STUDY

Requested by the IMCO committee

European Parliament

New technologies and new digital solutions for improved safety of products on the internal market

Tackling planned obsolescence practices, barriers to trade for recycled products and enhancing consumer information

Policy Department for Economic, Scientific and Quality of Life Policies
Directorate-General for Internal Policies
Authors: Gaëtan COATANROCH, Reda NAUSEDAITE, Morgane VEILLET LAVALLEE, Ivette OOMENS, Maarten BOTTERMAN, Jonathan CAVE, Elmar CLOOSTERMAN, Clara THEBERT, Frank ALLEWELDT

EN

PE 703.348 - June 2022

New technologies and new digital solutions for improved safety of products on the internal market

Tackling planned obsolescence practices, barriers to trade for recycled products and enhancing consumer information

Abstract

The General Product Safety Directive is a cornerstone of the EU product safety legislative framework. Issues and emerging trends have however impacted the effectiveness of the current Directive. This study examines how new technologies and digital solutions can help improve consumers' awareness, while also guaranteeing a better safety of the products placed on the Single Market. The study formulates recommendations that provide a framework for the better alignment of existing legislation on product safety and digital services, as well as the European Community sustainability objectives. This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies for the committee on Internal Market and Consumer Protection (IMCO).

This document was requested by the European Parliament's committee on the Internal Market and Consumer Protection

AUTHORS

Gaëtan COATANROCH, Technopolis
Reda NAUSEDAITE, Technopolis
Morgane VEILLET LAVALLEE, Technopolis
Ivette OOMENS, Technopolis
Maarten BOTTERMAN, GNKS Consult
Jonathan CAVE, GNKS Consult
Elmar CLOOSTERMAN, Technopolis
Clara THEBERT, Technopolis
Frank ALLEWELDT, Civic Consulting (second reader)

ADMINISTRATOR RESPONSIBLE

Barbara MARTINELLO

EDITORIAL ASSISTANT

Mina DRAGANSKA

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for email alert updates, please write to:
Policy Department for Economic, Scientific and Quality of Life Policies
European Parliament
L-2929 - Luxembourg
Email: http://www.europarl.europa.eu/supporting-analyses

Manuscript completed: June 2022
Date of publication: June 2022

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

For citation purposes, the publication should be referenced as: Technopolis, GNKS Consult 2022, *New technologies and new digital solutions for improved safety of products on the internal market*, Publication for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

CONTENTS

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
ANSSI	French National Cyber Security Agency (Agence Nationale de la Sécurité des Systèmes d'information)
BAuA	German Federal Institute for Occupational Safety and Health (Bundesanstalt für Arbeitsschutz und Arbeitsmedizin)
BSI	German Federal Cyber Security Authority (Bundesamt für Sicherheit in der Informationstechnik)
BYOD	Bring Your Own Device
CC	Common Criteria
CEN	The European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CoC	Code of Conduct
CSIF	Cloud Select Industry Group
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DSDA	Digital Services Act
DPP	Digital Product Passport
EC	European Commission
ENISA	European Union Agency for Cyber Security
EU	European Union
ESCloud	European Secure Cloud
ESO	European Standardisation Organisation
ETSI	European Telecommunications Standards Institute
FIPD	Food Imitating Products Directive
GDPR	General Data Protection Regulation

GPSD	General Product Safety Directive
GPSG	German Equipment and Product Safety Act (Geräte- und Produktsicherheitsgesetz)
GPSR	General Product Safety Regulation
GS label	Tested safety label (Geprüfte Sicherheit)
IaaS	Infrastructure-as-a-Service
ICSMS	Information and Communication System on Market Surveillance
ICT	Information and Communications Technology
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IMCO	Committee on the Internal Market and Consumer Protection
IoT	Internet of Things
IPP	Integrated Product Policy
MSA	Market Surveillance Authority
MUD	Manufacturer Usage Description Specification
NFC	Near Field Communication
OECD	Organisation for Economic Co-operation and Development
OJ EU	Official Journal of the European Union
PaaS	Platform-as-a-Service
PCDS	Product Circularity Data Sheet
PII	Personally-identifiable information
ProdSG	German Product Safety Act (Produktsicherheitsgesetz)
PSS model	Product as a Service model
QR Code	Quick Response Code
RAPEX	Rapid Exchange Information System

SaaS	Software-as-a-Service
SMEs	Small and Medium Enterprises
SPI	Sustainable Products Initiative
UN	United Nations
ZLS	Zentralstelle der Länder für Sicherheitstechnik
WTO	World Trade Organisation

EXECUTIVE SUMMARY

Background

Product safety evolves in an uncertain and fast-changing context. The European Consumer Summit 2022 underlined the pre-eminence of sustainability and inclusiveness to the consumer agenda. In the European Union (EU), the General Product Safety Directive (GPSD) plays a major role in regulating product safety in conjunction with other directives and regulations setting up requirements for product safety. The GPSD, which covers all products except for food, pharmaceuticals, and medical devices, is aimed at defining “safe products” and creating common standards among the Member States to ensure the health and safety of consumers in the Single Market. It also assigns responsibilities to producers and distributors, as well as to competent national authorities. As horizontal legislation, non-harmonised consumer products (e.g. bicycles, childcare products) fall directly under its scope and it provides an additional safety net for products for which specific EU regulations exist (e.g., toys, batteries). However, the emergence of new technologies and challenges in a global context raise a series of issues, notably linked to the definitions of “product” and “safety” given by the GPSD, which affect the effectiveness of the current Directive. As a result, the GPSD needs to be adapted, taking into account both novel technological aspects of product safety (such as cyber safety or data privacy), but also existing and upcoming regulations concerning environmental protection. Improving communication with EU consumers by raising their awareness of product safety is also essential for the achievement of full protection: better informed consumers can make better choices, allowing market forces to supplement regulatory requirements and standards as products and technologies evolve. Furthermore, the extent of interaction between the GPSD and other regulations has also increased. For example, products within scope of the GPSD currently include functions relating to privacy (linked to the General Data Protection Regulation (GDPR), contain materials governed by specific waste regulations and/or give rise to cybersecurity aspects regulated under “proper care" regulation.

Aim

This study has been commissioned by the Committee on Internal Market and Consumer Protection (IMCO). It aims to examine how new technologies and digital solutions can help improve the safety of products placed on the Single Market, especially by improving consumers’ access to information and awareness of product safety , while minimising unnecessary administrative burdens, esp. on small and medium-sized enterprises (SMEs). Moreover, the study aims to inform EU policymaking by formulating recommendations to improve the alignment of existing legislation on product safety and digital services, focusing in particular on the proposal for the General Product Safety Regulation (GPSR), while also helping the European Community meet its sustainability objectives.

Key Findings

State of play on new technologies and digital solutions

The emergence of new technologies and digital solutions embedded within products affects product safety. This, in turn, affects consumers, both in their decision-making and product use. How purchasing decisions are made, what consumers buy and how the products are used all influence product safety on the market and in use. Undeniably, new technologies and digital solutions provide unparalleled accessibility to products. Use of new smart connected devices can aid consumer purchasing decisions (e.g., QR codes, Digital Product Passport). They benefit consumers by informing them about standards compliance, but also, even in personalised ways, about the suitability of the product for that consumer's intended use and its compatibility with products the consumer already uses. Technologies employed in conjunction with others may boost traceability along the value chain and offer new opportunities to make products more sustainable: sourcing better materials, improving product design, enhancing processes, and improving reuse, remanufacturing, and recycling.

However, this does not mean that technology should be used simply to maximise communication and transparency of products. The use of multiple interacting technologies and digital solutions raises the issue of product ownership. There is concern about consumers losing agency of their choice due to the complex combined functionalities of different technologies and digital solutions, how these aspects of a product are presented and how consumer consent is asked for. It may no longer be safe to assume that informed consent provides the kind of meaningful consent on which consumer protection regulation relies. New technologies and digital solutions can also blur the lines of responsibility between distributors and producers, with producers and consumers linked via increasingly complex value chains.

The pace and complexity of technological change also fuel obsolescence, which raises several product-safety challenges, mainly relating to continuity of coverage of product safety protection and assurance, the collection and continued availability of data, support for products and liability and other aspects of consumer protection. Rapid and fragmented changes in the technologies used in many modern consumer products lead to unplanned as well as planned obsolescence. This leads to product safety concerns, especially if safety functions are impaired by changes in some component technologies or if the 'stranding' of technologies in obsolete configurations reduces producer incentives to maintain support for safety. In current EU legislation, digital technologies are seldom mentioned as a means to mitigate the problems caused by obsolescence despite their inherent potential to support product design for longevity, facilitate upgrades, increase cooperation along the value chain during product lifetimes and help consumers make more informed purchase, use and disposal decisions..

Finally, a revised GPSD could minimise unnecessary administrative burdens and other direct costs, e.g. by giving standing to common standards and certification and the creation and governance (or direct provision) of central repositories of product characteristics and consumer experiences. Further, the use of new technologies can lead to administrative efficiency gains, as illustrated by the use of AI for dispute resolutions.

International best practices and development across EU Member States

The study mapped standards, certificates and labels that have been developed by individual EU Member States or at EU level. From these mapped practices, a total of seven case studies were selected for detailed examination. Their analysis was supported by examining some of the recent high level international discourse regarding product safety in the digital age.

Analysis of the case studies shows that, in relation to product safety, labels, standards and certificates primarily serve to signal trustworthiness to (potential) consumers of a product and often result in more transparency for both consumers and stakeholders in the value chain. This enables consumers to make more informed choices more quickly. For companies, having a label or certificate increases their relative competitiveness; in particular, international standards give firms better access to wider market opportunities.

The case studies suggest that there are many benefits to the design and implementation of solutions by public entities, but that it is also valuable to adopt bottom-up approaches, especially when developing these practices. Furthermore, effective communication is necessary to promote existing initiatives and market surveillance can be enhanced by leveraging Digital Product Passports (DPPs), which can provide more trust in safety, knowing that it is subject to surveillance, and stronger incentives to improve safety by design. Finally, implementation of a decentralised database benefits both producers and consumers. When considering the development of a common European database, these existing practices could be used as lessons learned.

Recommendations

Proposed policy recommendations to improve EU support of product safety linked to new technologies and digital solutions include the following:

- By means of an EU Observatory, monitor ongoing activities in EU Member States related to product safety, highlighting those involving new technologies and digital solutions. In addition to a structured database of proposals, evaluations and assessments for policies and other initiatives, and a repository of significant cases, recalls and other aspects of product safety implementation, this Observatory should pay particular attention to the evolution of product ownership and the use of digital solutions to handle the associated complexities. This information should be retained in accordance with the FAIR (Findability, Accessibility, Interoperability, and Reuse of digital assets) principles[1];
- Improve transparency, data control and data management: it is recommended that the General Product Safety Regulation be supported by clear, legally reliable and practicable definitions of transparency, information control and information management (clarifying the roles of different actors in the value chain as regards providing and collecting safety-related information);
- Clarify the linkages between the General Product Safety Regulation and other policies affecting or affected by digital product safety and develop suitable guidelines for producers and others in scope of the GPSD;
- Tackle obsolescence from a product safety perspective: introduce minimum specifications to ensure product safety over explicit and evidence-based product lifetimes;
- Introduce automated information exchange: this includes exchange of real-time product and performance information among participants in the value chain (producers, distributors and service providers; between users and producers; and between firms and authorities in scope of the GPSD. This information can help in detecting emerging safety issues, minimising unnecessary administrative burdens, improving the alignment of market competition with product safety, enforcing traceability and monitoring producers' compliance with regulatory requirements;
- Communicate product safety to consumers: define the minimum level, content, methods and frequency of digital communication to be provided to consumers and users, position the EU as a global leader in defining product safety requirements with service providers and ensuring fair access to all consumers;
- Develop a suite of product safety-relevant definitions for new technologies, digital solutions and take a leading role in the development of global standards by ensuring coherent EU-wide legislative, technology-neutral future-proof action, and by supporting industry- and/or consumer-led approaches to developing and enforcing EU-wide standards, certificates and labels; and
- Strengthen product recall with digital technology assistance: ensure greater harmonisation and durable public documentation of recall practices through improved promotion and integration of digital technologies.

[1] The FAIR principles describe how data should be organised to be more easily accessible, understood, interoperable and reused.

1. OBJECTIVES, SCOPE AND METHODOLOGY

1.1. Objectives

This study has been commissioned by the IMCO Committee. It aims to examine how new technologies and digital solutions can help improve the safety of products placed on the Single Market, especially by improving consumers' access to information and awareness, while also minimising unnecessary administrative burdens, especially on SMEs. Moreover, the study aims to inform EU policymaking, by formulating recommendations that provide a framework for the better alignment of existing legislation on product safety and digital services, while also helping the European Community to meet its sustainability objectives.

The specific objectives of the study include:

- Providing an understanding of the potential of new technologies and digital solutions to improve product safety and provide consumers with clear and reliable product information, as well as to present recommendations for updating the GPSD and other Single Market legislation;
- Building on other IMCO Committee studies to clarify how tackling inefficient or counterproductive obsolescence practices and encouraging product sustainability and circularity can promote product safety;
- Identifying best practices in the EU Member States that could be used to develop the EU product safety and compliance legal framework to better promote product safety, as well as consumer safety and awareness;
- Analysing recent developments in the EU Member States and European Commission to formulate a view of relevant future scenarios using current trends, key uncertainties, and weak signals, from the perspective of product safety, consumer protection and consumer information. This includes market surveillance, internal market, and movement of goods; and
- Providing clear overviews, summaries, recommendations and conclusions on proposed reforms, notably the proposal for the GPSR.

1.2. Scope of the study

The study scope focuses on product safety, consumer protection and information to consumers (including market surveillance, internal market, and movement of goods) with consumer information and awareness considered as means to promote product safety. The study also considers the objectives formulated by the 2020 European Green Deal, notably in terms of sustainability, traceability and circularity of products. Geographically, the study includes the EU27, as well as Iceland, Liechtenstein, Norway, and Switzerland. A limited part of the study is dedicated to the impact that new technologies could have on SMEs.

Concerning the technology scope, the study considers the role of governments, businesses, and industries, as well as consumers and users and their interactions with technologies. When referring to new technologies and digital solutions, the investigation team has classified the new technologies as:

- **Artificial Intelligence (AI)**: the simulation of human cognitive and intelligence processes by machines, especially computer systems. It includes expert systems, voice recognition, machine learning and vision, natural language processing (NLP) and the interactions of such machines;
- **Connected products**: these include devices, machines, sensors and networks that make up the Internet of Things (IoT). These are smart, interconnected devices that use multi-directional communication over networks; and
- **Robotics**: technologies that encompass the design, building, implementation, and operation of machines (robots) to perform tasks traditionally done by human beings without further human intervention. Robotics differ from AI in that robotics builds and programmes machines to perform very specific duties; this usually does not require AI.

Digital solutions refers to technologies that enable users to connect to communications networks or facilitate connections among people and machines:

- **Cloud computing**: services and tools for remote data storage and processing, accessible from any suitable device via internet connection to the cloud;
- **Blockchain**: a digitally distributed ledger that uses peer-to-peer networks to store information or data which exists as nodes that are added to the chain;
- **Digital Product Passport (DPP)**: a digital document that provides updated product information through the value chain and product life (origin, composition, repair and disposing);
- **QR codes**: machine readable barcodes allowing the capture, storage and, upon scanning, presentation of information about the products to which the codes are attached; and
- **Near Field Communication (NFC)**: a contactless communication technology that enables device communication between devices in close proximity.

These new technologies and digital solutions are explored throughout the study, mentioning specific examples or instances as required. However, one problematic issue was the classification of software (updates and standalone software), and whether they are categorised as products under the GPSD. There are indeed very few EU Member States whose implementation of the Directive in national legislation refers specifically to software. Such differences create legal uncertainty, as well as an uneven levels of protection for consumers when it comes to software or the products in which they are embedded[2]. This topic, however ambiguous, has been included in the study. Similarly, the question of cyber security is considered for its impact on product safety (notably on connected devices with digital services), even though it is only partially within the scope of the study.

[2] Civic Consulting, 2021, *GPSD Evaluation*. Available at: https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety/study-support-preparation-evaluation-gpsd-well-impact-assessment-its-revision_en.

In particular, the above-mentioned new technologies and digital solutions are discussed across the following common criteria:

- **Technology maturity**, which aims at understanding how widespread the use of the technology is. In particular, the analysis of the technology will follow a breakdown over five different steps of diffusion: initial (development phase), managed (launched and piloted), defined (widely launched), quantitatively managed (finalised use), optimising (addressing emerging issues);
- **Technology acceptance**, which measures the perceived usefulness and actual use of the technology by the consumers. The analysis will therefore account for external variables (perceived usefulness and ease-of-use), and actual system use (measuring the impact of the technology use);
- **Technology complexity**, which analyses the interdependent variables operating within the same system. In particular, the analysis along this criterion will focus both on the internal variables that induce product safety (looking at the product features and the different technologies that compose it), and the external variables which influence product safety (such as product marketing); and
- **Technology transferability**, which analyses the transfer and development of the technology across different sectors.

This study encompasses both digital product and digital solutions' risks to product safety. Indeed, the former refers to risks arising from the use of digital products, including 'digital risks' such as information risk. The latter refers to situations where digital means can be used to manage or mitigate product safety concerns across a broad range of products and risks (e.g., smart home devices). For the sake of simplicity, both are mentioned in the document as 'digital product'.

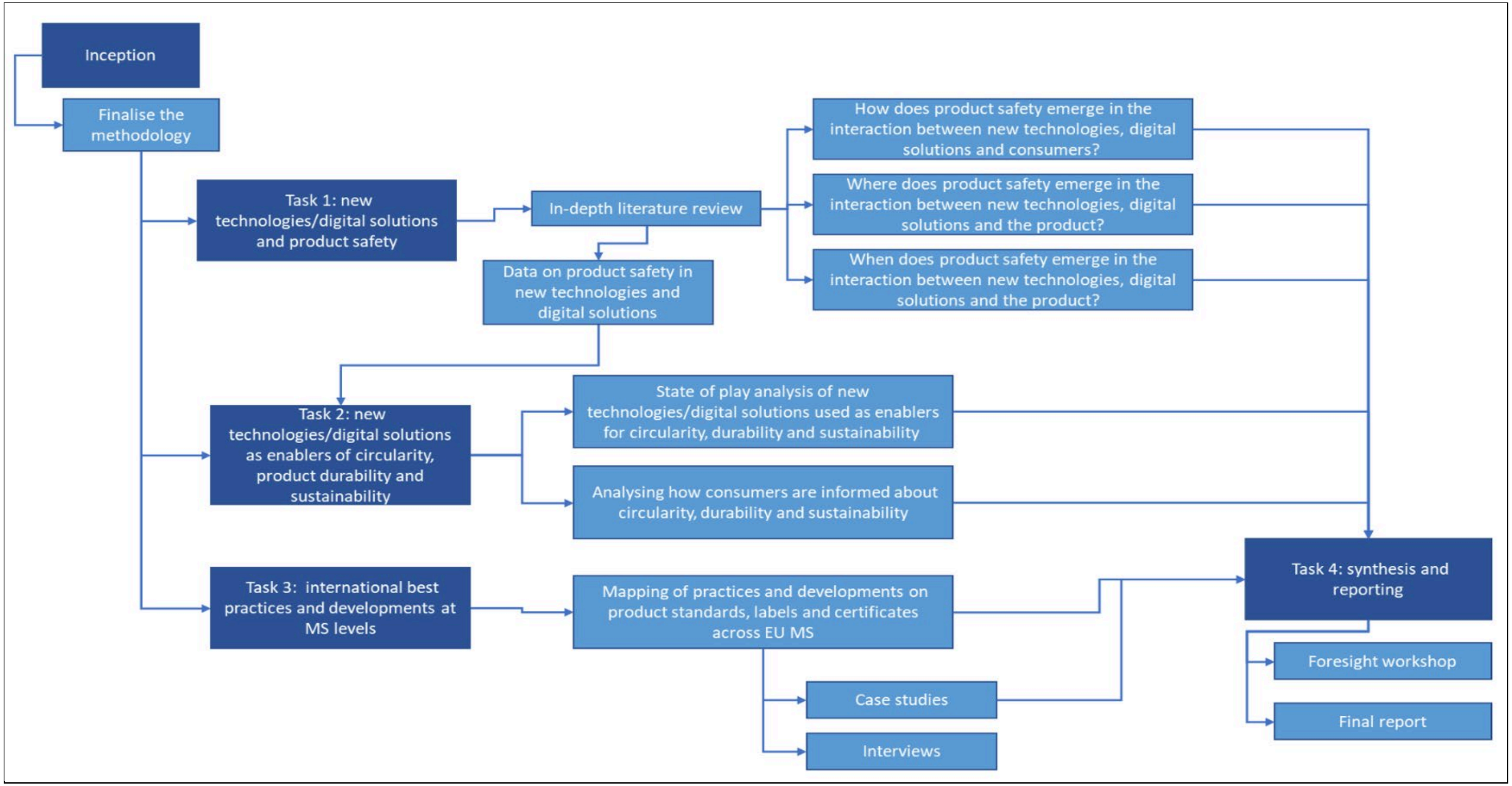
1.3. Methodology

The aim of the methodology is to provide a framework for the analysis of new technologies and digital solutions. In particular, the study focuses on the interaction between governments (which implement rules and regulations to promote product safety), and civil society (through the use and consumption of products by European citizens), and how this relationship has evolved in a changing digital context. It also aims to identify uses of new technologies to further support product safety.

The study thus consists of four complementary tasks:

- **Task 1:** New technologies and digital solutions and product safety, which includes an in-depth literature review (see References) and data collection on product safety related to new technologies;
- **Task 2:** New technologies/digital solutions as enablers of circularity, product durability, and sustainability, which is made of two parts. First a description of the state of play of the role of new technologies in the green transition. Second, of an analysis of consumers' information about circularity, sustainability, and durability;
- **Task 3:** International best practices and development at the EU Member State level, which is done by mapping practices through case studies and interviews; and
- **Task 4:** Synthesis and reporting, which includes a focus group with experts from different sectors (academics, civil society, businesses, etc.), and the drafting of the final report, conclusions, and recommendations.

Figure 1: Methodology for the study


Inception
Finalise the methodology
Task 1: new technologies/digital solutions and product safety
In-depth literature review
Data on product safety in new technologies and digital solutions
How does product safety emerge in the interaction between new technologies, digital solutions and consumers?
Where does product safety emerge in the interaction between new technologies, digital solutions and the product?
When does product safety emerge in the interaction between new technologies, digital solutions and the product?
Task 2: new technologies/digital solutions as enablers of circularity, product durability and sustainability
State of play analysis of new technologies/digital solutions used as enablers for circularity, durability and sustainability
Analysing how consumers are informed about circularity, durability and sustainability
Task 3: international best practices and developments at MS levels
Mapping of practices and developments on product standards, labels and certificates across EU MS
Case studies
Interviews
Task 4: synthesis and reporting
Foresight workshop
Final report

Source: Authors' own elaboration

2. CONTEXT OF THE STUDY

KEY FINDINGS

In the EU, the General Product Safety Directive (GPSD) provides the main safety requirements for consumer products that are being placed in the European Market. GPSD covers all products that are not covered by their sector-specific legislation and products for which the sector- specific legislation reflects a different level of protection. It defines what a "safe product" is, and creates a shared definition among the EU Member States to ensure the health of the Single Market's consumers. It also assigns responsibilities to producers and distributors, as well as competent national authorities.

However, there are issues, despite the decisive legal role that the GPSD has played in the last two decades to protect European consumers from dangerous products. Confronted with an increasing variety of challenges the GPSD runs the risk of becoming obsolete. This is in particular related to the uptake of new technologies and digital solutions such as Artificial Intelligence (AI), the Internet of Things (IoT), robotics, and blockchain. As such, the GPSD needs to adapt, by considering both the new technological aspects of product safety (such as cyber safety or data privacy), and the existing regulation concerning environment protection and the EU's global target for the next decades. The improvement of communication with EU consumers by raising their awareness about unsafe products is also key for the achievement of full protection: better informed consumers can make better choices. It should be noted that the interrelation with other regulations has increased. Now, products also contain aspects that relate to privacy, services, regulations dealing with waste, and regulations that relate to "proper care" in terms of cybersecurity.

2.1. The General Product Safety Directive (GSPD)

2.1.1. GPSD in the broader product safety framework

The GPSD provides the main safety requirements for consumer products that are being placed on the European Market. The GPSD can been seen as the 'catch all safety net intended to protect consumer health and safety'[3]. It fully applies to all non-food consumer goods that are placed on the EU market and are not covered by their own sector specific EU legislation (the so-called non-harmonised products). In contrast, the GPSD does not fully apply to consumer products that have their own specific EU legislation, such as cosmetic products (Regulation (EC) No 1223/2009[4]) and electrical products (Directive 2014/35/EU[5]). For these harmonised products, there is a 'residual effect' of the GPSD depending on whether the harmonised legislation reflects the same level of protection. According to the EC: "The General Product Safety Directive applies to consumer products when there are no specific provisions with the same objective in the rules of EU law governing the safety of the products concerned. That means it applies totally to products such as child care articles or certain COVID-19

[3] Intertek, n.d., *An overview of the General Product Safety Directive 2001/95/EC*. Available at: https://www.chamber-international.com/uploads/files/intertek-an_overview_of_the_general_product_safety_directive.pdf.

[4] European Commission, 2009, *Regulation (EC) No 1223/2009 of the European Parliament and of the Council of 30 November 2009 on cosmetic products*. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009R1223.

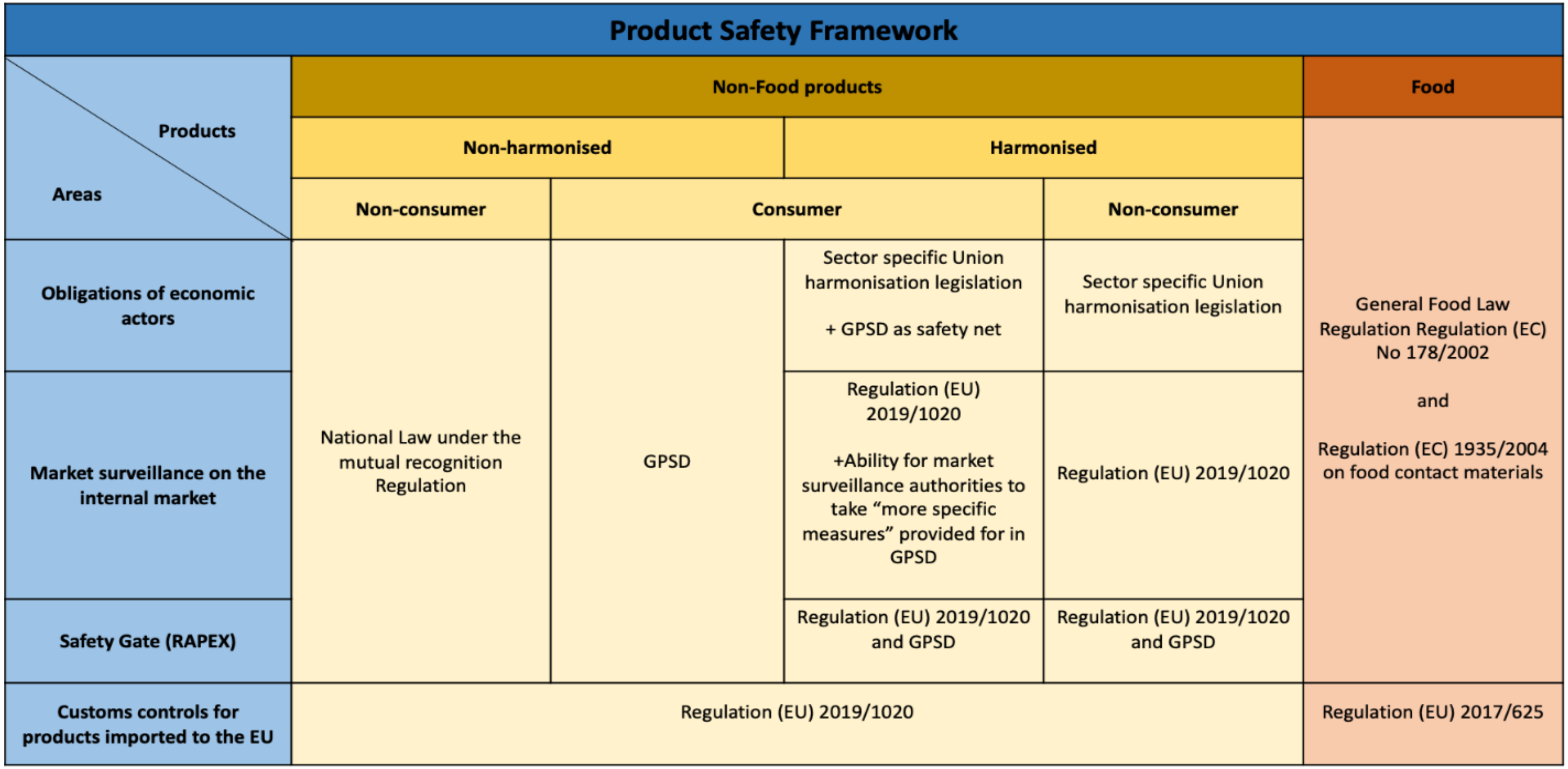
[5] European Commission, 2014, Directive 2014/35/eu of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0035.

related products, such as sanitising gels and certain type of face masks and only residually to products where sectorial legislation exists such as pharmaceuticals and medical devices."[6] As such, pharmaceuticals, medical devices and food are excluded from the scope of the GPSD.

