection Regulation (GDPR) and other legislation related to fundamental and human rights.
   ii. **Alignment with Legislation:** Ensure that new and existing standards align with legislative requirements and uphold the highest levels of consumer protection.
6. **Enforce Transparency, Accountability and availability of established PETs:**
   i. ICT solutions should enhance transparency and accountability in business practices, supporting ethical conduct reporting, whistleblower protection, and stakeholder engagement. Leveraging ICT ensures timely reporting of ethical violations and strengthens commitment to human rights.
   ii. Obligate Companies providing Services and Products in the EEA to offer PGP-encrypted emails. This technology has been an established best practice to encrypt email for over 3 decades now and it is very simple to implement. However many companies refuse to encrypt emails at all exposing large amounts of personal data ignoring the availability of established and easy to implement PETs.
   iii. Record keeping and logging and events and measures that are relevant for legal obligations should be mandatory to be recorded on a tamper-proof logging infrastructure that is transparent and accessible to the authorised stakeholders.

By implementing this holistic strategy, we can ensure that consumer rights are robustly protected across all relevant standards. This approach not only aligns with European values but also sets a precedent for global standards development, ultimately fostering safer, more trustworthy consumer environments.

2.4. Building better tech with a human rights lens - Benefits and challenges of integrating human rights considerations in ICT standards (authored by Veronique Lerch)

Technical standards were not originally designed to cover human rights. There are, however, increasing ethical and human rights implications of technical standards, especially concerning digital services, which positively and negatively impact the enjoyment of human rights. We therefore need to take a human rights-based approach in the development of the standards, taking into account especially the most impacted and most vulnerable members of society. For instance, children make up one third of internet users worldwide and one fifth of users in the EU. Many of the standards relating to digital services will therefore impact them particularly. Children live in a digital world designed by adults, for adults, and driven by commercial interests. The shift towards technical standards integrating a human rights approach is bringing some challenges but also some opportunities, like finding new and additional ways to realise human rights. This shift will certainly be accelerated with the entry into force of the AI act, which mentions technical standards as one way to meet the requirements under the EU AI Act. "The AI Act takes standards into the realm of fundamental rights protection [31]."

The benefits of integrating human rights considerations into technical standards are multiple:

- Standardisation processes can play a role in enabling human rights compliance of new technologies. Integrating human rights into standards helps to work on the implementation of human rights by breaking down the understanding of human rights at the local level, by operationalizing human rights conventions and laws; and by translating human rights principles into actionable standards.
- Human rights are internationally agreed frameworks. Their added value comes from those long negotiation processes to develop and adopt them, which results in standards with a nuanced language and a wide approval by States worldwide.
- Analysing new and emerging technologies from a human rights perspective is crucial to identify and mitigate current and future harms they could cause or exacerbate, and to implement necessary measures to prevent any potential harm to the enjoyment of human rights. Unless standards step up their game to include human rights assessments, they will not be a proper risk assessment tool for companies, which could move away from technical standards.

Still ***various challenges*** to integrating human rights considerations in technical standard setting processes exist

- **Very little mutual awareness between the international human rights community and the standardisation community**. Even though many of the standards have had

direct or indirect, positive or negative, impacts, the international human rights community has had minimal engagement with standardisation processes. Last year, the Office of the High Commissioner for Human Rights published a report on the relationship between human rights and technology-standard setting processes for new and emerging technologies [32]. This report can help to bring together the two communities and marks an increased awareness of the two communities about their work and their cooperation opportunities.

- **Lack of transparency and democratic accountability,** which does not favour wide involvement in the development and implementation of technical standards:
    - There is a lack of transparency and access to standards setting processes, making documentation accessible to the public, addressing the financial and cultural barriers to participation.
    - Standards are typically restricted behind paywalls. However, this may change following the Grand Chamber of the CJEU's decision on March 5, 2024, which recognized a paramount interest in the disclosure of harmonised standards. The ruling emphasised that free access to legal information takes precedence over copyright protection. In the Public.Resource.org case, the Grand Chamber highlighted the principles of transparency and openness that democratic institutions must adhere to under EU law [33].
- **Lack of expertise and capacity of standard-setting organisations on human rights/resistance**
    - Standardisation organisations lack the expertise to address fundamental rights adequately, and attempting to do so may lead to legitimacy challenges due to their industry-led composition.
    - Some studies also mention the resistance that some standard development organisations express towards a more human rights-based approach to the development of standards. “A recent ethnographic analysis of the IETF pointed to a cultural resistance among technical experts to including human rights considerations in standardisation, rooted in shared views of technology as largely apolitical and “non-prescriptive” in nature[34]”.
- More and more standardisation projects are relating to subjects, which do not correspond to conventional technical standardisation. Some of those subjects are in a grey zone and could also be the responsibility of law-makers or other policy makers. Due to this delicate positioning at the nexus of standards and policies, the standard development process in those cases might need to follow different rules than the more conventional technical standards.

Recommendations

For Civil Society Organisations and Human Rights Experts:

- Human rights experts should strengthen their awareness of technology development, internet infrastructure, and how SDOs operate to strengthen their capacity to participate in standard-setting processes.
- Mechanisms for sharing information about ongoing and forthcoming standard-setting processes should be developed.

For Standard Development Organisations:

To ensure that human rights are adequately considered in the standard-setting processes for new and emerging digital technologies, and in the implementation of the standards, it is essential to have:

- **Inclusive and Participatory Processes for the development of standards**: A key factor for the consideration of human rights in the development of ICT standards is the capacity to provide access and facilitate the participation to a broad range of stakeholders, especially those likely to be impacted by those standards.
    - This will require the removal of barriers to participation such as transparent information, prohibitive costs, as well as enhanced support to newcomers to reach the level of expertise needed to participate meaningfully, and creative thinking to institutionalise human rights thinking in technical processes.
- **Capacity-building** should be enhanced to bridge the gap between technical and human rights communities.
    - Technical experts participating in the development of ICT standards impacting human rights should develop a greater understanding of existing human rights standards (for example latest human rights guidance on surveillance technologies).
- **Human Rights Impact Assessments:** Conducting thorough assessments to understand the potential human rights implications of new standards and ensure that technical standards are consistent with established international human rights frameworks and norms.

