Date: 2022 -

prCWA XXXXX: XXXX

Secretariat: AFNOR

Digital Sovereignty — European perspectives, general approach, and implications on standardisation

ICS:

CCMC will prepare and attach the official title page.

This CEN/CENELEC Workshop Agreement is an agreement, developed and approved by an open independent workshop structure within the framework of the CEN-CENELEC system.

This CEN/CENELEC Workshop Agreement reflects the agreement of the registered participants responsible for its content, who decided to develop this document in accordance with the specific rules and practices available in CEN-CENELEC for the development and approval of CEN/CENELEC Workshop Agreements.

This CEN/CENELEC Workshop Agreement can in no way be held as being a European Standard (EN) developed by CEN/CENELEC, as it does not represent the wider level of consensus and transparency required for a European Standard (EN). Furthermore, it is not intended to support legislative requirements or to meet market needs where significant health and safety issues are to be addressed. For this reason, CEN/CENELEC cannot be held accountable for the technical content of this CEN/CENELEC Workshop Agreement, including in all cases of claims of compliance or conflict with standards or legislation.

The Workshop parties who drafted and approved this CEN/CENELEC Workshop Agreement, the names of which are indicated in the Foreword of this document, intend to offer market players a flexible and timely tool for achieving a technical agreement where there is no prevailing desire or support for a European Standard (EN) to be developed.

Contents

Page

European foreword

This CEN/CENELEC Workshop Agreement has been developed in accordance with the CEN-CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – A rapid prototyping to standardization" and with the relevant provisions of CEN/CENELEC Internal Regulations - Part 2. It was approved by a Workshop of representatives of interested parties on YYYY-MM-DD, the constitution of which was supported by CEN/CENELEC following the public call for participation made on YYYY-MM-DD. However, this CEN/CENELEC Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN/CENELEC Workshop Agreement was provided to CEN/CENELEC for publication on YYYY-MM-DD.

The following organizations and individuals approved this CEN/CENELEC Workshop Agreement:

- name organization/individual
- name organization/individual
- …

Attention is drawn to the possibility that some elements of this document may be subject to patent rights. CEN-CENELEC policy on patent rights is described in CEN-CENELEC Guide 8 "Guidelines for Implementation of the Common IPR Policy on Patent". CEN/CENELEC shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and non-technical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN/CENELEC Workshop Agreement shall be aware that neither the Workshop, nor CEN/CENELEC, can be held liable for damages or losses of any kind whatsoever. The use of this CEN/CENELEC Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk. The CEN/CENELEC Workshop Agreement should not be construed as legal advice authoritatively endorsed by CEN/CENELEC.

Introduction

Digital Sovereignty is rising on the agenda of many nations and trade blocks. The digital space has become a vital tool providing resilience, efficiencies, innovation and growth to states, organizations, and individuals, but also a tool of influence and power where dependencies, vulnerabilities and threats are created for individuals, organizations and states. The control of data, its accessibility, its protection and the governance of the digital space, and more generally the governance of digital resources, are becoming issues of sovereignty.

Expectations for sovereign governance of digital resources may be supported by recognized and accepted standards.

There are currently many potential definitions and perceptions associated with Digital Sovereignty, and even though there is more and more common understanding of what is at stake, the concept and the associated terminology remain somewhat undefined. For the European Union, Digital Sovereignty is not synonym of protectionism but is more about protecting its values and principles in cyberspace and, more globally, in the digitalised society, based on the rule of law in a free and democratic society, and on the protection of individual rights (such as human dignity, right to privacy, protection of personal data, freedom of expression) enshrined in the EU Charter of Fundamental Rights, the European Convention on Human Rights, and, globally, in the UN Universal Declaration of Human Rights, as well as its ability to make sovereign decisions.

While "Digital Sovereignty" might be considered as a subset of the concept of "Sovereignty", the digital dimension makes it difficult to operationalize the concept. This is all the more so as this notion, in itself has multiple meanings and is the subject of discussion on its scope and its implications.

In particular, key concepts such as "territory" or "boundaries" that generally come with the definition of sovereignty in the physical world are difficult to translate in cyberspace. To this end, the concept of jurisdiction has been used in order to deal with the scope of Digital Sovereignty and its implications.

Digital Sovereignty may cover many domains and objectives such as cybersecurity, data jurisdiction and enforcement, trustworthiness, protection of fundamental rights and strategic autonomy. Defining and recognising Digital Sovereignty while promoting an open and free market, such as the EU single market, also leads to a need for interoperability as well as technological neutrality.

Legally speaking, only a country or a group of countries (such as the European Union) is sovereign. However, confidentiality, integrity, resilience, trust, and independence expectations in the digital space are not limited to states. EU Institutions, civil society as well as economic stakeholders have been highlighting the need for all – individuals, businesses, and states – to be better positioned to face the new balances of power in digital relationships and activities.

All entities, private and public, individuals and legal persons, in the digital sphere have expectations about and are impacted by Digital Sovereignty. It is often difficult for individuals as well as companies to understand all the complexity and technical components of the digital world. Obviously all need to be empowered to cope with the consequences of "digitalization".

Therefore, in the context of pre-standardization, the "Digital Sovereignty" scope has been enlarged to encompass all stakeholders, including groups of countries, individuals, organizations including private companies.

For that matter, the CWA has developed a holistic approach:

- Digital Sovereignty from the perspective of states relates to sovereignty in cyberspace and the exercise of powers.
- Digital Sovereignty, as a concept transposed and adapted to organizations (public and private), relates to their objectives pursued through digital capabilities

- Digital Sovereignty, as a concept transposed and adapted to individuals, relates to their expectations and rights with regard to self-determination.

This document proposes a description of the concept of "Digital Sovereignty" seen from the perspective of standardization supporting and anticipating potential societal requirements.

Thus, the targeted audience of this document is any party interested in Digital Sovereignty, including, but not limited to, governments, policy makers, standardization organizations, lawyers, consumer associations, worker associations, business associations, organizations, and last but not least also individuals who have a need to better understand this notion and its implication on their self-determination in current and future digital worlds.

As a result, the present document also intends to be as much as possible self-explainable, comprehensive, and understandable for all stakeholders not used to the standardization "language".

1. Scope

This document provides a terminology and conceptual framework around the Digital Sovereignty concept, interconnecting the many terms that are used along such as strategic autonomy, digital commons, digital integrity, digital capabilities.

Eventually, the document proposes potential standardization activities supporting or connected to Digital Sovereignty.

2. Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

3. Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

autonomy
autonomous

<Digital Sovereignty> ability of an entity to modify its governing rules or its goals without external intervention, control, or oversight

Note 1 to entry: for a person or an organization, self-determination can be used as a synonym for autonomy

Source: adapted from ISO-IEC 22989:2022

3.2

commons

shared resources accessible to all members of a society, including natural materials such as air, water, and a habitable earth.

Note 1 to entry: commons can also be understood as natural resources that groups of people (communities, user groups) manage for individual and collective benefit.

Note 2 to entry: characteristically, this involves a variety of informal norms and values (social practice) employed for a governance mechanism.

Note 3 to entry: commons can be also defined as a social practice of governing a resource not by state or market but by a community of users that self-governs the resource through institutions that it creates.