The GPSD therefore is a cornerstone of the broader EU legislative framework for product safety. An overview of this broader framework can be found in Figure 2. It should be noted that the EC regularly reviews existing legislation to update it when needed. Therefore, the categories of consumer products for which the GPSD fully applies (non-harmonised products) on the one hand and the category of consumer products for which the Directive only residually applies because specific EU product safety legislation exists (harmonised products) on the other hand, are subject to change, as EU legislation concerning harmonised products is continuously updated and extended.

[6] European Commission, 2021, *The General Product Safety Directive*. Available at: https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety_en.

Figure 2: Overview of the Product Safety Framework



Product Safety Framework					
Products Areas	Non-Food products				Food
	Non-harmonised		Harmonised		
	Non-consumer	Consumer		Non-consumer	
Obligations of economic actors	National Law under the mutual recognition Regulation	GPSD	Sector specific Union harmonisation legislation + GPSD as safety net	Sector specific Union harmonisation legislation	General Food Law Regulation Regulation (EC) No 178/2002 and Regulation (EC) 1935/2004 on food contact materials
Market surveillance on the internal market			Regulation (EU) 2019/1020 +Ability for market surveillance authorities to take "more specific measures" provided for in GPSD	Regulation (EU) 2019/1020	
Safety Gate (RAPEX)			Regulation (EU) 2019/1020 and GPSD	Regulation (EU) 2019/1020 and GPSD	
Customs controls for products imported to the EU	Regulation (EU) 2019/1020				Regulation (EU) 2017/625

Source: European Commission, 2021, Impact Assessment accompanying the Proposal for a Regulation on general product safety.

2.1.2. Product safety within GPSD and surveillance thereof

As defined by the GPSD, a product is considered safe if it meets all statutory safety requirements under European or national law[7]. In the GPSD, Article 2 (b) defines a "safe product" as any product that does not represent any risk when normally used. The safety and health of the persons using the product are considered as a priority, as the Directive states that the following must be taken into consideration:

- "The characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance;
- The effect on other products, where it is reasonably foreseeable that it will be used with other products;
- The presentation of the product, the labelling, any warnings and instructions for its use and disposal, and any other indication or information regarding the product; and
- The categories of consumers at risk when using the product, in particular children and the elderly"[8].

It is relevant to point out that the GPSD follows the **principle of subsidiarity**, by which product safety becomes a competence shared between the EU and Member States. It would indeed be inefficient for the EU Member States to act alone when it comes to product safety, as on the internal market where goods freely circulate, a very high degree of cooperation, regular communication, and coherence of action is desirable. Thus, undertaking action at the EU level allows for the **market surveillance authorities to ensure a constant level of protection** for all European consumers by achieving economies of scale in surveillance, as well as a fair business environment and cost savings for firms that do not have to comply with heterogeneous standards across the EU[9]. Also, from an international perspective, having a common set of rules allows for better control of goods sold online by third countries notably[10]. Moreover, if under the GPSD, EU Member States have a convergent definition of what "product safety is", they can have specific national rules[11] regarding product safety applying on the territory where the product is marketed. Even in such cases, the European Union Rapid Information System 'RAPEX' includes both mandatory and non-mandatory guidelines for efficient notification of risky products which ensure that information about products that can pose health and safety risks is properly disseminated within the EU[12].

[7] European Commission, 2021, *The General Product Safety Directive*. Available at: https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety_fr.

[8] Directive 2001/95/EC - Article 2.

[9] European Commission, 2021, *Executive Summary of the impact assessment report on the proposal for a regulation on general product safety*. Available at: https://ec.europa.eu/info/sites/default/files/executive_summary.pdf.

[10] European Commission, 2021, *Proposal for a regulation of the EP and the Council on general product safety*. Available at: https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_general_product_safety.pdf.

[11] Directive 2001/95/EC - Article 3.

[12] Commission Implementing Decision (EU) 2019/417 of 8 November 2018 laying down guidelines for the management of the European Union Rapid Information System 'RAPEX' established under Article 12 of Directive 2001/95/EC on general product safety and its notification system (notified under document C(2018) 7334).

2.1.3. GPSD in relation to standards

Nationally defined standards are applied in cases where there is no existing specific EU regulation or EU standards[13]. A national standard is a standard introduced as a result of a government decision of the EU Member States, through a process referred to as **government-based standardisation**[14]. However, the European Single Market benefits from a more cohesive approach where EU Member States use common European standards.

A **European standard is defined by the European Standards Bodies** (the European Committee for Standardization or CEN, European Committee for Electrotechnical Standardization or CENELEC, and the European Telecommunications Standards Institute or ETSI), which draft a document, "established by consensus and approved by a recognised body that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context". EU standards are therefore based on scientific results, technology, and experimenting, aiming at the promotion of the community's best interest[15].

Importantly, European standards are developed either in compliance with European regulations or harmonise existing standards to better support regulations. Thus, European standards are a common set of rules and definitions that specify the product, process or service compliance with quality and safety as it is governed under EU regulations. As such, products marked as compliant with EU standards communicate to consumers that the product is of high quality and safe to use or consume. For manufacturers, compliance with European standards allows competing on the Single Market and represents the manufacturers aims towards quality and reliable products.

Once the new European standard is introduced the EU Member States must provide it with the same status as a national standard[16]. This process is made easier by the fact that national bodies are involved in the process of drafting a new European standard. This process is fairly open for organisations to approach CEN with a proposition for a new standard. However, it is most common that the process is initiated by members of CEN (national bodies responsible for standardisation) or EU bodies (i.e. the European Commission). Once the need for new standard emerges, the European Commission issues a Directive to set safety requirements for the product, beginning the process of standardisation.

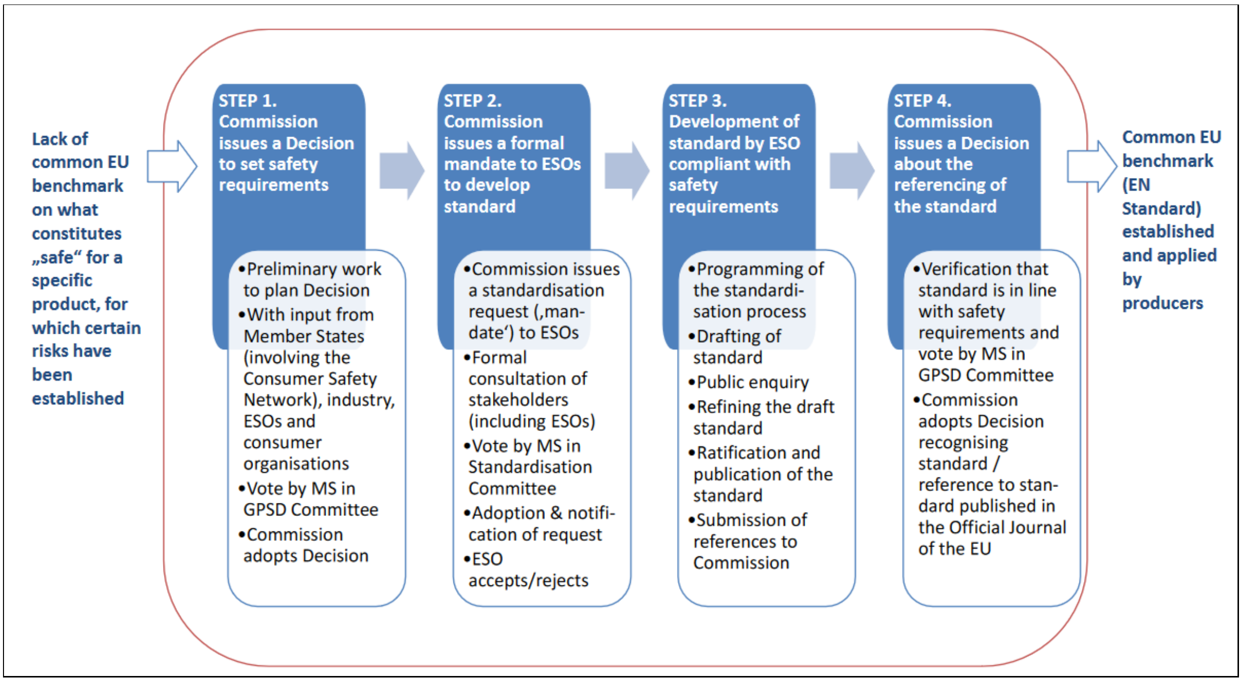
[13] Defined in the updated summary of references of European standards published in the Official Journal of the EU. Available at: https://ec.europa.eu/docsroom/documents/43968. In December 2020 the list included 111 standards on products such as outdoor furniture, gymnastic equipment, cycles.

[14] Wiegmann P., 2019, *Becoming the industry standard when standardisation is not standardized*. Available at: https://discovery.rsm.nl/articles/389-becoming-the-industry-standard-when-standardisation-is-not-standardised/.

[15] Cen Cenelec, 2022, *European Standards*. Available at: https://www.cencenelec.eu/european-standardization/european-standards/.

[16] Civic consulting, 2020, *Study for the preparation of an Implementation Report of the General Product Safety Directive. Final Report*. Available at: https://ec.europa.eu/info/sites/default/files/final_report-gpsd-part1-main_report-final-corrected2.pdf.

Figure 3: A simplified overview of the standardisation process under the GPSD


Lack of common EU benchmark on what constitutes „safe“ for a specific product, for which certain risks have been established
STEP 1. Commission issues a Decision to set safety requirements
•Preliminary work to plan Decision
•With input from Member States (involving the Consumer Safety Network), industry, ESOs and consumer organisations
•Vote by MS in GPSD Committee
•Commission adopts Decision
STEP 2. Commission issues a formal mandate to ESOs to develop standard
•Commission issues a standardisation request (‚mandate‘) to ESOs
•Formal consultation of stakeholders (including ESOs)
•Vote by MS in Standardisation Committee
•Adoption & notification of request
•ESO accepts/rejects
STEP 3. Development of standard by ESO compliant with safety requirements
•Programming of the standardisation process
•Drafting of standard
•Public enquiry
•Refining the draft standard
•Ratification and publication of the standard
•Submission of references to Commission
STEP 4. Commission issues a Decision about the referencing of the standard
•Verification that standard is in line with safety requirements and vote by MS in GPSD Committee
•Commission adopts Decision recognising standard / reference to standard published in the Official Journal of the EU
Common EU benchmark (EN Standard) established and applied by producers

Source: CIVIC Consulting, 2021, Study to support the preparation of an evaluation of the General Product Safety Directive as well as of an impact assessment on its potential revision.

The process of issuing the new standard involves two separate committees. A GPSD Committee is set up to vote on the suggested first draft of the standard during the preliminary stages and voting to verify the standard after it is fully developed. As for the development, a committee of European Standardisation Organisations (members of CEN) is created to oversee the drafting of the standard. The multi-stage process involves a considerable number of stakeholders in the preliminary work (establishing the basis from which a safety standard could be developed, unless the product is within a harmonised area which could provide a basis), to the process of accepting and formally requesting the development, to the process of developing, to the process of verifying the standard. While the stakeholder involvement across EU Member States should ensure that a consensus is reached and the final standard is adopted by the EU Member States, the evaluation report for the GPSD considered that the process could be streamlined to be more efficient[17].

[17] CIVIC Consulting, 2021, *Study to support the preparation of an evaluation of the General Product Safety Directive as well as of an impact assessment on its potential revision*. Available at: https://ec.europa.eu/info/sites/default/files/gpsd-final-report-part2-ia.pdf.

2.1.4. The development of GPSD in recent years and the proposed policy option

The GSPD originally came into place in 2001 by replacing the first directive on general product safety (the 1992 Directive)[18]. The 1992 Directive was deemed necessary because differences in product safety legislation (or lack thereof) between Member States posed risks for creating trade barriers and therefore impeding competition within the internal market.[19] However, the co-legislators considered the 1992 Directive 'incomplete and some of its provisions indistinct'[20], and also due to relevant developments in product safety, the 1992 Directive was recast and replaced by the 2001 GPSD.

Because product safety legislation is considered to be quite fragmented, as some products are regulated by the GPSD and other products by sector-specific legislation[21], there were some efforts to simplify this system. In 2013, the **first proposal for the revision of the GPSD** was presented by the European Commission to simplify the existing system with a package including two regulations: one for consumer product safety and one for market surveillance. However, because of a negotiation deadlock between the EU Member States concerning disagreements over the provisions on the country-of-origin labelling, the package was withdrawn seven years later. In 2019, only the proposal on the **new Market Surveillance and Compliance Regulation**[22] was passed. This regulation aims at improving the rules on market surveillance for harmonised products[23], especially those sold online[24].

More recently, in June 2021, the European Commission adopted a **proposal for a regulation on general product safety**. It was stated that the 2001 Directive was 'nearly 20 years old and as such does not reflect any more the developments in products and markets. It does not explicitly address the fact that new technologies, in particular AI, can impact product safety.'[25] Furthermore, the increased importance of online marketplaces poses new challenges to consumers that had to be addressed.

[18] Council Directive 92/59/EEC of 29 June 1992 on general product safety. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31992L0059&from=EN.

[19] European Parliament, 2021, Briefing: *Revision of the General Product Safety Directive.* Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/694202/EPRS_BRI(2021)694202_EN.pdf.

[20] Ibid.

[21] Ibid.

[22] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32019R1020.

[23] The further revision of the GPSD is now looking at an update of the rules for both harmonised and non-harmonised products.

[24] European Parliament, 2021, *Legislative train schedule on the GPSD*. Available at: https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-revision-of-the-general-product-safety-directive.

[25] European Commission, 2021, *Review of the general product safety directive: proposal for a regulation on general product safety.* Available at: https://eur-lex.europa.eu/legal-content/EN/PIN/?uri=pi_com:Ares(2020)3256809.

Given these developments, the European Commission performed an Impact Assessment[26], in which four policy options are identified to deal with the shortcomings of the current GPSD. These options account for all the products targeted by the GPSD and address the following objectives:

- General objectives: ensuring the protection of EU consumers from unsafe products, while contributing to the proper functioning of the Single Market, in particular a level playing field for businesses.
- Specific objectives:
  - (1) Ensure the EU legal framework provides for general safety rules for all consumer products and safety risks, including those linked to new technologies;
  - (2) address product safety challenges in online sales channels;
  - (3) make product recalls more effective and efficient in keeping unsafe products away from consumers;
  - (4) enhance market surveillance and ensure better alignment of rules for harmonised and non-harmonised consumer products; and
  - (5) address safety issues related to food imitating products.

To achieve these objectives**, 4 options** for how the GPSD could be developed were elaborated, with each option representing growing complexity in implementation:

- **Option 1: Improved implementation and enforcement of the existing legal framework**, mainly through increased guidance and promotion of the current tools but without legal revision of the GPSD (only the Food-Imitating Product Directive would be revised);
- **Option 2**: **Targeted revision of the GPSD**, as a Directive or Regulation, addressing the coverage of new risks, making several provisions inspired by the Product Safety Pledge provisions legally binding, introducing mandatory requirements for product recalls, aligning with the market surveillance rules for harmonised products and integrating rules for food-imitating products into the GPSD;
- **Option 3**: **Full revision of the GPSD** in the form of a Regulation providing for, beyond Option 2, clarifications of safety rules linked to software, additional obligations related to online sales and product recalls, stronger enforcement powers to EU Member States, setting an arbitration mechanism for disputes between them in relation with divergent risk assessments, and enhancing product traceability; and
- **Option 4: Integration of the legal instruments on market surveillance**, beyond the provisions under Option 3.

According to the "Proposal for a Regulation of the European Parliament and of the Council on General Product Safety", option 3 would be preferred as it would best be able to tackle the five objectives related to the EU legal framework: online sales channels, product recalls, market surveillance, simplification of standardisation procedures, and food imitating products[27]. This shows that the

[26] European Commission, 2021, *Commission Staff Working Document accompanying the document Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council.*

[27] European Commission, 2021, *Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0346.

European Parliament and the Council expect significant changes with the revised GPSD, in order to adequately address the new challenges that arose in connection with new technologies.

The challenges that new technologies and digital solutions pose for consumer safety are reflected in the proposed changes to the GPSD. A resolution from the European Parliament notes that the revised GPSD should clarify the terms of 'product' and 'safe product' to: "reflect the complexity of emerging technologies, including products with AI, IoT and robotics embedded in them, standalone software and software or updates which entail substantial modification to the product leading to a de facto new product"[28]. The following chapters present a more extensive overview of the identified shortcomings of the GPSD, and the different actions that reflect how the revision of the GPSD could account for this.

2.2. The identified shortcomings

Despite the decisive legal role that the GPSD has played in the last two decades to protect European consumers from dangerous products, it is confronted with an increasing variety of challenges. Because it does not consider the influence of new technologies and connected devices on product safety, the current legislation has become outdated, and urgently needs to be revised to adapt to the new challenges which include the uptake of new technologies and digital solutions such as AI, the IoT, robotics, blockchain, etc. In particular, most salient shortcomings are:

- **The definition of "safety" and "product**". Emerging new technologies and their daily use by consumers imply new risks that have not been fully defined yet. Some products placed on the Single Market can indeed access an internet connection, use, and generate data, and allow for an important degree of human-product interaction. These new characteristics of products entail risks, related to cyber-security, personal safety, and mental health. These issues are particularly salient in the case of technologies such as AI or robotics, which are capable of adapting their behaviour to their immediate environment[29]. Similarly, the concept of environmental protection is not covered in the current GPSD. The definition given to a "product" is also evolving, especially when it comes to dematerialised goods such as software, which are also used to access different services[30];

- **Online sales channels and the coverage** to address the product safety issues arising from products sold on online marketplaces. This issue is highly divisive between the EU Member States: should online marketplaces and other intermediaries be explicitly acknowledged by the Directive, or should responsibility be strengthened across the supply chain[31]?;

- **The lack of effectiveness in product recalls**. The GPSD does not lay out any specific rules with respect to the recalling of unsafe or dangerous products. The issue is that besides the lack of centralised recalling procedures across the EU, many consumers are not actually aware of

[28] European Parliament, 2020, *European Parliament resolution of 25 November 2020 on addressing product safety in the Single Market*. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0319_EN.pdf.

[29] European Commission, 2020, *Opinion of the sub-group on AI, connected products and other new challenges in product safety to the consumer safety network*. Available at https://ec.europa.eu/safety/consumers/consumers_safety_gate/home/documents/Subgroup_opinion_final_format.pdf.

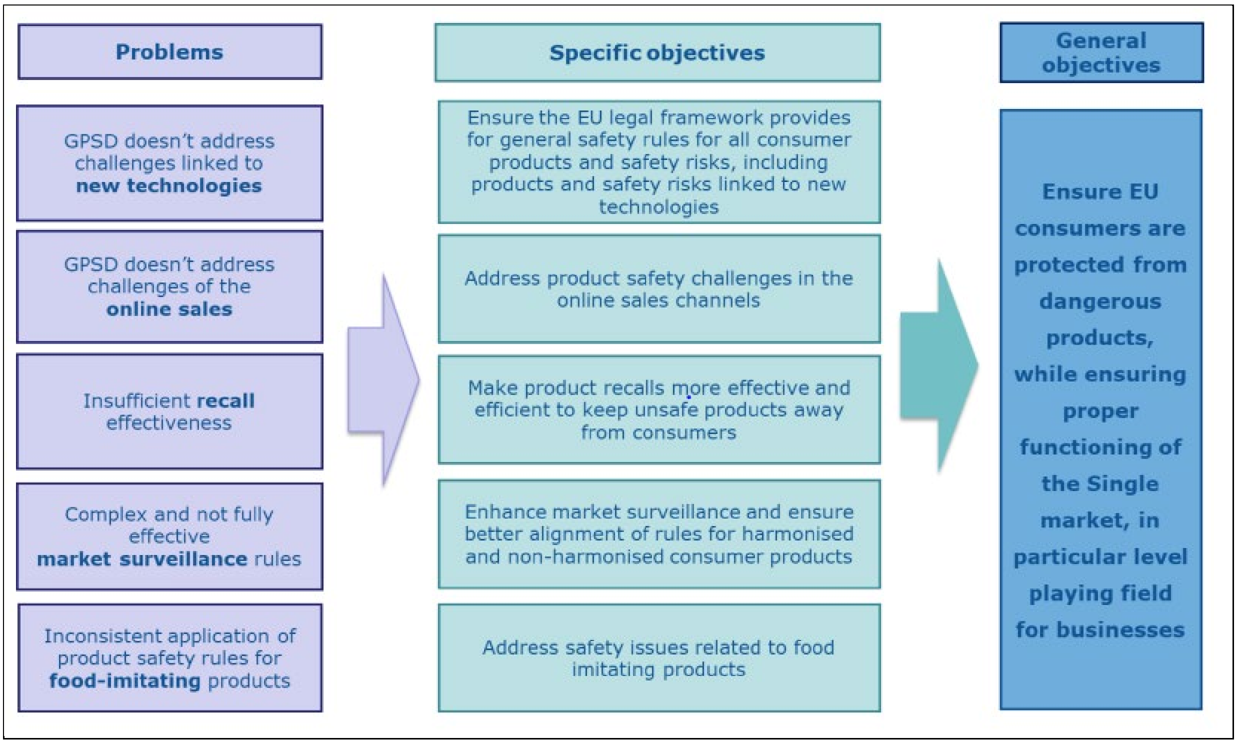
[30] Ibid.

[31] European Commission, 2017, *Notice on the market surveillance of products sold online*. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017XC0801(01)&from=EN.

ongoing recalls, and even if they are aware, they tend to minimise the risks associated with a dangerous product partly because of incorrect communication[32];

- **The insufficient market surveillance**. There are parallel rules on market surveillance when it comes to harmonised versus non-harmonised products. Market authorities indeed enjoy different degrees of control over harmonised products (such as children's toys), versus non-harmonised (childcare products), which implies inefficiencies in terms of applications of the GPSD, and risks for the consumers' safety[33]; and
- **The uneven application of the rules for food-imitating products across the EU**. The rules detailed in the Directive 87/357/EEC (Food Imitating Products Directive – FIPD) are not homogeneously applied across the EU Member States[34].

Figure 4: Overview of the problems and objectives of the GPSD


Problems
GPSD doesn't address challenges linked to **new technologies**
GPSD doesn't address challenges of the **online sales**
Insufficient **recall** effectiveness
Complex and not fully effective **market surveillance** rules
Inconsistent application of product safety rules for **food-imitating** products
Specific objectives
Ensure the EU legal framework provides for general safety rules for all consumer products and safety risks, including products and safety risks linked to new technologies
Address product safety challenges in the online sales channels
Make product recalls more effective and efficient to keep unsafe products away from consumers
Enhance market surveillance and ensure better alignment of rules for harmonised and non-harmonised consumer products
Address safety issues related to food imitating products
General objectives
Ensure EU consumers are protected from dangerous products, while ensuring proper functioning of the Single market, in particular level playing field for businesses

Source: European Commission, June 2021. Impact Assessment on General Product Safety.

[32] European Commission, 2021, *Impact Assessment on the Proposal for a regulation*. Available at: https://ec.europa.eu/info/sites/default/files/impact_assessment.pdf.

[33] Ibid.

[34] Ibid.

The impact assessment on the Commission's revision proposal[35] highlights that while the GPSD has been a valid instrument so far and has met the goals that were set, there still are many unsafe products circulating on the internal market. Such a situation creates both an unfair business environment for distributors, and a heavy cost for European consumers. It is indeed estimated that the consumer injuries and deaths caused by unsafe products are responsible for a preventable detriment of €11.5 bn yearly to EU consumers, while the total value of unsafe non-harmonised consumer products on the EU market is estimated at €19.3 bn[36] [37].

2.3. The existing legislative framework

Any revision of the GPSD should ensure that the EU legal framework evolves to guarantee the safety of European consumers and prevent the risks arising from the placement of products related to new technologies on the market. In addition, given the objectives of the current proposal for revision of GPSD, any recommendation formulated for the improvement of product safety rules should take into consideration both aspects of the existing EU framework: the new technologies aspect, and the sustainable aspect of product safety. Therefore, the broader legislative frameworks of these aspects, and their recent developments, should be explored. This chapter lists several of these developments in the fields of product safety, digital products, and protection of the environment.

Firstly, **the new Consumer Agenda was adopted in November 2020**, presenting the EU Member States' vision on the consumer policy for the period 2020-2025, as the previous 2012 Agenda had expired in 2020. Taking the context of the COVID-19 pandemic into account, the programme seeks to address the immediate product safety-related needs of EU consumers by promoting five priority areas: the green and digital transitions, the protection of consumers' rights, the protection of exposed consumers, and international cooperation. Coming as a complement to other EU initiatives, such as the Circular Economy Action Plan (March 2020), it proposes the tools for a sustainable and digitally driven recovery in the post-COVID-19 world[38].

[35] European Commission, 2021, Study to support the preparation of an evaluation of the General Product Safety Directive as well as of an impact assessment on its potential revision. Part 2: impact assessment on the potential revision of the General Product safety Directive. Available at: https://ec.europa.eu/info/sites/default/files/gpsd-final-report-part2-ia.pdf.

[36] The values have been calculated using 2019 as the baseline year and include both online and offline sales channels.

[37] European Comission, 2021, *Executive Summary of the Impact Assessment Report: Proposal for a Regulation of the European Parliament And of the Council*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021SC0169&rid=2.

[38] European Commission, 2020, *New Consumer Agenda. Strengthening consumer resilience for sustainable recovery*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0696&qid=1605887353618.

On the digital side, there are several relevant initiatives and pieces of legislation that, to some extent, play a role in product safety:

- **The European civil law rules on robotics**, which is a study commissioned by the European Parliament in 2016, aiming at drawing first rules around new technologies. This document, which includes proposals for the creation of legislative instruments, served as a basis for the recent proposal[39] of the European Commission to revise the GPSD[40];
- **The General Data Protection Regulation** (GDPR, Regulation (EU) 2016/679), which imposes important obligations in terms of privacy and data security onto organisations located in the EU, which collect data related to European citizens[41];
- **The Cybersecurity Act** (Regulation (EU) 2019/881), which comes to strengthen the EU Agency for Cybersecurity (ENISA) and introduced an EU-wide "cybersecurity certification framework for products and services"[42]. The Act was adopted in April 2019 and benefits the distributors of digital products across the EU, by enabling them to certify their ICT products[43];
- **The Digital Services Act (DSA)** (COM/2020/825), which goal is to create a safer digital space by regulating the responsibility of services providers online. Adopted by the Commission in December 2020, the proposal for a regulation includes online platforms such as social media and online marketplaces which can offer potentially illegal content, products, and services to their users[44]. A formal agreement was reached in April 2022 between the European Parliament and the Council to implement the proposal for DSA. It is expected that DSA will come into effect on 1 January 2024[45] [46]; and
- **The legislative proposal on AI (COM/2021/206)**, which aims at harmonising the rules between the EU Member States for the progressive placement of AI products on the common market. Presented in April 2021, its rules will put a particular emphasis on the protection of the health and safety of users as well as their fundamental rights. The objective is to set a definite frame both for the providers and users of such systems which will protect the public interest[47].

[39] European Commission, 2021, Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0346&qid=1628522210573.

[40] European Parliament, 2016, *The European Civil Law Rules in Robotics.* Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf.

[41] GDPR.EU, 2022, *What is GDPR, the EU's new data protection law?* Available at: https://gdpr.eu/what-is-gdpr.

[42] European Commission, 2022, *The EU Cybersecurity Act.* Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

[43] European Parliament, 2019, 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 (Cybersecurity Act). Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0881.

[44] European Commission, 2021, *Proposal for a regulation of the EP and the Council on general product safety*. Available at: https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_general_product_safety.pdf.

[45] European Commission, 2022, *Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment.* Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545.

[46] The adoption of DSA was announced after the data gathering for this study had taken place. Therefore, the relevance of DSA is not accounted for in this study.

[47] European Commission, 2021, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence act) and amending certain union legislative acts*. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206.

In parallel, other initiatives, programmes and pieces of legislation have been launched by the European Commission, in the last decade, the most recent being placed under the framework of the 2020 EU Green Deal. The relevant ongoing initiatives identified by the team of consultants are the following:

- **The Integrated Product Policy** (IPP) and the **Sustainable Products Initiative** (SPI). Adopted by the Commission in 2003, the IPP built on the idea that all products cause environmental degradation, from the extraction of natural resources to their manufacturing, use, and disposal. The IPP, therefore, adopted a very innovative "Life-Cycle Thinking"[48], aiming at coherent action to lower the environmental impact of production and use of goods and services. Its biggest goal was to create one umbrella tool, which allowed to have one single policy covering all products and impacts, thus strengthening the coordination between the EU Member States[49]. Additionally, on March 2022 the Commission adopted the SPI which aims at boosting the placing of sustainable products on the internal market[50]. It notably covers electronic equipment and ICT, steel, textiles, furniture, and chemicals thus ensuring the EU's smooth transition towards a "modern, climate-neutral, resource-efficient and circular economy"[51]. The SPI also aims to introduce a DPP as a policy measure to increase transparency on the environmental footprint of products[52];

- **The Eco-design Directive (2009/125/EC) and the Energy Labelling Regulation (2017/1369)**. Adopted in 2009 and 2017 respectively, they aim at providing the EU Member States with consistent rules on the environmental characteristics of products (including household appliances or ICT). The labelling regulation complements the Eco-design Directive with the introduction of compulsory labelling requirements on certain products[53];

- **The Circular Economy Action Plan (COM(2020)98)**, adopted in March 2020, is the lead policy for the transition from a linear to a circular economy. The plan aims at drastic waste reduction by the inducement of re-use, reparation, and high-level recycling. It puts a particular emphasis on product safety, which must be the plan's primary objective[54]; and

- **The Chemicals Strategy for Sustainability Towards a Toxic-Free Environment (COM(2020) 667)**, which was adopted in October 2020 by the Commission to ban dangerous chemicals present in products and thus not only to protect the consumers' health but also the environment from hazardous products[55].