For the European Commission

- Events organised by the European Commission could offer opportunities for both communities to interact through a combination of training sessions, workshops, and panels.

Conclusions

Advancing the integration of human rights into technical standard-setting processes is crucial for ensuring that standards are both high-quality and supportive of human rights in the digital age. If the challenges associated with integrating human rights in standardisation are taken seriously, there might be a shift in the way the standards development organisations operate. If human rights are neglected in the development of technical standards, the process of standardisation could undermine the human rights frameworks that have been carefully established over the past 75 years. Looking at standards through a human rights lens, we can build better tech that protects human rights, ensuring that technical advancements benefit all.

2.5. Health in the digital era (authored by Gabriela Garnham)

Health as a Fundamental Human Right: Telemedicine and Digital Health, bridging Healthcare Gaps Through Digital Care

Health is a fundamental human right, as recognised by the World Health Organisation (WHO) and enshrined in international human rights instruments. The right to health implies that everyone should have access to the health services they need without suffering financial hardship. In the digital era, telemedicine has emerged as a powerful tool to realise this right, especially for populations that are geographically isolated or lack access to traditional healthcare services. Telemedicine not only improves the quality of care but also enhances the cost-effectiveness of healthcare delivery.

The WHO's Global Strategy[2] defines digital health as a valuable means to support equitable and universal access to quality health services. It aims to enhance the efficiency and sustainability of health systems by delivering quality, affordable, and equitable care. Additionally, digital health strengthens health promotion, disease prevention, diagnosis, management, rehabilitation, and palliative care—both before and after epidemics or pandemics. All of this occurs within a system that respects patient privacy and security.

Digital health encompasses a broad field of knowledge and practice associated with the development and use of digital technologies to improve health outcomes. It extends beyond eHealth to include advanced computing sciences such as "big data," genomics, and artificial intelligence. Digital health also embraces a wider range of smart devices, medical devices, and connected technologies. These include wearables, mobile health apps, and the Internet of Things (IoT), as well as artificial intelligence, big data, and robotics.

Key components of digital health interventions include:

- Electronic Health Records (EHRs): Digital systems for storing and managing patient health information.
- Wearable Devices: Fitness trackers and smartwatches that monitor health metrics.
- Mobile Health Applications (Apps): Designed for health monitoring, symptom tracking, and communication with healthcare providers.
- Medical Devices: Instruments or machines used in the prevention, diagnosis, or treatment of illness. These devices modify the structure or function of the body for health purposes, excluding pharmacological, immunological, or metabolic means.
- Internet of Medical Things (IoMT): Interconnected medical devices and sensors.

[2] https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

As health systems increasingly digitise, adherence to principles of transparency, accessibility, scalability, replicability, interoperability, privacy, security, and confidentiality becomes crucial.

Telemedicine, as part of digital care, plays a pivotal role in healthcare delivery; as a tool for healthcare delivery, leverages Information and Communication Technology (ICT) to provide timely, cost-effective, and high-quality care to individuals regardless of their geographical location. It becomes more widespread, helping alleviate the pressure on overburdened healthcare facilities. And while it doesn't take the place of in-person appointments, it can be an important addition to patient care, by enabling remote healthcare delivery, telemedicine plays a crucial role in disease prevention, health monitoring, and medical service provision—especially evident during the COVID-19 pandemic. Implementing ICT standards on telemedicine impact on the contribution to **global health equity** by making quality healthcare accessible to underserved populations in remote or rural areas. Also ICT standards ensure effective communication between different telemedicine systems (**Interoperability**). This seamless exchange of medical data and information across platforms and devices significantly impacts patient outcomes. Examples of relevant standards include ISO/TR 16056-1:2004 on **Quality of Care, as** adherence to established ICT standards ensures that telemedicine services maintain a high level of quality. Guidelines cover aspects such as data security, patient privacy, and service delivery, ensuring safe and effective care. (ISO 13131:2021). In the case of Chile, for example, the quality of care in Telemedicine is defined by CH norm 5838, which is based on ISO 13131. This will ensures that the care delivered through telemedicine meets a certain level of quality providing guidelines on various aspects such as data security, patient privacy, and service delivery, ensuring that patients receive safe and effective care. The reason ISO 13131 was not homologated was mainly due to translation from English to Spanish. There are concepts that in English mean just one thing but Spanish the same word can mean different things depending on the context. But as the bases are the same, ICT standards help maintain alignment on understanding what is "high quality of care" by ensuring that telemedicine services are reliable, secure, and efficient, regardless of their location, not only in Chile but globally.

ICT can also have an impact on **Legal, Ethical, and Regulatory Compliance, as** many countries have regulations governing telemedicine services. ICT standards provide a framework for addressing legal and ethical considerations. Ensuring patient privacy and data protection helps telemedicine providers comply with these requirements. Standards allow for the replication of telemedicine frameworks, facilitating the scaling of services. Widespread adoption of telemedicine further increases access to healthcare.

However, implementing and maintaining ICT standards in telemedicine can be challenging due to several factors:

- **Technical Aspects**: Poor internet connection and lack of universal access to technology can hinder the effective use of telemedicine. This includes issues with integrating

telemedicine into traditional practice, technology access, and identifying user-friendly platforms.

- **Privacy, Data Confidentiality, and Reimbursement**: Concerns about patient privacy and data confidentiality can complicate the use of telemedicine. There are also challenges with integrating with insurance companies for managing reimbursements.
- **Physical Examination and Diagnostics**: Certain procedures and physical examinations are impossible to perform via telemedicine, which can limit its effectiveness.
- **Training of Healthcare Providers and Patients:** There can be a deficiency in training both healthcare providers and patients on how to use telemedicine effectively.
- **Doctor-Patient Relationship:** The doctor-patient relationship can be affected by telemedicine, and there can be reluctance from both healthcare providers and patients to use telemedicine.
- **Legal and Regulatory Issues:** Noncompliance with regulations such as the Health Insurance

The objective of the ISO 215 committee is to standardise health informatics, aiming to facilitate the capture, interchange, and utilization of health-related data, information, and knowledge to support and enable all aspects of the health system. To date, the committee has published 237 standards, with 63 more currently under development. Adopting these standards as best regulatory practices will benefit patients, healthcare providers, the industry, and public organisations, making processes more efficient and seamless for everyone involved.