SOURCE: Wikipedia (modified)

3.3

cyberspace

interconnected digital environment of networks, services, systems, and processes

SOURCE: ISO/IEC 27102:2019(en), 3.6

3.4

digital capability

ability to perform or support a function based on digital resources

3.5

digital commons

commons of a digital nature including data, information and knowledge

3.6

digital dependency

reliance on the use of digital resources

3.7

digital identity

set of information in cyberspace that allows the unique identification of any physical and virtual subject or object

Note 1 to entry: physical and virtual subjects or objects may include, but not limited to, individuals, organizations, objects, avatars, processes, data, software or concepts

Note 2 to entry: the set of information is understood as any characteristic or quality attributed to a physical and virtual subject or object concerned, such as name, date of birth, date of manufacturing, nationality or origin, address…

3.8

digital integrity

<Digital Sovereignty> fundamental and intrinsic protection granted to a person in order to remain without alteration or undue influence.

Note 1 to entry: digital integrity applies to both natural and legal persons.

3.9

Digital Sovereignty

ability to analyze, decide or act according to a set of values, principles, interests, and goals while managing digital dependencies and risks on digital capabilities.

Note 1 to entry: managing risks include identifying threats and considering factors such as vulnerabilities and possible events.

3.10

digital resources

component, stock, supply of materials or assets that can be drawn on through digital means when needed

Note 1 to entry: digital resources should be understood as resources supporting digital ecosystems and activities

3.11

entity

any individual, organization and (group of) state(s)

Note 1 to entry: the term entity encompasses the three main actors of Digital Sovereignty, translating the holistic approach followed in the document

3.12

governing body

person or group of people who have ultimate accountability for the whole organization

[SOURCE: ISO 37000:2021, 3.3.4 modified with Note 1, 2 and 3 removed]

3.13

interoperability

ability of two or more systems or components to exchange information and to use the information that has been exchanged

[SOURCE: IEEE 610-1990 – IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries]

3.14

organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO Directives Part 1 Annex SL Appendix 2 modified with Note 2 removed]

3.15

strategic autonomy

willingness and readiness of a country (or group of countries) to protect its autonomy

3.16

resilience

ability to absorb and adapt in a changing environment

Note 1 to entry: absorbing and adapting includes recovering in an acceptable time frame from any stress or shock while continuing to assess, decide and act

[SOURCE: ISO 22300 modified with Note 1 added]

3.17

stakeholder

interested party

any entity that can affect, be affected by, or perceive itself to be affected by a decision or activity.

[SOURCE: ISO/IEC 38500:2015, with “individual, group, or organization” replaced by “entity”]

3.18

threat

potential source of danger, harm, or other undesirable outcome

Note 1 to entry: threats can be on or come from data, software, processes, digital knowledge, human resources, hardware, digital infrastructure, engineering methods and tools, or any entity values, principles, interests, or goals.

Note 2 to entry: A threat is a negative situation in which loss is likely and over which one has relatively little control.

Note 3 to entry: A threat to one party may pose an opportunity to another.

[SOURCE: ISO 31073-2022, modified with Note 1 added]

3.19

trusted third party

entity that is recognized as being independent of the parties involved, as concerns the issue in question, and that is trusted by other entities based inter alia on competencies, with respect to related activities

[SOURCE:ISO/IEC 9798–1:2010, 3.38, modified, “security authority or its agent” replaced by “entity” and “security” removed]

3.20

trustworthiness

ability to meet stakeholders' expectations in a verifiable way

Note 1 to entry: Depending on the context or sector, and also on the specific product or service, data and technology used, different characteristics apply and require verification to ensure stakeholders' expectations are met.

Note 2 to entry: Characteristics of trustworthiness include, for instance, reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability and accuracy.

Note 3 to entry: Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as, in the context of governance, to organizations.

[SOURCE: ISO/IEC 30145-2:2020, 3.9]

4. General approach

4.1 Concept

Digital Sovereignty is a core concept aimed at promoting autonomy and resilience. It refers to the ability for each concerned entity to analyze, decide and act independently in the digital ecosystem based *inter alia* on digital resources and/or digital capabilities.

Nevertheless, in a globalized and interconnected society, no entity is fully independent, and no entity is free from digital dependencies. Therefore, it has to be recognized that Digital Sovereignty may come with different degrees.

Degrees of Digital Sovereignty may come through the management of dependencies, threats, and vulnerabilities on digital resources. It will be based on the analysis and the understanding of natural dependencies as well as relationships with external interested parties, or external factors or sources of influences, which can include potential threats (e.g., undesired influences, manipulations, and constraints).

Dependencies and threats should be regarded in how they affect an entity’s major and vital interests, in light of a core set of values, principles, interests, and goals.

Applicable regulations and policies in a given jurisdiction enable entities to benefit from rights including Digital Sovereignty components in their interaction with digital capabilities. As each jurisdiction is limited, in principle, in its area of competence, any entity can only enjoy and exercise its Digital Sovereignty within the limits of the competent jurisdiction.

4.2 Principles

Digital Sovereignty is a concept based on a set of common principles, applicable equally to individuals, organizations, and states. They read as follows:

- First principle: Digital Sovereignty relates to the ability of entities to exercise their autonomy or self-determination in cyberspace
- Second principle: Digital Sovereignty presumes the ability of an entity to independently analyze, decide and act
- Third principle: Organizations and individuals subject to a state's jurisdiction are entitled to self-determination in the digital space as in the physical world
- Fourth principle: Competent jurisdictions defines boundaries for an entity to exercise its Digital Sovereignty.
- Fifth principle: Digital Sovereignty shall be based on fundamental values, rights and principles and national, regional and international regulation.

4.3 Jurisdiction

4.3.1 General context

Digital Sovereignty relies on a set of fundamental values and principles as well as regulatory frameworks supporting its main characteristics[1] within one or several jurisdictions.

For a country, the ability to develop and enforce regulations requires that both natural and legal persons acting in cyberspace - by themselves or through a third party and/or by using any object or system (including data, software and hardware) under their control - are unambiguously linked to a jurisdiction, known as "competent" jurisdiction.

Regulations in a given jurisdiction – at national, regional, or international level - may grant rights and obligations, elaborate rules, allow transactions and enable ownership in cyberspace. Regulation may also put regulatory requirements on persons in charge of, and liable for certain objects or systems within a given jurisdiction to be identified and protected in cyberspace. Certain connected or purely digital objects may also be linked to be able to determine the applicable legal regime and, where appropriate, their ownership (e.g. health data, objects in the metaverse).

Against this background the social, economic or political relations that unfold in the digital world always fall within a given jurisdiction. Therefore, the Digital Sovereignty of any entity is underpinned by the competent jurisdiction.

4.3.2 Competent jurisdiction in cyberspace

The identification of the competent jurisdiction to a given situation in the digital ecosystem is crucial for any entity to preserve its Digital Sovereignty and to implement the related prerogatives. "Digital-Sovereignty supporting standards" may be developed and applied in various jurisdiction worldwide in order to ensure that Digital Sovereignty characteristics are respected by all stakeholders.

[1] Defined below, clause 8.

Having jurisdiction will allow the competent authorities:

- to assess the compliance of any behaviour of stakeholders, such as foreign organizations or countries – with the Digital Sovereignty of an entity.
- as well as to enforce any prerogative arising from an entity's Digital Sovereignty, based on the applicable rules, values or standards.

For each given situation implying a given entity, the competent jurisdiction in cyberspace – as well as in the physical world – is to be determined in accordance with pre-established criteria, such as citizenship (or nationality), sovereign territory, place of establishment, habitual residence or domicile, main place of provision of activities or services, etc.