[48] European Commission, 2004, *Building on Environmental Life-Cycle Thinking*. Available at: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2003)302&lang=en.

[49] European Commission, 2008, *Report on the state of implementation of the Integrated Product Policy*. Available at: https://ec.europa.eu/environment/ipp/pdf/bio_ipp.pdf.

[50] European Commission, 2022, *Questions and Answers: Sustainable Products Initiative*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2014.

[51] EU Agenda, 2021, *Boosting the Sustainable Product's Initiative in the EU*. Available at: https://euagenda.eu/events/2021/12/01/boosting-the-sustainable-products-initiative-spi-in-the-eu.

[52] The adoption of SPI was announced after the data gathering for this study had taken place. Therefore, the relevance of SPI is not accounted for in this study.

[53] European Commission, 2022, Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products. Available at: https://ec.europa.eu/growth/industry/sustainability/sustainable-product-policy-ecodesign_en.

[54] European Commission, 2021, Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions A new Circular Economy Action Plan For a cleaner and more competitive Europe. Available at: https://ec.europa.eu/environment/strategy/circular-economy-action-plan.

[55] European Commission, 2020, Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions Chemicals Strategy for Sustainability Towards a Toxic-Free Environment. Available at: https://ec.europa.eu/environment/strategy/chemicals-strategy_nl.

3. STATE OF PLAY ON NEW TECHNOLOGIES AND DIGITAL SOLUTIONS

KEY FINDINGS

The emergence of new technologies and digital solutions is affecting how product safety is embedded within products and affects consumers' choice and use of products. Undeniably, new technologies and digital solutions create **unparalleled access to products.** The use of connected devices can influence consumers' safety by allowing them more easily to understand and compare different options, both for choosing safe products and for using them in the most appropriate ways. This is not just a matter of generic safety; such technologies and solutions also benefit consumers by allowing them to personalise these effects – from personalisd comparisons to individual-specific operational parameters. Technologies employed in connection to others may boost traceability along the value chain (allowing safety incentives and responsibilities to operate effectively) and provide new opportunities to make products safer and more sustainable by sourcing better materials, improving product design (e.g. to match actual behaviour), enhancing processes and improving the end-of-life processes of reuse, remanufacturing, and recycling.

However, benefits of increased communication and transparency of product information via technology are not guaranteed or without potential risks. The combined use of multiple interacting technologies and digital solutions calls into question traditional concepts of **product ownership.** How do the solutions affect safety? What happens to products when, for example, online services stop being updated or shut down, when data or functionality are lost as a result of data corruption or when safety is compromised due to a product being hacked? Holding developers accountable for communication to consumers throughout the product life cycle (in line with traditional strict product liability concepts) is challenging and may be counterproductive. **Interoperability and standards are necessary to ensure that all stakeholders along the value chain agree to appropriate information sharing** and take responsibility for their parts of the value chain. This applies to producers, distributors, service provider and sometimes even users – all of them can take actions that influence what products are and how they function. The product passport for instance can also serve as a compliance and audit tool to facilitate information transmission along the value chain.

There is concern about consumers losing agency of their choice due to the complex ways in which the functionalities of different technologies and digital solutions are presented and consumer consent is obtained. The challenge is balancing effective communication and building consumer trust that their personal data and welfare are protected in the digital age. These concerns vary by technology; AI and IoT appear to raise the most concerns.

New technologies and digital solutions blur the lines of responsibility between distributors and producers. Producers and consumers are linked via increasingly complex value chains. The complexity and dynamism of the current situation and the variety of legal settings (e.g., country of origin principle) clearly call both for more flexible and participatory forms of governance and for a more active negotiation of roles in contrast to the relatively fixed responsibilities of traditional product safety settings. Legislation will need to change to support a new way of value delivery to consumers.

This chapter also discusses **safety challenges associated with obsolescence**, mainly relating to continuity of product safety coverage, the collection and continued availability of data, support for products and liability and consumer protection. In current EU legislation, digital technologies are seldom mentioned as ways to tackle the harms associated with product obsolescence, despite their inherent potential to adapt product design for greater product longevity, facilitate upgrades, increase cooperation along the value chain during the product lifetime and help consumers make more informed decisions.

Lastly, the chapter covers **administrative burden and other direct costs**, and how they might be minimised, mitigated and/or redistributed in efficient and proportionate ways. The revised GPSD can minimise such burdens, by giving standing to common standards and certification and the creation and governance (or direct provision) of central repositories of product characteristics and consumer experiences. Further, the use of new technologies can lead to efficiency gains, as illustrated by the use of AI for dispute resolutions.

The following subsections reflect on the effects of new technologies and digital solutions on product safety, product sustainability and consumer awareness. The analysis is based on the analysis of various new technologies and digital solutions, for which detailed fiches are provided in Annex 2.

3.1. Effects of new technologies and digital solutions on safety

New technologies and digital solutions provide developers with new tools in ensuring consumers benefit from safer products. At the same time, the introduction of these technologies and solutions causes new challenges due to shifting paradigms.

This chapter presents how new technologies and digital solutions relate to product safety across three topics:

- An **exploration of the state of play of new technologies and digital solutions** looks at the novel approaches to product safety that are being enabled by their deployment. At the same time, the emerging issues are brought up, reflecting ways in which the technologies and solutions challenge developers in ensuring consumers are properly informed about their purchases and their safety features;
- This is followed by examining the **opportunities that new technologies and digital solutions present to further enhance product safety**. This includes looking into further integration of technologies and solutions across the value chain for monitoring and tracing products as well as new ways of providing data to consumers for more informed decision making; and
- Lastly, a brief discussion on **how new technologies and digital solutions challenge the concept of ownership** is presented. An argument is made for moving towards a more flexible definition for ownership, combining aspects of control and co-owning between buyer and seller, especially in light of digital software.

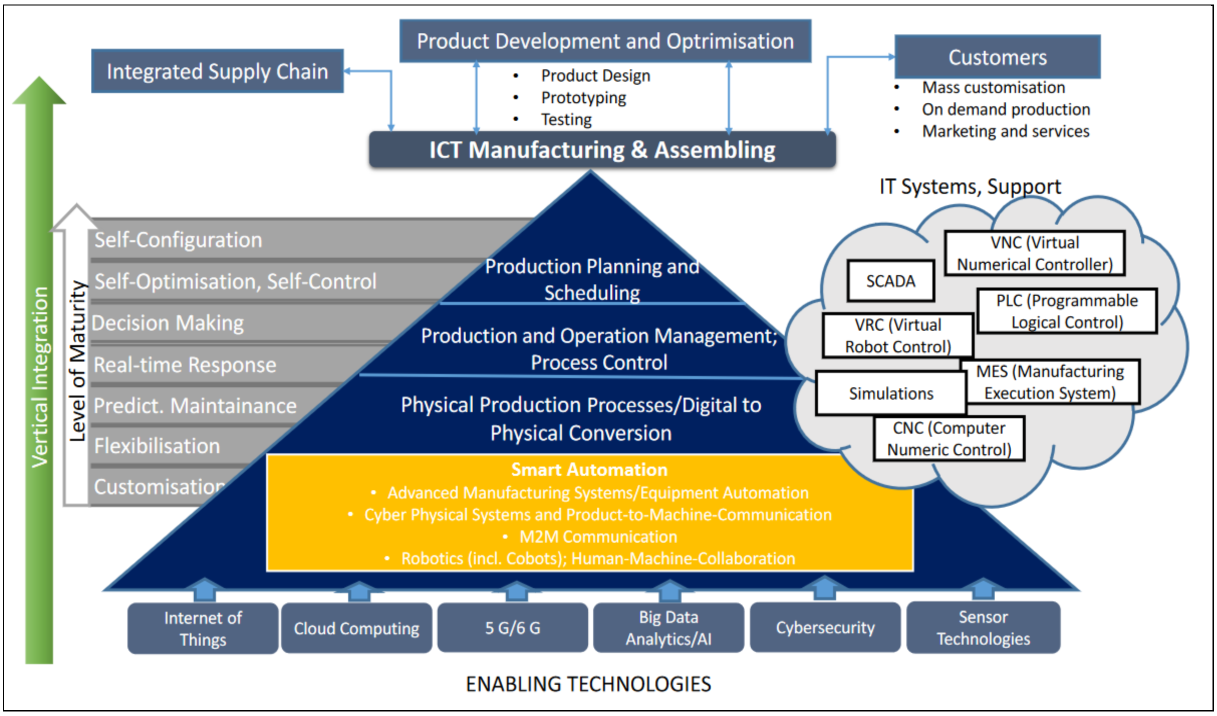
3.1.1. State of play and challenges of new technologies/digital solutions used as enablers for safety

One of the important considerations on product safety and new technologies and digital solutions is examining them as part of a system rather than in a vacuum. Indeed, technologies and digital solutions discussed in this paper are increasingly **employed in connection to other technologies** rather than as single systems. In essence, it means that safety features (and safety concerns) emerge not only within the technology or digital solution itself, but also in their interaction with other components and digital solutions within the product (be it a physical consumer good or a software).

The use of interconnected technology and solutions, particularly with AI at the centre, is being explored, especially in connection to Industry 4.0. (IoT and connected devices supplying AI with information to enhance its machine learning). This combines the limited autonomy inherent to the emerging solutions with human input in the form of objectives to lead towards a more data driven manufacturing and maintenance process. In turn, this allows embedding product safety features by collecting and analysing data from comparable, analogue products, including stumbles in their safety design, and taking this into account to design a product with enhanced safety features that learn from past failures and circumvent potential failure points.

The integration of new technologies and digital solutions into the manufacturing process is discussed in the 2021 Product Watch report "Advanced Technologies for Industry". The report analyses the emergence of Industry 4.0 and presents an overview of integrating new technologies and digital solutions within manufacturing value chains. Figure 5 shows how technologies and digital solutions create opportunities for enhanced product optimisation, product monitoring which translate into increased product safety[56].

Figure 5 Value chain of Industry 4.0 in ICT Manufacturing


Product Development and Optrimisation
Integrated Supply Chain
Customers
Product Design
Prototyping
Testing
Mass customisation
On demand production
Marketing and services
ICT Manufacturing & Assembling
IT Systems, Support
Vertical Integration
Level of Maturity
Self-Configuration
Self-Optimisation, Self-Control
Decision Making
Real-time Response
Predict. Maintainance
Flexibilisation
Customisation
Production Planning and Scheduling
Production and Operation Management; Process Control
Physical Production Processes/Digital to Physical Conversion
Smart Automation
Advanced Manufacturing Systems/Equipment Automation
Cyber Physical Systems and Product-to-Machine-Communication
M2M Communication
Robotics (incl. Cobots); Human-Machine-Collaboration
SCADA
VNC (Virtual Numerical Controller)
VRC (Virtual Robot Control)
PLC (Programmable Logical Control)
Simulations
MES (Manufacturing Execution System)
CNC (Computer Numeric Control)
Internet of Things
Cloud Computing
5 G/6 G
Big Data Analytics/AI
Cybersecurity
Sensor Technologies
ENABLING TECHNOLOGIES

Source: European Commission, 2021, Advanced Technologies for Industry – Product Watch.

[56] European Commission, 2021, *Advanced Technologies for Industry – Product Watch*. Available at: https://ati.ec.europa.eu/reports/Product-Watch.

Some technologies have a more widespread uptake among manufacturers (e.g., robotics appears to be much more embedded in industry as opposed to AI, which the Product Watch report notes as still emerging). However, AI is also being explored by manufacturers of robotics to better connect several robots. This not only shows how the new technologies and digital solutions are being linked, but it also suggests that these technologies and solutions (AI in this case) have several pathways to enter the value chain. They are integrated by either the industrial manufacturers or the suppliers of technologies to the manufacturing process.

Another important point is how the level of maturity for technology integration (as seen on the left side of Figure 5) corresponds to product safety features. At the lower end of technology maturity, value chains achieve greater product customisation and flexibilisation which are related more to overall efficiency and effectiveness of manufacturing. As the technology maturity level rises, value chains start displaying features such as predictable maintenance and real-time response. These advanced features allow addressing challenges, such as faulty products and product recall, through pre-emptive measures taken during manufacturing or product updates. Thus, from the value chain perspective, greater technological maturity in the manufacturing process translates into more sophisticated product safety features.

Device connectivity that supports product safety features raises the issue of **product or activity continuity** (e.g. when a developer/manufacturer stops supporting the product or shuts down the services; for instance, the termination of online services could affect wearable medical devices that rely on updates to provide users with accurate input about their health). While termination of services may not make the product itself dangerous, lack of connectivity and/or further updates can translate into products being more open to safety issues (e.g., discovery of security breaches or malfunctions due to changes in other connected products and services). This issue is further discussed below (Section 3.2.3).

Another challenge is **informing consumers** well in advance about plans to end services that will affect their product functionality and ensuring that consumers understand this as an outcome when they make their purchasing decisions. **The communication itself may be subject to challenges**, especially if developers fail to meet promised development or update deadlines. A recent example of this is seen with the concept of roadmaps that are designed to showcase the introduction of updates and features to devices or services. While consumers make their purchasing decision based on communication promising a long product life cycle, roadmaps can be delayed or dropped early without fulfilling the promised development. The challenge is **holding developers accountable to such communication activities,** as the promise of continuous updates can create positive consumer perceptions towards safety embedded in products. The scope for such a modified ownership concept is further developed in Section 3.1.3.

Finally, the relationship between product safety and privacy should be discussed. The information that service providers and product suppliers could use to enhance product safety can, in principle, be employed in two different forms:

- the first way allows for user anonymity to be maintained. From the perspective of product and service design and collective provision, such information (regarding e.g., how products are used and safety outcomes on a population basis), while they do involve potentially personal information, do not generally rest on identification and can be processed in strongly anonymised ways;

- the second form is based on data linked to particular customers (e.g., protections or compensation linked to specific safety instances or patterns of use). In this case, at a minimum, explicit consumer consent must be obtained and maintained in the manner prescribed by the GDPR. However, the potential for data repurposing – including by automated processing - is always present, spread across many entities in the product/service value chain and may not be easy to control, given the way GDPR defines legitimate purposes (including public interest, see more details on value chain in 3.4).

This is a complex area, with legal, ethical and technical dimensions that are far beyond the scope of the current study. However, we would note that the interests of users stem both from their fundamental privacy rights and from safety considerations, so balancing is required. Privacy rules need to ensure that data can be used for increased safety while limiting the extent to which providers can act as data controllers, and to what extent and in what way they are able to share data.

3.1.2. Opportunities for new technologies/digital solutions to be used as enablers for safety

While challenges continue to exist, the new technologies and digital solutions offer opportunities to enhance product safety by:

- Creating better conditions to monitor product development across the value chain;
- Creating conditions to trace products and directly communicate with them;
- Leveraging market data surveillance and analysis to inform consumers;
- Providing consumers with assistance when making purchasing decisions; and
- Offering safety measures to block unwanted behaviour.

Interconnected technologies and solutions create better conditions for using **monitoring and predictions to inform product development across the value chain**. For companies, they enable the manufacturing process to benefit from different aspects and strengths of the technologies while reducing their limitations. For example, use of connected devices and AI to create a larger data input stream from the devices to the AI to facilitate communication and autonomy of AI that allows it to make better informed decisions or predictions for the manufacturing process. Companies can use the new technologies and digital solutions to enhance their capacity to track and trace the whereabouts of defective products across the supply chain but also identify weak signals on issues encountered by their solution.

This **enhanced traceability** also creates conditions to better monitor and repair defective products remotely (for example, through software patches). **Directly embedding communication within the product provides manufacturers and developers with better tools to avoid safety issues for consumers**.

Further to their potential **contribution to data analysis for market surveillance** (both from a business and an administrative perspective), digital technologies and solutions have potential in the way they address consumers. For instance, for consumer assistance, they can support users in a resource-efficient way, using chatbots able to process huge amounts of possible answers to provide a specific reply to individual issues raised by users.

The use of new smart connected devices can also **assist consumers in making purchasing decisions**. Particularly, opportunities emerge in the form of digital assistants which can guide consumer decisions free from behavioural bias. In other words, digital solutions can help consumers make the right decision by reducing variables that could influence them. Technologies and digital solutions can provide input based on consumer past behaviour and preferences but also on different parameters that include a **greater level of objectivity**.

There is an argument about how much of an unbiased decision does an AI make if its machine learning algorithm is based on biased consumer behaviour patterns. To ensure that new technologies and digital solutions facilitate purchasing decisions to the **consumers benefit,** their use must ensure the capacity to set **operational parameters for technologies that provide them with information,** but also the **compliance with fundamental rights** (e.g., consumer rights when using a dispute resolution solution based on AI).

The use of parameters and their benefits are evident when the product has the capacity to make monetary transactions. In such cases, consumers can benefit from the greater availability of tools and options designed to limit or entirely block users from making purchases. Commonly, this can take the form of parental controls designed to remove children's access from spending money (e.g., through devices that allow online gaming). But it can likewise allow people with known gambling addictions to block devices from accessing their bank accounts to reduce the risk of gambling.

To support the process of connecting different technologies and digital solutions, companies benefit from **interoperability standards**. They are meant to ensure that devices and digital solutions or services remain open to upgrades and updates regardless of the systems interacting within the products (e.g., several software from different manufacturers) or the point of sale (whether direct sale or bought through third parties). Thus, interoperability standards can help significantly in ensuring that the products purchased by consumers will benefit from maintenance and reparability regardless of the point of purchase.

At the same time, the connectivity of these new technologies and digital solutions is raising challenges regarding the concept of product ownership. An OECD paper questions how traditional consumer notions about ownership are affected by licencing conditions. Consumers purchasing new technologies may find that there is a "limit the degree to which a product may be repaired, modified, resold, or interoperable with other devices"[57]. Thus, while offering opportunities to ensure product safety, new technologies and digital solutions also present a need to look at how product ownership is defined.

3.1.3. A modified definition of ownership

The introduction of new technologies and digital solutions brings new complexities towards how ownership is defined. Device connectivity raises further challenges when distinguishing between products and service, hardware and software[58] as connectivity, interoperability raises questions of who owns the product, who is responsible for the products safety when there may be multiple stakeholders (developers of hardware, developers of software, consumers) whose interactions affect the product (and its safety). Due to the uptake of digital technologies and solutions these questions will grow in importance and need to establish clear definitions, ensuring clarity in the marketplace. One possible solution is changing the **concept of 'ownership', replacing it with something more flexible, adaptive, negotiable and nuanced.** Previous product law (consumer protection, product safety, etc.) has largely been based on a transfer of ownership from seller to buyer at the point of sale and bundling together various responsibilities and rights (including rights to collect and share information) with

[57] OECD, 2019, *Challenges to consumer policy in the digital age.* Available at: https://www.oecd.org/digital/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf.

[58] OECD, 2018, *Consumer product safety in the Internet of Things*. Available at: https://doi.org/10.1787/7c45fa66-en.

ownership status. Over time, this model has been 'patched' to fix market failures (e.g., incomplete/asymmetric information), to provide incentives for sellers to inform prospective buyers in order to meet several objectives.

One objective is to **allow consumers to choose products that best meet their needs and capabilities**, including the ability to understand and take precautions during use.

A second objective is to **foster product design and development practices that promote safe product use**. This means that product makers are encouraged to understand and anticipate 'unsafe' or 'unintended' product uses and implement design decision that safeguard against unsafe use of products. This does raise the question of who is responsible for the safety of consumers whose use does not fit the model used by producers.

A third objective for extending the concept of ownership is to **create a (market) mechanism that enables producers to learn about consumer preferences in order to improve product safety at the design stage, and to provide competitive incentives** (via warranties and compensation mechanisms) for dealing with problems that are uncertain or depend on things not known at the point of sale. It should be noted that their effectiveness may be limited though by 'recommend use' exceptions to such protections.

But for digital products these things may need to be unbundled – services provide a different model, but neither the 'product' and 'service' models provide one-size-fits-all solutions, and both can result in unhelpful shifts of responsibility. Both are also harder to enforce consistently across global supply chains, leading to potentially damaging trade, innovation and competition impacts, which might affect product safety and business burdens.

An analogy of such alterations in ownership is provided by personal information, which in the EU cannot be owned but which retains a mix of oversight and control for the ultimate party (data subjects).

The current product and service situations are also linked to binary relationships (e.g., one buyer and one seller). This may not easily extend to digital products or products using digital technologies. Instead of a buyer who buys a single product from a seller, these products are sold and used in ways that involve multiple economic entities in complex networked relationships on both 'sides' of the transaction and products that work in linkage with many other products, not all of which are visible to let alone controllable or contractually connected to the user(s). In addition, such products generally involve service provision; a single service may be provided over many product platforms and may behave differently on all of them, so putting responsibility on the service provider may not be equitable or efficient. Moreover, services are provided and used in networks and thus depend on each other; similarly, a single product may 'host' many services.

With specific reference to product safety, it is also important to note that, in contrast to either the buyer-owned or pure service provider models, information relevant to product safety may be observable in many places. It needs to be aggregated and shared with actors across the supply chain in order to produce safer designs, standards, market outcomes and use patterns – and thus better safety. Additionally, the updating of software on a product may change its function in ways that make some patterns of use unsafe, but which might not be anticipated by the software provider. Thus, a suitably flexible, negotiable and shared form of ownership, control and informational rights may need to be implemented (or allowed to evolve).

Lastly, with digital tools, there is a great potential in rethinking business models from a consumer perspective – leasing rather than owning a product, for instance. These practices can encourage product longevity, reusability and sharing; reduce demand for materials and negative externalities (e.g., waste) and ultimately support dematerialisation. There is a considerable rise in **circular business models using digital technologies** and **changing consumer interaction with products: product-as-a-service** (PSS), or 'servitisation', is one important illustration of this. Servitisation loosely refers to changes in the capabilities and processes of manufacturing to diversify from products into product-service systems[59]. However, the circularity benefits of PSS models should not be overstressed. Like most circular business models, the specific business needs to be studied in detail to fully assess its true circularity potential and any negative externalities.

3.2. Effects of new technologies and digital solutions on durability

New technologies and digital solutions increase the transparency and traceability of products alongside the value chain. They are increasingly considered as an enabler for circularity, although these technologies are also resource and energy intensive.

- The first sub-section explores how different technologies (QR codes, blockchain, AI, robotics…) can address circular challenges (e.g., lack of transparency at different stages of the value chain) and contribute to the increased sustainability of products with concrete examples in sectors;
- The second sub-section explains how consumers are empowered to make more sustainable decisions through digital technologies. It also looks at how new business models are emerging as a response to consumers' demand for verified, clear and comprehensive information on products; and
- The last sub-section looks at the safety challenges raised by obsolescence and how digital technologies can help to address them. Obsolescence also affects the sustainability of products and digital technologies can facilitate the development of standards and eco design measures, although the ability for digital technologies to tackle obsolescence measures is seldom mentioned in current EU legislation.

3.2.1. State of play analysis of new technologies/digital solutions used as enablers for durability

The **alignment of the different political green and digital agendas in Europe is recent**. For a long time, sustainability and digital transition were perceived as separate things. In the context of the COVID-19 pandemic, the push for a twin transition, both digital and green, was emphasised. There is a growing recognition[60] that digitalisation is an enabler for addressing some of the dual societal and environmental challenges.

Digital solutions as an enabler for circularity have already existed for decades, with technologies such as sensors for tracking and separation being used in the waste management sector. These solutions however have been focused above all on the end-of-life stage of a product. New studies point to the considerable potential of applying digital technologies to address the **various challenges in the circular value chain**, in sourcing materials, improving product design, enhancing processes, and improving reuse, reparability, remanufacturing, and recycling. Digitalisation addresses complexity, which makes it a very useful tool for addressing the various bottlenecks of the circular economy[61].

[59] Technopolis et al. for the European Commission, 2018, *Study on the potential of servitisation and other forms of product-service provision for EU-SMEs.* Available at : https://op.europa.eu/en/publication-detail/-/publication/0d1ed8aa-8649-11e8-ac6a-01aa75ed71a1/language-en/format-PDF/source-80915761.

[60] EPC, 2020, *The circular economy: Going digital.* Available at: https://www.epc.eu/en/publications/The-circular-economy-Going-digital~30c848.

[61] Ibid.

The collection, integration and sharing of data enabled by digital technologies such as sensors, connected devices and online platforms have the potential to lead to a smarter use of resources. By providing data on the state of components in real time, sensors placed on products like tires and elevators enable companies to anticipate failures and know when to maintain, replace or repair components. This enables predictive maintenance and extends the lifetime of a product. Similarly, labels using QR technology (e.g., the EU Ecolabel) can help to inform consumers further on the lifetime of their product.

As repeatedly stressed in various studies, 70% to 80% of the environmental impact of a majority of consumer products occur at the design phases[62]. Prospecting with **AI** is being used to improve design processes for greater circularity, allowing producers to manage data and play with different materials to manage the complexity and the criteria that designers need to address. **3D modelling** is also one technology that is being used in construction and deconstruction to improve efficiency, effective recycling and cost savings[63]. One ongoing Interreg[64] project looks at how smart devices are developed to make circular construction possible, integrating various digital tools such as 3D scanning, Building Information Modelling (BIM), a digital material and building database, blockchain technology[65].

Digital solutions can be used to extend the life cycle of products. There are various examples of **online digital platforms** that can provide guidance on how to repair and recycle products. IoT with self-diagnostic functions is a great solution for preventive maintenance in the industry and is being more widely implemented in a range of general public products**. Industrial IoT** is quite well advanced in Europe today, although there is scope to do more. **Augmented reality glasses** can be used to repair with guidance manuals. **3D printing** can help to remanufacture products and the components that need to be used for product repair and reuse.

A considerable challenge for the circularity of products is that information does not currently travel along value chains. Tracking and tracing valuable critical raw materials and substances of concern could enable safer and more efficient reuse and recycling. This is particularly important for products that hold harmful chemicals for instance, where safe repair and recycling is necessary. Currently, great efforts are being deployed by European legislators to develop **DPPs** at EU level with the entry into force of the revised Batteries Directive and of the SPI. **Blockchain and QR codes** are technologies that can be used to facilitate the implementation of DPPs (see Box 1 below). In the future, information storing and sharing could be improved with distributed ledger technologies like **blockchain**. Indeed, blockchain carries the potential to share and store data in a secure and efficient way, while also respecting intellectual property rights which is often a challenge for companies that do not want to share information. Sectors in which they are currently being developed are mainly construction and textiles.

[62] For instance, Radjou N & Prabhu J, 2014, *Frugal Innovation: How to do more with less,* The Economist. Available at http://naviradjou.com/wordpress/wp-content/uploads/2016/12/Frugal-Innovation_Intro-Chapter.pdf.

[63] For instance, Timothy M. O'Grady, 2021, *Circular economy and Virtual Reality in Advanced BIM-Based Prefabricated Construction,* Energies. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwij1q-zsu31AhXpx4UKHay6AgUQFnoECBEQAQ&url=https%3A%2F%2Fwww.mdpi.com%2F1996-1073%2F14%2F13%2F4065%2Fpdf&usg=AOvVaw2nmQFZf_xuc4aGBy8kT0AM.

[64] Interreg is an instrument of the European Union (EU) to support cooperation across borders through project funding.

[65] For instance, Interreg. Available at: https://www.nweurope.eu/projects/project-search/digital-deconstruction/.

Box 1 Focus on DPPs

This is a relatively recent technology tool, that is still under evaluation. Its benefits (transparency and traceability for consumers, compliance for policy makers and recyclability for manufacturers) are still being debated against its limits. Currently, DPPs appear to be a concern for policy makers as there is no common definition for them. Manufacturers are still undecided on how to best implement DPPs into the value chain and ensure its usage. All actors along the supply chain have yet to agree on standards and measures, so that company secrecy is ensured. Blockchain and QR codes are being considered to facilitate DPP implementation. Further information on the DPP is available in the Technology Fiche in the Appendix.

While digitalisation is leverage for circularity, it is important to bear in mind that digitalisation can lead to **unsustainable practices**. For instance, as it is largely technologically and turnover-driven following linear production and consumption levels, the introduction of smart technologies and automation may lead to increased consumption behaviour, energy use and environmental impacts[66]. The digital industry has a large environmental footprint. Before investing in new digital technologies, stakeholders should, as much as possible, assess that the negative impacts throughout the technologies' lifecycles do not offset the expected gains.

3.2.2. Analysing how consumers are informed about durability

One of the biggest challenges lying ahead for a successful deployment of digital solutions for circularity is to **empower citizens and consumers to participate in the transition**. Currently, the lack of awareness, capacities and convenience makes it difficult for consumers to actively contribute to the circular economy. Moreover, the overload or lack of information on products complicates consumers' ability to make sustainable choices. Data and digitalisation can be used to **inform, educate, and influence people**, enable them to make sustainable choices and convert them into active participants in the data economy and co-creators of knowledge[67].

A study shows that although consumers are enthusiastic about the circular economy, their actual engagement in circular economy practices is low[68]. Around 36% of consumers do not repair products and around 90% have no experience renting, leasing, or buying second-hand products. The study suggests that the reason for this discrepancy is driven by a lack of access to information and convenience – sometimes designed for regular full replacement by purpose[69].

As previously stressed, **information sharing is one of the major barriers** to achieving a circular economy. Consumers would benefit from having information on how to maintain, repair and recycle a product. Digitalisation can support these efforts. Applications and platforms are already influencing how consumers can play a more interactive role in the circular economy, and future legislation, including the formalisation of a DPP in the Batteries Directive and the SPI, should accelerate this trend.