Conclusion

Telemedicine has the potential to significantly contribute to the realisation of health as a human right. However, it is crucial to address the existing challenges to optimise its benefits. Policymakers, healthcare providers, and technology developers need to collaborate to improve the accessibility, quality, and efficiency of telemedicine services. It is important to address the challenges to ensure the successful integration of telemedicine into healthcare systems and to maximise its benefits for patient care.

Recommendations:

1. Leverage Digital Health Technologies for Improved Healthcare Delivery: Digital health technologies, including e-Health, m-Health, and telemedicine, can be used to improve healthcare delivery and patient outcomes. These technologies can expand access to quality healthcare, especially for patients with chronic conditions.

2. Ensure Privacy and Confidentiality: Digital health technologies can present threats to privacy and confidentiality, which can lead to discrimination and violence, resulting in violations of human rights. Therefore, it is crucial to implement proper planning and safeguards to protect

individuals' data and privacy. This includes adhering to data and interoperability standards, and ensuring transparency about how data is collected, stored, and used.

3. Promote Equity and Inclusion: ICT can contribute to expanding health inequity if not properly managed. Therefore, it's important to ensure that digital health interventions are designed and implemented in a way that promotes equity and inclusion. This includes considering the needs of marginalized and vulnerable populations, and ensuring they have equal access to digital health technologies.

2.6. Balancing Data Accessibility and Privacy in ICT Standards (authored by Charles Kiser Webb)

The Dual Imperative: Data Accessibility and Privacy

In the modern digital era, the intersection of data accessibility and privacy in Information and Communication Technology (ICT) standards is a crucial issue. As the volume of data generated and collected continues to expand exponentially, there is a growing need to balance the accessibility of this data with the imperative to protect individual privacy. Achieving this balance is not only a technical and regulatory challenge but also a fundamental human rights concern. This section and topic of the document explores how balancing data accessibility and privacy in ICT standards enhances human rights, discussing the mechanisms for achieving this balance and the broader societal implications.

Data accessibility is vital for innovation, economic growth, and the provision of services. Open data initiatives, big data analytics, and the use of data in artificial intelligence and machine learning are all predicated on the availability of large, diverse datasets. For instance, accessible health data can drive medical research, improve public health outcomes, and facilitate personalised medicine. Similarly, accessible data in education can help tailor learning experiences and improve educational outcomes.

However, the accessibility of data must be carefully managed to protect individual privacy. Privacy is a fundamental human right, enshrined in various international declarations and conventions, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. It protects individuals from surveillance, identity theft, and other forms of personal intrusion. When data is accessible without adequate privacy protections, it can lead to significant harms, including discrimination, stigmatisation, and loss of autonomy.

Digital HealthCare and Data Privacy: a Latin America Approach

A case to analyse is implementing European Quality, Regulatory, and Assurance (QARA) best practices in Latin America that can significantly enhance medical device safety, efficacy, and data accessibility and privacy, with a focus on Brazil and Colombia.

Regulatory Harmonisation: First, aligning Latin American regulations with the European Medical Device Regulation (MDR) can elevate safety standards. Brazil's ANVISA and Colombia's INVIMA are leading efforts to incorporate MDR principles, such as rigorous clinical evaluations and post-market surveillance. By establishing Mutual Recognition Agreements with European bodies, these agencies can streamline the approval process for MDR-certified devices, ensuring that high-quality, safe devices are available more quickly.

Quality Management Systems: Next, adopting ISO 13485, an international standard for Quality Management Systems, is crucial. Brazil's ANVISA and Colombia's INVIMA are partnering with industry associations to provide training and certification programs. These initiatives ensure consistent quality and regulatory compliance, boosting trust in medical devices manufactured in Europe and Latin America.

Information Security and Data Privacy: Information security and data privacy are paramount. Inspired by the European GDPR, Brazil's General Data Protection Law (LGPD) and Colombia's data protection regulations are being strictly enforced. Both countries are promoting ISO/IEC 27001 certification to ensure robust information security. This certification helps healthcare organisations and manufacturers protect patient data, building trust and complying with international standards.

Impact and Benefits: Implementing these best practices brings multiple benefits. It improves the safety and efficacy of medical devices, reducing risks and enhancing patient outcomes. Streamlined regulatory processes and high-quality standards attract foreign investment, driving economic growth. Enhanced data protection measures build trust in the healthcare system, ensuring patient data remains secure.

In conclusion, adopting European QARA best practices in Latin America, particularly through the efforts of Brazil's ANVISA and Colombia's INVIMA, can significantly improve healthcare outcomes, protect patient rights, and foster economic development. By working together and embracing these high standards, we can create a more equitable, effective and data privacy centred healthcare system for all.

Recommendations

To effectively implement European QARA best practices in Latin America, there are several recommendations targeted at Standards Development Organizations (SDOs), companies, policymakers, and Research and Innovation (R&I) projects.

Standards Development Organizations (SDOs):

1. Harmonise Standards: Collaborate with Latin American regulatory bodies to harmonise medical device standards with ISO 13485 and ISO/IEC 27001. This ensures consistency in quality management and information security.

2. Training Programs: Develop and offer training programs tailored to the needs of Latin American manufacturers and regulators, focusing on MDR principles and GDPR compliance.

Companies:

1. Adopt International Standards: Pursue ISO 13485 and ISO/IEC 27001 certification to ensure high quality and secure products. This will not only improve safety but also enhance market access.

2. Invest in Compliance: Allocate resources to comply with local regulations inspired by MDR and GDPR. This includes investing in robust QMS and information security systems.

Policymakers (e.g., European Commission):

1. Support Mutual Recognition Agreements (MRAs): Facilitate MRAs between the EU and Latin American countries like Brazil and Colombia. This will streamline the approval process for medical devices, ensuring quicker access to high-quality products.

2. Provide Technical Assistance: Offer technical assistance and funding to Latin American regulatory bodies to help them align with European standards and practices.

Research and Innovation Projects:

1. Collaborative Projects: Encourage and fund collaborative projects between European and Latin American institutions focusing on medical device innovation, quality assurance, and data security.

2. Knowledge Transfer: Promote knowledge transfer initiatives that share best practices and technological advancements in QARA, fostering a culture of continuous improvement and innovation in Latin America.