This would mean that the scope of Digital Sovereignty of any entity would be defined according to and under the control of the jurisdiction in which the entity concerned has the main centre of its interests. For a country, this would be its sovereign territory transposed to cyberspace; for an organization, it would be the jurisdiction in which it has its principal activity and central administration; for an individual, it could be the jurisdiction in which he or she has his or her habitual residence.

4.3.3 Extraterritoriality

From a legal perspective, the determination that a state has extraterritorial jurisdiction means that a given provision laid down by such jurisdiction applies beyond its geographical scope of application and the boundaries of this jurisdiction. This may include provisions with regard to external behaviours (i.e. coming from foreign entities, connected to foreign jurisdictions) that impact the regulation of a domestic market, the respect of fundamental values of the jurisdiction or even the territorial integrity of a state. These provisions may also protect individuals against infringements of their fundamental rights, derived from these foreign harmful behaviours.

The jurisdiction's boundaries are traditionally materialised, in the physical world, by the borders of sovereign states, their territory and their legal order. In cyberspace, they must be understood more flexibly as referring both:

- to the scope of application of regulatory frameworks of sovereign jurisdiction
- and to technological boundaries defined in particular (but not limited to) logs, protocols or exchanges of cybersecurity messages

In cyberspace, each entity aims to ensure its Digital Sovereignty since it may be at risk in its relationships with other stakeholders. In this context, some characteristics of Digital Sovereignty may be exposed to extraterritoriality. These dimensions involve public interests, understood as all mandatory requirements and core values within a given jurisdiction. Therefore, extraterritorial jurisdiction may (exceptionally) be used to obtain the compliance of external behaviours to domestic public interests and thereby to Digital Sovereignty, with respect for fundamental rights and values.

Example:

This is the case, for instance, in the field of personal data protection rights. Those rights are regulated differently by various jurisdictions worldwide; the processing of personal data may give rise to extraterritorial application of the requirements of a given jurisdiction in order to ensure a higher level of protection (e.g. those requirements may be applicable to data controllers established outside the jurisdiction). Such extraterritorial application may be analysed as being an expression of the Digital Sovereignty of the entity concerned (i.e. the country which lays down this regulation) since it aims to protect the rights of data protection within its domestic market and of its citizens, including their digital

integrity. In the data sphere, the sovereignty's dimension at stake may be described as "personal data sovereignty", which includes 'personal data ownership', 'right to a secure connection' and, more in general, 'European values and principles' in the field.

4.4 Digital commons

"Digital commons" bears the idea that parts of the digital ecosystem shall be governed at the benefits of a community. It indicates the willingness of some organizations, including public authorities, to develop a human-and-citizen-centric trust in digital ecosystem, underpinned by the principles of equality and non-discrimination.

In digital commons, authorized commercial practices may have to comply with rules and digital behaviours set by the community authorities.

For states, digital commons may be shaped by their regulation, values, and principles. The digital commons concept is scalable and can be replicated at regional and local levels. Hence, a city can develop its own digital commons bringing in all of its public services.

Important part of the digital commons shall be dedicated to ensuring the equal accessibility and inclusion of all individuals in a given community.

An illustration of a "digital common" is given in the use cases annex "Territorial Multi-sectorial data space" to be found in Annex A1.

4.5 Digital identity

Digital identity is a key concept in cyberspace and is necessary for certain transactions, supporting on the one hand confidence and transparency and on the other hand transactions and accountability. The identification of a subject and/or an object makes it possible to determine ownership or custodianship where necessary. In such a case, digital features of entities and assets must be traceable in both physical and cyber world.

The participation of any entity or asset to the digital ecosystem gives rise to an identification scheme. The digital identity is the result of such a scheme. Within the context of this paper, it is important to remain open to both centralised and de-centralised alternatives.

In particular for the individual it will be crucial to have access to decentralised options like the use of personal data stores and self-sovereign identity. The technological need for some form of digital identity should be balanced with the entitlement of individuals to self-determination, also in cyberspace.

From the perspective of Digital Sovereignty, every entity and asset involved in the digital ecosystem is subject to, or part of, a competent jurisdiction based on its digital identity. Therefore, the rights, obligations and fundamental values applicable in this jurisdiction may be implemented in the digital sphere – as they are in the physical world – by or vis-à-vis these entities or assets (via its owner or custodian) through digital identification. Any entity may also, for itself or for an asset in its custody, assert/invoke the attributes of its Digital Sovereignty that would be challenged in the digital ecosystem.

To this end, it seems important to promote robust authentication schemes understood as "an electronic process that enables the electronical identification of a natural or legal person [or an asset], or the origin and integrity of data [and set of attributes] in electronic form to be confirmed".

It may be necessary, in certain circumstances, to involve a trusted third party to ensure the authenticity and probative value of this digital identity[2].

[2] Already several proposals exist, for example the European Regulation on Electronic Identification, Authentication and Trust Services (eIDAS Regulation), and the latest proposal for a Regulation on Digital Identity.

4.6 Digital Sovereignty characteristics

The mitigation of digital dependencies, threats and influences organization should be based on a set of actions, in the societal, digital and physical domain. Those actions may support one or more sovereign characteristics in the digital space, such as:

- Autonomy
- Digital integrity
- Dependencies and threats awareness
- Resilience
- Indispensability
- Dispensability
- Protection
- Interoperability
- Openness

Where:

- Autonomy is the ability to modify its governing rules or its goals without external intervention, control or oversight
- Digital integrity is a key component of Digital Sovereignty. It allows individuals to benefit from an equivalent fundamental protection in cyberspace as in the "physical world". Indeed, digital integrity may be seen as a transplantation of the right to integrity of the person, following the broader concept of human dignity, into the digital area. It aims to ensure that the person's humanity, including his or her conscience is respected. Regarding organizations and countries, digital integrity offers an upgraded level of protection in cyberspace, to ensure inter alia the intangible protection of their critical infrastructures which are vital for the continuity of economic and political activities in the digital ecosystem.
- Resilience is the ability to recover from a disruptive event,
- Indispensability refers to an entity being indispensable to other stakeholders. In that situation, an entity is protected to some extent by its indispensability,
- Dispensability refers to an entity not depending on a single source,
- Protection refers to the ability to identify threats activities, investigate the origin and react accordingly,
- Openness and interoperability refer to the ability to mitigate dependability by relying on the dynamic adaptiveness of an open market to resolve issues.

Entities may develop their own set of metrics for assessing their Digital Sovereignty.

5. Perspectives of individuals, countries and organizations

5.1 Individuals

5.1.1 General

Individuals are entitled to self-determination in the digital space. However, not all individuals have the expertise to be aware and cope with external factors or sources of influences, which can include potential threats/pressures (e.g. undesired influences, manipulations, constraints, bullying, harassment, abuse).

Thus, Digital Sovereignty in the context of individuals goes beyond the mere ability to access and have ownership of a person's own information including personal data. It refers to the ability for individuals to decide and take actions in the digital ecosystem, regarding their own life and to shape their life trajectory within their own cultural and social contexts.

This implies that the asymmetry of information and knowledge, the asymmetry in power, between individuals and organizations, whether public or private, must be mitigated with the help of standards and legislation applicable to cyberspace, its access and the situations and relationships created within.