[66] ECERA, 2020, *Digital Circular economy: a cornerstone of a sustainable European industry transformation*. White paper – ECERA European Circular Economy Research Alliance. Available at: https://www.era-min.eu/sites/default/files/publications/201023_ecera_white_paper_on_digital_circular_economy.pdf.

[67] EPC, 2020, *The circular economy: Going digital*. Available at: https://www.epc.eu/en/publications/The-circular-economy-Going-digital~30c848.

[68] EC, 2018, *Behavioural Study on Consumers' Engagement in the Circular Economy*. Available at: https://ec.europa.eu/info/sites/default/files/ec_circular_economy_final_report_0.pdf.

[69] Ibid.

Several important challenges are associated with the wider deployment of digital products for consumers. The first is on trust and safeguarding privacy. The second is on accessibility and whether consumers have the necessary infrastructure and digital skills to engage in such tools. Technology can help to prioritise and organise the wealth of information that is available on products. Labels can help consumers for instance but are not easy to navigate through. Applications that centralise data and labels to rank products are considered much more impactful[70].

3.2.3. The influence of new technologies and digital solutions on obsolescence

One aspect of durability, from the market and consumer perspective, concerns obsolescence. This has a functional definition: when a product is superseded by another, or when changes in needs, other products and contextual factors mean that it no longer (safely or efficiently) performs in the way users desire. However, digital products are not simply superseded; they may be updated, no longer be supported or fail to interoperate with updated or new products and services. In addition, the obsolescence of products may sometimes be triggered by the disappearance of the firms that provided them and which are in general responsible for maintaining them and collecting information about their performance.

In effect, **obsolescence raises several product-safety challenges in relation to**:

- **Continuity of coverage of product safety** (and consumer information and protection) arrangements;
- **Collection and continued availability of data** (e.g., in-service and version data relating both to product characteristics and to user experience);
- **Support for products** (in the form of replacement, repair and refurbishment); and
- **Liability and consumer protection** (which may expire when a product reaches the end of its service life or the supplier or vendor goes out of business) and the operation of recall, compensation and replacement programmes.

Obsolescence can affect product safety, but can also be influenced by strategic market considerations (see extensive literature on versioning and planned obsolescence: "[a] strategy used by companies that consists of designing products so that they become unfashionable or no longer functional after a period that is shorter than the product's technical requirements and properties would allow"[71]). Set against the revenue-orientated analysis, changes designed to force consumers continually to update (thus reducing circularity) can still generate some potential positives. These include **modular design** to permit partial updating and facilitate repairs and an incentive for the products in use to have roughly the same vintage and thereby to remain reasonably up-to-date and effectively and safely interoperable, which cannot be guaranteed when a wide distribution of product vintages is in interoperable use. We would note a tension in this, however. If versioning is used to drive up turnover (and prices), consumers will face strong financial incentives to update less frequently, widening the distribution of ages, keeping unsupported products in use and generally increasing the risk of unsafe products.

[70] EPC, 2020, *The circular economy: Going digital*. Available at: https://www.epc.eu/en/publications/The-circular-economy-Going-digital~30c848.

[71] Montalvo, C. et al., 2016, *A Longer Lifetime for Products: Benefits for Consumers and Companies*, publication for the Committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg. Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/579000/IPOL_STU(2016)579000_EN.pdf.

Moreover, a **well-articulated digital product ecosystem will keep track of the safety associated with products in use and will therefore be in a stronger position to respond to new technologies and new safety challenges with product changes**. This is difficult to mandate (compare the relatively regular 'generations' of Apple products with the more variable lifetimes of Android devices), but the requirements to adhere to the Product Safety Pledge and other proposed constraints will create incentives for this kind of coordinated evolution. It is coordinated in the sense that product obsolescence reduces the utility of the existing version for *most* users and triggers a coordinated replacement that in turn can pay for more extensive safety, R&D and redesign. It may also be coordinated across interoperating families of products due to their complementarity.

The European legal framework has evolved in recent years and now addresses the issue of planned obsolescence (e.g., Right to repair; revised Unfair Commercial Practices Directive (UPCD)). IMCO has played a key role in pushing forward the subject[72]. Currently, **digital technologies are still not explicitly mentioned as a solution to help tackle planned obsolescence practices**. IMCO's report on promoting product longevity underlines the necessity for existing product policy legislation to accommodate the needs for minimum product lifetime as well as to inform prospective customers but without listing relevant technologies[73]. Similarly, in the European Consumer Summit 2022, consumer protection organisations were very vocal on the right solutions to tackle planned obsolescence, through the development of standards, eco-design measures, reparability and guarantee rights, but seldom mentioned **digital technologies as a facilitator**. The European Commission has started exploring the concept of DDP to increase product transparency and consumer awareness with a gradual development from 2023, but the goal is not explicitly to combat obsolescence but rather to increase circularity[74].

Our research underlines the ability of digital technologies to help adapt product design for longevity, facilitate upgrades, increase cooperation along the value chain during the product lifetime and help consumers make informed decisions. Technologies such as QR codes, NFC and DPP can help consumers chose products, by judging its reparability potential and the availability of spare parts. In addition, when used in conjunction, AI, IoT and robotics can tackle obsolescence through interactive and personalised consumer relations, improved product design, predictive maintenance, and later remanufacturing, sorting and disassembly. Tackling planned obsolescence practices can effectively reduce waste and boost circular business models (reuse, repair, remanufacture).

[72] European Parliament, 2020, *Towards a more sustainable Single Market for business and consumers*, Publication for the committee on the Internal Market and Consumer Protection. Available at : https://www.europarl.europa.eu/doceo/document/A-9-2020-0209_EN.html#.

[73] Marcus J. S., et al, 2020, *Promoting product longevity: how can the EU product safety and compliance framework help promote product durability and tackle planned obsolescence?,* Publication for the committee on the Internal Market and Consumer Protection, European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648767/IPOL_STU(2020)648767_EN.pdf.

[74] European Commission 2021, *Digital Product Passport: sustainable and circular systems.* Available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2021-trust-01-digipass.

3.3. The role of communication and marketing in driving consumer behaviour towards safer products

With the studied new technologies and digital solutions comes a need for greater transparency, and disclosure for consumers about these products and their safety. This is needed to **build consumer trust**, enable the purchase of safe products, ensure correct, safe, and ethical use and updates and to make it possible to properly dispose of a product when it reaches its end-of-life cycle.

There is a lot of potential for digital solutions as a means to address questions from customers and to inform them. Blockchain (or distributed ledger technology), combined with unique identifier technologies such as QR codes and NFC tags[75] tagged to a product, provides opportunities for better information transparency and communication on product safety: supply chain transparency is expected to improve with blockchain allowing for better product traceability. The location and distribution of faulty products can be pinpointed instantly, and safety issues might be taken care of before they happen. In the case of a product recall, a product can be traced, and product authenticity is easier to ensure. Prerequisites for the use of blockchain, QR codes and NFC tags to be used for better transparency are proper industry standards that enable parts of the value chain to communicate with each other. Furthermore, when companies want to keep certain information about their value chain private the technology should not give away strategic advantages.

Similarly, a **DPP** with information on the composition, repair and dismantling possibilities of a technology **creates more transparency about a product,** including the resources used and the manufacturing process. The product passport can also be seen as a compliance and audit tool. Also with product passports, actors along the supply chain need to agree on standards.

Without blockchain technology, **NFC tags and QR codes can also be used to easily engage with a product in an interactive way**, providing access to information and product options. QR codes are already compatible with most cameras on phones and can easily be printed on packaging and labels, for example to provide assembly instructions for the unboxing of a product. NFC tags provide for more interaction between the consumer and product provider.

There is a lot of potential for digital solutions to address answers from consumers in a more effective and efficient manner and to better inform consumers. The possibilities offered by technologies such as AI or IoT should however be carefully assessed as they should solve consumer problems, and not create new problems. New technologies such as AI and IoT create and use a vast amount of consumer data that provides many opportunities for businesses to engage with their consumers. **Devices can be used to communicate important safety information to consumers**, both at the time the product is activated and through the entire lifecycle, from safe installation and setup instructions (including self-diagnostic in case of errors) to reminders about safe use and product updates.

The size of the collected data however also enables consumer profiling and tailored marketing. While it is possible to use this information to personalise offers for the benefit of consumers, the collected data can also be used to discriminate against consumers or take advantage of certain behavioural biases. There is a possibility of unfair commercial practices or "digital market manipulation" where especially vulnerable or disadvantaged consumers are taken advantage of. Furthermore, there is **concern about consumers losing agency of their choice due to the complexity of the different technologies and digital solutions** and the way consumer consent is asked for. An example is the

[75] Near Field Communication uses "inductive coupled devices operating at the centre frequency of 13,56 MHz for interconnection of computer peripherals", ISO/IEC 18092:2013 information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1).

legal language surrounding the use of AI for data collection, which results in consumers signing online agreements they do not have the time to read or the legal knowledge to fully understand. As such, documents that are created to communicate with consumers may achieve the opposite effect of consumers deliberately ignoring communication that they perceive as too difficult to understand.

What must be noted is that transparency may not be enough for most consumers to fully understand the processes involving AI and data collection/use especially concerning the "subject who is in control". It is unclear whether greater consumer awareness about the technologies could also translate into an opposition to the technologies rather than acceptance[76]. Furthermore, there is **a difference in the demand for safety and security-related information by consumers per type of technology**. For example, consumers in general are often more concerned about security of a cloud computing platform (e.g., when critical business information will be stored) than when purchasing a robot, where usability, functionality and competitive prices are considered of higher importance. This might result in a different demand for information on security from the user, while security risks can be equally high.. For example when a robot is used to deliver medicines to patients, it can have severe consequences when this robot is hacked and delivers the wrong medicine.

Though intelligent machines taking over human lives may be the subject of science fiction, the increasing complexity and sophistication of technologies can meet opposition from consumers, especially the more consumers are informed. Thus, the challenge becomes balancing not only building effective communication, but also **building consumer trust in the technologies** and policies that their personal data and livelihoods are protected in the digital age.

[76] OECD, 2019, *Challenges to consumer policy in the digital age*. Available at: https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf.

3.4. Embeddedness of technologies and digital solutions across the value chain. Effects on industries and consumers

New technologies and digital solutions impact the relationship between actors across the value chain, and have consequences on the administrative burden for economic operators:

- The first sub-section explores the evolution of the embeddedness of technologies and digital solutions across the value chain; and
- The second sub-section looks at related administrative burdens.

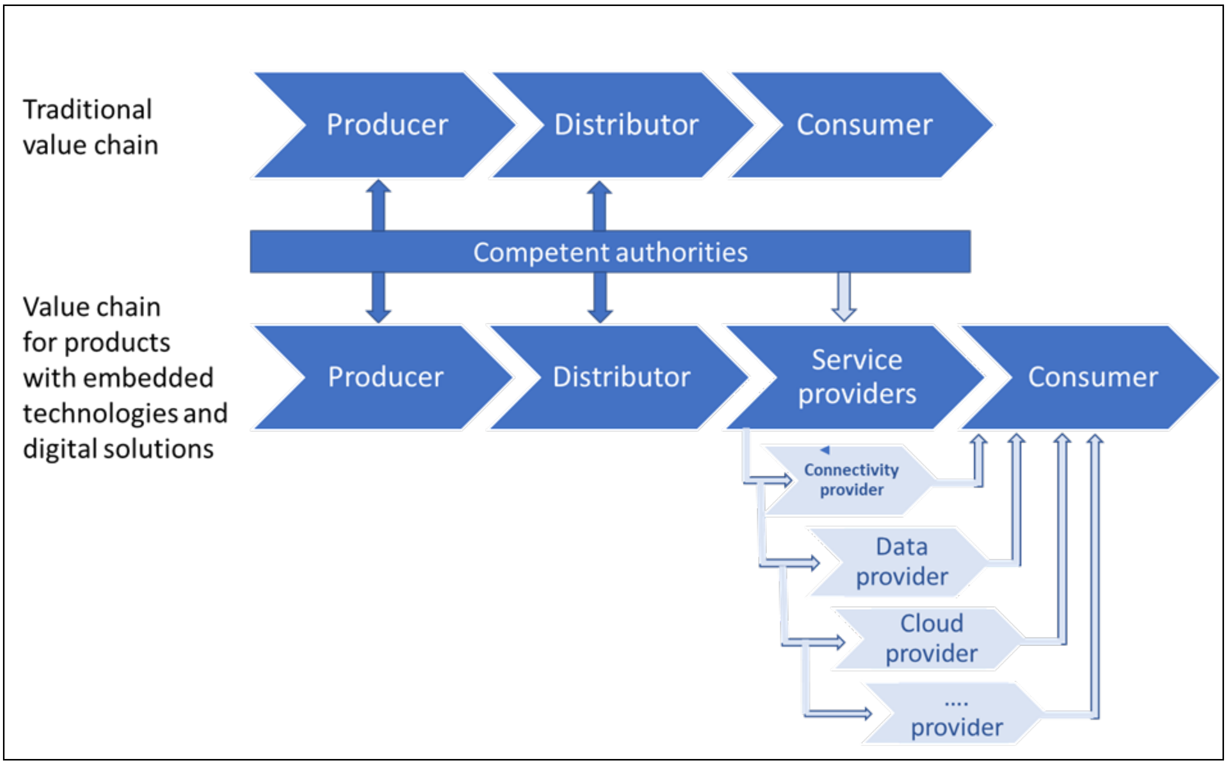
3.4.1. Impact of technologies and digital solutions on the value chain

Increasingly, the **boundary between products and services is blurring**; this is particularly true for "connected products" that use connectivity with the internet to deliver value to users. This also means that **producers and consumers are linked via increasingly complex value chains**. This is not only a challenge to consumers, but also to producers and other value chain participants but it also departs from assumptions about ownership, control, consent, and responsibility underpinning the regulatory framework. Digital value creation and business models are fundamentally different from those that produced traditional product portfolios; they require a very different approach that goes well beyond direct revenue and profit and current management techniques[77]. One thing is for sure; **the increasing complexity of the value network[78] system affects all stakeholders**: producers, distributors, service providers, competent authorities for consumer protection, and consumers themselves. Another implication is that many of the issues of highest concern to regulators are emergent. They are not directly visible or controllable from the perspective of individual products, producers, distributors, other service providers or use cases. **It is thus key to consider flexible and future approaches when regulating.**

[77] Markus A., 2019, *Value Creation with Digital Products and Services: Digital Value Canvas.* Available at: https://www.linkedin.com/pulse/value-creation-digital-products-services-canvas-markus-anding/.

[78] Allee, V., 2000, *Reconfiguring the Value Network*, Journal of Business Strategy, Vol. 21, N4, July-Aug; Allee, V. (2005) *Understanding value networks*. A brief article by Verna Allee; Allee, V., ,2003, *The Future of Knowledge: Increasing Prosperity through Value Networks*, Butterworth-Heinemann 2003.

Figure 6: Value Chain with new technologies and digital solutions



Source: GNKS Consult BV, 2022.

From Figure 6, it is clear that legislation will need to change to support new ways of delivering value to consumers. Services in the past were often delivered as complementary to "products" and thus covered by traditional product sales models (e.g. "change the oil in the car" or even "update the software on the computer"); now service providers are increasingly acting as product distributors, or even producers. For example, 'mobility as a service' is supplied using vehicles that may or may not be owned by the consumer and services that are managed by signals sent from connected devices in the car itself directly to the maintenance provider. Increasingly, these 'shared product models' also involve services provided in product-flexible or even product-neutral ways – with the same consumer needs addressed by a single provider through a range of shared or independently consumer-provided ('bring your own device' or BYOD) products – all need to be interoperable in order to preserve the safe and effective function of the system on which the consumer relies. This in turn rewires the relations between producers, consumers and other participants in ways that are both complex and highly dynamic. Because safety is affected both by design and by utilisation, and because both monitoring and ensuring appropriate safety depend on the points of observation and control provided by these relationships, regulation must also become more agile and relationship-and technology-neutral. This challenge must be considered when competent authorities act. It also highlights the need for consumers to deal with several service providers, each of which may or may not be responsible for solving a specific problem when it emerges. For instance, when there is a problem with a game on a computer, who should be contacted: the game provider; the computer provider; the operating system provider?

In essence, the **traditional model of product safety was tied to a simple linear value chain** exemplified by the outright sale of products; some safety aspects could be most effectively observed and addressed at the producer level (hence strict product liability), while in other cases, safe use depended on choices made by informed consumers and regulation took the form of required information disclosure or even caveat emptor ("Let the buyer beware"). When services came into the picture, this was supplemented by e.g., professional and/or other fiduciary responsibilities and indemnification for service providers, but it was still clear that the products involved could be regarded as under the control of a well-defined party. The complexity and dynamism of the current situation and the variety of legal settings (e.g., country of origin principle) clearly calls both for more flexible and participatory forms of governance and for a more active negotiation of roles in contrast to the relatively fixed responsibilities of traditional product safety settings.

The challenges of ensuring continued and appropriate levels of consumer protection are increased by the **increasingly complex integration of products and services**. Solutions must therefore be principles- or performance-based to accommodate changes in the definitions and nature of safety expectations and requirements. They must also seek to maintain technology/solution-neutrality to provide scope and incentives for safety-enhancing innovation without leading to lock-in and other forms of market failure.

Producers, distributors, and other service providers in the chain will also need to take responsibility for ensuring that information about safety issues is monitored and that the appropriate responses – redesign, recall, consumer information, etc. are implemented. Next to managing their own roles in the value chain, they also need to take joint and several responsibilities for interaction with other service providers and product manufacturers.

3.4.2. The impact on burdens for economic operators

It is worth linking this evolution to the burdens potentially imposed by legislative intervention. Of course, not all direct burdens of regulation are bad; some have the effect of helping firms and markets to internalise the costs associated with unsafe products; indeed, in relation to safety risks associated with digital technologies, it may not always be obvious how such risks should be mitigated (e.g. to what extent risks should be reduced, transferred to stakeholders better-placed to bear them or their effects minimised or compensated).

In this respect, policy measures involving *regulation* (e.g. design standards, mandatory product certification, testing and labelling, compulsory information collection and sharing, liability for harms from unsafe products or unsafe use of products) impose both avoidable and unavoidable burdens on firms. The avoidable burdens can be minimised or bypassed by changes in firm behaviour, which may involve simply compliance with *ex-ante* or 'black-letter' (rule-based) regulatory requirements or may allow firms to choose optimal ways of complying with outcome-based, principles-based or *ex-post* regulation. These changes, which should have the effect of mitigating risks, may involve product redesign or complementary/updated software and services, changes in payment and contracting arrangements, new or altered information collection and sharing, etc. In this context, the burdens associated with e.g., direct compliance are intended to induce behavioural change by businesses and their customers. Especially in the case of outcome- or principles-based regulation, or implementation by way of comply-or-explain processes and/or self- or co-regulation[79], such approaches are designed to stimulate innovation and the burdens should thus be regarded as (in part) necessary. However, this does not mean that they should be ignored. In some cases, the response of business may be to shift risk to parties not well-placed to manage it, as when they provide product users with information that cannot be effectively understood or used to reduce safety failures in product use; Thus impact assessment, monitoring and evaluation are needed to keep track of how burden-based incentives are perfoming. Moreover, residual burdens, in the form of increased costs to firms (and the costs of safety failures to users) can impose deadweight loss on the market that should be balanced against the value

[79] Well-designed self-regulation and co-regulation both can allow the rules to reflect specific and dynamic changes in technologies and behaviour and can operate at lower administrative cost. See e.g. Section 3.1 of the European Commission Better Regulation Toolbox Available at: https://ec.europa.eu/info/sites/info/files/better-regulation-toolbox.pdf (accessied 11/05/2022).

of safety improvements. This argues in favour of a risk-based approach to safety assessment, at least in cases where it is appropriate and necessary evidence and analysis can be used.

The objective here is to minimise inefficient distortions to behaviour. Finally, **it is important to avoid *unnecessary* burdens, especially those associated with unavoidable costs. In this regard, administrative burdens stand out as connected more closely to the means than the ends of regulation;** it is thus appropriate to minimise them, subject to attaining the policy objectives. To clarify this, the following paragraphs discuss:

- the **general issue of administrative and other direct costs** (as distinct from indirect and wider impacts, which reflect the market/value chain context) ; and
- **ways in which administrative costs might be mitigated or redistributed in more proportionate and less distorting ways**. Administrative costs are generally viewed as something to minimise, being least connected with the objectives of regulation. However, different types of firms will manage and minimise or pass along these costs in different ways; in this, they resemble other direct costs.

These direct burdens of regulatory compliance include product redesign to meet legal standards and collection and sharing of safety-related information. These may be higher for digital products, where safety issues may come from the interaction of products, or from the ways consumers use the products. This means that it is not always obvious where burdens should fall or how regulatory burdens will affect product safety. For example, a regulation that requires the provision of updated consumer information may damage product safety if the resulting costs encourage firms to make fewer or less frequent updates or to inform consumers about risks that might be more efficiently handled by product redesign. **These distortions can, however, be minimised by appropriate technologies**, such as automated updates to product software, alerts on products when the suggested use changes (possibly triggered by risky uses to avoid 'notification fatigue'), and the use of QR codes to connect consumers to coordinated information relating to products that are used in combination.

Regarding administrative costs, the implementation of regulations can be streamlined to minimise firm burdens e.g. by **accepting automated regulatory reports**, based as closely as possible on information that firms already have or are required to produce for consumers and other firms. This information provision can also take place via 'regtech[80]' if it is automated, done in (close to) real time and with minimal human intervention. This can reduce burdens and improve regulatory effectiveness in several ways: first, by eliminating periodic and burdensome reporting, it minimises the cost and disruption to small and micro enterprises, whose opportunity cost of compliance is highest.

Moreover, **the collection of 'real-time information', especially when done in an automated fashion, minimises the risk of intentional or accidental mistakes**. Regulatory changes (e.g. alerts or recall requirements) can be implemented more promptly and in a more proportionate fashion, and the damage (to users and firms) associated with lags and overshoot minimised. Indeed, in some cases the flow of information and control among firms, retail outlets, users and products can be reversed vehicles as in the case of smart roads built up from smart vehicles and smart grids involving networks of smart meters and other smart home appliances. The richer data streams associated with this kind of regtech

[80] Regtech refers to the management of regulatory processes through technology; its main functions of regtech to date include regulatory monitoring, reporting, and compliance, but it has been suggested that in some cases, digital communications between regulators and regulated firms could be used to provide more agile 'real-time' adjustment of regulatory provisions (e.g. standards, guidelines and approvals). The term was first used in relation to financial regulation (See Financial Conduct Authority, 2015,, Call for Input: Supporting the development and adoption of RegTech, Available at: https://regtechuk.com/uploads/3/5/8/3/35836616/fca-regtech-call-for-input-fintechuk.pdf.

ecosystem can, in turn be analysed to identify elements of market and user behaviour that were previously unobserved or poorly accessible.

Some of the direct cost burdens falling on the firms whose activities are directly regulated are activity-based procedural costs of the sort normally accounted for by e.g., the Standard Cost Methodology. Some of these are transitional or start-up costs (e.g., familiarisation, set-up for product information and reporting systems, extension of consumer relation management systems, etc.) and initial certification. Others are ongoing costs of compliance (e.g., collection, processing and reporting of specific information, participation costs in industry-based or multi-stakeholder bodies, costs of attaining and maintaining certification and/or standards compliance and the impacts of participation in standardisation activities). It is worth noting that costs of compliance may be unevenly distributed, because some firms will already be in compliance and others will face different costs depending on how far they are from compliance with new provisions and how different their existing systems are from those needed to fit the new rules. But this situation is not specific to digital product safety, and we will not further expand on it here.

Of course, **administrative costs rarely stay with the firms on whom they initially fall**: they will be passed on (to suppliers and customers) and **trigger changes in market structure and performance**. This may be a simple matter of increasing the market shares of compliant firms or those whose costs of coming into compliance are smallest. This, in turn, makes compliance more efficient and increases the extent to which users can rely on the safety of products on the market. But it may also involve realignment between EU and foreign firms in direct competition or along value/production chains extending beyond the Single Market. The costs may also affect market structure: the size distribution of firms, vertical integration and/or platform structure of digital product/service markets and the potential for new market segments to provide compliance as a service. These will depend on the way the chosen option is implemented. It is to be expected that these non-administrative impacts will be assessed in conjunction with existing law and other forthcoming legislation (e.g., the Digital Services Act, the Digital Markets Act, and the Data Act). Thus the assessment of administrative costs may need to pay particular attention to competition impacts.

As a final comment, since administrative burdens also fall on governments, we note that the same regtech and suptech[81] technologies used to reduce the burdens and improve the quality of firms' compliance with regulations can be used to reduce burdens on authorities, in terms of monitoring and enforcement and especially market surveillance. The most important aspects are whether the extent and pattern of these burdens is likely to affect the policy objectives or produce other adverse impacts and whether implementation and monitoring can be adjusted to address such shortcomings. As usual in assessment, **it can be anticipated that some administrative, transitional and ongoing costs may fall disproportionately on SMEs and/or on specific 'layers' of the digital product value chain** (e.g., software providers). For SMEs, this is not simply a matter of the ratio of costs to turnover, since the opportunity cost of transition and compliance may be higher for micro enterprises (who do not have scope for specialised compliance personnel); the result may be the exit or acquisition of such firms; in particular, since such firms are more likely to provide bespoke services or software than physical products, the consequence may be firm exit, greater vertical integration and possibly reduced product safety.

[81] "Suptech" is related to regtech (see footnote 80). Whereas regtech refers to applications of innovative technologies that support compliance with regulatory and reporting requirements by regulated institutions, suptech refers to technologies used by supervisory agencies themselves.

The specific requirements of the Commission option for a full revision of GSPD contain a number of provisions that will impose administrative burdens, though the provisions mainly 'level up' firm performance e.g., as regards the Product Safety Pledge, recall policies, interoperation with market surveillance regimes, online sales and the like. Some of the harmonisation provisions will reduce administrative burdens that stem from the need for firms simultaneously to comply with multiple and differing Member State provisions; in other cases, the direct administrative costs will be offset by market-based benefits (e.g., improved consumer willingness-to-pay for safer products and reduced costs associated with consumer harm from unsafe product use). In other respects, **implementation of the revised GPSD can be designed to minimise such burdens, e.g., by giving standing to common standards and certification and the creation and governance (or direct provision) of central repositories of product characteristics and consumer experiences**. Further, **the use of new technologies and digital solution could lead to efficiency** gains, as illustrated by the use of AI for dispute resolutions; the use of digital technologies (e.g., chatbots), especially in conjunction with databases of product characteristics and consumer records, could allow companies to handle more cases, faster and more effectively and to learn more efficiently about user-reported problems[82].

[82] This was further discussed during the European Consumer Summit 2022, Avaliable at: https://european-consumer-summit-2022.b2match.io/home. To clarify the example, if a product consumer support site had a suitably-configured chatbot, it could rapidly diagnose consumer problems and suggest solutions basd on recorded information. The digital implementation would provide a consistent real-time record of problems and the effectiveness of solutions. This record could be analysed using machine-learning (e.g. context-aware natural language processing (NLP) to continually improve the firm's understanding of the in-service performance of its products, changes in th operational environment (e.g. cybersecurity exploits) and user behaviour. The user-initiated engagement would help to mitigate privacy-related concerns with automated 'safety surveillance'.

4. BEST PRACTICES AND DEVELOPMENT FOR STANDARDS, CERTIFICATES AND LABELS FOR PRODUCT SAFETY ACROSS EU MEMBER STATES

KEY FINDINGS

A mapping of standards, certificates and labels that are developed by individual EU Member States or at EU level was performed. From these mapped practices, a total of seven case studies were selected that examined the practices in greater detail.

Analysis of the case studies shows that when it comes to product safety, labels, standards and certificates are foremostly a sign of trust to (potential) consumers of a product and often result in more transparency for both consumers and stakeholders in the value chain. This way, consumers can make more informed choices with less time investment. For companies, having a label or certificate can increase their competitiveness compared to other companies, and in particular international standards provide for access to wider market opportunities.

It is concluded that there are many benefits to the design and implementation of solutions by public entities, but that it is preferable to still take a bottom-up approach when developing these practices. Furthermore, effective communication campaigns are key to promoting existing initiatives and added value can be obtained by combining for example labels and certificates (e.g., a label indicating that a certificate has been awarded).

The analysis of standards, certificates and labels was chosen due to how these initiatives target product safety and supports decision making for the consumer. Standards, certification and labelling represent approaches that may combine product safety with consumer decision making through increased transparency of information in this respect. They may impact business operations as business applicants demonstrate adherence to a predetermined set of criteria while benefitting from new market opportunities. As such, they are positioned as a very visible representation of product safety and their analysis in the study represents another way in which product safety is maintained in EU Member States. However, the use of standards, certificates and labels presents a challenge on an international level, as differences in legislation need to be accounted for in order to achieve cross-border usability. The standards referred to in this section cover 2 types of standards: industry standards and government standards. Industry standards are voluntary and result either from committee activities or competition on the market. Committee-based standardisation is a process through which a group of stakeholders decides on how things should be made and the agreement of the group. Market-based standardisation is a process through which the market leader sets the standard practice of what is used. On the other hand, government-based standardisation is bound in legislation and is enforceable by the government[83]. The case studies examined industry standards even if government bodies are involved in supporting their uptake (i.e. the Luxembourg Product Circularity Data Sheet which, despite official support from the Luxembourg Ministry of Economy, is considered an industry standard[84]). For the sake of brevity, chapter 4 uses "standard" in reference to industry standards.

[83] Wiegman P., 2019, *Becoming the industry standard when standardisation is not standardized*. Available at: https://discovery.rsm.nl/articles/389-becoming-the-industry-standard-when-standardisation-is-not-standardised/.