By following some of these recommendations, we can boost the implementation of European QARA best practices in Latin America not only to improve healthcare outcomes and patient safety but also drive economic growth and foster international collaboration.

2.7. Empowering Responsible Business: ISO Norms, Ethical Leadership, and Human Rights in Chile (authored by Monica Martinez Vargas)

The value of implementing robust ethical standards in businesses in Chile lies in fostering trust, driving sustainable growth, and upholding corporate social responsibility. By setting a precedent for ethical behaviour, businesses can positively impact the economy, society, and environment while securing their long-term viability and success.

Implementing robust ethical standards in businesses, especially in Chile, offers several benefits and significant value:

1.Trust and Reputation: Ethical practices build trust with customers, investors, and the public. When companies adhere to high standards, their reputation improves, leading to long-term success.

2.Risk Mitigation: Ethical standards help prevent legal and financial risks. Compliance with regulations reduces the likelihood of fines, lawsuits, and damage to the company's image.

3.Employee Morale and Productivity: Ethical workplaces attract and retain talented employees. When employees feel their company operates ethically, they are more motivated, productive, and loyal.

4.Sustainable Growth: Ethical practices contribute to long-term sustainability. Companies that prioritise ethics are better positioned to adapt to changing markets and environmental challenges.

5.Social Impact: Ethical businesses positively impact society. By respecting human rights and promoting fair practices, they contribute to a better quality of life for all.

In summary, robust ethical standards benefit businesses by fostering trust, reducing risks, enhancing employee satisfaction, promoting sustainability, and positively impacting society.

The Importance of Business Ethics Programs:

Business ethics programs play a vital role in shaping the behaviour and values of organisations. They outline principles and guidelines that guide decision-making

processes and establish a framework for ethical conduct. These programs help companies identify and manage ethical risks, ensuring that their operations align with ethical standards and respect for human rights

ISO 19600: Establishing Compliance Management Systems

ISO 19600 provides guidelines for establishing compliance management systems within organisations. This standard emphasises the importance of a systematic approach to compliance, including the identification of legal and regulatory requirements, the establishment of policies and procedures, and the implementation of monitoring and control mechanisms. By adopting ISO 19600, companies in Chile can develop robust compliance management systems that not only address business ethics but also ensure respect for human rights.

Addressing Human Rights Through ISO Norms

While business ethics programs set the foundation for responsible conduct, integrating human rights considerations is crucial for sustainable and ethical business practices

ISO 26000 offers guidance on social responsibility, including the integration of human rights principles into business practices. ISO 37001 focuses on anti-bribery management systems, which are essential for preventing human rights abuses related to corruption. By implementing these standards, companies can ensure that human rights considerations are integrated into their ethical frameworks.

ISO 37000: Promoting Ethical Leadership

Ethical leadership is the compass that guides organisations towards responsible business practices and human rights respect

ISO 37000 provides guidance on ethical leadership, emphasising the role of leaders in fostering an ethical culture within organisations. It encourages leaders to promote ethical behaviour, establish clear values and expectations, and ensure accountability within the company. By implementing ISO 37000, companies in Chile can develop ethical leadership practices that align with human rights principles and contribute to a responsible business culture.

The Role of ICT in Promoting Transparency and Accountability

Information and Communication Technologies (ICT) serve as powerful tools for enhancing transparency and accountability in business practices, ensuring respect for human rights

ICT solutions can be utilised for effective reporting and monitoring of ethical conduct, whistleblower protection, and stakeholder engagement. By leveraging ICT, companies can enhance transparency, ensure timely reporting of ethical violations, and strengthen their commitment to human rights

Recommendations for Standards Development Organisations (SDOs):

1. **Promote Open Source Policies:** SDOs should consider adopting open source policies that encourage collaboration and the sharing of knowledge and resources among participants. This can be done by providing templates and examples of open source policies
2. **Facilitate Consensus-Based Processes:** SDOs should continue to follow consensus-based processes, allowing stakeholders to contribute their expertise and perspectives in the development of standards. This ensures that standards are widely accepted and reflect the needs of various stakeholders
3. **Engage with the Open Source Community:** SDOs can actively engage with the open source community to foster collaboration and knowledge exchange. This can be done through partnerships, participation in open source events, and providing resources and support for open source projects.

Recommendations for Companies:

1. **Establish Comprehensive Business Ethics Programmes:** Companies should develop and implement comprehensive business ethics programmes that integrate human rights considerations. These programmes should align with ISO 26000 guidelines and provide clear guidelines for ethical conduct within the organisation.
2. **Adopt ISO 19600:** Companies should adopt ISO 19600 to establish robust compliance management systems that address both business ethics and human rights. This standard provides guidelines for identifying legal and regulatory requirements, establishing policies and procedures, and implementing monitoring and control mechanisms.
3. **Embrace Ethical Leadership Practices:** Leaders within companies should embrace ethical leadership practices guided by ISO 37000. This includes promoting ethical behaviour, establishing clear values and expectations, and ensuring accountability within the organisation.
4. **Leverage ICT Solutions:** Companies should leverage Information and Communication Technologies (ICT) to enhance transparency, accountability, and stakeholder engagement. ICT solutions can be used for effective reporting and monitoring of ethical conduct, whistleblower protection, and facilitating communication with stakeholders.

Recommendations for Policy Makers:

1. **Promote RRI-like Practices:** Policy makers can design regulations that promote Responsible Research and Innovation (RRI)-like practices and reward companies that

incorporate socio-ethical concerns in their research and innovation work. This can include including ethical stage-gates to access public funding or fostering participatory processes from a quadruple helix perspective

2. **Facilitate Engagement of the Private Sector:** Policy makers can adopt domain-specific measures to facilitate the engagement of the private sector in RRI-like practices. This can include the development of STEM education programs for women, minorities, or disadvantaged groups to increase access to diverse research and innovation teams
3. **Require Transparency and Impact Assessments:** Policy makers should require companies to publish information about potential human rights impacts or harms, including those related to freedom of expression and privacy. They should also encourage companies to implement proactive and comprehensive impact assessments and establish effective grievance and remedy mechanisms

Recommendations for Research and Innovation (R&I) Projects:

1. **Incorporate RRI-like Practices:** R&I projects should aim to incorporate Responsible Research and Innovation (RRI)-like practices into their work. This includes considering socio-ethical concerns, engaging stakeholders, and ensuring transparency and accountability in research and innovation activities
2. **Collaborate with Policy Makers and SDOs:** R&I projects can collaborate with policy makers and Standards Development Organizations (SDOs) to align their work with relevant regulations and standards. This collaboration can help ensure that R&I projects contribute to responsible and ethical practices.
3. **Promote Diversity and Inclusion:** R&I projects should strive to promote diversity and inclusion in their research teams. This can be done by actively seeking diverse perspectives and ensuring equal opportunities for participation.