5.1.2 Context and concepts

Individuals use digital services, buy digital devices, participate in online communities, consult doctors, install smart home appliances, and so on. As a by-product of these digital lives and products, millions of data traces are left behind, which, in many cases, are re-used and re-packaged in subsequent iterations with individuals. Algorithms may limit options offered, nudge into buying certain products, or manipulate to spend more money while gambling. In general, this is not obvious to individuals. And even if it were, is there an alternative? Therefore, taking into account individuals as stakeholders is critical, as digitalisation affect their work and private life in important ways.

Since Digital Sovereignty is based on the understanding of digital dependencies, and the related risks, it is crucial for individuals as a minimum to be given the information and the means to exercise their rights, ensure they expected benefits and to address their needs and expectations.

Dimensions of the concept of Digital Sovereignty for individuals can include (but are not limited to):

- Protection of human rights and fundamental values
- Consumer protection
- Responsible design and use of life sciences
- Protection of minors
- Privacy and personal data protection
- Providing trustworthy AI
- Preventing discrimination and undue bias
- Preserving democratic processes and values

All these dimensions are examples of how Digital Sovereignty may impact individuals. Therefore, both states and private and public organisations should determine how Digital Sovereignty, in the stakes and dimensions applicable to them, intersect with the interest of individuals, their rights, needs and expectations and how to adapt their activities/behaviours accordingly.

Individuals are present within cyberspace and thus are fully concerned by self-determination in digital ecosystem.

Individuals buy digital goods, use digital services and participate in digital communities. In the near future, they may spend more and more time in cyberspace, for instance in metaverse, working as well as living part of their private life there.

With regard to the use of personal data in a metaverse environment, the amount of biometrically-inferred data required to operate services offered, will be very high and will largely exceed, for example, current data volumes used for user-profiling. This implies additional challenges from a self-determination perspective.

Since Digital Sovereignty is based on the understanding of interdependencies, and/or legitimised via external factors or sources of influences, which can include potential threats, it is crucial for individuals to be empowered to understand these risks, to learn how to manage them and to benefit from mechanisms like digital integrity to protect themselves in this ecosystem. This implies that information and transparency alone will not be sufficient to break the asymmetry. of information and knowledge.

Therefore, standardisation should benefit individuals by shaping the behaviour of private and public organizations (including countries and regulators) in cyberspace respecting the Digital Sovereignty of individuals.

5.1.3 Specific dimension of the fifth principle

The fifth principle, already identified in 4.2, implies standards in the domain of Digital Sovereignty to take a humanist approach, based on human rights and principle to ensure, for example, human solidarity and inclusion, freedom of choice, participation in the digital public space, safety and security and empowerment, human well-being, self-determination and sustainability, and, more in general, to guarantee self-determination and digital integrity.

In the European Union, this principle is directly supported by the fundamental values, rights and principles referenced in the 2022 EU Declaration on Digital Rights and Principles, and the EU Charter of Fundamental Rights.

5.1.4 Rights and expectations

In the digital age, individuals expect both from public and private organizations that their rights are respected and extended where necessary to strengthen their right to self-determination. Standardization should thus benefit individuals and be supporting their digital rights, needs and well-being.

Standards related to Digital Sovereignty thus should enable individuals to understand the digital environment in which they are involved (i.e. requirements of intelligibility and transparency), as well as to protect their rights and well-being enshrined in the Digital Sovereignty (i.e. requirement of effectiveness).

Digital Sovereignty supporting standards should lay down mechanisms, techniques and/or objectives, to be implemented by states and organizations, which support individuals' rights and their enforcement (including remedies schemes in case of harm), their well-being, their needs and expectations, their free will, their self-determination and that respect their digital integrity[3].This approach will allow individuals to freely make decisions and act in a self-determined way, and should be respected at all times in any digital ecosystem.

[3] Examples of such standards already exist, for example in the IEEE 7000 series of standards, such as IEEE 7010 for Well-being Metrics, or IEEE 2089 Standard for Age Appropriate Digital Services Framework.

5.2 Countries

5.2.1 General

Although in the context of the 1945 United Nations Charter[4] sovereignty is spoken of as a principle of sovereign equality among state members with an implied admission of territorial integrity and political independence, in the context of this document, sovereignty is considered an ability with different characteristics that could lead to technical specifications and recommendations.

Sovereign states are expected to independently make their own risks and opportunities analysis, and accordingly independently make decisions or take actions, considering their core set of values, principles, interests, and goals.

In a globalized and networked economy, no country is fully independent. Some degrees of dependency should be considered with a focus on major and vital interests, based on, but not limited to, the rule of law, a core set of values, principles, interests, and goals.

When applied to digital resources, sovereignty is called Digital Sovereignty and includes a strategy to protect vital digital resources.

From a country perspective, Digital Sovereignty implies a strategic autonomy policy which relates to its willingness and readiness to protect its autonomy, to protect its values and principles, and to pursue its interests and goals, notwithstanding the need to interoperate.

In order to achieve strategic autonomy of digital resources, a country shall be aware of its digital dependencies and potential threats and influences. Eventually, a risk identification and assessment process may be conducted, followed by the mitigation of the identified risks.

For a given country, the approach and implications of Digital Sovereignty will depend on context, regime, laws, policies, etc. Digital Sovereignty is always understood in a context where economic actors, other countries and jurisdictions, and other stakeholders may have an influence or impact on its Digital Sovereignty. Digital Sovereignty shall be implemented in compliance with a human-centered approach, following the fifth principle laid down above.

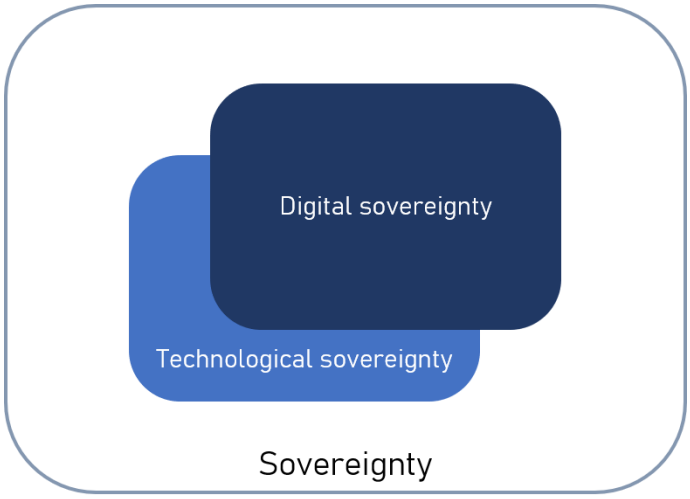
5.2.2 Associated concepts

5.2.2.1 Technological sovereignty

As the notion of technological sovereignty is also used in the context of digital resources, a representation of the relationship between technological and Digital Sovereignty is proposed:

[4] *UN charter:*

- *article 2.1: The Organization is based on the principle of the sovereign equality of all its Members.*
- *article 2.4: All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*



Where:

- Sovereignty is the ability of a country to autonomously analyse (understand/assess a situation), decide and act accordingly (those lead to the notions of autonomy of assessment, autonomy of decision, autonomy of action with a transverse notion of autonomy of governance),
- Digital Sovereignty is the ability to perform or support a function based on digital resources which include but are not limited to, data, information, software, processes, digital knowledge, human resources, hardware, digital infrastructure, engineering methods and tools
- Technological sovereignty and Digital Sovereignty, while strongly overlapping (on hardware, infrastructure, engineering methods and tools) differ by the facts that:
  - Technological sovereignty includes non-digital technology (mechanical technology…)
  - Technological sovereignty does not include data, information and human resources

5.2.2.2 Strategic autonomy

Terms like "autonomy", "self-determination" and "freedom" are used sometimes indifferently and usually refer to the same needs of some level of "interdependence" in choosing paths.