[84] PCDS, 2021, *Circularity Dataset Initiative.* Available at: https://pcds.lu/circularity-dataset-initiative/.

A mapping of standards, certificates and labels was performed to develop an overview of the availability of these types of practices in connection to the new technologies and digital solutions analysed by this study. The mapping includes practices that are offered and used in the EU and concerns international standards, certificates, and labels as well as those developed by individual EU Member States for their markets. In the end, the mapped practices were compared to select seven practices that were further developed as case studies. Considerations of the selection process were:

- **Exploring scaling up examples of actions implemented on the national level.** This is important when considering practice transferability and scalability, in particular as one of the challenges appears to be supporting greater cross-border cooperation for consumer protection, including the development of common actions, such as certificates;
- **A balance between standards, certificates, and labels**. The mapping resulted in several examples that concern a combination of standard and label or certificate and label. This allowed for case studies to represent several practices and achieve a higher representation. Even though there are seven case studies, each of the standards, certificates and labels is examined through three cases;
- **A balance between the technologies and digital solutions** that are targeted or used in the implementation of the standard, certificate, and label. This ensures that the case studies support the analysis of a wider range of technologies and solutions to see what the differences and similarities between practices are; and
- **Representing product safety but also looking into durability, sustainability/circularity, and end-of-life cycles**. While most mapped practices focus on product safety, the study team felt it important to also represent aspects of durability, sustainability/circularity, and end-of-life cycles as they relate to and are supported by the different standards, certificates and labels.

The case studies examine in greater detail the selected standards, certificates, and labels according to the following factors:

- The **development and subsequent management of the practice:** how and why the practice was launched, details about the stakeholders involved in the development and management and support of its implementation. Importantly, linkages to other standards, labels, certificates and links to policies and regulations for product safety are considered. The latter can shed light on how new technologies and digital solutions are reflected by product safety legislation and allow considering how such practices could support the development of the GPSD;
- The **technologies and digital solutions that are used or affected by the standards, certificates, and labels.** This includes examining the application of different technologies in support of product safety and the way technologies facilitate communication on safety. This allows us to further ground our work not only in what needs to be done on the policy level to enable these practices, but also what kind of technology infrastructure is necessary to have these practices working;
- **The impacts of introducing and using the standards, certificates and labels on companies and consumers**. Attention is given to the added value of having the standard, certificate and label supporting product safety and to how the adoption and uptake of the standard, certificate and label is supported. The latter includes the policy support and technology support that enable the launch and maintenance of the standard, certificate and label. Consumer and company support concerns facilitating actions that allow the measure to become an embedded practice for companies and consumers; and

- **How the standards, certificates and labels help communicate product safety information.** This part specifically focuses on the consumer perspective, i.e. how consumers are informed about the practice and in particular how product safety information is communicated to the consumer.

These case studies conclude by reflecting on how the standard, certificate and label can offer lessons learned for the GPSD.

4.1. Analysis of approaches and impact on standards, certificates and labels in the EU Member States

Our study team has focused on solutions including product standards, security qualifications certificates, and labels awarded by entitled organisations in the context of product safety and other relevant areas (including cloud and cybersecurity). The cases present how new technologies and digital solutions are used to support the implementation of standards, certificates and labels (i.e. use of QR codes to scan product safety labels). Or they examine how standards, certificates and labels target the use of new technologies and digital solutions to ensure safer products for consumers.

Furthermore, the case studies examine how standards, certificates and labels affect not only products but also services. This is in light of connected devices which can make use of services (i.e., software updates to maintain product safety, connecting to the cloud to access data or protection from hacking). As discussed in Chapter 3.1, the discourse surrounding product safety needs to account for services that affect connected products, or even ensure their core functions. For this reason, the analysis of standards, certificates and labels that involved not only products, but also services, is done to support this discussion and provide input into topics which might be relevant or become relevant in the future. The table below presents the case studies that were identified and analysed.

Table 1: Best practices identified across EU Member States

Solution name	Solution type	Country	Entity in charge	Targeted at	Intended objectives
Security Visa - 2018	Certification	France	The French National Cybersecurity Agency (ANSSI)	Companies implementing security solutions	•Service with national competence •Contributes to information security by participating in research, development, and promotion of security technologies
EU Cloud Code of Conduct (CoC) - 2017	Code/Standard	EU	•EU Cloud Code of Conduct General Assembly •EU Cloud Code of Conduct Steering Board •EU Cloud Code of Conduct Secretariat	Cloud Service Providers	•Voluntary instrument •Allows a Cloud Service Provider to evaluate and demonstrate its adherence to the Code's requirements
European Secure Cloud (E Cloud) - failed	Label	France & Germany	ANSSI - French National Cybersecurity Agency (France) •BSI – Federal Cybersecurity	Cloud Service Providers, Product Suppliers and Consumers	•Improved IT security in France and Germany •Created a common basis for European cloud computing security by identifying reliable providers
Finnish Cybersecurity Label - 2019	Label/Certification	Finland	•Finnish Transport and Communications Agency Cyber Security Centre Finland	IoT companies and their users	•Identifies products which safely collect and transmit data in digital format •Tackles the most common security threats affecting consumers on the Internet

Geprüfte Sicherheit (GS) Label - 1988	Label	Germany and Western Europe	The Central Office of the Länder for Safety Engineering	Consumers	•Demonstrates to consumers that the product is subject to voluntary safety test by an officially recognised test centre •Indicates that the health and safety of consumers is not at risk during the foreseeable use
Manufacturer Usage Description Specification (MUD) - 2019	Software Standard	International community	Internet Engineering Task Force	Agents on behalf of the consumer	•Allows IoT device makers to advertise device specifications •Signals what sort of access and network functionality the device requires to properly function
Product Circularity Data Sheet (PCDS) - 2019	Standard	Luxembourg	The Ministry of the Economy of Luxembourg +Impakt (private consulting)	Companies and consumers	•Establishes a standard to communicate data and information on the circular economy characteristics of a product

Source: Author's own elaboration.

4.1.1. Approaches taken in the development and introduction of standards, certificates and labels for product safety

Before examining the technologies and communication used to support standards, certificates and labels as well as their added value to users, it is first worth developing a broad view of how EU Member States approach their development. To effectively create and deploy a national initiative, **different stakeholders have to come together,** including actors from the public and/or private sector. In the public sector, the actors are either national ministries or government agencies. The private sector includes all the firms, organisations, consulting companies, product suppliers, and service providers at large. Before diving deeper into the approaches to stakeholder involvement, it is worth noting that stakeholder involvement is not a rule followed by every EU Member State.

The **ANSSI Security Visa, for example,** is an initiative to reward French companies that implement reliable digital security systems through a process of certification. The Security Visa is implemented and managed by the French National Cybersecurity Agency (ANSSI). Not only is the agency the initiator of this approach to product security, but it also ensures that the security tests and the entire evaluation process are performed by laboratories recognised by the agency itself. As such, the Security Visa is an example of centralising the process of development and management within a single government entity, without direct stakeholder involvement. This process is perhaps necessitated because the certificate deals with cybersecurity, requiring tighter oversight. But it does highlight the aspect of consumer trust. Because the Security Visa is issued by a national agency (ANNSI), companies and consumers have high trust in products and services offered by certified companies. Thus, the Security Visa shows that the successful deployment and uptake of a certificate can be achieved in part due to consumer trust in the issuing agency. At the same time, it also highlights how the introduction of standards, certificates and labels should consider the consumer perception towards the involved stakeholders.

As for other examples that saw the involvement of the different parties, the reviewed initiatives use different consultation and management systems, which aim not only at developing the initiative but also to **gain visibility among potential users, beneficiaries**, and **attract new stakeholders**. In the case of labels, for instance, this could mean attracting new applicants to the solution.

- The **EU Cloud Code of Conduct (CoC)** is a voluntary instrument that has been developed by the Cloud Select Industry Group (CSIG) and allows Cloud Service Providers (CSPs) to evaluate and demonstrate their adherence to the CoC's requirements (regarding security and data protection requirements that are GDPR-compliant). As the CSIG includes representatives of European and multinational companies and organisations, together with authorities of the European Commission (involvement of DG Connect and DG Justice), as well as the Working Party representing Data Protection Authorities, the governance is organised around a General Assembly, a Steering Board, and an independent monitoring body. The monitoring body has a pricing scheme to cover its costs. The General Assembly is open to everyone adhering to the General Data Protection Regulation (GDPR). The reasoning behind this is that standard development is a matter where everyone should be able to participate; and

- In the case of the **Product Circularity Data Sheet (PCDS) in Luxembourg**, the standardised digital "fingerprint" for sharing trusted data on the circularity of a product, the main public stakeholder involved is the Ministry of the economy of Luxembourg, which represents the national government in the initiative. However, the governance of the PCDS is shared with the consulting enterprise +Impakt, recruited after a call for tender, which has provided external support as circular economy expert to the government. In terms of digital enabler, it is the digital firm Cobuilder that was chosen to create and develop the use of the standardised PCDS templates. Additionally, more than 60 international and regional companies from the private sector are collaborating with both the Ministry and +Impakt, to provide information on all products supplied by these companies[85]. Finally, there are "accredited auditors", who are commissioned by the Ministry to verify the data entered by the manufacturer of the product into the standardised PCDS template[86]. They play a crucial role in increasing the consumer's trust related to the capability of the entire process[87]. The stakeholders are managed through a close and continuous consultation between the public authorities in charge, and the private organisations[88]. The initial developers, meaning the Ministry of Economy, supported by the consulting firm +Impakt and the digital enabler Cobuilder are responsible for the implementation of the standard. To promote co-creation and stakeholder involvement, focus groups have been created on different topics such as auditing, Information Technology, business models, technical aspects, etc. Additionally, a webinar is organised three to four times a year by the Ministry to keep the stakeholders informed of the initiative's advancement[89].

One of the benefits of **stakeholder inclusion** emerging from these examples is the **legitimisation of the initiatives**. They help reduce the concerns arising from a top-down model that the standards, certificates, or labels are introduced without understanding the actual needs of the industries they should support. Yet the example of ANSSI Security Visa, which has centralised development and implementation, reportedly achieves a similar result of legitimising the certificate because it is connected to a government agency. Thus, the development of these initiatives shows that uptake of standards, certificates and labels is affected by creating mechanisms (in the case of EU Cloud CoC) to build trust or leveraging trust in stakeholders involved in the process (PCDS) or leveraging trust in government agencies (ANSSI Security Visa).

From the examined case studies, there is one example of an initiative that was ambitious yet failed to take off. The ESCloud was an attempt between France and Germany to merge two national initiatives aimed at Cloud security: the French SecNumCloud and the C5 German catalogue[90]. These intentions to cooperate were based on two comparable approaches to a security issue, with the final objectives of not only identifying safe providers of Cloud computing services in France and Germany but also of progressively deploying the initiative at the European level. The two countries were hoping that an initial Franco-German collaboration for a label would have spurred other countries to follow them. However, according to the German Federal Office for Security in the Information Technology, the technical conditions were not met for the label to be properly launched, and despite the close collaboration for several years and great potential benefits of the security solution, various obstacles prevented its creation. In particular, the **following issues** were identified:

[85] PCDS Luxembourg, 2022, The Circularity Dataset Initiative.

[86] Cobuilder, 2022, *Luxembourg launces product circularity data sheets in a bid to boost circularity*. Available at: https://cobuilder.com/en/luxembourg-launches-product-circularity-data-sheets/.

[87] PCDS Luxembourg, 2022, *The audit system*. Available at: https://pcds.lu/the-audit-system/.

[88] Luxembourg Trade & Invest, 2021, *New Luxembourg Strategy for the Circular Economy*. Available at: https://www.tradeandinvest.lu/news/new-luxembourg-strategy-for-the-circular-economy/.

[89] Interview with the PCDS Representative.

[90] ANSSI, 2022, ESCLOUD – *Un label franco-allemand pour les services d'informatique en nuage de confiance*. Available at: https://www.ssi.gouv.fr/actualite/escloud-un-label-franco-allemand-pour-les-services-informatique-en-nuage-de-confiance/.

- For the label to have gained visibility, it would have been necessary to have a **wider marketing campaign across the EU**, not only to show the benefits of the label but also to encourage similar bilateral and multilateral initiatives across the EU Member States;
- The **competitiveness of the label**, with respect to other private solutions, should be at the forefront of the development and launch to demonstrate the added value for companies to apply for the label; and
- Such a label should be **very clear and transparent** on the new rules and norms that a cloud computing service should fulfil. In particular, the label had established a list of fifteen requirements, which were common with pre-existing rules in the two countries.

At the same time, ESCloud does help highlight the interest in use of international standards concerning new technologies and digital solutions. In 2019 the World Trade Organisation (WTO) Technical Barriers to Trade Committee found that there are: "significant benefits to using standards as a regulatory tool, the importance of monitoring standards referenced in regulations".[91] Monitoring of emerging standards signals importance of cooperation and use of best practices in standard adoption. For example, the Standards Council of Canada notes that 56.9% of standards for electronics, information, technology and telecommunications products in Canada are in fact international standards adopted by the Standards Council.[92] Similarly, a presentation by Directorate-General for Internal Market noted that international standards are prioritised as a basis for European Standard development.[93] Australia further showcases a high level of trust in international standards, where the Australian Government position notes that: "if a system, service or product has been approved under a trusted international standard or risk assessment, then Australia's regulators should not impose any additional requirements for approval in Australia"[94].

4.1.2. Technologies facilitating product safety through standards, certificates and labels

Beyond the managing decisions that support the launch of standards, certificates and labels, the case studies also explore the use of technologies and digital solutions as facilitators or enablers for these initiatives. The following table presents a non-exhaustive list of different technologies employed across the examined initiatives.

[91] WHO, 2019, *WTO members discuss product quality, safety and standards, debate new trade concerns*. Available at: https://www.wto.org/english/news_e/news19_e/tbt_16nov19_e.htm.

[92] Standards Council of Canada, 2019, *Incorporation of Standards by Reference in Canada: Considerations for Trade.* Available at: https://www.wto.org/english/tratop_e/tbt_e/01_a_p1a_canada.pdf.

[93] Vaccaro S., 2019, *Referencing standards in EU legislation.* Available at: https://www.wto.org/english/tratop_e/tbt_e/01_c_p1c_eu_vaccaro.pdf.

[94] Department of the Prime Minister and Cabinet, 2022, *Acceptance of international standards and risk assessments for product approvals.* Available at: https://www.pmc.gov.au/domestic-policy/taskforces-past-domestic-policy-initiatives/industry-innovation-and-competitiveness-agenda/acceptance-international-standards-and-risk-assessments-product-approvals.

Table 2: Impacts of the initiatives analysed on product safety and durability

Name of initiative	Technology	Use	Opportunities and challenges for product safety and durability
GS Label	QR code	QR codes are printed next to the GS label, that link to a GS database so that consumers can check whether the label is real and request additional information about the product.	The use of QR codes and a continuously updated database increases product safety, as more extensive product descriptions or even instructional videos on how the product should be used can be added.
	GS database	The GS maintains different databases for each GS body. These databases contain product information that is accessible to consumers who scan the QR code next to the GS label. For an additional fee, manufacturers can add extra information about the product in the database.	The fees collected from companies add to the sustainability of the GS label as these fees can cover the costs of maintaining the label and its database. The existing challenge is the lack of centralisation as each GS body has its own database in which GS certifications and corresponding product information are listed. This limits comparability and searchability of products for consumers who need to access different databases under individual GS bodies.
Finnish Cybersecurity Label	ETSI criteria	ETSI criteria are used as the basis for the labels requirements. Applicants for the label need to meet criteria that have been adapted from ETSI to meet the specific needs posed by security threats concerning consumer devices	The Cybersecurity label requirements are designed to comply with a wide range of national and international requirements and recommendations. This helps ensure that the work required for the label can also be applied in other environments at the international level
ANSSI Security Visa	Label	ANSSI opted for a simpler approach where companies and products meeting the cybersecurity standards can display a label signifying that the product meets ANSSI certification requirements.	Security labels are a straightforward and efficient way (if an unsophisticated in the context of technologies and solutions discussed in this analysis) of promoting product safety. They have a lower cost of entry for businesses while offering benefits for both suppliers and consumers.

Product Circularity Data Sheet (PCDS)	Digital Product Passport (DPP)	DPP takes the form of a Data Template where all the information about the products is collected along the supply chain. The system is backed by a decentralised information exchange system, which also secures the producer's intellectual property, The DPP can be updated and revised as soon as there is a change in the product (composition, regulation, recycling, etc.).	DPP provides benefits for the developers and, suppliers across the value-chain, increasing the available information to businesses and facilitating the transfer of information. Consumers have access to the DPP data integrated by the producer. The main concern is the complexity of the information received which can be hard to understand for the consumer. While there is an opportunity here to develop a more consumer friendly database, there currently are no such plans.
EU Cloud Code of Conduct (CoC)	Scanning and monitoring solutions	The Monitoring Body of the EU Cloud CoC is responsible for the annual and ad hoc monitoring of certified cloud service providers for their adherence to the GDPR. The Monitoring Body is currently looking for ways to automate the monitoring process.	The main challenge is the current lack of technologies that would have the capacity to effectively monitor legislative developments and data submitted to the Monitoring Body. The importance of such technologies is highlighted by the growing complexity of cloud services while ensuring adherence to the GDPR.
Manufacturer Usage Description Specification (MUD)	Embedded software standard	MUD functions as an embedded software standard which allows devices using IoT to send information to network about the functionality and level of access the device requires from the network to properly function. The network can use this information to ensure a context-specific access policy.	MUD is primarily aimed at device manufacturers and network service providers, creating a method that is easy to use while being scalable. The communication enabled between the device and the network is meant to reduce threat to devices (MUD defines the types of communications the device accepts from a network).

Source: Authors' own elaboration.

When discussing the use of these technologies it is important to consider the role of communicating safety information to different stakeholders. Examination of case studies reveals different approaches and purposes for communicating information about product safety.

Communication to applicants involves actions meant to inform, market the initiative to businesses and attract their participation. Cases, such as the ANSSI for its Security Visa, use the expertise and legitimacy provided by its experience as a government agency and communicating to its partners and stakeholders on the evaluation process necessary to obtain the Visa and promoting the solutions it offers.

Communication between applicants represents actions and technologies that allow different actors across the value chain to communicate information relevant to product safety. A primary example of this is DPP under PCDS which collects information about production materials, the product manufacturing, the distribution, the consumption and finally the recycling features of the product. At any stage along the supply chain, stakeholders can request data about the product in development or supply and renew information relevant to the product development. Because the goal of PCDS is to support communication about the circular economy characteristics of products, the DPP contributes towards product sustainability.

Communication to consumers showcases actions and technologies that provide users with knowledge about the standards, certificates and labels and communicate product safety information. The use of QR codes with the GS Label is a prime example of employing new technologies to present useful information to consumers. Here it is possible to compare GS Label with the ANSSI Security Visa which uses a more traditional label applied on the product. The GS Label, through the QR code, offers consumers with much more information about the product (the QR code takes the consumer to a database containing product information). But the GS Label is also dependent on the consumers having access to a smart device capable of reading QR codes, which can limit consumers in gaining the full benefits. The label for ANSSI Security Visa is not dependent on access to smart devices (or any technology) but it provides consumers with more limited information essentially only informing them that the product meets ANSSI standards. Comparatively, the GS Label offers more flexibility for businesses with different pricing tiers allowing to provide more information for consumers (higher priced tiers allow businesses to embed more information about the product in the GS database). ANSSI Security Visa label is cheaper and easier to apply for businesses, but the GS Label, through expanded information, offers better marketing opportunities. Both approaches have their benefits and drawbacks and the application of either approach should be weighed against the targeted consumers.

Raising consumer awareness involves communication that not only informs consumers about the direct benefits of the initiative, but also contribute to their wider understanding of product safety. This is paricularly evident when actions concern new technologies and digital solutions. For example, the Finish Cyber Security Label concerns the safety of IoT devices, which is considered a novel concept for both manufacturers and consumers. As such, the label contributes not only towards supporting manufacturers and consumers of labelled devices, but also to raise awareness of the importance of digital product safety. This showcases the importance of visibility for product safety initiatives as increased exposure to them contribute to wider consumer understanding about product safety.

4.1.3. The added value of standards, certificates, and labels to enhance product safety

Putting our research into perspective, it is important to highlight the lack of clear data that can be retrieved from primary-resource research. While we know that these initiatives exist and have been deployed successfully, it is hard to understand how many actual applicants to labels or certifications there are, or how many users really refer to the standards or databases when making a consumption decision.

At the same time, we strove to aggregate the available information to discuss the added value of labels, certifications, as well as standards. To achieve this, this added value was evaluated separately for two groups of stakeholders.

a. The added value for companies

For companies, **labels** show a sign of **trust** to consumers as they offer more information on their products' characteristics. The label can therefore add value to a product, by signalling safety to consumers. **The Finnish Cybersecurity Label** is for instance designed to help consumers make safe choices when purchasing IoT devices and services. By applying the label to their products, Finnish companies show consumers that the device is secure by design, and consumers thus know that attention has been paid to its information security. This provides the companies that have been awarded a label with a **competitive advantage**, as they make room for a more informed consumers' choice. Similarly, **the German GS label** is one of the oldest and most recognised labels for the safety assurance of products in the German market, and provides these companies with a non-negligible advantage on the national territory, as well as in other countries where the product could be exported to and where the label is recognised[95]. In 2007, almost 20 years after the initiative's launch, 60,000 licenses had been issued by (bodies accredited by) the Federal Ministry of Labour and Social Affairs[96]. On an international scale, during a WTO thematic session on labelling members acknowledge that labels are an effective method for providing information to consumers. At the same time, it was recognised that use of labels can be challenging as they continue to incorporate more parts of the value chain into their messaging. This raises the subject of responsibility for different actors across the value chain to monitor product labelling and ensure that the product that reaches consumers matches health and safety requirements[97]. **Certifications** provide their own advantages. For instance, the French **ANSSI Security Visa** allows those companies which are awarded the label (either product suppliers or service providers), to gain in competitiveness compared to other French companies providing security services, but also internationally. The recognition of the Visa by the French government provides a relevant **proof of the robustness of the product** (as the certification is awarded only after a resilience to simulated cyber threat is proven by a licensed laboratory). Besides, the certification based on the Common Criteria (CC) allows the companies to **access wider market opportunities** as this international standard is based on mutual recognition agreement for product safety[98].

Standards have similar benefits, as they create a common outline to display the information, thus **increasing transparency and creating added value** on the market. The Manufacturer Usage Description (MUD) is an example of a standard providing further transparency on the safety conditions

[95] TUVRheinland, 2022, *GS Mark – Geprüfte Sicherheit (Tested Safety)*. Available at: https://www.tuv.com/world/en/gs-mark.html.

[96] EFTA, 2007, *EFTA study on certification and marks in Europe*. Available at: https://www.efta.int/publications/study-certification-marks/efta-study-on-certification-and-marks-in-europe-full-report.

[97] TWO, 2020, *Thematic Session on Technical Regulations: Marking and Labelling*. Available at: https://www.wto.org/english/tratop_e/tbt_e/tbtthematcimarkinlabel27102020_e.htm.

[98] Ibid.

of devices. MUDs are an embedded software standard that allows IoT device makers to advertise device specifications, including the intended communication patterns for their device when it connects to the network. The network can use this information to ensure a context-specific access policy for all users (end users who make use of automation, manufacturers, and service providers). What is interesting within the context of GPSD is that the **MUD is an evolving framework** that is less mature than an Internet Standard. It is being **developed by an international communit**y, the Internet Engineering Task Force (IETF) which is composed of network designers, operators and researchers. While the IETF proposes developments for MUD, modifications are only approved by the Internet Engineering Steering Group (IESG). In other words, an international consultation and consensus between different actors propose modifications while a centralised steering group is responsible for their approval. By the nature of the IETF, it is also a "recommended" standard, not enforced by any legislation or compliance action – it is adopted because it makes sense to the internet community. The standards discussed in this document are either European standards or national standards, and are enforced. MUD is developed through a shared interest of stakeholders coming together to solve a challenge through the creation of a common approach[99].

Similarly, for the **Luxembourg PCDS** which permits the circulation of trusted data on the sustainability of a product, the standard has a facilitator role to the companies adhering to it. There is indeed growing pressure on the part of policy makers to provide greater transparency on the sustainability of products, particularly with the revision of the SPI and the introduction of a DPP, which the initiative allows to overcome thanks to its information on-demand decentralised system. There is additionally full trust around the system, as not only is the producer's property protected, but the system of third-party auditing[100] generates increased credibility and international recognition. The reporting costs are also reduced thanks to the standardised information exchange, which allows to reduce duplicates and to answer to high solicitation levels. The platform especially eases communication for SMEs at the beginning of the value chain, which allows important savings in terms of time and money on information collection. There is a general pressure to modify products' properties and make them circular, which will open new needs on design and business models in the end-of life stage. All the companies additionally benefit from being part of a large network that collaborates directly with the government on safety and sustainability, thus favouring brand reputation and market access.

The three safety solutions presented above tend to produce **similar benefits to companies: by boosting their competitive advantag**e, they allow product suppliers and service providers to gain a dominant position on the national market where the initiative is implemented, and even **opens international opportunities** for them, especially when these solutions' credibility is reinforced by the government's support.

In addition, when a label makes use of an online database that consumers can access to find product information (either by using a QR code or searching the database manually), there are possible additional benefits for producers and the managing bodies of the label. For instance, some so-called 'GS bodies' (e.g., organisations that have the accreditation to test products for the GS label) offer 'premium' database entries in which manufacturers can, for a fee, add additional information about their product or company[101]. Not only can this increase product safety, as more extensive product descriptions or even instructional videos on how the product should be used can be added, but it can

[99] Wiegmann P., 2019, *Becoming the industry standard when standardisation is not standardized*. Available at: https://discovery.rsm.nl/articles/389-becoming-the-industry-standard-when-standardisation-is-not-standardised/.

[100] PCDS Luxembourg, 2022, *The audit system*. Available at: https://pcds.lu/the-audit-system/.

[101] Certipedia, 2015, Available at: https://www.certipedia.com/your_certipedia_entry?locale=en.

also add sustainability for the label as these fees can cover the costs of maintaining the label and its database.

b. The added value for the consumers

The same considerations on the benefits of certificates, labels and standards are now evaluated for consumers. Firstly, in the case of the **Finnish Cybersecurity label**, the consumers' choices are informed in a very direct and clear manner, **reducing the time investment** needed to understand the product safety concerns by codifying the idea of approval and certification within the label. Similarly, in the case of the GS label, the use of the QR code provides consumers with a quick option for accessing information about the product's safety features[102]. The **GS label and the QR code** also allows consumers to make **more informed decisions** about their purchases. It is therefore meant to communicate the added value of the product for its compliance with product safety standards.

Similarly, in the case of a certification such as **ANSSI's initiative**, the Security Visa serves to **improve communication** between the product suppliers or service providers and the consumers, and thus **increases transparency** on the efficiency of security solutions, as well as clarity of information and reliability. Thanks to the Visa, consumers can develop a better understanding of which existing products best fit their needs and save costs (both in terms of time and money) to collect information on the reliability of the product they are purchasing. It is especially of interest given that it can be hard for average citizens or firms to be aware of the technical details for cybersecurity-related products, and of the risks they face in case of selecting the wrong product for their needs.

As for standards, a practice like the **EU Cloud CoC** similarly promotes **transparency** and easy access of information to consumers, by allowing consumers to understand whether the Cloud Service under consideration is appropriate for their use case. Besides, consumers' rights are guaranteed by the CoC, as if they believe that something is off, it is possible to anonymously file a complaint with the Monitoring Authority. Similarly, the MUD, which is a software standard, provides consumers with the benefit of reducing the vulnerability of the device and the potential of the device to do harm. However, the MUD focuses on agents on behalf of the consumer that will make an expert decision on what to tell the consumer and how to tell them. Finally, if the PCDS has as a final aim to improve the communication between the supply chain actors and the consumers, the Ministry does not intend to create any information platform directly made available to the citizens.

In general, product safety solutions improve the quality of the information provided to the consumers by making it more easily accessible, and thus increasing transparency on a product's characteristics and/or safety features. This is beneficial to consumers, as it may be difficult for them to have a good understanding of such technical issues, and therefore facilitates their tasks by saving them time and money they would have had to invest to collect such information.

[102] TÜVRheinland, *CE Marking and GS MARK - The difference*s. Available at: http://www.za.tuv.com/content-media-files/master-content/services/products/0175-tuv-rheinland-gs-mark/tuv-rheinland-gs-mark-faq-differences-ce-marking-gs-mark-en.pdf.