Conclusion

For Chile, the integration of ISO norms, ethical leadership, and a strong commitment to human rights are not just strategic advantages but necessities for sustainable development. Implementing robust ethical standards in Chilean businesses is not only a moral imperative but also a strategic advantage. By prioritising ethical behaviour, companies can build trust, mitigate risks, enhance employee satisfaction, and contribute to a more sustainable and socially responsible business environment. Furthermore, business ethics programs serve as essential frameworks for guiding decision-making processes and ensuring ethical conduct across organisations.

Chilean practices in ethical business standards and human rights can also serve as a **model for European companies and policy makers**. By adopting similar standards and

learning from Chile's implementation strategies, European organisations can enhance their own ethical frameworks and contribute to a global culture of responsible business. Collaborative efforts between Chile and Europe in developing and promoting ISO norms can lead to harmonised practices that benefit international trade and investment, fostering a more ethically conscious global business environment.

3. Recommendations

Introduction

The integration of human rights into technical standards is a multifaceted issue that has garnered attention from various experts. These perspectives encompass the need for more fundamental right performance metrics, the importance of privacy and trustworthiness, the distinct developmental paths of technical standards and human rights in the EU, and the challenges posed by digital technologies. Furthermore, the integration of human rights into standards, particularly in the ICT domain, encounters significant resistance due to the divergent understanding between technical experts and human rights advocates. Additionally, the need for ethical practices and the role of ICT in enhancing transparency and accountability are highlighted. This chapter firstly highlights some fundamental challenges related to the integration of human rights into ICT standardisation and then proceeds with two main sections:

- Recommendations directly derived from the workshop that originated this report, which emphasise policy commitments, technical considerations, and societal impacts to bridge the gap between human rights and technical standards.
- Additional recommendations synthesising the viewpoints of the seven different authors, categorised by stakeholder, to provide a broader perspective and further guidance on the integration of human rights into technical standards.

Challenges

Technical standards and human rights have evolved on separate tracks, creating a disconnect that complicates the integration of these two crucial areas. Climate change, digital technologies, and the increasing ethical implications of digital services necessitate a convergence of technical standards and human rights. However, the current risk management frameworks, such as ISO 31000, often exclude considerations of hazards and hazardous situations, creating a gap in addressing the fundamental right to safety within technical standards. This gap is particularly evident in the ICT domains, where technical experts often lack a comprehensive understanding of fundamental rights and practical safety, leading to resistance against integrating these concepts into standardisation processes.

The lack of interaction and mutual awareness between the human rights community and the standardisation community further exacerbates this issue. The standardisation processes are

often perceived as non-transparent and lacking democratic accountability, restricting public access and participation. This situation is compounded by the insufficient expertise within technical committees to address fundamental rights adequately, and the cultural view of technology as apolitical.

Recommendations from the Human Rights and ICT standardisation workshop

A. Policy Commitment

- **Ensure standards compliance with human rights:** It is crucial that standards comply with human rights to maintain their applicability within the EU. Non-compliance could render standards unusable, which would be detrimental to stakeholders.
- **Consider stakeholder interests:** When addressing human rights issues, it is essential to consider all stakeholder interests, including commercial-business interests and interoperability. This holistic approach ensures that human rights, business efficiency, and technical interoperability coexist harmoniously.
- **Follow Human Rights Council guidance:** The Human Rights Council, through its 2021 Resolution 47/23, has called for closer cooperation between the OHCHR and SDOs, including ITU. This cooperation aims to consider the relationship between human rights and technical standards more effectively.
- **Support AI Act implementation:** The AI Act, specifically Recital 121, emphasises the need for a balanced representation of all relevant stakeholders, including SMEs, consumer organisations, and environmental and social stakeholders, in the development of standards. This ensures that diverse perspectives are included in accordance with Articles 5 and 6 of Regulation (EU) No 1025/2012.

B. Technical

- **Link technical concepts to human rights**: As urged by ITU, it is important to establish clear links between technical concepts and human rights. This involves translating human rights principles into technical terms and embedding these principles into technical standards.
- **Human rights by design:** Implementing human rights “by design” in standardisation is essential. While high-level visions are valuable, practical execution plans must be in place to avoid turning these visions into mere aspirations. Lessons learned indicate that many necessary conditions are not yet in place.
- **Market-driven standards with ethical considerations:** Although multiple technical standards exist, it is ultimately the market that decides the winning standard. Designers must tailor standards to account for ethics and human rights, ensuring that these considerations are integral to the design process.

C. Societal

- **Integrate human rights experts in standardisation**: Bringing human rights experts, particularly those with technical knowledge, into standardisation activities is crucial for bridging the gap between technical and human rights domains. This integration facilitates more comprehensive and informed standard development.
- **Enhance transparency in standardisation**: A significant challenge in the standardisation process is the lack of transparency, due to standards being often behind paywalls in some SDOs. A recent ECJ ruling from March 2024 refers to this issue in specific cases related to EU legislation.. Free access to standards that may have impact on human rights would reduce the perceived non-transparency and increase accountability in standardisation processes.
- **Support sustainable fintech:** Encouraging sustainable fintech initiatives is vital for supporting Sustainable Development Goals (SDGs) and engaging with other fintech experts. This approach promotes financial technologies that are not only innovative but also socially and environmentally responsible.
- **Promote ethical business practices**: "Good ethics is good business." Implementing standards that support human rights, such as privacy, security, safety, and quality of life, is beneficial for the bottom line. It helps avoid financial, legal, and reputational damage.
- **Public recognition of standardisation**: Promote standardisation to a point where the public recognises a “flag/stamp” of quality and sees value in it. This public awareness can drive demand for products and services that adhere to high standards.
- **Highlight best practices**: There should be a call for successful examples and best practices of integrating human rights considerations into ICT standards. Platforms like StandICT.eu and HSBooster.eu, along with various SDO committees, can facilitate this sharing of knowledge and practices.