For states, the term "autonomy" is largely used and the notion of strategic autonomy that goes along indicates a focus on important and potentially vital elements of autonomy.

Strategic autonomy can be seen as the willingness and readiness of a country to protect its sovereignty from sources of risks with impacts on resilience. It implies foresight analysis of potential dependencies, future threats, future crisis, and the development of mitigation strategies.

Most states aim at developing an open strategic autonomy policy. Such policy excludes market protectionism. Instead, it should foster the emergence of fair, clear and open rules for entering a market and for interacting with out-of-country entities, with the purpose to serve the countries' values, principles, and interests.

5.2.3 Stakeholders

As "Digital Sovereignty" and "strategic autonomy" are the keystones of public life and trust, the list of actors and stakeholders is extensive and includes:

- individuals

- economic actors, businesses
- governmental organizations
- non-governmental organizations, associations
- other countries
- social partners

5.2.4 Digital Sovereignty governance and risk management

Within a country (or group of countries), the governing body sets directions for its policies and public actions. Digital Sovereignty is a relevant topic to be driven by policies and regulations, so that the country can consistently address and manage dependencies and threats it may face.

From a state perspective, there can be many stakes or dimensions for which Digital Sovereignty will be a factor, such as:

- desired level of economic opportunities, societal benefit
- protection of critical supply chain
- critical infrastructure
- resilience
- independence vis-à-vis stakeholder X or digital resource Y
- investments (foreign) dependency
- protection of democratic processes
- values (e.g. freedom of speech)

Dependencies, threats or influences on digital resources can impact and affect national/governmental interests, including people and organizations. Potential impacts are on:

- political stability and democratic processes (e.g. manipulation through fake news)
- principles and values (e.g. non-discrimination, freedom of information and expression, autonomous decision-making…
- economic prosperity and cultural identity

A state, an association of states or a public authority can among other options also take a risk-based approach in pursuing its objectives related to Digital Sovereignty.

Therefore, in the context of Digital Sovereignty, a state may consider:

- its dependencies on digital resources, including, but not limited to, software, AI, data, algorithms, infrastructure, engineering tools, …
- the threats or influences targeting the digital resources as listed previously,
- the threats or influences targeting individuals and organizations under the state jurisdiction, while using digital means.

By developing a risk-based strategy covering, but not limited to, identification, assessment, monitoring of dependencies and threats, anticipation, adaptation, recovering, protection, intervention, a country may consider itself strategically autonomous and digitally sovereign.

A state can also raise Digital Sovereignty objectives awareness among citizens and organizations. Under a social responsibilities framework, organizations can indeed contribute to a state Digital Sovereignty and strategic autonomy while setting up policies and taking actions related to a state digital resources, and related digital capabilities.

In that context, standards may play a role by supporting organizations in their contribution to a state's Digital Sovereignty objectives.

5.3 Organizations

Within an organization, the governing body sets directions for its governance and policies. Digital Sovereignty is a relevant topic to be driven by governance and policies, so that the organization can consistently address and manage its dependencies.

For a given organization, the approach and implications of Digital Sovereignty will depend on the context of the organization, whatever its type or size. The organization whose Digital Sovereignty is valued, is always in a context where other stakeholders may have an influence or impact on its objectives.

Stakeholders can include (but are not limited to):
Customers

- regulators
- governmental organizations
- competitors
- providers
- individuals towards who the organization has responsibilities / impact on Persons under the control of the organization

The relationships between the organization and the other stakeholders are essential for the description of the context, and can be of diverse types: regulatory commitments, commercial, contractual, etc.

Between stakeholders, there can be many stakes or dimensions for which Digital Sovereignty will be a factor, such as the following examples:

- desired level of value extraction, economic opportunities, social benefit
- protection of IP
- protection of supply chain
- critical infrastructure
- resilience
- contractual obligations… e.g. the ability to operate system xy for purposes of …
- independence vis-à-vis stakeholder X or resource Y
- protection from vendor lock in
- investments (foreign) dependency
- protection of democratic processes
- values (e.g. speech freedom …)

There can be many other elements relevant to the context analysis with respect to Digital Sovereignty, up to the organization to identify including the impact of the competent jurisdictions (territoriality, extra-territoriality, cross-border regulation, etc.).

One of the first necessary steps is to understand the goals and objectives of the organization, which can be indirectly or directly linked to digital capabilities and Digital Sovereignty. The organizational objectives then determine what digital assets and digital capabilities are required to enable or support the achievement of those objectives. Some objectives will depend entirely on digital capabilities, others will just be supported by them.

For example, for an organization manufacturing tangible product, the internal network can be an important digital capability, but maybe not as important as the digital capabilities to support material management, new design innovations and testing through simulations. In this case, the Digital Sovereignty objectives will be higher for all digital capabilities which are directly impacting the organization's core objectives, than for the digital capabilities which do not constitute a differentiating factor for the organization or any of its stakeholders.

Thus, the Digital Sovereignty objectives depend, for each digital capability, on the overall organization's objectives and on the impact of stakeholders.

Digital Sovereignty for organizations shall be implemented in compliance with a human-centered approach, following the fifth principle laid down above in clause 4.2.

6. Reasons for developing standards supporting Digital Sovereignty

6.1 Impact on individuals

Standardization supporting Digital Sovereignty will benefit individuals and civil society as a whole.

States and organizations should develop and implement technologies, based on standards and policies, to ensure a holistic approach to Digital Sovereignty for individuals. Such approach should allow individuals to freely make decisions and act in a self-determined manner in any digital ecosystem.

Without putting any expectations or duties on individuals, Digital Sovereignty standards should help individuals to understand the digital environment in which they are involved (i.e. requirements of intelligibility and transparency), as well as to know and/or exercise their rights enshrined in the Digital Sovereignty (i.e. requirement of effectiveness).

Sometimes, an organization's digital capabilities or policies can have impacts on individuals, in which case the individuals are to be considered stakeholders.

This is the case, for example, if digital capabilities or policies are impacting:

- personal data
- automated decision making, systems making recommendations, etc.
- continuity of social life, businesses, and administration
- fundamental rights (e.g. freedom of speech)
- free flow of information
- data and information manipulation

These are just examples and are not meant to be an exhaustive list for types of impact.

Such impacts on individuals, once evaluated, are an input to the risk Digital Sovereignty management process.

6.2 Societal impact

Digital Sovereignty and strategic autonomy are essential as they are the keystones of an eco-system of trust while strongly contributing to the confidence of organizations and citizens in the ability of any public or private entity to protect their interests.

By contrast, a lack of Digital Sovereignty and strategic autonomy, may lead individuals and organizations to distrust public and private authorities which are exhibiting neither long term situation assessment nor willingness to anticipate.

At its extreme, this situation, where organizations and individuals do not feel protected against threats, influences, and overdue dependencies may prove to be a threat on the values and principles that cement a community, a threat to the economy and a threat to a chosen way of life. This could also lead to the exclusion of individuals from accessing cyberspace, an important domain of human endeavour in the 21st century.

Digital capabilities impact on society and other stakeholders which should be considered during Digital Sovereignty risk managements process are:

- impact on democracy
- impact on values and principles (e.g. speech freedom …)
- impact on economic opportunities
- impact on economic value (for private organizations)

- impact on social benefit
- impact on societal resilience

7. Risk management

7.1 Risk based approach

Risk management[5] is a fundamental concept in many areas as diverse as finance, medical devices, safety. In the digital area, it is the foundation of information security.