4.2. Conclusions and lessons learnt

After careful consideration of these examples of case studies and best practices deployed within the EU, it is possible to identify key lessons:

- **There are many benefits from the design and implementation of solutions by public entities** (ministries or governmental agencies) that could provide insights into actions taken on the EU level. Firstly, the involvement of public entities provides legitimacy to the standard (e.g., PCDS) or certification (e.g., ANSSI Security Visa), as the government has no direct financial interest in the deployment of the initiative, thus ensuring credibility to users. Secondly, public entities facilitate the involvement of multiple stakeholders, for instance through calls for tenders, or in general the organisation of public consultations. These examples can be scaled up to the EU level where initiatives can likewise benefit from the EU experience in stakeholder consultations and managing large-scale initiatives;

- Although the involvement of a public entity favours the initiative's deployment, **it is also noteworthy to resort to bottom-up approaches,** by using specific national and sector initiatives, and deploying them at the European level to increasingly cover diverse sectors and EU Member States (e.g., PCSD). One of the explored examples, the MUD Specification, is in a position to adapt to technology developments because it is an open international community consisting of network designers, operators, researchers, and vendors that aims to make the internet work better. As any interested and qualified person can work for the IETF, the MUD is directly influenced by technology experts. Such bottom-up stakeholder input could be introduced not only as stakeholder consultation during development for product safety policy, standards, etc. but even as a continuous process that allows for more flexibility in reacting to emerging technologies and digital solutions;

- **Effective communication** is key to promoting existing initiatives. This is true not only to promote existing solutions such as labels to potential applicant firms, which could be interested in gaining the competitive advantage deriving from it, but also for end-users and consumers. It is important for the latter category to be able to recognise and understand the logos (labels) and information (QR codes or certifications), they may see on the products' packages. Furthermore, it is crucial that they then understand how to retrieve the information and process it efficiently. To that end, the EU should organise the promotion and advertisement of existing solutions to its citizens. Without investment and advocacy for existing security solutions, there can be no spill over across sectors and borders within the EU;

- **Market surveillance for products could be enhanced** by leveraging DPPs, such as the PCDS in Luxembourg. PCDS tracks detailed information across the value chain, offering authorities large amounts of relevant data about product development, components, manufacturers, and suppliers. A third-party verification system audits the data input from manufacturers, checking for potential errors and deviations from the expected product composition or characteristics (in the case of PCDS, the use of circular product). The verification system enhances trust in the product and provides tools for ongoing monitoring. PCDS could be used as the basis for scaled up approaches for monitoring and data sharing between EU Member States. Such a system would allow contacting manufacturers that use the identified component in their manufacturing process and track the products that are further along the value chain. The creation of a common information-sharing system would enable more effective market surveillance for the EU, tracking not only faulty products but even faulty parts or software; and

- Finally, the **recourse to decentralised databases**, such as in the cases of PCDS and the GS label bring many benefits, both for the producers and the consumers. Even though the creation of a unique common European database to collect and group products' features seems unrealistic for now, the EU could draw on these good practices to promote consumers' awareness and consider exploring such ambitious undertakings in the future.

5. RECOMMENDATIONS

The study showed that new technologies and digital solutions can have an increasingly important role regarding product safety. This chapter highlights key findings and proposes recommendations to address them.

- The first section summarises, under a SWOT analysis, the findings from the study and the potential roles of new technologies and digital solutions to address product safety; and
- The second section proposes legislative and non-legislative recommendations stemming from these findings. In light of existing practices, the GPSD could have an important role in minimising market fragmentation and harmonising the ways new technologies, digital solutions and related aspects of product safety are defined and subsequently treated within the Single Market. The recommendations are articulated along three main dimensions: (i) better framing and monitoring of product safety in relation to the landscape of new technologies and digital solutions, (ii) avoiding potential detrimental effects related to product safety and (iii) strengthening the roles of these technologies and solutions in enhancing product safety when that creates net value. When relevant, references to provisions of the proposed GPSR are made.

5.1. Findings on the potential influence of new technologies and digital solutions in relation to product safety

As a summary of the findings, the study team produced a SWOT analysis.

Table 3: SWOT analysis of the potential influence of new technologies and digital solutions in relation to product safety

Strengths	Weaknesses
• Increased product traceability and transparency; • Improved accessibility of product information for consumers, and enhanced ability to improve the quality and utility of that information; • Efficient provision of tailored responses to individual issues; and • Remotely product updates to address defects.	• Gaps in digital literacy and network access, not allowing to fully rely on new technologies and digital solutions to address product-safety, for reasons of fairness and inclusiveness; • Fragmented landscape of policies, regulations and (often ambiguous) definitions of technologies and digital solutions across EU Member States, use cases and sectors; and • Impact of technologies and digital solutions (in concert with other trends, such as growth in e-commerce and transition from product to services) on product ownership, which can dilute or distort responsibility across the value chain; • Gaps in continuity of services related to product safety over time; • Increased complexity resulting from interconnectedness between technologies; • Inadequate information sharing among stakeholders along the value-chain.
Opportunities	**Threats**
• Facilitated access to information can improve product recalls and the efficiency and effectiveness of market surveillance (more accessible information related to products, components, producers and distributors) (e.g. via QR codes); • Paving the way for international standard-setting and ensuring awareness of European values in global standard setting activities; • Potential use of traceability functions to improve product sustainability and circularity; • Potential to further empower consumers; and • Ability to analyse complex amounts of data, for instance for market surveillance and understanding consumer behaviour.	• Need for flexibility due to constant evolution of the digital ecosystem and emergence of new technologies and digital solutions; • Lack of long-lasting interoperability between various technologiesPotential negative impacts of algorithms; • Difficult to "get it right" because of increasing complexity in relation to side-matters and articulation with other policy initiatives related to data privacy, consumer right, product sustainability or digital services for instance; and • Due to potentially high negative environmental impacts related to energy, resource consumption and unnecessary obsolescence, global costs may outweigh global benefits, but not be fully taken into account by e.g. producers and consumers.

Source: Authors' own elaboration.

5.2. Our recommendations

The following tables present an overview of policy recommendations to the EU in support of product safety linked to new technologies and digital solutions. These recommendations are further discussed in the subsequent sections.

Some of these recommendations are related to legislative change, while others are more general and might not require legislative evolution.

Table 4: Overview of the policy recommendations

General objective	Issues addressed	Specific objectives	Stakeholders involved	Timeline	Means
Framing and monitoring					
Monitor Member State activities related to new technologies, digital solutions and product safety	Lack of overview on the different practices emerging in EU Member States, risking market fragmentation but providing useful 'natural experiments' with a potential for replication at a larger scale	Implement an EU Observatory for product safety linked to existing systems (Safety Gate, ICSMS), with a focus on new technologies and digital solutions Attach product safety to existing initiatives e.g. adding product safety sections to the country profiles in the Eco-Innovation Observatory	European Commission, in close cooperation with national bodies for product and service safety	The observatory could be launched following implementation of the revised GPSD. The Eco-Innovation Observatory reports are ongoing.	The costs of developing and sustaining such an observatory can be compared with those of existing observatories (e.g., milk, meat, sugar…). The observatory is expected to have a web interface and can be managed by existing staff members of the EC. As for the Eco-Innovation Observatory country profiles, some additional days of research (10-15) should be budgeted.
Use digital solutions to handle complexities associated with evolving nature of product ownership	Digital solutions affect various stakeholders along the value chain and question the concept of	Develop repositories of information relating to (at a minimum) product characteristics, producer activities (e.g., recalls, repairs etc.), safe use	European institutions	To be developed in the context of the adoption of the GPSR	Relationships between stakeholders should be made technology-neutral (or at least flexible) and principles-based.

	product, ownership, including through blurring lines between products and services, leading to market and informational failures	instructions and safety incidents.			The repository could be implemented by a distributed ledger to ensure data integrity, accessibility and authenticity.
Clarify the linkages between the General Product Safety Regulation and other regulations affecting aspects of digital product safety	With increasing overlap between products and services, other regulations and initiatives linked to one or the other may have broader effects, including on product safety. Note: the GPSD does not currently cover services	In the revised GPSD, differentiate between digital product risks and digital solutions to product safety (Chapter II of the regulation dealing with safety requirements) Expand the minimum level of requirements provisioned in article 7 Articulate parallel initiatives, such as the Digital Product Passport introduced by the Sustainable Product Initiative with product-safety related matters	European Parliament	During the revision of the current GPSD	Legal work development should be internalised in EP committees responsible for overviewing the GPSD

Limiting potential detrimental effects related to product safety					
Improve transparency, data control and data management	Potential counter-productive effects of too much information Unclear definitions of transparency and personally-identifiable information (PII) as related to product use	Provide consumer-relevant information in a consumer-friendly manner Mitigate the risk of consumer overconfidence Updated GPSD should include clear and relevant definitions of transparency, information control, information management	European Parliament and European Commission, in conjunction with industry and consumer association representatives	Definitions should be included in the update of the GPSD	Legal work development should be internalised in EP committees responsible for overviewing the GPSD The means needed relate mostly to coordination costs, as well as potential external legal support
Tackle obsolescence from a product safety perspective	Products may need updates throughout their useful life to remain safe	Introduce minimum specifications to ensure product safety for a publicly-disclosed period of time into Article 7 of the proposed GPSR. The legal requirement to set such a period should allow differences by product. Obligations should remain proportionate and minimise competitive foreclosure.	European Parliament	During the revision of the proposed GPSR	Legal work development should be internalised in EP committees responsible for overviewing the proposed GPSR

Encourage the use of new technologies and digital solutions to enhance product safety					
Introduce automated information exchange	Potential for greater efficiency and reduced administrative burden	Modify proposals for labelling and certification to include automated verification of compliance Impose automated reported to Market Surveillance authorities by producers and distributors of information required by regulation Modify consumer information provision to require producers and distributors to inform users of safety issues detected by automated information exchange Inclusive provisions for technological means of verifying standards compliance with products offered for sale	European Commission, European Parliament, industry and consumer/civil society organisations	During the revision of the proposed GPSR	Incorporation of technology-neutral incentives to adhere to state-of-the-art technology standards and measures (legal work development should be internalised in EP committees responsible for overviewing the proposed GPSR)[103]

[103] Some efficiency gains could be made through the stimulation of European research cooperation on the use of new technologies and digital solution, including exploring the use of digital labels and AI.

Communicate product safety to consumers	Potential for improved effectiveness and efficiency Help consumers make informed decisions Align market forces with improved product safety and facilitate the incorporation of user experience and other in-service feedback into the value chain	Define minimum level and type of communication to users (including information required under Art. 5 of GPSD) Facilitate competition on the basis of product information provision; and Ensure fair access to all (potential) consumers.	European Commission, industry and consumer/civil society organisations	GPSD implementation and monitoring, drawing on lay participation and evidence collection.	Explicit lay participation in standards and monitoring, dedicated consultation on understandability and usefulness of product safety information.
Develop definitions for new technologies and digital solutions, while playing a leading role in global standards development	As new products and components come from all over the world, global standards should reflect European values. European initiatives can also strengthen global	Coherent EU-wide technology-neutral and future-proof legislative action Support bottom-up approaches to EU-wide standards, certificates, and labels	European Parliament to suggest technology-neutral safety definitions and specific legal definitions for technologies and	Legal definition development: in the context of the revision of the GPSD Campaign: following the approval of the proposed GPSR, aligned with the	Legal work development should be internalised in EP committees responsible for overviewing the GPSD revision Communication campaign means can be compared to those of similar initiatives, e.g., for the Eco-Label

	development and use of digital solutions to environmental issues (e.g., combining DPP with Sustainable Product Initative)		digital solutions (top-down) Body of international EU experts (bottom-up) European Commission to support the campaign (bottom-up approach)	adoption of certificates, standards or labels	
Strengthen product recall with digital technology	Little harmonisation across EU Member States in terms of product recall procedures Product recalls allow for greater communication and interaction along the value chain, and also create more transparency for consumers	Greater harmonisation of recall practices through promotion and integration of digital technologies, including for online marketplaces.	European Parliament and European Commission, in relation with representatives of industry and consumer organisations at European level	To be reviewed in the context of the development of the proposed GPSR and specifically article 34 on the recall notice	None necessary

Source: Authors' own elaboration.

5.1.1. Monitor ongoing activities in EU Member States related to new technologies, digital solutions and product safety

Our benchmark analysis of how EU Member States are tackling new technologies and digital solutions, both in legislation and application, shows that **uneven approaches** have over time created a landscape where achieving cross-border collaboration in product safety actions is difficult and likely to become more challenging over time.

A good example of this is the ESCloud, which was an attempt by the French National Cybersecurity Agency (Agence Nationale de la Sécurité des Systèmes Informatiques – ANSSI) and the German Federal Cyber Security Authority (Bundesamt für Sicherheit in der Informationstechnik – BSI) (see 4.1.1). The **EU Safety Gate rapid alert system is already set up** to collect a lot of relevant information related to product safety and actions being taken by the EU Member States to address them. The information and Communication System on Market Surveillance (ICSMS) also provides background information on unsafe products. However, dedicated reporting focusing on the launch of standards, certificates and labels by EU Member States, as well as the use of new technology to enable product safety actions could further improve monitoring activities for product safety.

Our recommendation would thus be to **implement an EU Observatory for product safety that is linked to existing systems (namely the EU Safety Gate and the ICSMS)**, with a focus on the new technologies and digital solutions. An Observatory would also provide better background material for further revisions of the GPSD.

An alternative recommendation is to **attach monitoring of product safety activities to existing initiatives.** This could include a section on product safety in the Eco-Innovation Observatory as part of the country reports. The analysed new technologies and digital solutions are already being connected to the circularity and the circular economy. Such topics have been among the primary features of the recent Eco-Innovation Observatory reports. Practically, the EU could start building a repository of data using existing research infrastructure (bi-annual reports) of the Eco-Innovation Observatory. This could be followed up by establishing a separate product safety observatory at a future date.

5.1.2. Clarify complexities associated to product ownership

As discussed in Section 3.1.3, the emergence of digital products, alongside other trends (e.g., online marketplace), complicates the definition and utility of concepts of ownership, compared to the way ownership is understood in relation to conventional products and used to deal with safety issues. Not only do the number of parties, products and services involved in product uses create safety issues, but the way ownership and responsibility are assigned may distort behaviour throughout the value chain[104]. Furthermore, within the context of connected devices and the availability of product updates, the relationship between consumer and seller will evolve and require some changes. This is to account for emergent technologies, such as machine learning, but also the existence of product updates, which can/will result in changing products over time and the transparency and utility of information provided to consumers.

[104] For example, a product may be 'owned' by a user, but operated in ways that are affected by networked connections to products belong to others; the way they function may not be wholly under the user's control, and the relevant technical and even operational information may be (partially) controlled by a remote manufacturer or service provider. For conventional products, it would normally be appropriate to regard the controlling party as responsible; modest degrees of shared responsibility (e.g. the suitability of a product's design for a given use) could be mediated by contractual and regulatory assignments of liability. But for connected products there may not be sufficient privity of contract among the parties involved and safety-relevant information may not be available in an understandable and actionable form.

As noted in our analysis, **this relationship should be made technology-neutral (or at least flexible) and principles-based to allow for these changing dynamics**. Such a relationship may be better understood as linking consumers to service providers rather than to sellers; the purchase of products that can and will be updated (thus changed) over time can be regarded as a service contract. Furthermore, flexibility is necessary to account for the increasing number of possible actors that provide the technologies, software and services interacting within consumer products. Finally, the relationships that influence safety through product lifetimes are no longer binary; users will exchange information about their experiences with the products they use in the form of 'hacks' and other forms of guidance on product use[105]. This guidance influences product safety, but is essentially not under the control of manufacturers, and information may not always be fed back into subsequent improvements in design or authorised guidance.

To mitigate this type of market and informational failure, and to provide relevant and reliable information about a changing landscape, it would be very useful to have **repositories of information** relating to (at a minimum) product characteristics, producer activities (e.g., recalls, repairs etc.), safe use instructions and (potentially) safety incidents. On the other hand, such a database could be enormously complicated and costly, and its control and operation subject to strategic manipulation[106].

One approach might be to require (or invite) producers of such products to maintain this kind of 'observatory' following the general frameworks provided by e.g., **regulatory product fiche requirements** (e.g., in the Energy-related Product Labelling Directive) and the European Interoperability Framework. Even this could prove quite burdensome for the firms involved and difficult to maintain in relation to obsolete products and business exits. A suitable digital alternative could be provided by a **distributed ledger**, using a suitable technology implementation (e.g., blockchain) to provide a long-term repository that could absorb new information, ensure data integrity and authenticity and a controllable structure for access or confidentiality.

5.1.3. Establish clear boundaries between the General Product Safety Regulation and other aspects of digital product safety

From the evidence gathered in this study, and especially the Workshop, it seems appropriate to differentiate between digital product risks and digital solutions to product safety. *Digital product risks* arise from the use of digital products, including information risk. They also include risks that might not be digital *per se*, but depend for their special character on the digital nature of products, such as risks arising from product software updates or interactions among connected products. *Digital solutions* involve the use of digital means to manage or mitigate product safety concerns across a broad range of products and risks. These can range from digital products used to enhance safety (e.g., smart home devices) to digital services used to promote product safety (e.g., the above-mentioned distributed product safety ledger(s) or online and automated customer support portals for addressing safety concerns and collecting safety-related information). Importantly, both digital product risks and digital solutions concern both products and services that are usually enabled through connected devices. Because of this, digital product risks and digital solutions involve product safety on the end user's, service providers' and producers' sides. While both fall within the overall scope of the proposed General Product Safety Regulation, they raise different types of concern.

[105] This also complicates the ability of manufacturers to analyse and respond to in-service information, because such peer-to-per guidance induces correlations among user behaviour that cannot be directly observed but do influence the statistical analysis of safety-related information.

[106] This includes the problem of information relating to counterfeit goods.

For digital product risks, regulation provides a 'floor' in the form of **minimal standards, procedures, information sharing, testing and market surveillance**. Importantly, due to the nature of connected devices, the regulation should take into account the roles of product manufacturers, developers and service providers. This should be aligned with other product-specific Delegated Acts, harmonised across product classes and updated periodically as requirements change. It would also include product-specific provisions needed for consistency and coherence with other regulations, such as for instance the GDPR, Digital Services Act and the pending Data Act, and take account of the potential for such products to generate the flows of in-service information needed to track and report on safety provision.

Specifically, in the case of the GDPR, there is an opportunity for jurisprudence and regulatory activity relating to GDPR to account for the role of digital service providers offering services to connected products that mitigate digital risks or offering digital solutions that enable product functions related to product safety (i.e., updates) e.g. as constituting a legitimate interest in defined circumstances. The current proposal recognises the role of digital services in product safety in two contexts: those that fall under the Digital Services Act (DSA) which regulates the responsibilities of intermediary online services and those that fall under the Cybersecurity Act which establishes a certification framework for the cybersecurity of ICT products, While the proposal for the GPSR attempts to introduce further protection in the form of the minimum cybersecurity requirements, this could be expanded, especially since the minimum requirements ("the appropriate cybersecurity features necessary to protect the product against external influences, including malicious third parties, when such an influence might have an impact on the safety of the product") are concerned more with product manufacturers than service providers (article 7.1(h)).

For digital solutions to product safety, the provisions would need to **consider the functional and operational requirements of safety-enhancing or providing products** (e.g., standards, certification and testing against a range of risks), digital knowledge exchange between customers and product providers and the use of automation in safety-related consumer information, support and protection services. There are further issues relating to the use of AI e.g. in CRM and in monitoring and responding to a dynamic product safety environment, as addressed in the Artificial Intelligence Act. This needs further study, which could consider measures designed to ensure that consumer safety issues are accurately identified and effectively (and ethically) addressed, and that AI-enabled systems are able to track and respond to unforeseen variation or changes in consumer use patterns with safety implications. This information would not only be used for consumer information and advice, but could also be linked to warranty, recall and other measures. Any such provision, however, would also have to include alternative means for supporting consumers who are less able to contact the firm electronically. The assessment of such provisions would also have to consider the potential for adverse impacts on innovation and competition (esp. vertical market power[107]).

Lastly, the development of parallel initiatives introducing new technologies to improve traceability, such as the Digital Product Passport introduced by the Sustainable Product Initiative, needs to be articulated with product-safety related matters.

[107] Specifically, the current reconsideration of the Vertical Block Exemption Regulation to take account of digital markets could have specific implications for the relations between product manufacturers and software and service providers, especially when anticompetitive impacts could arrisee from actions justified by product safety concerns. See e.g. the discussion in the Commission. Staff Working Document Evaluation of thee Vertical Block Exemption Regulation, SWD (2020) 173. Available at: https://ec.europa.eu/competition/consultations/2018_vber/staff_working_document.pdf (accessed 11/5/2022).

5.1.4. Improve transparency of information, data control and data management

While actions to increase transparency of information are usually seen as beneficial to consumers, they may have negative impacts. As covered in section 3.3, information disclosure may not be proportionately effective or may even be counter-productive. In fact, **too much information risks diminishing the effectiveness of information control and transparency,** as consumers "accept the terms and conditions" without reading them or assume that documented risks have been 'handled' by product manufacturers (e.g., mandatory 'safety inserts' provided with electrical equipment and drugs). In other words, information transparency may encourage producers and consumers each to assume that the other will take care of safety. Specifically, information provision can (be thought to) increase safety by enabling consumers to choose safer products and by informing them about safe use. But these mechanisms may not operate well and may interfere with each other.

While EU legislation (e.g., GDPR, Digital Services Act) reduces the burden of responsibility for the consumer, it raises other challenges for product safety. Chiefly, it may lead to consumer overconfidence in measures that are perceived as beneficial and removes the perceived need for consumers to be informed about product safety. According to OECD, 'consumers are generally "overconfident", tend to believe that their search is adequate, and tend to overlook other possibilities. Such behavioural bias can affect consumers' perception of risk and may lead them to underestimate such risk'[108]. Examples of such 'perverse incentives' (or moral hazard) include relaxing vigilance as to private information disclosures and blindly accepting privacy policies, relying on cybersecurity measures to prevent tampering or damaging reuse by unauthorised parties. Relating to product safety and the GPSD, policies on information transparency and information control must be careful **not to exacerbate consumer overconfidence**, especially by maintaining consumers' interest and understanding of their role in relation to product safety. This is not a simple matter: the information disclosure needed for informed consent (e.g., to AI processing) is not the same as that needed to enable users to hold firms accountable for failing in their fiduciary product safety duties. This, in turn, is not generally the same as the information needed to enable users to make safe use of a product. Finally, the **information necessary may vary across consumers** in ways that are difficult to specify in e.g., a mandatory disclosure policy. Twinned to this is the **need for an interactive exchange of information** between manufacturers and consumers (over platforms that provide search, purchase and ancillary services) to enable the market to track and update information continuously, provide the right information to the right people and support the evaluation of policy in this area.

The subject of responsibility is particularly relevant in the changing dynamic of the value chain, particularly as connected devices **reduce the role of intermediaries** (disintermediation) who may sell products but do not provide device updates or track in-service information (see Section 5.2.6**.** This is further incentive for the proposed GDPR to introduce further clarification about the role of service providers for product safety.

Our recommendation is that **the advancements relating to data transparency made by the GPSR should be supported by actions aimed at providing consumer-relevant information in a consumer-friendly manner** (e.g., using labelling and technologies such as QR codes to rapidly offer consumers access to up-to-date data for informed decision making). Directives such as GDPR and the Digital Services Act need to ensure that actions taken to protect consumer data do not lead consumers completely to hand over their responsibility to the GPSD and measures connected to it (see Section

[108] OECD, 2016, *Online Product Safety Trends and Challenges*. Available at: https://www.oecd-ilibrary.org/science-and-technology/online-product-safety_5jlnb5q93jlt-en.

5.2.7). Likewise, such actions also need to account for personally-identifiable information (PII) governed under the GDPR.

GPSR focuses on how the use of consumer information to reinforce recall procedures for faulty products and consumers' rights to remedy (chapter VIII). However, the revised GPSD could be expanded towards discussing minimum transparency requirements for connected devices e.g., provision of up-to-date information related to product safety; and provision of safety information that is understandable and understandable by consumers.

Connected to this, if the GPSR does address information transparency, it should include explicit definitions of "transparency" (including the amount of information that should be presented to the consumer), "information control" and "information management". This is especially important considering that the GPSD focuses on the use of transparency for product traceability and recalls. In other words, while the GPSD primarily considers transparency from the perspective of governments and manufacturers, many important impacts of transparency measures fall on consumers (e.g., those that result in product recalls). The introduction of "information control" and "information management" definitions into the GPSR would expand information transparency to more actively include consumers as beneficiaries. Furthermore, the inclusion of these definitions would benefit from supporting measures to ensure that consumers can exercise this control effectively.

An example of how data transparency could be supported is provided by Luxembourg's Product Circularity Data Sheet (PCDS), which tracks detailed information across the value chain, offering authorities, producers and consumers large amounts of relevant data about product development, components, manufacturers and suppliers. PCDS uses DPP technology to enable participating organisations to ensure storage of accurate details about the product on an accessible digital document. The focus of the PCDS is circularity (thus the product information covers use of circular materials in manufacturing), but the principle could be scaled up in the EU by granular introduction, for example targeting specific products or industries as a proof of concept. The resulting information sharing across EU Member States would enable more effective market surveillance, tracking of manufacturing process (potential linked to other development goals) and more informed consumer decision making. On the latter, it is advisable that implementation of a DPP should seek to ensure information readability by different stakeholder groups. The way consumers process information and the type of information that is beneficial to them differs from how manufacturers or regulators do. Usability of a DPP should be matched to the needs and capabilitis of target audiences.

5.1.5. Tackle obsolescence from a product safety perspective

As developed in section 3.2.3, obsolescence raises product-safety challenges in relation to continuity of coverage, collection and continued availability of data, support for products and consumer protection. Linked devices, such as smoke sensors linked to the internet, can become open to cyberattacks when no longer supported with software updates. Planned (and even unplanned) obsolescence are also extremely detrimental to product sustainability more generally.

Currently, the GPSR proposal does not mention obsolescence and associated safety risks, although minimum cybersecurity safety requirements are mentioned in article 7. To avoid and limit issues relating to safety and obsolescence in digital products, **our recommendation is to introduce minimum safety-related support lifetimes for connected products into Article 7 of the proposal of the GPSR.** Ultimately, these should be described in product sale contracts. However, because such contracts link the consumer and the producer, an associated recommendation is to set durable obligations for firms acquiring producers to maintain a safety-linked duty of care. Even this may not completely resolve the issue, in cases where producers fail, exit from the market or are acquired by firms not operating within the Single Market. In such cases, the repositories recommended below can at least provide a public register of safety issues linked to unsupported products to facilitate product replacement.

It is nevertheless important to stress that such obligations should remain proportionate and minimise competitive foreclosure. Sub-options including self- or co-regulatory alternatives could also be considered, along with the appropriate mechanism for meeting costs.

5.1.6. Introduce automated information exchange

New technologies and digital solutions have a **potential to improve the effectiveness, flexibility and proportionality of product safety regulation**. The possibilities offered by automated user exchanges with users, regulators and platforms (regtech and suptech) could indeed permit more agile and proportionate regulation, minimise unnecessary administrative burden and reduce the potential for accidental or intentional mistakes in the information shared.

To put this in context, we note that automated exchange can be: i) among producers, retailers and others in the value chain; ii) between users and those 'responsible' for product safety (usually producers); and iii) between responsible parties and authority. They do different things.

Exchanges among value chain participants help with detecting emerging issues, identifying obsolescence, monitoring the effectiveness of safety-improving measures, etc. They can in theory help consumers make better decisions and thus improve the alignment of market forces with safety, but this isn't guaranteed; such information may be regarded as proprietary, may not be understandable by consumers or used to facilitate collusion.

Exchanges between users and those with responsibility for products safety allow two-way flows of information; consumers can be kept informed and their products up to date, while at the same time providing producers with real-time in-service data on how their products are performing. The concerns here are that such data can infringe on privacy rights and give producers excessive market power and that cybersecurity failures can threaten safety.

Exchanges between responsible parties and the authorities are the regtech side. They allow more flexible, adaptable and light-touch (or proportionate and effective) regulation while reducing both administrative costs and the risks of mistakes or strategic 'gaming' of the system.

Any product-related regulation must include provisions for monitoring and enforcing compliance with its requirements. Products made available within the European Single Market must comply with a broad range of regulatory requirements, including those relating to product safety (chapter V of the GPSR proposal). This applies both to the compliance of ‘official’ products and the threat of non-compliant products counterfeiting compliant ones. It also applies to the presence on the market (and thus in use) of obsolete products. The proposed GPSR introduces specific traceability requirements for specific product groups through delegated acts.

The task is made more difficult by the existence of multiple ‘brands’ for products whose actual producers are hard for consumers to identify (e.g., those sold on online marketplaces) and by the global sourcing, self-certification of compliance and reactive ‘notice and action’ form of much current regulation. This issue is fairly standard; the Market Surveillance Regulation, which entered into force on 16th July 2021, places responsibilities on designated National Authorities to ensure *inter alia* that products offered for sale do not endanger European consumers and workers. It includes actions such as product withdrawals, recalls and the application of sanctions to stop the circulation of non-compliant products and/or bring them into compliance. It sits next to a range of other legislation that potentially sets standards for these authorities to monitor and enforce. These include the Artificial

Intelligence Act, the Digital Services Act and the Digital Markets Act. However, these laws are difficult to apply to online marketplaces and fulfilment service providers facilitating illegal imports in the EU, as they are limited to a 'notice and action' approach.

These examples illustrate the increasing complexity of ownership and responsibility for (part of) the value chain delivery of products to consumers. Technology is a necessary element to help taking that responsibility without blowing the administrative burden out of proportion. In contrast to on-request provision of information (art. 14), the collection of this information in close to real time by (at least partially) automated means will reduce costs and allow more timely and proportionate responses (whether enforcement or change of standards, redesign of products or consumer information or user instructions). Such information can include in-use experience that can quickly detect emerging safety issues and help in evaluating changes already deployed, while respecting user privacy. It would also support to improve the alignment of market competition with product safety by reducing the payback period for producer-initiated safety enhancements; improving the reliability of labelling and certification; enhancing the cost-effectiveness of market surveillance; and allowing implementation of measures to minimise adverse competition, innovation and trade impacts. It is expected that the level of complexity will continue to increase over time, and the ability to deal with that effectively will need to continue to be improved.

It is proposed that the European Parliament and the European Commission, in partnership with industry and consumer associations' representatives, take the following actions:

- a) modify proposals for labelling and certification to include automated verification of compliance;
- b) impose automated reporting to Market Surveillance Authorities by producers and distributors of information required by regulation;
- c) modify consumer information provision to require producers and distributors to inform users (by both electronic and non-electronic means) of safety issues detected by automated information exchange; and
- d) include provisions for technological means of verifying standards compliance with products offered for sale.