Additional Recommendations from the authors for different Stakeholders

A. Recommendations for Standards Development Organisations (SDOs)

1. **Building a Framework for Integration**:
    - Incorporate ethical, legal and human rights expertise into Standard Development Organizations (SDOs) to bridge the gap between human rights and technical standards.
    - Develop a common language for interdisciplinary work items and align engineering practices with human rights principles and regulatory terms.
    - **Promote diversity and inclusion:** Foster collaboration not only between ISO technical working groups but also externally with other organisations.
    - Align established consumer standards with human rights and promote the consideration of these standards as normative references in technical standards.

- Revise barriers that prevent human right experts and ANNEX III organisations from participating in international standardisation work (i.e., SDO's entry fees for expert nomination).

2. **Harmonising Standards**:
   - Collaborate with local regulatory bodies to harmonise international ,regional and national standards to ensure consistency in the protection of human rights.
   - **Continuation of Existing Work:** Build on existing standards like ISO 10377 to develop general guidelines for privacy, safety, and trustworthiness, aligning with European values and protection levels.
   - **Particular Recommendations:** Harmonise ongoing developments in risk management standards with consumer product standards, focusing on privacy by design, inclusive service, and good practices in the software lifecycle.
3. **Training and Capacity Building**:
   - Develop and offer training programs tailored to the needs of various stakeholders, focusing on principles and good practices related to fundamental rights, privacy by design and inclusive service.
   - Provide concrete guidance on relevant consumer standards to technical experts to help them understand and embed fundamental rights in standards development.
4. **Facilitating Consensus-Based Processes**:
   - Ensure standards reflect diverse stakeholder needs through inclusive and transparent, consensus-based processes.
   - Promote open-source policies to encourage collaboration and knowledge sharing.
   - Engage with the open-source community through partnerships and participation in events.
5. **Expert Collaboration and Integration:**
   - **Dedicated Consumer Rights Experts:** Establish teams within SDOs (such as ITU, ISO and CEN/CENELEC) to work with technical experts, ensuring consumer needs and human rights are integrated during standards development and revision.
   - **Foster Knowledge Transfer:** Form teams including human and consumer rights experts, technical experts, and other stakeholders to facilitate seamless integration of consumer concerns into technical standards. We recommend to focus particularly on sustainability, safety and trustworthiness standards reflecting fundamental rights in already existing standards.
   - **Interdisciplinary Approach:** Encourage interdisciplinary thought leaders to create examples of integrating human rights with technical standards, such as the work done in CEN JTC21 WG2 on "EN AI Risk Management System."

B. Recommendations for Civil Society/Human Rights Organisations

1. **Expanding Technical Understanding**:
    - Increase understanding of technology development and standardisation processes to participate effectively in standard-setting.
    - Establish mechanisms for sharing information about ongoing and forthcoming standard-setting processes.
2. **Capacity Building and Participation**:
    - Strengthen capacity to ensure effective participation in standard-setting processes regarding new and emerging ICT.
    - Conduct thorough Human Rights Impact Assessments to understand the implications of new standards and ensure they align with international human rights frameworks.
3. **Promoting Open Source Policies and practices**:
    - Advocate for open source policies and practices to encourage collaboration and knowledge sharing.
    - Further facilitate consensus-based processes to ensure standards reflect diverse stakeholder needs.
4. **Effective and active participation:**
    - **Reflect consumer interests in the SBP (Strategic Business Plan):** Get involved in the drafting of the SBP of technical committees. Consumers are one of the core stakeholder groups of standardisation organisations and topics like safety, trustworthiness and sustainability should be a central aspect in every strategic business plan.

C. Recommendations for the European Commission

1. **Supporting Harmonization and Recognition**:
    - Facilitate Mutual Recognition Agreements (MRAs), e.g., between the EU and Latin American countries like Brazil and Colombia. This will streamline the approval process for medical devices, ensuring quicker access to high-quality products.
2. **Providing Technical and Financial Assistance**:
    - Offer technical assistance and funding to non-european regulatory bodies to help them align with European standards and practices.
    - Provide additional financial resources to ANNEX III organisations to enable effective and proactive participation in the form of contributions and the ability to actively drive the content standards.
3. **Promoting Responsible Research and Innovation (RRI)**:

- Design regulations that promote Responsible Research and Innovation (RRI) practices and engage the private sector in these initiatives.
- Mandate companies to conduct comprehensive impact assessments and publish information on human rights impacts.
- Organise events that facilitate interaction between the human rights and standardisation communities through training sessions, workshops, and panels.

4. **Enforce Transparency, Accountability and availability of established PETs:**
   - ICT solutions should enhance transparency and accountability in business practices, supporting ethical conduct reporting, whistleblower protection, and stakeholder engagement. Leveraging ICT ensures timely reporting of ethical violations and strengthens commitment to human rights.
   - Oblige Companies providing Services and Products in the EEA to offer PGP-encrypted emails. This technology has been an established best practice to encrypt email for over 3 decades now and it is very simple to implement. However many companies refuse to encrypt emails at all exposing large amounts of personal data ignoring the availability of established and easy to implement PETs.
   - Record keeping and logging and events and measures that are relevant for legal obligations should be mandatory to be recorded on a tamper-proof logging infrastructure that is transparent and accessible to the authorised stakeholders.
5. **Holistic Strategy for Harmonised ICT Standards:**
   - **Harmonized European Horizontal Standards:**
     i. **Standardisation Requests:** Continue launching Standardisation Requests (SReqs) for European laws like the GDPR, ensuring standards align with legislative requirements and uphold human rights and high levels of consumer protection.
     ii. Target horizontal standards like **ISO 10377** to develop general guidelines for privacy, safety, and trustworthiness, aligning with European values and protection levels. Promote consideration of these consumer-centric standards as normative references in technical standards.
     iii. **Critical Industry Standards:** Harmonise ongoing developments in risk management and other widely used industry standards with consumer product standards, focusing on privacy by design, inclusive service, and other good practices supporting the protection of fundamental rights.
   - **International Adaptation and Participation:**
     i. **Adaptation of Standards:** Propose adapting guidelines and standards internationally to maintain high consumer protection levels globally while ensuring that those guidelines and standards respect human rights..
     ii. **Active Consumer Representation:** Ensure consumer organisations and human rights organisations have sufficient resources for active

participation in standardisation, drafting contributions, defending positions, and holding key positions in standardisation processes.