Risk management is also essential for Digital Sovereignty as an organization's interest is also to manage risks related to its Digital Sovereignty objectives (dependability, indispensability, resilience…).

A risk-based approach may include either formal or non-formal activities. Furthermore, it should be part of the general social responsibility of an organization to include in its analysis the interests of all stakeholders. Hence, private organizations should consider the Digital Sovereignty expectations and needs of individuals (privacy, self-determination…) as well as the expectations and needs of states (strategic autonomy).

Different types of action can be developed to treat the risks associated to threats and undue digital dependencies and influences. While most actions and protection measures will be in the pure "cyberspace", some mitigation actions shall be envisioned outside cyberspace: regulation, policy, organizational, physical measures, or even proper human behaviour and human management.

Therefore, in order to properly build and assess the effectiveness and comprehensiveness of a risk mitigation strategy, whereas dealing with complexity, different "Digital Sovereignty dimensions" of this strategy should be explored.

Those "dimensions" may include, but are not limited to:

- Social/organization considerations
- Human considerations
- Software and data considerations
- Hardware and components considerations
- Geographical and jurisdiction considerations
- Cyber-identity considerations

Note: The "cyber identity" dimension allows the interconnection of entities, assets, digital constituents and contains the digital identities necessary for intra- and inter-dimension exchanges.

In order to develop its dependencies and threats treatment strategy, an entity needs to identify whether given elements fall under extra-territorial jurisdiction and control.

The approach to make possible Digital Sovereignty at the individual scale should result in preserving the individual interests protection and self-determination within the respect of the applicable jurisdictions.

Digital Sovereignty is not about stating what individuals should do or think , but it is, from the perspective of an organization to:

[5] ISO 31000 provides principles, a framework and a process for managing risk, that can be used by any organization regardless of its size, activity or sector.

- determine how Digital Sovereignty as analysed by the organization, in terms of context risks, can affect the fulfilment of obligations towards individuals and/or their interest and needs
- treat the related risks as appropriate.

Examples of actions that could be envision by entities in each dimension:

- Social/organization dimension: Development of international, national or local digital policy and regulation. Development of standards and best practices;
- Human dimension: Development of digital education. Training on best practices. Development of ethical values;
- Software and dimension: Development of trustworthiness characteristics and standards in cyberspace;
- Hardware and components dimension: Development of a multi-sourcing strategy;
- Geographical dimension: Deployment of cloud-based infrastructures on controlled physical locations;
- Cyber-identity dimension: Development of a trusted digital identification system covering entities, data, software, assets, digital commons.

7.2 Risk assessment

In order to pursue its mission interests and goals, in accordance with its values and principles and the values, rights and principles of the countries in which the organization operates (For Europe, see https://ec.europa.eu/component-library/eu/about/eu-values/, Article 2 of the treaty of Lisbon and European Declaration on European Digital Rights[6] for European values), it is necessary that the organization assesses the risks related to Digital Sovereignty.

The first step for risk assessment is to analyze digital capabilities, dependencies, and potential threats and influences.

When assessing the risks, the following elements can be considered:

- digital dependencies such as software, data, algorithms, AI systems, infrastructure, engineering tools
  - the threats which could affect the above elements
  - the threats related to individuals, organizations, and countries in their use of digital capabilities (i.e. their digital skills, their digital representation). Besides threats identification, the potential impacts can also be a factor of risk assessment as well as any estimation or measure of their frequency of occurrence.

7.3 Risk treatment

The treatment of risks related to digital dependencies, to threats and influences or likelihood/frequency of events, can be based on a set of policies, measures, involving human resources, digital capabilities, infrastructure and physical resources.

The treatment of risks can be related to dimensions including, but not limited to, resilience, indispensability, dispensability, protection, interoperability, openness

By developing a risk management strategy covering, but not limited to, identification, assessment, monitoring of dependencies, threats and influences and related risks, anticipation, adaptation,

[6] https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles

recovering, protection, intervention, an organization may consider itself strategically autonomous and digitally sovereign.

For an organization, its governing body can set the high-level principles from which organizational and technical measures can be derived (metrics, actions for staff, etc.).

8. Implications on standardization

8.1 Preliminary considerations on standardization organizations

It is recommended that standardization organizations observe the principles of Digital Sovereignty and ensure:

- awareness of the standardization participants' interests and goals. In that regard, transparency is essential,
- management of undue influences and dependencies in standardization,
- management of standardization actors that do not exhibit social responsibilities behaviours,
- sound organizational integrity so that standards are chosen on merit.

There are also concerns regarding the time it takes to develop standards. Indeed, in a fast technological pace, it is essential that standards are developed in due time, and do not lag behind market developments, in order to limit potential risks related to Digital Sovereignty. .

8.2 Standardization objectives

Digital Sovereignty supporting standards should support any organizations, whether public or private, that aim to manage its dependencies and to protect its interests. Furthermore, those standards should have a holistic dimension and consider the interests of individuals, organizations, and states.

Digital Sovereignty supporting standards could include objectives such as:

- Protection of both personal and non-personal data
- Digital identity
- Resilience
- Cybersecurity
- Trustworthiness
- Fairness in (private/public) contractual relationships
- Fairness in information flows
- Protection of vulnerable persons (such as children)
- Compliance with key-aspects of national laws (e.g. tax law, data protection legislation, environmental requirements)

Standards are already instrumental for sovereignty as they can be used to support compliance with regulation. Still, Digital Sovereignty supporting standards new objectives may be to also provide regulation with appropriate technical frameworks, concepts, and terminology.

8.3 Ethical assessment

Digital Sovereignty supporting standards must include assessment of ethical and societal elements, including human well-being. Engineers have always met basic ethical standards concerning safety, security and functionality. However, issues related to, for example, justice, bias, addiction, privacy, and

787 indirect societal harms, were traditionally considered out of scope. Today, it is no longer acceptable that
788 technology is blindly released into the world, leaving others to deal with the consequences.[7]

789 For an ethical assessment, tools like ethical standards, ethical guidelines and ethical certification marks
790 should be available, and always backed up with a fundamental rights evaluation in the design phase.

791 For standards development in general and in the area of Digital Sovereignty in particular, this implies the
792 need for (a) standard development work to include explicitly ethical and societal 'safety'; and (b)
793 standard development work uniquely devoted to create a portfolio of ethical standards. Ideally, like with
794 product safety, a conformity mark should be developed.

795 It should be noted that such developments are already underway[8].

796 As a side note it is important to realize that ethical standards work will require the involvement of experts
797 traditionally not working in this field, from disciplines other than technology. Examples are consumer
798 organizations, psychologists, sociologists, human right lawyers, trade unions, NGOs. This needs to be
799 raised among others in the current EU assessment of the governance structure of (national) standard
800 bodies.

801

802 8.4 Potential standardization items

803 In the course of the workshop, a certain number of potential "Digital Sovereignty" related standardization
804 items have been identified:

805 - Governance of digital commons
806 - Governance of metaverse
807 - Metaverse interoperability
808 - Digital identity in cyberspace
809 - Data traceability, tagging and data ownership (including for individuals)
810 - Data connectors/interfaces, and interoperability
811 - Physical, and digital local controls of data
812 - Overview concept and terminology on cyberspace jurisdiction
813 - Overview concept and terminology on avatars
814 - Law enforcement support

815 8.5 Metaverse

816 Etymologically, the word metaverse is a combination of 'Meta', the Greek prefix for beyond, across or
817 after, and universe. The term is typically used to describe the concept of a future iteration of the internet,
818 made up of persistent, shared, 3D virtual spaces linked to a perceived virtual universe.