It is suggested to incorporate in the revised GPSD technology-neutral incentives to adhere to state-of-the-art technology standards and measures.

A non-regulatory complement is to support regtech and suptech research, in combination with digital labels and AI, to further explore the potential of smart technologies to enable agile and light-touch regulation, reduce the burdens, reliability and flexibility of industry responses, and to ensure that consumers have a better mix of reliable products and clear and timely guidance as to their safe use.

5.1.7. Encourage the use of new technologies and digital solutions to communicate product safety to consumers.

Any EU action to support product safety connected to new technologies and digital solutions should account for consumer awareness and communication. Particularly, the benchmark work (see Chapter 4) has shown the **importance of improving communication between consumers and national and supranational authorities** (e.g., EU, WTO[109], CPTPP). This is necessary to enable consumers to make informed purchasing decisions, understand where to seek information regarding product safety and identify who should receive safety concern reports. This, in turn, will better align market forces with improved product safety and facilitate the incorporation of user experience and other in-service feedback into the value chain.

The analysis also showed that new technologies and digital solutions have a tremendous potential to address consumers issues related to product safety in an efficient way (e.g., chatbots using AI to provide quickly individualised answers), provided they comply with the regulatory framework (see. 5.2.3).

Actions relating to communication with consumers need to ensure personal data protection. Importantly, different technologies and digital solutions seem to differ in terms of how increased information affects consumer trust (e.g., increased understanding of AI functionalities may result in negative rather than positive perceptions). The key point here is to foster appropriate levels of trust; when product safety reflects how products are used, it is not always the case that more trust leads to greater safety. **Information should be provided as a "platform service" enabling product suppliers and users to communicate in both directions**, since real-world experience of using products may differ from design modelling, especially for AI-enabled devices that change as they are used. Furthermore, communication to consumers should **take accessibility, fairness and inclusiveness into account**. As levels of digital literacy differ across the population, specific attention should be paid to combine both digital and non-digital communication.

Our **recommendation is that the GPSD should seek to define benchmark levels of communication** (e.g., what minimal information is to be provided, by whom, how and when and with what mechanisms for redress or gaining further information) to be provided to consumers in order to build appropriate levels of confidence and trust. It is not intended that this benchmark should apply uniformly; rather it should establish a useful common 'floor' that suppliers can compete to raise by providing enhanced information that users value and find useful. Further actions and specific measures can be approached by sectoral regulations that can account for how different technologies and solutions are perceived, but the GPSD should provide the foundation for such specifications. The Impact Assessment of the revised Toy Safety Directive introduces the idea of digital labelling and a Digital Product Passport[110]; similar sectoral revisions are expected in the future.

The roles of service providers need to be considered in this context, and how (if at all) they should be regulated. Service providers have relationships with other responsible parties (online marketplaces, manufacturers) as well as with consumers. The challenge is thus to enable service providers to provide understandable and actionable advice to foster consumer protection without fear of breaking other regulations or distorting manufacturers' and merchants' incentives. When it comes to communicating it is just as important to provide the tools for intermediaries to understand emergent safety concerns and how to address them as it is for manufacturers and end users.

[109] WTO Agreement on Technical Barriers to Trade (TBT) deals directly with product safety measures.

[110] European Commission, 2021, *Protecting children from unsafe toys and strengthening the Single Market – revision of the Toy Safety Directive* Available at : https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13164-Protecting-children-from-unsafe-toys-and-strengthening-the-Single-Market-revision-of-the-Toy-Safety-Directive_en.

A possible approach is a supporting role for EU Member States' consumer organisations as well as trade organisations to provide an aggregated view based on an understanding of multiple new technologies, digital solutions and their interactions that may create risks to product safety. Consumer organisations ensure that user perspectives are broadly considered by providing 'lay' representation in self- and co-regulatory initiatives (e.g., standards development organisations or registries), raising consumer awareness, hosting exchange of information among users and between consumers and businesses and by collecting and curating information on the real-world performance of products and services linked to safety concerns. The latter may be particularly important for complex digital and AI-enabled systems because safety issues are as likely to arise at system level as they are in relation to individual products or services. Most existing monitoring and information systems are organised around individual products and could miss emerging complex issues. As the affected parties, consumers are best-placed to take a more panoptic view of safety.

The EU could particularly support both consumer and industry-representative organisations in raising consumer awareness, using the views collected to raise mutual awareness among these stakeholders about the information counterpart organisations can provide and by actively using information resources they collect and develop. Furthermore, **the EU can contribute to the effectiveness of consumer organisations through networking and knowledge sharing tools**, initiatives to increase the know-how of consumer organisations about new technologies, digital solutions and their impacts on consumer goods and safety especially in relation to the New Consumer Agenda of the European Commission[111]. At the most fundamental level, consumers are the eyes and ears of society on matters of safety; better informed consumers make smarter choices, therewith ensuring alignment of the market with regulatory objectives.

5.1.8. Lead the development of global standards for product safety with new technologies and digital solutions

The information collected during the study, particularly during the focus group, suggests that global product safety standards for new technologies and digital solutions are limited in number and scope. This indicates that the global landscape is still fragmented, even featuring devices that have different functionalities based on the region and the local standards in play. The European Commission's Sustainable Product Initiative aims to introduce a digital product passport to enhance circularity and that could provide a platform for product safety purposes.

Within this context, while following the current discourse calling for global standardisation is an option, taking an active part in this discourse is important as to ensure that European values, where relevant, are factored into global standards development. The most important consideration in this regard is **maintaining the protection of customers and citizens.** The ethical position that ubnderpins such standards can contribute towards a culture that supports consumer protection.

It is important to recall that there are different routes for elaborating standards. Our recommendation is to **support the process of EU-wide standards with technology-neutral actions** based on common principles and incentives for technology developers, producers, etc. to follow them. This recognises that the EU itself is usually slow to react to emergent technology development with technology-specific regulations or detailed legislative action. Attempting to rely on 'standard' civil law processes would leave the EU reacting to past challenges while new ones are already emerging. A **technology-neutral approach** creates conditions to introduce foresight into the GPSD while allowing sectoral

[111] European Commission, 2020, *New Consumer Agenda: European Commission to empower consumers to become the driver of transition.* Available at : https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2069).

actions to be taken within specific domains into which product safety crosses over (for example, cybersecurity).

Here the EU can take a top-down or a bottom-up approach to support new standards**. From the perspective of top-down actions**, a considerable contribution by the EU towards product safety would be to provide **new legal definitions** concerning the new technologies and digital solutions and for the relationships between and with them by various stakeholders.

The role of such definitions is important in recognising that consumer goods become changeable due to the inclusion of these technologies and solutions. This only increases when multiple technologies and solutions function within/with the same consumer good. Such emergent relationships raise questions on device ownership, whether consumers are buying products or services and the responsibilities of consumers, manufacturers, developers, sellers at the point of sale and beyond (updates to the device, third-party software installed on a device, etc).

As discussed in relation to standards, the inclusion of such definitions in the GPSD would benefit from a technology-neutral approach, that is to say definitions that are broader in scope, broader in applicability. This would allow sectoral (e.g. delegated) regulations to work with specifics. Our recommendation is that GPSD could provide the framework definitions onto which **sectoral specifications can be added where and when necessary, in separate texts** (e.g., Toy, Battery Directives, etc).

As for bottom-up actions the EU can take example of how the Manufacturer Usage Description Specification (MUD) as a flexible and inclusive approach of multiple international stakeholders contributing towards a common goal of creating a standard. But there is still a central body (the Internet Engineering Task Force) that has the responsibility of making final decisions. This is a possible pathway forward for the EU: supporting the launch of a similar body of experts responsible for developing EU standards, certificates, labels for new technologies, digital solutions, and product safety. This body would have the flexibility to include consultations and experts as new technological developments arise. In other words, the **EU should catalyse bottom-up initiatives** to benefit from the flexibility to react to developments faster than policy makers could. At the same time, the EU could support bottom-up initiatives through robust communication campaigns that should introduce the benefits of the new standards, certificates and labels to consumers. It would also carry the message that such transnational actions are possible for product safety and encourage further bottom-up initiatives across EU.

Table 5: Comparison of top-down and bottom-up approach

	Top-down	Bottom-up
Advantages	• Allows EU to introduce new legal definitions concerning the new technologies and digital solutions. • Offers opportunities to lead the way in Europe and Globally in supporting consumers and ensuring safer products enter the market.	• Allows using best practice examples of existing initiatives towards wider application: – Either as scale-up initiatives that EU adopts. – Or by encouraging spread of best practice across EU Member States.
Disadvantages	• Requires understanding the current legal environment to identify gaps that are unlikely to be filled by the actions of individual countries or where legal inconsistencies between countries emerge.	• Requires monitoring to recognise emerging best practices in the EU that could be supported. • Requires accounting for difficulties in crocc-border application of practices (for example due to differences in the legal system).
When to use	• When there is a need for faster adoption of new standards, new legal definitions across the entire EU. • When it is unlikely that cross-border application of common practices is possible without EU's intervention.	• When countries show interest in cooperation for cross-border application of practices the EU should support such initiatives to ensure their success.

Source: Authors' own elaboration.

5.2.9. Strengthen product recall with digital technology assistance

Strengthening product recall is already an objective of the GPSD revision, covered by a number of Articles (notably Article 34). The preferred policy option underlines the necessity to include additional obligations related to online sales and product recalls. Section 2 points to the lack of effectiveness in product recalls. The current GPSD does not lay out any specific rules with respect to the recalling of unsafe or dangerous products. The issue is that besides the lack of centralised recalling procedures across the EU, many consumers are not actually aware of ongoing recalls, and even if they are aware, they tend to minimise the risks associated with a dangerous product partly because of incorrect communication.

Our analysis in section 4 shows that there is little harmonisation across EU Member States in terms of product recall procedures, where half of the EU Member States even lack guidelines for recalls. As such, there is **clear added value from the EU introducing centralised actions,** at least in terms of informing consumers (see also recommendations related to communication).

Our recommendation **confirms the need for specific product recall measures**, as introduced by Article 34 (Recall notice) in the GPSR proposal, in order to lean towards a **greater harmonisation of recall practices**. Similarly, we confirm the need for online market places to also cooperate to ensure effective product recalls (Article 20).

Our research has underlined the ability of digital technologies to facilitate product recalls, as they permit greater communication and interaction along the value chain, and also create more transparency for consumers. Smart technology is already changing the way manufacturers detect and respond to product recalls, with robotics using optical character recognition to inspect, identify and measure products, or blockchain technology helping track-and-trade products from origin to point of sale and allow companies to provide their customers with all the required information. Overall, we recommend leveraging the new technologies and digital solutions (e.g., eSIM/iSIM) as a method to effectively address emerging product safety concerns in connected devices and support product recall if such actions become necessary.

6. CONCLUSIONS

The overall aim of the research was to investigate the role of new technologies and digital solutions in providing more information to consumers, better guarantee the safety of products, while at the same time reducing the administrative burden for economic operators, especially SMEs, and enhancing product sustainability.

Section 3 of the report focused on analysing how new technologies and digital solutions could enhance product traceability and safety. The opportunities and challenges for product safety were analysed individually for a group of 8 technologies, several of them raising more concerns than others (AI, IoT). The research shows that the key opportunities arising from these technologies are an unparalleled accessibility to products, the personalisation of services, and increased sustainability. The research also highlighted some of the key concerns in using such technologies, such as product ownership, the consumers' ability to choose, and the necessity to ensure interoperability and standards to clarify the responsibility of producers and distributors. Challenges pertaining to software and cybersecurity were not in the scope of the analysis. Challenges relating to the protection of investment by consumers (such as software updates availability) were also not in the scope of the analysis and are perhaps more in scope of the Digital Services Act underway.

Section 3 also focused on how technologies can enhance product durability and sustainability. Technologies permitting traceability along the value chain, such as blockchain and QR codes, offer new opportunities for sourcing better materials, improving product design, enhancing processes, and improving reuse, remanufacturing, and recycling. Nevertheless, the belief that the environmental costs of digital technology can be offset by its potential gains should not be considered a given and requires further research. The section also looks at obsolescence from both a sustainability and safety perspective and finds key challenges in relation to the continuity of coverage of product safety, the collection and continued availability of data, support for products and liability and consumer protection. Currently, European legislation seldom mentions the potential of technology to help tackle obsolescence, which shows a gap to be filled in the near future. Lastly, the section finds that the revised GPSD can minimise administrative burdens e.g., by giving standing to common standards and certification and the creation and governance (or direct provision) of central repositories of product characteristics and consumer experiences.

Section 4 explored recent developments in Member States and at the EU level to develop product safety and compliance with new technologies. Most of these have emerged in recent years and are national in their scope. Governance models vary, and the cases studies indicate that there is not one preferred approach as both solutions designed by public entities and bottom-up approaches have been successful. Communication campaigns are key to promoting existing initiatives in order to effectively inform citizens and ensure spillovers across sectors and borders of the EU. Another conclusion drawn from the case studies is that the EU should draw on the use of decentralised and sectoral databases: initiatives that are too large in their scope have not performed well. EU intervention is necessary to allow existing initiatives to gain full visibility across different Member States. Market fragmentation is a risk in the future if the EU does not intervene.

Finally, the report ends with a series of policy recommendations which are aligned with the current revision of the GPSD as a regulation. Some of these are related to legislative change (e.g., defining a minimum benchmark level of communication to be provided to consumers, and promoting the use of digital technologies in recall practices), while other are more general and might not require legislative evolution (e.g., implementing an EU Observatory for product safety, supporting bottom-up approaches to develop EU-wide standards, certificates and labels). More than ever, it will be important to consider that some elements of consumer protection may relate to the scope of the GPSD but are at the core of other initiatives, such as GDPR and DSA.

REFERENCES

- Alaranta, J. et al., 2020*, How to reach a safe circular economy? Perspectives on reconciling the waste, product and chemical regulation*. Available at: https://academic.oup.com/jel/article/33/1/113/5919851?login=true.
- Allee, V., 2000, *Reconfiguring the Value Network,* Journal of Business Strategy, Vol. 21, N4, July-Aug.
- Allee, V., 2003, *The Future of Knowledge: Increasing Prosperity through Value Networks*, Butterworth-Heinemann 2003. Available at: http://www.vernaallee.com/value_networks/Understanding_Value_Networks.html.
- Allee, V., 2005, *Understanding value networks*. A brief article by Verna Allee;
- Amron, M. T., & Noh, N. H. M., 2021, *Technology acceptance model (TAM) for analysing cloud computing acceptance in higher education institution (HEI).* In IOP Conference Series: Materials Science and Engineering (Vol. 1176, No. 1, p. 012036). IOP Publishing.
- Arcese, G. et al., 2014, *Near field communication: Technology and market trends. Technologies*, 2(3), 143-163.
- Batstone, O., 2017, *What AI means for Designers*. Retrieved fromAvailable at: https://becominghuman.ai/what-ai-means-for-designers-5c27130a5e0e.
- Bazaeea, G., Hassanib, M., & Shahmansouric, A., 2020, *Identifying Blockchain Technology Maturity's Levels in the Oil and Gas Industry*.
- Cassidy, T. et al., 2018. *Consumer Product Safety in an IoT World*. Available at: https://static1.squarespace.com/static/586aff8559cc688787ce6a34/t/5b295fb770a6ada64f8a752e/1529438142453/Physical+Safety+in+an+IoT+World+%284%29.pdf.
- Cen Cenelec, 2022, *European Standards*. Available at https://www.cencenelec.eu/european-standardization/european-standards/.
- Civic consulting, 2020, *Study for the preparation of an Implementation Report of the General Product Safety Directive. Final Report.* Available at: https://ec.europa.eu/info/sites/default/files/final_report-gpsd-part1-main_report-final-corrected2.pdf.
- Civitta, 2020, Blockchain in SMEs Maturity Report 2020.
- Consumer Product Safety Commision, 2019, *Status Report on the Internet of Things (IoT) and Consumer Product Safety.* Available at: https://cpsc-d8-media-prod.s3.amazonaws.com/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf.
- Cory, N., 2021, *How E-labels Can Support Trade and Innovation in ICT, Medical, and Other Products*. Available at: https://itif.org/publications/2021/10/27/how-e-labels-can-support-trade-and-innovation-ict-medical-and-other-products.
- Council of the European Union, 2020, *Council Conclusions on the cybersecurity of connected devices.* Available at: https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf.
- CSPcert, 2019, *Recommendations for the implementation of the CSP certification scheme.* Available at: https://ecp.nl/wp-content/uploads/2020/01/PT-2019-CSP-CERT-WG-Recommendations-for-the-implementation-of-the-CSP-Certification-scheme-20190607-Final-version.pdf.

- De Romph, T., 2018, *The legal transition towards a circular economy - Eu environmental law examined.* Available at: https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS1966325&context=L&vid=Lirias&search_scope=Lirias&tab=default_tab&lang=en_US&fromSitemap=1.

- De Tweede Kamer der Staten-Generaal, 2020, *Voortgang Roadmap Digitaal Veilige Hard- en Software.* Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2020/12/14/kamerbrief-over-voortgang-roadmap-digitaal-veilige-hard-en-software.

- Department of the Prime Minister and Cabinet ,2022, *Acceptance of international standards and risk assessments for product approvals*. Available at: https://www.pmc.gov.au/domestic-policy/taskforces-past-domestic-policy-initiatives/industry-innovation-and-competitiveness-agenda/acceptance-international-standards-and-risk-assessments-product-approvals.

- Ellen Macarthur Foundation, 2020, *Artificial intelligence for recycling: AMP Robotics*. Available at: https://ellenmacarthurfoundation.org/circular-examples/artificial-intelligence-for-recycling-amp-robotics.

- EPC, 2020, *The circular economy: Going digital.* Available at: https://www.epc.eu/en/publications/The-circular-economy-Going-digital~30c848.

- ETSI, 2019, *ETSI releases first globally applicable standard for consumer IOT security*. Available at: https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security.

- European Commission, 2009, *Report on the state of implementation of the Integrated Product Policy*. Available at: https://ec.europa.eu/environment/ipp/pdf/bio_ipp.pdf.

- European Commission, 2011, *New Consumer Agenda. Strengthening consumer resilience for sustainable recovery.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0696&qid=1605887353618.

- European Commission, 2012, *Manifesto & Policy Recommendations: European Resource Efficiency Platform*. Available at: https://ec.europa.eu/environment/resource_efficiency/documents/erep_manifesto_and_policy_recommendations_31-03-2014.pdf.

- European Commission, 2012, *Unleashing the potential of Cloud Computing in Europe.*

- European Commission, 2014, *Directive 2014/35/EU of theEuropean Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0035.

- European Commission, 2017, *Notice on the market surveillance of products sold online. Official Journal of the European Union*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017XC0801%2801%29.

- European Commission, 2019, *Commission Implementing Decision (EU) 2019/417 of 8 November 2018 laying down guidelines for the management of the European Union Rapid Information System 'RAPEX' established under Article 12 of Directive 2001/95/EC on general product safety and its notification system (notified under document C(2018) 7334).*

- European Commission, 2019, *The Cybersecurity Act strengthens Europe's cybersecurity*. Available at: https://digital-strategy.ec.europa.eu/en/news/cybersecurity-act-strengthens-europes-cybersecurity.
- European Commission, 2019, *The EU Cybersecurity Act*. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.
- European Commission, 2020, *Digital Finance package*. Available at : https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.
- European Commission, 2020, *Opinion of the sub-group on artificial intelligence (AI), connected products and other new challenges in product safety to the consumer safety network*. Available at: https://ec.europa.eu/safety/consumers/consumers_safety_gate/home/documents/Subgroup_opinion_final_format.pdf.
- European Commission, 2020, *Opinion of the sub-group on artificial intelligence (AI), connected products and other new challenges in product safety to the consumer safety network*. Available at: https://ec.europa.eu/safety/consumers/consumers_safety_gate/home/documents/Subgroup_opinion_final_format.pdf.
- European Commission, 2020, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0064&from=en.
- European Commission, 2021, *Advanced Technologies for industry - product watch. Advanced manufacturing and robotics for ICT manufacturing*. Available at: https://ati.ec.europa.eu/reports/product-watch/advanced-manufacturing-and-robotics-ict-manufacturing.
- European Commission, 2021, *Commission Staff Working Document accompanying the document Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council.*
- European Commission, 2021, Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions, *A new Circular Economy Action Plan For a cleaner and more competitive Europe*. Available at: https://ec.europa.eu/environment/strategy/circular-economy-action-plan.
- European Commission, 2021, *European Blockchain Services Infrastructure*. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure.
- European Commission, 2021, *Executive Summary of the impact assessment report on the proposal for a regulation on general product safety*. Available at: https://ec.europa.eu/info/sites/default/files/executive_summary.pdf.
- European Commission, 2021, *Laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.
- European Commission, 2021, *Proposal for a regulation of the EP and the Council on general product safety*. Available at: https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_general_product_safety.pdf.

- European Commission, 2021, *Regulation of the European Parliament and* of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.
- European Commission, 2021, *Shaping Europe's digital future*. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy.
- European Commission, 2021, *Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach*.
- European Commission, 2021, *Study to support the preparation of an evaluation of the General Product Safety Directive as well as of an impact assessment on its potential revision. Part 2: impact assessment on the potential revision of the General Product safety Directive*. Available at: https://ec.europa.eu/info/sites/default/files/gpsd-final-report-part2-ia.pdf.
- European Commission, 2021, Sustainable product policy & eco-design. Available at: https://ec.europa.eu/growth/industry/sustainability/sustainable-product-policy-ecodesign_en.
- European Commission, 2021, *The General Product Safety Directive*. Available at: https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety_en.
- European Commission, 2021, *The General Product Safety Directive*. Available at: https://ec.europa.eu/info/business-economy-euro/product-safety-and-requirements/product-safety/consumer-product-safety_fr.
- European Commission, 2022, *Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment.* Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545.
- European Commission, 2022, Directive 2009/125/EC of the European Parliament *and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products*. Available at: https://ec.europa.eu/growth/industry/sustainability/sustainable-product-policy-ecodesign_en.
- European Commission, 2022, *Questions and Answers: Sustainable Products Initiative.* Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2014
- European Commission,2009, *Regulation (EC) No 1223/2009 of the European Parliament and of the Council of 30 November 2009 on cosmetic products.* Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009R1223.
- European Consumer Centre, 2017, *The impact of counterfeiting on online consumer rights in Europe.* Available at: https://www.europe-consommateurs.eu/fileadmin/Media/PDF/publications/etudes_et_rapports/Etudes_EN/The_impact_of_counterfeiting.pdf.
- European Medicine Agency, 2017, *Quick Response (QR) codes in the labelling and/or package leaflet of veterinary medicinal products authorised via the centralised (CP), mutual recognition (MRP), decentralised procedures (DCP) and national procedures.* Available at: https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/quick-response-qr-codes-labelling/package-leaflet-veterinary-medicinal-products-authorised-centralised-cp-mutual-recognition-mrp_en.pdf.

- European Medicine Agency, 2018, *Mobile scanning and other technologies in the labelling and package leaflet of centrally authorised medicinal products.* Available at: https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/mobile-scanning-other-technologies-labelling-package-leaflet-centrally-authorised-medicinal-products_en.pdf.
- European Parliament Research Service, 2015, *Consumer protection aspects of mobile payments.* Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564354/EPRS_BRI(2015)564354_EN.pdf.
- European Parliament, 2016, *The European Civil Law Rules in Robotics*. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf.
- European Parliament, 2020, *Sustainable consumption and consumer legislation protection.* Available at:https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/648769/IPOL_IDA(2020)648769_EN.pdf.
- European Parliament, 2020, *Sustainable Consumption and Consumer Protection Legislation. How can sustainable consumption and longer lifetime of products be promoted through consumer protection legislation?*
- European Parliament, 2021, *Committee on Petitions. Notice to Members.* Available at: https://www.europarl.europa.eu/doceo/document/PETI-CM-692920_EN.pdf.
- European Parliament, 2021, *Legislative Train.* Available at: https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/a-european-green-deal/file/new-circular-economy-action-plan.
- European Policy Centre, 2020, *Towards a green, competitive and resilient econoly, how can digitalisation help?* Available at: https://www.epc.eu/content/PDF/2020/Towards_a_green_competitive_and_resilient_EU_economy.pdf.
- European Union Agency for Cybersecurity, 2020, *EUCS - Cloud Services Scheme*. Available at: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.
- Ferri, L., Spanò, R., Maffei, M., & Fiondella, C., 2020, *How risk perception influences CEOs' technological decisions: extending the technology acceptance model to small and medium-sized enterprises' technology decision makers*. European Journal of Innovation Management.
- Fosch-Villaronga, E., & Mahler, T., 2021, *Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. Computer Law & Security Review*, 41, 105528.
- Generation Climate Europe, 2021, Call for an ambitious Digital Product Passport: analysing the results of Generation Climate Europe survey, available at: https://gceurope.org/call-for-an-ambitious-digital-product-passport-analysing-the-results-of-generation-climate-europe-survey/?utm_source=rss&utm_medium=rss&utm_campaign=call-for-an-ambitious-digital-product-passport-analysing-the-results-of-generation-climate-europe-survey.
- Global Policy Watch, 2017, *What is a Robot under EU law?* Available at: https://www.globalpolicywatch.com/2017/08/what-is-a-robot-under-eu-law/.

- Grover, P., Kar, A. K., Janssen, M., & Ilavarasan, P. V., 2019, *Perceived usefulness, ease of use and user acceptance of blockchain technology for digital transactions–insights from user-generated content on Twitter*. Enterprise Information Systems, 13(6), 771-800.
- Gursoy, D., Chi, O. H., Lu, L., & Nunkoo, R., 2019, *Consumers acceptance of artificially intelligent (AI) device use in service delivery*. International Journal of Information Management, 49, 157-169.
- Hartmann F. et al, 2021, *Becoming Sustainable, The New Frontier in Soft Robotics*. Adv Mater.
- Infosec, 2019, *Concerns Related to NFC Technology for Payments*. Available at: https://resources.infosecinstitute.com/topic/nfc-technology-payments-concerns/.
- M. Javais, M., 2021, *Substantial capabilities of robotics in enhancing industry 4.0 implementation*. Cognitive robotics. Science Direct.
- Kawshalya, K. T. G. D., 2020, *Factors Affecting Slow Adoption of NFC-enabled Payment Services: Sri Lankan Consumers' and Service Providers' Perspective*.
- Kellen Browning, 2021, *'Crucial Time' for Cloud Gaming, which wants to change how you play*. Available at: https://www.nytimes.com/2021/07/01/technology/cloud-gaming-latest-wave.html.
- Luna, I. R. D. et al, 2017, *NFC technology acceptance for mobile payments: A Brazilian Perspective*. Revista brasileira de gestão de negócios, 19, 82-103.
- Luxembourg Trade & Invest, 2021, *New Luxembourg Strategy for the Circular Economy*. Available at: https://www.tradeandinvest.lu/news/new-luxembourg-strategy-for-the-circular-economy/.
- Ministry of Economic Affairs of The Netherlands, 2019, *Strategisch Actieplan voor Artificiële Intelligentie*. Available at: https://www.rijksoverheid.nl/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificiele-intelligentie.
- Mohr, S., & Kühl, R., 2021, *Acceptance of artificial intelligence in German agriculture: an application of the technology acceptance model and the theory of planned behavior*. Precision Agriculture, 1-29.
- Montalvo, C. et al., 2016, *A Longer Lifetime for Products: Benefits for Consumers and Companies, Publication for the Committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies*, European Parliament, Luxembourg. Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/579000/IPOL_STU(2016)579000_EN.pdf.
- Nagy, S., & Hajdú, N., 2021, *Consumer Acceptance of the Use of Artificial Intelligence in Online Shopping: Evidence from Hungary*. Amfiteatru Economic, 23(56).
- OECD, 2016, *Online Product Safety Trends and Challenges*. Available at: https://www.oecd-ilibrary.org/science-and-technology/online-product-safety_5jlnb5q93jlt-en.
- OECD, 2018, *Consumer policy and the smart home*. Available at: https://www.oecd-ilibrary.org/docserver/e124c34a-en.pdf?expires=1636044917&id=id&accname=guest&checksum=3868B7B6DDDB5B7CAED13AAFF69D6591.
- OECD, 2018, *Consumer product safety in the Internet of Things,* OECD Digital Economy Papers, No. 267, OECD Publishing, Paris. Available at: https://www.oecd-ilibrary.org/science-and-technology/consumer-product-safety-in-the-internet-of-things_7c45fa66-en;jsessionid=CXUEkEsGVYvjbfKycNemqIEz.ip-10-240-5-134.