By implementing this holistic strategy, consumer rights and human rights can be robustly protected across all relevant standards, aligning with European values and setting a precedent for global standards development. This approach will foster safer, more trustworthy consumer environments.

D. Recommendations for Companies

1. **Adopting International Standards**:
    - Pursue certification procedures such as ISO 13485 and ISO/IEC 27001 to ensure high quality and safe products.
    - Establish comprehensive business ethics programs integrating human rights considerations, aligning with ISO 26000.
2. **Implementing Compliance Management Systems**:
    - Implement compliance management systems guided by ISO 19600, addressing business ethics and human rights.
    - Embrace ethical leadership practices, promoting ethical behaviour and accountability guided by ISO 37000.
3. **Leveraging ICT for Transparency**:
    - Use ICT solutions to enhance transparency, accountability, and stakeholder engagement.
    - Maintain distributed ledgers, validate transactions without intermediaries, and use smart contracts to simplify processes with digital signatures.

E. Recommendations for Research and Innovation (R&I) Projects

1. **Encouraging Collaborative Projects**:
    - Fund collaborative projects focusing on medical device innovation, quality assurance, and data security.
    - Promote knowledge transfer initiatives that share best practices and technological advancements in Quality Assurance and Regulatory Affairs (QARA), fostering a culture of continuous improvement and innovation in Latin America.
2. **Promoting Knowledge Transfer**:
    - Initiate knowledge transfer activities to share best practices and technological advancements.
3. **Integrating Socio-Ethical Concerns**:
    - Incorporate socio-ethical concerns and stakeholder engagement into R&I activities.

- Collaborate with policymakers and SDOs to align R&I projects with regulations and standards to ensure responsible practices.
- Promote diversity and inclusion by actively seeking diverse perspectives and ensuring equal participation opportunities.

4. Conclusions

Integrating human rights into technical standard-setting processes is essential for ensuring high-quality standards that support human rights in the digital age. Addressing the challenges associated with this integration can transform the operations of standard development organisations, prevent the undermining of established human rights frameworks and foster the implementation and use of standards. Viewing standards through a human rights lens will help build better technology that protects human rights, ensuring that technological advancements benefit all.

Implementing robust ethical standards in businesses fosters trust, mitigates risks, enhances employee satisfaction, and promotes a sustainable and socially responsible business environment.

Appendix I: Bibliography and Reference documents

Bibliography

[1] The predecessor of the International Telecommunications Union was formed in 1865, almost a century before the adoption of the Universal Declaration of Human Rights, adopted by the United Nations General Assembly in 1948 and heralding the contemporary understanding of human rights.

[2] Benedict Kingsbury, Nico Krisch and Richard B. Stewart, 'The Emergence of Global Administrative Law' (2005) 68 Law and Contemporary Problems 68, 15-61; European Union', in JL Contreras (ed), The Cambridge Handbook of Technical Standardisation Law (Cambridge, Cambridge University Press, 2019).

[3] See at https://www.ohchr.org/en/instruments-and-mechanisms/international-human-rights-law.

[4] See Damian Chalmers, Gareth Davis and Giorgio Monti, European Union Law (Fourth Edition 2019), pp. 644-6 and 713-20.

[5] Charter of Fundamental Rights of the European Union [2012] OJ C326/391 (CFR).

[6] General Data Protection Regulation (EU) 2016/679 [2016] OJ L119/1 (GDPR).

[7] Technical standards are mentioned, for instance, in Rec 168 and Art 43(9); design is mentioned in Rec 78 and the famous 'by design' provision in Art 25.

[8] European Commission, 'Commission implementing decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy. Mandate M/530'; Standard EN 17529:2022 shop.standards.ie/enie/standards/is en 17529 2022 1299700_saig_nsai_nsai_3142494/.

[9] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and Information systems across the Union [2016] OJ L194/1; Directive (EU(2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80; Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L151/15.

[10] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC), OJ L.

[11] European Commission, 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, COM(2022) 454 final, Brussels, 15.9.2022.

[12] Shin-Yi Peng, Private Cybersecurity Standards: Cyberspace Governance, Multistakeholderism, and the (Ir)Relevance of the TBT Regime, 51 CORNELL INT'l L.J. 445 (2018).

[13] Maria Grazia Porcedda, 'The Effacement of Information Technology from EU Law: The Need for collaborative Approaches to Redesign the EU's Regulatory Architecture', in F. Bieker, S. De Conca, I. Schiering, N. Gruschka. M. Jensen, Proceedings of the 18th IFIP Summer School 2023, Advances in Information and Communication Technology (Springer 2024). Preprint at: https://www.tcd.ie/law/researchpapers/Maria.Grazia.Porcedda-The_Effacement_of_Information_Technology_from_EU_Law.pdf

[14] Maria Grazia Porcedda, 'Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technology Analysis' (Hart Publishing 2023), ch 5. Maria Grazia Porcedda, Privacy by Design in EU law. Matching Privacy Protection Goals with the Essence of the Rights to Private Life and Data Protection (Lecture Notes in Computer Science, 2018).

[15] United Nations Environment Programme, *Climate Change and Human Rights*. Available: https://wedocs.unep.org/20.500.11822/9530. [Accessed: Jun. 23, 2024].

[16] United Nations Environment Programme, *Climate Change and Human Rights*. Available: https://wedocs.unep.org/20.500.11822/9530. [Accessed: Jun. 23, 2024].

[17] ISO's Climate Commitment. Available: https://www.iso.org/ClimateAction/LondonDeclaration.html[Accessed: Jun. 23, 2024].

[18] IAF/ISO Joint Communiqué on the addition of Climate Change considerations to Management Systems Standards.https://www.iso.org/files/live/sites/isoorg/files/standards/popular_standards/management_systems/ISO-IAF%20Joint%20Communique%20Feb%202024.pdf [Accessed: Jun. 23, 2024].