819 The metaverse is often presented as an extended reality artefact that includes and emphasizes the social
820 element of immersion by allowing multiple users to interact in a virtual or augmented environment.
821 Metaverse standardisation work is currently still in an early stage[9]. There is also a lack of clear
822 governance standards. The latter is very important, as metaverse developments may magnify the social

[7] Responsible AI – Two frameworks for Ethical Design Practice, Dorian Peters, Karina Vold, Diana Robinson, and Rafael A. Calvo, in: IEEE Transactions on Technology and Society, Vol.1, No.1, March 2020.

[8] IEEE CertifAIed

[9] See, for example, within IEEE the Consumer Technology Society / Metaverse Standards Committee (CTS/MSC) and the AR/VR Advisory Board (https://standards.ieee.org/industry-connections/vrar-advisory-board/)

823 impact of online echo chambers or digitally alienating spaces.For example, corruption, non-ethical
824 behaviors, and the creation of dependencies, influences in the metaverse will lead to sovereignty and
825 trustworthiness issues and to the need for governance and for a data jurisdiction.

826 Trustworthiness characteristics in metaverse could be defined and may cover expectations like
827 transparency, inclusiveness, auditability, ethical behaviors, law enforcement.

828 Further work should be carried out in this area, to provide specific guidance to the standardisation efforts
829 in the area of metaverse. In particular, governance of metaverse in the context of Digital Sovereignty is
830 an issue that should be consider as soon as possible on top of the general guidance provided in this
831 document.

832 ## 8.6 Avatars

833 The term avatar is usually used to refer to the sets of information, or digital characters[10] that represent
834 the inhabitants of virtual worlds, or in some cases a digital replica of a physical asset[11]. The avatar, as a
835 projective identity, is the product of the player's interpretation and, as a techno semiotic system, is
836 conditioned by the interface used. However, the current notion of avatar goes further: it includes
837 meanings that go beyond its traditional definition as a "character manipulated by the player"[12]. The
838 avatar can therefore be “disconnected” from the (verifiable) realities of the physical world and thus
839 mislead others.

840 The avatar can be changed at any time, so it is a digital extension of the person, although an avatar can
841 look exactly like the user or be completely different.

842 A clarification of the concept of avatar is essential, in particular with regard to its uniqueness or plurality,
843 its potential link to a legal entity or a digital identity, and what this may imply in terms of liability.

844 Since it is a digital extension of the person, an individual should be able to have an avatar, times the
845 number of accounts created (pluralities of possible avatars).

846 Therefore, in the context of a natural person, the avatar as a digital extension of this person, or even of a
847 object, could be linked to a digital identity and a digital jurisdiction. Furthermore, in some types of
848 avatars, a continuum between avatars, individuals’ Digital Sovereignty, and individuals’ liability for the
849 behaviour of their avatars should be envisioned. The same should apply for legal persons and their
850 avatars, since a private company or a state may also use a digital representation of themselves.

851 A standard on the concept and terminology of avatars (with a typology of avatars according to their role
852 and real-world impacts), including the potential link with digital identity) is essential, since such digital
853 representation may be used in the exercise of Digital Sovereignty by any entity.

854

[10] ISO/IEC 27032:2012 Guidelines for cybersecurity

Avatar: representation of a person participating in Cyberspace

Note 1 to entry: An avatar can also be referred to as the person's alter ego.

Note 2 to entry: An avatar can also be seen as an "object" representing the embodiment of the user.

[11] ISO/TR 24464:2020 Visualization elements of digital twins: Avatar: digital replica of a physical asset

[12] Source: https://www.bercynumerique.finances.gouv.fr/l-information-en-continu/les avatars-your-digital-extension-in-the-metaverse

9. Bibliography

ISO 31000:2018 Risk management — Guidelines

ISO 37000:2021 Governance of organizations — Guidance

IEEE 7010-2020 Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-being

Official Journal of the European Union, 26.10.2012, C326 - Fundamental rights: Fundamental rights in the European Union are defined by the UE charter of fundamental rights of the European Union.

AFNOR, Digital Territory, A joint exploratory concept, 2020

S. Conchon, J. Caire, The Security Continuum, presented at Lambda-Mu Conference 2021

S. Conchon, J. Caire, Meta-Sovereignty, presented at Lambda-Mu Conference 2022

Annex A

A.1 Compilation of use cases for Digital Sovereignty

Use case 1: "Tools dependency – standards openness"

Description of the use case:

Tools for processing data and developing trustworthy AI are essential. The cost of developing and maintaining those tools is incredibly important, especially for Industrial AI with safety and business critical issues.

Note: in a process flow, AI tools will not be limited to software but will include mapping AI algorithms on specific hardware.

The integration and comprehensiveness of the set of AI tools will be paramount to any enterprise and one of their biggest value-chain assets. Therefore, a resilient "AI toolbox" is needed. As the toolbox is going to be a mixture of different building blocks from different origin (nations, industry), a dependency risk analysis shall be conducted.

Still, the induced dependency by each of the building blocks may be governed by more than just free market principles, as shown in ITAR.

Challenge to be solved:

Making sure that "essential bricks" of the "AI toolbox" can be replaced in order to avoid unnecessary dependencies coming from either state or commercial decisions.

Potential standardization approach:

Identify pivotal open interoperability standards between "essential bricks" to avoid too much dependencies.

Use case 2: "A metaverse hosted in the cloud"

Description of the use case:

The metaverse concept aims at providing a new unique cyber experience where users will be immersed in virtual spaces, offering new experiences and new opportunities.

The metaverse will most likely replicate mechanisms, issues, and behaviours of the physical world, for example:

- Users will pay fees to access to the metaverse and/or fees to access to services,
- Users will have to reveal personal information/data to access the metaverse and its services,
- Users, with respect to certain services, will be required to reveal high volumes of biometrically inferred data,
- Crypto money will be developed and be the base for transactions in metaverse,
- Virtual services, including advertisement, virtual stores, and virtual assets will be monetized with legal ownership issues,
- Influence and subliminal manipulations that may be impossible for an individual to recognize, may develop,
- Fake news, conspiracy theories and scam may proliferate,

As an illustration of the looming issues, sexual harassment has already been reported in the metaverse[13] .

For an entity, sovereignty implies the possibility to establish rules, to enforce them while protecting its values and principles (and its citizens). Therefore, traceability, identification and accountability means should be available, as well as clear determination of the competent jurisdiction.

Metaverse governance issues:

For a nation, the metaverse connection to a "jurisdiction" will need clarification and technical standards to support regulation. It will also require transparency on the beneficial owner of the accounts holders (cryptocurrencies account holder, bots, avatars, digital twins holders, NFT, tokens holders). For example, the NFT protocol will enable the transfer of ownership rights. This authentication certificate which is based on blockchain technology hides the identity of the beneficial owners of the transaction. The decentralised structure of the blockchain makes the identification of the competent jurisdiction delicate. In criminal procedures, a legal basis is required to punish infractions which take place in the metaverse.