[19] https://committee.iso.org/home/tc322 [Accessed: Jun. 20, 2024].

[20] ISO Technical Committee 322 Sustainable Finance 2023-2025 Strategic Plan. Ballot to approve TC322 AHG3 FinTech in Carbon Markets, AHG3 Convenor.

[21] https://www.consilium.europa.eu/en/policies/climate-change/ [Accessed: Jun. 23, 2024].

[22] Espenan, Nicholas P. (2023) "Improving Voluntary Carbon Markets Through Standardization and Blockchain Technology," Wyoming Law Review: Vol. 23: No. 1, Article 4.

[23] Vilkov, A.; Tian, G. Blockchain's Scope and Purpose in Carbon Markets: A Systematic Literature Review. Sustainability 2023, 15, 8495.

[24]https://medium.com/open-forest-protocol/how-blockchain-will-open-a-new-standard-for-carbon-credits-8822558e14a9 [Accessed: Jun. 23, 2024].

[25] Vilkov, A.; Tian, G. Blockchain's Scope and Purpose in Carbon Markets: A Systematic Literature Review. *Sustainability* 2023, *15*,8495. See additionally, https://www.theclimatewarehouse.org/ [Accessed: Jun. 22, 2024].
[26] Vilkov, A.; Tian, G. Blockchain's Scope and Purpose in Carbon Markets: A Systematic Literature Review. *Sustainability* 2023, *15*,8495.
[27] https://rmi.org/what-can-blockchain-do-for-carbon-markets/ [Accessed: Jun. 23, 2024].
[28] Ballot to approve TC322 AHG3 FinTech in Carbon Markets, AHG3 Convenor.
[29] Ballot to approve TC322 AHG3 FinTech in Carbon Markets, AHG3 Convenor.
[30]Baiz, Pedro (2024). Blockchain and Carbon Markets: Standards Overview. https://arxiv.org/pdf/2403.03865 [Accessed: Jun. 23, 2024].
[31] Mélanie Gornet, Winston Maxwell. The European approach to regulating AI through technical standards. 2024. Ffhal-04254949v2f
[32] UN General Assembly, Human Rights and technical standard-setting processes for new and emerging digital technologies, 18 September 2023, A/HRC/53/42
[33] Judgement of the General Court (Fifth Chamber, Extended Composition) of 14 July 2021. Public.Resource.Org, Inc. and Right to Know CLG v European Commission.
[34] Christopher Sabatani (Ed), Reclaiming human rights in a changing world order, Brookings Institution Press, October 10, 2022. ISBN: 9780815739753

Further readings

Bagolle, Alexandre; Casco, Mario; Nelson, Jennifer; Orefice, Pablo; Raygada, Georgina; Tejerina, Luis. The Golden Opportunity of Digital Health for Latin America and the Caribbean. Inter-American Development Bank, 2022.
Brown, A. (2020). Harnessing the Power of ICT for Responsible Business Practices. Journal of Business Ethics, 45(2), 109-126.
Christopher Sabatani (Ed), Reclaiming human rights in a changing world order, Brookings Institution Press, October 10, 2022. ISBN: 9780815739753
Digital health platform handbook: building a digital information infrastructure (infostructure) for health. Geneva: World Health Organization and International Telecommunication Union, 2020. Licence: CC BY-NC-SA 3.0 IGO.
Garcia, L. (2017). Ethical Leadership: Guiding Organizations towards Responsible Business Practices.
Global strategy on digital health 2020-2025.
ISO. (2014). ISO 19600:2014 - Compliance Management Systems. Retrieved from https://www.iso.org/standard/56723.html
Jones, M. (2019). Integrating Human Rights into Business Ethics Programs. Business Ethics Quarterly, 32(1), 1-18.

Judgement of the General Court (Fifth Chamber, Extended Composition) of 14 July 2021. Public.Resource.Org, Inc. and Right to Know CLG v European Commission.

Mélanie Gornet, Winston Maxwell. The European approach to regulating AI through technical standards. 2024. ffhal-04254949v2f

Smith, J. (2018). The Foundations of Business Ethics: A Comprehensive Approach. New York, NY: Routledge

UN General Assembly, Human Rights and technical standard-setting processes for new and emerging digital technologies, 18 September 2023, A/HRC/53/42

Appendix II: Workshop on "Human Rights & ICT Standardisation" Agenda Date: 6th June 2024

15:30 - Welcome and Introduction, **Silvana Muscella**, *StandICT.eu 2026 Project Coordinator*

15:35 - Policy perspectives, **Emilio Davila Gonzalez**, *Head of ICT Standardisation Sector, DG CONNECT, European Commission*

15:45 - Enhancing the EU Standardisation Strategy, **Jochen Friedrich**, *Member of the ETSI Board, IBM*

15:55 - The role of international standardisation bodies in addressing Human Rights concerns in ICT standardisation, **Olivier Alais**, *ITU*

16:05 - The intersection of cybersecurity and Human Rights in the context of ICT standardisation, **Arnaud Taddei**, *Broadcom and ITU*

16:15 - Panel discussion moderated by **Nicholas Ferguson**, *HSbooster.eu* Project Coordinator "Human Rights and ICT standardisation: examples and best practices across diverse SDOs" *with StandICT.eu fellows and HSbooster.eu experts.* Invited panellists:

- **Viveka Bonde**, Partner, Bonde Advokate, ISO (StandICT.eu Fellow)
- **Christian Grafenauer**, ISO & CEN-CENELEC (StandICT.eu Fellow)
- **Shakira Bedoya,** Senior Compliance Officer, Danske Bank, ISO (StandICT.eu & Seeblocks Fellow and HSbooster.eu expert)
- **Maria Grazia Porcedda**, Assistant Professor, Trinity College Dublin
- **Veronique Lerch,** Independent Human Rights Consultant
- **Gabriela Garham,** ISO, General Manager at ADIMECH AG
- **Monica Martinez Vargas**, Executive Director of Strategy 2 Succeed
- **Charles Kiser Webb**, Senior Information Technology Executive

17:15 - Q&A preliminary recommendations

17:30 - Wrap-Up with main findings

Recordings and slides are available online at this link