Potential standardization approach:

Develop traceability, identification, and accountability standards to ensure that values and principles of any entity from a given jurisdiction are protected within "metaverse" based on the protection laid down by this jurisdiction. Transparency of beneficial holders of digital accounts (bots, avatars, NFT, Digital Twins, Tokens, Cryptocurrencies, etc) on metaverse is required to identify the competent jurisdiction.

[13] https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/

Use case 3: "Integrity and confidentiality of data produced by a robot"

Description of the use case:

A robot, and by extension any automated system, may send digital data (mission data, sensor data...) to unauthorised external actors: the complexity of the system, purchased off the shelf, prevents the qualification of its software according to sovereignty criteria. The cost of this "sovereignty" qualification, which would have to be carried out each time the software is updated, and the associated processes prove to be a deterrent.

In France, this generic and multi-sectoral case has already been encountered in the case of the use of foreign aerial drones by the gendarmerie and police services for inspection and surveillance of sensitive sites. Several cybersecurity studies have shown that the aerial drones used systematically export (and continue to export) flight data and metadata to foreign servers. These data exfiltrations are carried out in a stealthy manner by obfuscated code in the UAV hardware (cf. SYNACKTIV studies, the "Berthier-Vuillard" report submitted to the Ministry of the Armed Forces, the Ministry of the Interior, the SGDSN and the ANSSI; Volume 2 of the JM MIS parliamentary report submitted to the Prime Minister; and the SALA-Berthier 95-page contribution on a Senate hearing on robotics to the security forces.

One of the latest SYNACKTIV studies on the exfiltration of flight data from aerial drones: https://www.synacktiv.com/en/publications/dji-android-go-4-application-securityanalysis.html

More and more household devices get connected to the Internet. Typical use cases are:

- Control of the device via a smartphone
- Remote update of the software in the device

Typical devices are:

- Vacuum cleaners, that more or less autonomously navigate through the household
- Refrigerators, that support their owners with management of the stored goods
- Cooking devices like cooking machines or stoves, that can be controlled remotely, e.g. preheated or starting to prepare a morning coffee, while their owners are still sleeping
- Toys like dolls, that talk with children using microphones and remote AI or robots with cameras
- Home surveillance systems
- Health devices
- Smart meters

In the case of the use of robots via applications on phones (Android...), the digital data captured can also be that of the phone.

Challenge to be solved:

Data leakage is against the law and impacts the sovereignty of states, yet these practices continue and are increasingly difficult to detect and sanction. Non-legal measures must therefore be put in place to ensure that data produced by a robot is not accessible.

For states, the issue of security and confidentiality of digital data is linked to internal security.

For companies or individuals, the issue of personal and business data management and confidentiality is a matter of cybersecurity, privacy, and trust.

Possible threat and protection dimension of misuse are:

Confidentiality:

- Vacuum cleaners learn about the layout of the house and the household and their sensors can detect and identify valuable goods
- Refrigerators can report the goods stored and the ways these goods are used, from which habits and lifestyle can be derived, also potentially unhealthy behaviour like misuse of alcohol or sugar
- Cooking devices can report the goods cooked and the times they are used, from which habits and lifestyle can be derived, also potentially unhealthy behaviour like unhealthy eating habits
- Toys can with their microphones overhear communication of children and other people
- Camera's from the home security system will store biometric data from visitors
- Health devices will provide insights into (un)healthy behaviour
- Smart meters will provide insights into living patterns and can be monitored for unlawful purposes

Integrity:

- Vacuum cleaners can be manipulated to clean less perfect than wished or to subtly spread the dust they collected to trigger allergies
- Refrigerators can subtly reduce their cooling function for some time to make food spoil and create stress or to even cause food poisoning by letting food spoil unnoticed
- Cooking devices can act similar to refrigerators but also overheat and cause fires
- Toys can issue sounds that openly (loud noise) or subtly (undertone frequencies) create stress. They may also be used as communication devices to make children behave against their own interest or even prepare a cyber grooming
- Camera's can be manipulated to allow access to unwanted persons
- Health devices can provide contradictory recommendations causing harm
- Smart meters can be manipulated for unlawful purposes
- IoT enabled devices including home security and air-conditioning can be remotely used for abuse and harassement.

Above activities can not only be labelled as surveillance at the state, industrial and individual level, but are a threat to democratic values. On top of that at the individual level, the right to self-determination as enshrined in European privacy regulation is heavily impacted by above developments.

Potential standardization approach:

Several options could be considered:

At the hardware level: integration of a "sovereign module" into the systems

- Specification of physical, electrical and software interfaces
- Specification of local controls
- Specification of functions, that cannot or not completely be controlled by software, e.g. mechanical protections against overheating

985 At the data level:

986 • Local and locally controlled storage of data
987 • Local and locally controlled processing of data
988 • Local over-ride of remotely accessible controls, and logging of remote accesses
989 • Encryption and/or tagging of data
990 • Data traceability
991 • Blockchain

992

993

Use case 4: "Territorial Multi-sectorial data space"[14]

Description of the use case:

The project "Territorial Multi-sectorial Data Space" (TMSDS) aims at creating a range of services allowing the emergence of innovative and trust-based uses of digital resources, on a given territory. It will thus be able to:

- Equip public and private organizations as well as citizens to be functioning and interoperable with a set of existing infrastructures;
- Diffuse good habits and uses in regard to data sharing and processing;
- Promote trustworthy and/or public-interest initiatives;
- Coordinate public and private organizations with suitable infrastructures at a national or European level (Data Hub, European Data Space, Health Data Hub…) and with other territories.

This project is subdivided in three main modules. The first module consists of a digital citizen portal aiming at empowering citizens regarding data uses. The second module includes a updated directory contact for actors and projects of the data economic environment, as well as a collaborative contribution platform for digital projects. Finally, the third module will enable the display of metadata and the processing of data through a meta-catalogue and a third party sharing system.

Although each module is independent, they all work together to allow the needs of the actors involved to be fully met. .

Challenges to be addressed:

Citizen portal:

- The identification of individuals
- The adaptation of this component to self-data and even metaverse services
- The establishment of altruistic organizations
- The possibility to allow the creation of data trusts to centralize (via a trusted intermediary for both citizens and service providers) the management of consents and the collection of citizen data for a multitude of services. This would limit the digital load and create a real dashboard for citizens.[15]
- The definition of selection criteria to identify "trusted", "sovereign" alternative solutions that can be recommended to citizens and organizations.
- The definition and the assurance of guarantees given by service providers to ensure the respect of citizens' data and therefore trust.

Project Forum:

- The creation of innovative and alternative business models to value collaboration, co-opetition and co-ownership as well as the sharing and reuse of new knowledge.

[14] Based on Ekitia's work

[15] Alternatives for individuals exist, i.e. to allow individuals to control their own data without making use of a trusted service

- Meta-catalogue:
  - The creation of a sovereign, decentralized, and open source case of cataloguing, meta-cataloguing, sharing, and valuing new knowledge.
  - The enablement of the interoperability of such a case with the infrastructures and resources of the actors of the ecosystem.
  - The enablement of the definition and enforcement by design of the governance rules (norms, standards), so other data spaces can be infinitely created and enabled to complete these governance rules (digital commons)

Potential standardization approach:

Regarding construction and infrastructure:

- Interoperability
- Replicability
- Security

Regarding the functioning of the different elements:

- Blockchain
- Decentralization
- Open source
- Interoperability
- Governance via a token
- Ownership of the data and knowledge generated

Regarding the use of each of the modules:

- Indentification of individuals