- OECD, 2018, *Consumer product safety in the Internet of Things.* Available at: https://doi.org/10.1787/7c45fa66-en.
- OECD, 2019, *Challenges to consumer policy in the digital age*. Available at: https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf.
- Ok, K. et al, ,2010, *Current benefits and future directions of NFC services*. In 2010 International Conference on Education and Management Technology (pp. 334-338). IEEE.
- QRcode Tiger, 2021, *How are QR codes used in Europe?* Available at: www.qrcode-tiger.com/how-qr-codes-are-emerging-in-europe-now-that-they-have-utilized-them-in-almost-every-field.
- Radjou N & Prabhu J, 2014, *Frugal Innovation: How to do more with less*, The Economist, available at http://naviradjou.com/wordpress/wp-content/uploads/2016/12/Frugal-Innovation_Intro-Chapter.pdf.
- Rodriguez F. et al, 2017, *Cybersecurity of robotics and autonomous systems: privacy and safety*.
- Rue, N., 2019, *How AI Can Improve Product Safety*. Retrieved from: https://becominghuman.ai/how-ai-can-improve-product-safety-820d391775d3.
- Schellekens et al., 2019, *Blockchain en het recht*. Retrieved from: https://repository.wodc.nl/handle/20.500.12832/2336.
- SGS, 2021, *EU Battery Proposal released to replace the Battery Directive*. Available at: https://www.sgs.com/en/news/2021/03/safeguards-04121-eu-battery-regulation-proposal-released-to-replace-the-battery-directive-2006-66-ec.
- Soeparno, H., & Perbangsa, A. S., 2021, *Cloud Quantum Computing Concept and Development: A Systematic Literature Review*. Procedia Computer Science, 179, 944-954.
- Song, Y. W., 2019*, User acceptance of an artificial intelligence (AI) virtual assistant: an extension of the technology acceptance model* (Doctoral dissertation).
- SPARC, 2017, *Smart Robots for Smart Regions (i): Strategies to unleash the potential of the digital economy in Europe*. Available at: https://www.eu-robotics.net/sparc/newsroom/press/smart-robots-for-smart-regions-strategies-to-unleash-the-potential-of-the-digital-economy-in-europe.html.
- Standards Council of Canada, 2019, *Incorporation of Standards by Reference in Canada: Considerations for Trade*. Available at: https://www.wto.org/english/tratop_e/tbt_e/01_a_p1a_canada.pdf.
- The consumer goods forum, 2017, *AI and robotics automation in consumer-driven supply chains.* Available at: https://www.theconsumergoodsforum.com/wp-content/uploads/2018/04/201805-CGF-AI-Robotics-Report-with-PA-Consulting.pdf.
- Timothy M. O'Grady, 2021, *Circular economy and Virtual Reality in Advanced BIM-Based Prefabricated Construction, energies*.
- TWO, 2020, *Thematic Session on Technical Regulations: Marking and Labelling*. Available at: https://www.wto.org/english/tratop_e/tbt_e/tbtthematcimarkinlabel27102020_e.htm.
- Vaccaro S., 2019, *Referencing standards in EU legislation*. Available at: https://www.wto.org/english/tratop_e/tbt_e/01_c_p1c_eu_vaccaro.pdf.

- van Wynsberghe, A., 2021, *Sustainable AI: AI for sustainability and the sustainability of AI.* AI Ethics 1, 213–218 (2021). https://doi.org/10.1007/s43681-021-00043-6.
- van Wynsberghe, A., Donhauser, J., 2018, *The Dawning of the Ethics of Environmental Robots.* Sci Eng Ethics 24, 1777–1800. Available at: https://doi.org/10.1007/s11948-017-9990-3.
- Walsh, D., 2021, *Majority of Europeans want their countries to regulate crypto, not the EU.* Retrieved from: https://www.euronews.com/next/2021/09/01/majority-of-europeans-want-their-countries-to-regulate-crypto-not-the-eu-exclusive-euronew.
- Wanitcharakkhakul, L., & Rotchanakitumnuai, S. ,2017, *Blockchain technology acceptance in electronic medical record system.* In The 17th International Conference on Electronic Business, Dubai, UAE.
- WHO, 2019, *WTO members discuss product quality, safety and standards, debate new trade concerns.* Availabe at: https://www.wto.org/english/news_e/news19_e/tbt_16nov19_e.htm.
- Wiegmann P., 2019, *Becoming the industry standard when standardisation is not standardized.* Available at: https://discovery.rsm.nl/articles/389-becoming-the-industry-standard-when-standardisation-is-not-standardised/.
- Zenrobotics, 2020, *Circular Economy amid the pandemic – how AI-powered sorting robotics lead to better safety and recovery.* Available at: https://zenrobotics.com/blog/circular-economy-amid-the-pandemic-how-ai-powered-sorting-robotics-lead-to-better-safety-and-recovery/.

ANNEX 1 CASE STUDIES

Table 6: List of interviewed organisations

Organisation name	Organisation type
ANSSI	Government Agency
Cisco/IETF	Business/ Community
Ministry of economy of Luxembourg	Government
SCOPE-Europe	Association
Federal Ministry of Labour and Social Affairs (Germany)	Government
Federal institute for Occupational Safety and Health (Germany)	Government Agency

Source: Authors' own elaboration.

1.1. Case 1: GS label in Germany

The GS label is a seal of approval for product safety "Geprüfte Sicherheit" (Tested safety) and is regulated by the German Product Safety Act (Produktsicherheitsgesetz, ProdSG). For manufacturers, the GS label demonstrates to consumers that the products are subjected to a voluntary product and safety test by an officially recognised test centre. The label indicates that the health and safety of consumers are not at risk during the intended and foreseeable use and during the foreseeable misuse of the product.

1.1.1. Development and Management

a. Management

The GS label was introduced in 1988 to meet the demands of labour organisations, insurers, and consumer protection organisations. Although the mark originated in Germany, it is recognised in several Western European countries.

The GS label can be given out by so-called GS-bodies. These are organisations that test whether product specifications are sufficient to meet the GS mark requirements. Some of these GS bodies, such as TÜV Rheinland, add a QR code on the product next to the printed GS mark. Consumers can scan the affixed QR code that is linked to the online portal (www.certipedia.com) in which all the products with a GS label (given out by this GS body) are listed. Also, blacklisted products/manufacturers are listed in this portal. The QR code only links to a database managed by the corresponding GS body. This database is not linked to other GS bodies. There is, however, a centralised database in which misuse of the label is listed and which is managed by the Federal Institute for Occupational Safety and Health (Bundesanstalt für Arbeitsschutz und Arbeitsmedizin or BAuA).

Product safety tests for the GS mark can only be performed by GS-bodies that are accredited by the Central Office of the Federal States for Safety Engineering (Zentralstelle der Länder für Sicherheitstechnik or ZLS). In short, a GS mark certifies that the safety and health of the user are not at risk as long as the marked product is used according to its intended purpose as well as in cases where the use is unintended but foreseeable (e.g., misuse). Functional tests, however, are only included in the scope of testing to the extent that they are necessary for testing safety.

b. Application process

The path to obtaining the GS mark for manufacturers is as follows:

- The manufacturer, or their authorised representative, applies for testing to a recognised GS body;
- Based on specific tests given the product-type, the GS body provides proof that the tested prototype complies with the requirements in the Product Safety Act;
- A test report is issued by the GS body, which includes test results and describes requirements to be complied with during the manufacturing of the product;
- The GS body carries out control measures to monitor the manufacturing of the products. This includes a primary inspection as well as a follow-up audits. This ensures that during the period of validity of the GS-mark (max 5 years) the production is in accordance with the originally tested prototype. These follow-up audits can take place during the full period of validity of the mark. If the requirements for the awarding of the GS mark are no longer fulfilled, the GS body will withdraw the right of the manufacturer to use the mark; and
- The GS body issues a certificate for the awarding of the GS mark.

c. Legislative basis

The rules on the award of the GS mark are provided for in the ProdSG which replaced the German Equipment and Product Safety Act (Geräte- und Produktsicherheitsgesetz or GPSG) in 2011. The ProdSG regulates the safety requirements for products, which are made available, exhibited or used for the first time in the context of a commercial activity on the German or European market. It incorporates rules for the protection of consumers that govern transparency, information and market surveillance. This includes the provision that comprehensive information must be made available to consumers and that the manufacturer and/or the importer must be clearly identified.

d. Scope and relation to other labels

Awarding of the GS mark means that the product meets the safety requirements set out in the ProdSG and, if applicable, relevant European safety standards. Moreover, the GS Mark certification requirements can exceed those of the mandatory CE mark. The GS mark is not a comprehensive quality seal seeking to say anything about the lifespan or performance of a product, but it does provide - in contrast to the CE marking - genuine confirmation of safety.

All products that fall within the scope of the ProdSG can be given the GS mark. Products that in their use might pose health and safety hazards, like firearms, cannot be awarded a GS mark. In addition, ethical factors are also considered. For instance, a GS mark cannot be awarded to toys or games that glorify warfare. Also, trivial products that pose no potential hazard or risk are also excluded from the mark[112]. Currently the databases to which the QR-codes redirect are not centralised. Each GS body has their own database in which GS certifications and corresponding product information is listed.

[112] Federal Insitute for Occupational Safety and Health, n.d., *Questions and answers about the GS mark*. Available at: https://www.baua.de/EN/Tasks/Statutory-and-sovereign-tasks/Product-safety-act/FAQ/FAQ_node.html.

1.1.2. Technologies

Some of the GS bodies that give out the GS label use QR codes which are printed next to the GS label, that link to a database of the respective GS body, so that consumers can check whether the label is real and request additional information about the product. Manufacturers may add additional information about the product in the database. As the QR codes are linked to this database, scanning the QR code offers consumers up-to-date product information. If for instance, the label is not viable anymore because it has expired, this will likewise be stated in the database.

Some of these GS bodies include a 'freemium' business model to their certification database. That is: they offer 'premium' database entries in which manufacturers can, for a fee, add additional information about their product or company. Not only can this increase product safety, as more extensive product descriptions or even instructional videos on how the product should be used can be added, but it can also add to the sustainability of the label as these fees can cover the costs of maintaining the label and its database.

1.1.3. Users

The GS label is one of the most recognised marks for the safety assurance of products in the German markets and is recognised in other countries. The higher safety standard and reliable certification source might ensure that consumers are willing to pay a premium over cheaper but non-certified products. In addition, there are additional marketing benefits as producers can add information to the database that consumers can access by scanning the QR code.

The GS label is not mandatory. Companies are free to decide whether they want to get their products tested and to receive a GS label.

The use of the QR code provides consumers with a quick option for accessing information about the product's safety feature. The GC mark and the QR code also facilitate a certain degree of marketing (that the products are tested and safe) and allow consumers to make more informed decisions about their purchases. It is therefore meant to communicate the added value of the product for its compliance with product safety standards.

1.1.4. Information

The GC label provides consumers with the following information: certification holder, number, fulfilled standards, date of issue, certificate type. Depending on the GS body that gave out the GS mark, consumers can either access this information by the affixed QR code or search for this information online.

1.1.5. Conclusions & recommendations

- As the GS mark is one of the oldest labels in Germany, it is highly recognised by both manufacturers and consumers. This ensures that there is a benefit for manufacturers to file a request for the label as it offers them the possibility to signal that their product is safe and thoroughly tested. As a result, consumers are willing to pay a premium;
- The use of QR codes by some GS bodies improves accessibility of product information for consumers. This increases the possibilities for consumers to make informed choices;
- Currently only the database which registers misuse is centralised. Each GS body has their own database in which GS certifications and corresponding product information are listed. A centralised database of certified products (and products that misuse the label) increases the

transparency of the label and allows consumers to specifically search for (GS tested) safe products; and

- The option that GS bodies give to manufacturers to add information about their firm, product and/or the use of the product for a fee presses costs of maintaining the label and hence increases the sustainability (or even profitability) of the label in the long term.

1.2. Case 2: Cyberssecurity label in Finland

The Finnish Transport and Communications Agency (Traficom) has created the Cybersecurity Label to help consumers make more secure choices when purchasing IoT devices or services. The Label also helps companies to show that making devices and services secure by design is one of their priorities[113].

The Label can be given to products which collect and transmit data in digital format. The aim of the Label is to tackle the most common security threats affecting consumers on the Internet. It does not try to solve physical access-related security issues.

In 2019 Traficom studied consumers' attitudes and wishes related to the purchase and use of smart devices through a consumer survey[114]. Key finding was that every other Finnish person is concerned about the information security in smart devices. In addition, two-thirds of the respondents find it very important that there is easy to understand information available on the security of these devices.

1.2.1. Development and Management

Development of the label began at the end of 2018. It was developed in a pilot project led by the National Cyber Security Centre Finland (NCSC-FI) in collaboration with Finnish smart devices manufacturer Cozify Oy, DNA Plc and Polar Electro Oy. The first labels have been awarded to the products of these companies, which include smart sports watches (Polar) and smart home systems (Cozify).

The requirements are based on the EN 303 645 draft standard issued by the European standards organisation (ETSI). The ETSI criteria have been adapted to meet the specific needs posed by security threats concerning consumer devices. The Cybersecurity Label requirements are also designed to comply with a wide range of national and international requirements and recommendations. This helps ensure that the work required for the label can also be applied in other environments at the international level. As a result, Finland and Singapore have reached an agreement on the mutual recognition of cybersecurity labels issued by each other[115].

For the label the NCSC-FI and Traficom developed a certification process which Traficom administers. Receiving the label requires that products meet the criteria set by the NCSC-FI, which is verified by testing devices.

After applying for the label, the device or service must be secured from the most common IoT threats. Traficom's NSCS has set security requirements which must be met. These include the use of unique default passwords, having a secure software updating mechanism in place, and the availability of information for consumers on what personal data is processed[116]. After the applying company has submitted a statement of compliance, the device or service will be inspected by a third party (inspecting body), which may be a security company chosen by the applying company and approved by Traficom. Before the testing starts, Traficom approves the threat modelling and the testing plan drafted by the inspecting body. Testing by the inspecting body is done in cooperation with the company. Lastly, Traficom reviews the test results and decides whether the label can be awarded.

[113] Tietoturva,n.d, *What is the Finnish Cybersecurity Label?* Available at: https://tietoturvamerkki.fi/en/.

[114] See: https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label. Report of the consumer survey not publicly available.

[115] ScandAsia, 2021, *Singapore and Finland sign agreement to mutually recognise IoT security labels*. Available at: https://scandasia.com/singapore-and-finland-sign-agreement-to-mutually-recognize-iot-security-labels/.

[116] Tietoturva, n.d.,*Statement of compliance for the Cybersecurity Label*. Available at: https://tietoturvamerkki.fi/files/statement-of-compliance-for-the-cybersecurity-label.pdf.

Traficom also has a process for the maintenance of the label in place. Each product or service is reviewed annually to extend the right to use the cybersecurity label. During this review process, the applicant submits information on the changes made to the product or service after the last inspection. If these changes are of significance and might affect the security of the product or service, Traficom might decide that the initial inspection has to be undertaken again. If no major changes have been made, there is direct approval of the right to use the label[117].

1.2.2. Technologies

The certificate focusses on IoT. The label was implemented to provide consumers with basic information about IoT products that can meet digital security standards. Through this system, Traficom wants to raise the awareness of technology users in the country on issues related to information security and the use of connected equipment. Traficom saw a quick rise in attacks targeting IoT devices and networks throughout 2018. Therefore, they found it necessary to introduce regulations and security certificates for IoT products.

in order to ensure consumers are provided with up-to-date information, product pages are updated if newer versions of products are available and/or if new firmware updates change the security level of the product. Consumers therefore can access the latest information when making a purchasing decision.

1.2.3. Users

It is argued that the label adds value to a product (and therefore competitive advantage) by signaling product safety. By seeing the label, consumers know that a certain level of attention has been paid to the information security of the product. And that the information security assessment has been conducted by an independent authority. In addition, it is seen as an opportunity for companies to guide their consumers through the world of information security and increase their opportunities to make informed choices.

Besides competitive advantages offered by the label, the online database also provides up-to-date and easily understandable information on the technical solutions and protection methods of the product for consumers. This is relevant to consumers, as many consumers find it difficult to find information about the safety features related to information security. As such, a label such as the cybersecurity label makes it easier to make informed choices and reduces the time investment needed to understand the product safety concerns by codifying the idea of approval and certification within the label. In addition, producers are made more aware of the most frequent and/or pressing cybersecurity issues in connected products and ways to mitigate these issues.

[117] For full application and review process, see: https://tietoturvamerkki.fi/files/cybersecurity_label_presentation-280920.pdf.

1.2.4. Information

In terms of the information that the label communicates, it offers the product description, support period, security guidance, other certifications and an overview of how the product is protected against common IoT threats. More specifically, the statement of compliance for the label consists of the following[118]:

- Product description: a description of the key information security features of the product or service and the related ecosystem, including information on the intended support period and security guidance as well as other certifications the product received;
- Access control: a description of the methods used to control access to a product or service, such as passwords, certificates or third-party authentication procedures;
- Software security: a description of the software used, and how it is kept secure and up-to-date;
- Data protection: a description of how, for what purpose, and by whom personal data is collected;
- Secure transfer and storage of data: a description of data protection methods during transfer and storage, such as data transfer, authentication and encryption methods, and key management procedures;
- Security of network services and ecosystem interfaces: the product or service must minimise unnecessary online services and comply with the principles of minimum rights in their implementation. The interfaces provided by the ecosystem must be secure. All interfaces must check the feeds accessing them; and
- Secure default settings: the default settings for the product or service should be set to protect the user, meaning that the installation of the device should involve minimal decisions to ensure the highest level of security.

1.2.5. Conclusions & recommendations

- The Finnish cybersecurity label is a relatively new label that specifically focusses on connected IoT devices. It has been developed together with manufacturers of products that use this technology while following international standards. The label therefore adheres to ETSI criteria;
- As the safety of IoT devices is a relatively new thing of interest for both manufacturers and consumers., the label also raises awareness of the importance of digital product safety. In addition, companies are made aware of up-to-date technical solutions and protection methods of the product against common threats during the process; and
- Consumers are able to look up up-to-date product information online on the products that have received the label, hence increasing transparency on product safety.

[118] See: https://tietoturvamerkki.fi/en/requirements/.

1.3. Case 3: The ANSSI security Visa in France

Created by decree in July 2009, the French National Cybersecurity Agency (Agence Nationale de la Sécurité des Systèmes Informatiques – ANSSI) is a service with national competence attached to the general secretariat for Defence and Security. Its role notably is to contribute to information security, by participating in the research, development, and promotion of security technologies[119].

In June 2018 ANSSI delivered its first security Visas. As a governmental agency, it has undertaken the task of identifying and recognising reliable security companies which provide products or services for cyber security protection[120]. This system of valorisation of existing cyber security solutions has three objectives:

- Regulatory: to ensure cyber security solutions match both national and European rules;
- Contractual: for public and private actors that demand the solutions they use to have the security Visa; and
- Commercial: to allow both service providers and users to increase their competitivity[121].

1.3.1. Development and management

The security Visa was developed by the government agency ANSSI and the French government itself. When a cyber security product receives the Visa, it is considered as recommended by the French State and guarantees the legitimacy of the security Visa and its trustworthiness to other actors. There are both French and European rules that regulate the use of cyber security solutions that feature a good level of robustness, proven by trials and tests. As noted in the introduction, one of the three main objectives of the security Visa is to fit both national and European regulations[122].

While there already are many existing labels on the market, given not only by public authorities but also by private actors[123], ANSSI benefits from the legitimacy of being a national government agency, which brings more credibility to its label awarding process and to the Visa itself. For private actors, such legitimacy offers important benefits from obtaining the Visa, both in terms of credibility towards their product/service consumers and users, and in terms of competitivity.

Since the introduction of the security Visa, ANSSI has led an inclusive approach to increase its label's visibility. This approach includes using the expertise and legitimacy provided by its experience as a government agency and communicating to its partners and stakeholders on the evaluation process necessary to obtain the Visa and promoting the solutions it offers[124].

ANSSI is fully responsible for the management and implementation of the label and certificate that the Visa represents. Not only is the agency the initiator of this new approach to product security, but it also ensures that the security tests and the entire evaluation process are performed by laboratories recognised by the agency itself. Finally, ANSSI is the entity which ultimately delivers the Visa to the product supplier.

[119] Historique de l'ANSSI. Available at: https://www.ssi.gouv.fr/agence/cybersecurite/lanssi/historique-de-lanssi/.

[120] ANSSI website. Available at: https://www.ssi.gouv.fr/administration/visa-de-securite/.

[121] Matthieu Dualt, n.d., *Qu'est-ce que le Visa de sécurité délivré par l'ANSSI* ? Available at: https://yousign.com/fr-fr/blog/visa-de-securite-anssi.

[122] ANSSI. Security Certification of products.

[123] L. Adam, 2015, *Qui se cache derrière le Label France Cybersecurity ?* Available at: www.zdnet.fr/actualites/qui-se-cache-derriere-le-label-france-cybersecurity-39814500.htm.

[124] Press release 2018.

The security Visa is only delivered by ANSSI upon completion of the evaluation performed by the licensed laboratories. This Visa, "depending on the context and need[125]" can take the form of either a certification or a qualification. In the former case, the certificate delivered, which can then take the form of a label used on the product, demonstrates its robustness to users[126]. In the latter situation and after ANSSI's approval, qualified products are recommended by the French government[127].

1.3.2. Users

For the companies that are either product suppliers or service providers, the Visa presents two main advantages. First, the gain in competitiveness both with other French actors and international actors on the cyber security market, as the Visa is a credible proof of the robustness of the product since it is recognised by the French government. Second, the access to wider market opportunities, thanks to the common criteria certification, which recognises the Visa as adhering to an international standard based on mutual recognition agreement for product safety[128]. Additionally, the Visa allows to improve communication between product suppliers and service providers and consumers, via the labelling.

The companies are closely followed during the process of evaluation of the product's robustness. Besides, two pathways have been identified, one for users and one for product providers and services suppliers, offering direct answers depending on the legislative frameworks and the type of market the companies want to access[129].

Consumers are directly impacted by the Visa as it facilitates their choice of a cyber security service. Similarly, the Visa guarantees the efficiency of the security solution, as the many tests performed under ANSSI's supervision prove the resistance and safety of the product or service.

Just as the suppliers, the users can find guidelines on the website to understand which Visa they should look for when they want to buy a cyber security solution[130]. They can also contact the Visa team directly via their e-mail address to obtain further information.

Overall, the security Visa improves communication between the product suppliers or service providers and the consumers, and thus increases transparency on the efficiency of security solutions, as well as clarity of information and reliability. Thanks to the Visa, consumers can develop a better understanding about which existing products best fit their needs and save the costs (both in terms of time and money) to collect information on the reliability of the product they are purchasing. It is especially of interest given that it can be hard for average citizens or firms to be aware of the technical details for cyber-security related products, and of the risks they face in case of selecting the wrong product for their needs.

[125] ANSSI, n.d., *Security VISA*. Available at: https://www.ssi.gouv.fr/en/security-visa/security-visa-catalogue/.

[126] ANSSI, n.d., *Security certification of products*. Available at: https://www.ssi.gouv.fr/uploads/2018/01/security-certification-of-products_security_visa_anssi.pdf.

[127] ANSSI, n.d., *Qualification of solutions*. Available at: https://www.ssi.gouv.fr/uploads/2018/01/qualification-of-solutions_security_visa_anssi.pdf.

[128] Ibid.

[129] Ibid.

[130] Available at: https://www.ssi.gouv.fr/uploads/2018/01/visasecu_2017_schema_utilisateurs_p13.png.

1.3.3. Information

Products issued the ANSSI security Visa can display a label signifying that the product meets ANSSI certification requirements[131]. This is a direct method of communicating to consumers that the product is holding the Visa and as such has undergone an evaluation and met standards set on the national level for cybersecurity products.

The certification of security delivered by the Visa demonstrates the resilience of a product against simulated attempts to penetrate the protected systems by a third party, under the supervision of ANSSI[132].

1.3.4. Conclusions & recommendations

- The development of the Visa by a public authority (the agency) supported by a national government increases the perceived credibility of the products approved by ANSSI. Their role as an intermediary decreases the information cost necessary to understand which products or services are reliable on a complicated yet critical topic;
- Security labels are a straightforward and efficient manner of promoting product safety as they impose the minimum cost on product suppliers and provide great benefits for both suppliers (in terms of competitivity) and users (in terms of safety); and
- Continuous interaction and accompaniment of service or product suppliers are key for the success of the Visa.

[131] ANSSI, n.d., Security Certification of products.

[132] ANSSI, n.d., *What is the purpose of ANSSI security Visas*. Available at: https://www.ssi.gouv.fr/en/security-visa/.

1.4. Case 4: The Product Circularity Datasheet in Luxembourg

Launched in 2019 by the Luxembourg Ministry of the Economy, and as part of the Circularity Dataset Standardization Initiative[133], the objective of the Product Circularity Data Sheet (PCDS) is to establish a recognised standard to communicate data and information on the circular economy characteristics of products[134]. As a matter of fact, it is currently difficult both for the industry and consumers to access reliable data on the circular properties of a product, thus clarifying the necessity of having an internationally accepted dataset to allow for reparability, recycling, and re-use of products. Thus, the PCDS is a "*standardised digital fingerprint*" used to share reliable data on the circular features of products across the supply chain[135].

1.4.1. Development and Management

The main public stakeholder involved in the PCDS is the Ministry of the Economy of Luxembourg, which represents the national government in the initiative. However, the governance of the PCDS is also shared with the private consulting enterprise +Impakt, which has provided external support in its capacity as a circular economy expert to the government. In terms of digital enabler, it is the digital firm Cobuilder that has been chosen to create and develop the use of the standardised PCDS templates[136]. Additionally, more than 50 international and regional companies from the private sector are collaborating with both the Ministry and +Impakt, to provide information on all products supplied by these companies[137]. Finally, there are the "accredited auditors", who are commissioned by the Ministry to verify the data entered by the manufacturer of the product into the standardised PCDS template. They play a crucial role in increasing the consumer's trust related to the capability of the entire process[138]. The stakeholders are managed through a close and continuous consultation between the Ministry of Economy of Luxembourg and private organisations[139].

The initial developers, meaning the Ministry of Economy, supported by the consulting firm +Impakt and the digital enabler Cobuilder, are responsible for the implementation of the standard. Firstly, the Ministry and the consulting firm, through their collaboration, share the know-how on product circularity and how to implement the initiative. Secondly, Cobuilder has the enabling capacity of collecting the necessary data, and then creating, developing, and deploying the use of the standardised data sheet template, as well as creating the digital "fingerprint[140]".

The standard, therefore, is linked to a "fingerprint", or a DPP, which carries information that is then made available to the consumers. This creates added value to the consumers, as it helps to raise awareness and provide consistent data (thanks to the standardised data source and data presentation) about the circular characteristics of a product. Besides, the availability of such information provides

[133] This initiative has the objective to establish an official standard for communicating data on the circular economy properties of products, in consultation with other standards organisations.

[134] PCDS Luxembourg, n.d., *The Circularity Dataset Initiative*. Available at: https://pcds.lu.

[135] Cobuilder, n.d., *Luxembourg launches product circularity data sheets in a bid to boost circularity*. Available at: https://cobuilder.com/en/luxembourg-launches-product-circularity-data-sheets/.

[136] Ibid.

[137] PCDS Luxembourg, n.d., The Circularity Dataset Initiative.

[138] PCDS Luxembourg, n.d., *The audit system*. Available at: https://pcds.lu/the-audit-system/.

[139] *New Luxembourg Strategy for the Circular Economy*, 2021, Available at: https://www.tradeandinvest.lu/news/new-luxembourg-strategy-for-the-circular-economy/.

[140] Cobuilder (n.d). Luxembourg launches product circularity data sheets in a bid to boost circularity.

transparency about the supply chain, and thus on the components and manufacturing used to make the product. This is key to helping consumers make informed choices when buying new products[141].

There were many challenges to the introduction of the standard. Firstly, there was no dataset under a standardised format, nor a single system for exchanging product characteristics information along the supply chain previously. Besides, the data was usually not validated by an independent third party. Further, the data collection is costly and time-consuming and consists of an approximation resulting from the use of different information sources[142]. These challenges have been solved by allowing the enterprises to have a common system for information collection along the supply chain, and information exchange, backed by a system of third-party auditing to guarantee the reliability of the data shared with the consumers[143].

1.4.2. Technologies

The standard is backed by a product passport, which takes the form of a Data Template[144], where all the information about the products is collected along the supply chain. Then, the system is backed by a decentralised information exchange system[145].

To support the standard, the Data Sheet can be updated and revised as soon as there is a change in the product (composition, regulation, recycling, etc[146]).

The main challenge, however, was the "originality" of the technology as no such system had been set up in Luxembourg in the past. This was overcome with close and continuous consultations between the government and the 50 organisations involved.

1.4.3. Users

Benefits of the PCDS for the companies are being part of a network of companies that work in close collaboration with the government and adhering to similar standards as their counterparts. The companies also gain in brand reputation, which can both attract new consumers and open new markets for them. Besides, Luxembourg represents an attractive economic environment for companies that are looking to create values while reducing their impact in terms of pollution, waste production, or energy use[147]. Companies are supported by the PCSD team itself to adapt to the standard, and they can find all the different documents ad information available on the official website of the Initiative.

Consumers can make better-informed choices regarding both, when they purchase and when they dispose of a product. They can learn more about its components (and maybe make a decision depending on them), and the recycling possibilities of the product. They can also learn about reparability and re-use options. The fact that the information is provided directly by the producer also facilitates the task for the consumer, who does not have to spend the money and time to look for the information.

The standard improves the communication between the consumers and the companies, as there is a uniform process and technique to collect the data and make the information about the product's

[141] The European Union, n.d., *PCDS: a solution to access circularity* data. Available at: https://circulareconomy.europa.eu/platform/fr/good-practices/product-circularity-data-sheet-solution-access-circularity-data.

[142] *The product circularity datasheet Luxembourg*. Available at: https://luxembourg.public.lu/fr/investir/innovation/pcds.html.

[143] Ibid.

[144] PCDS on the Data Template website. Available at: https://pcds.lu/pcds-system/#data-template.

[145] The product circularity datasheet Luxembourg. Available at: https://luxembourg.public.lu/fr/investir/innovation/pcds.html.

[146] Handling the OCDS. Available at: https://pcds.lu/pcds-system/#handling-pcds.

[147] Luxembourg Trade & Invest, 2021, New Luxembourg Strategy for the Circular Economy.

circularity available to the consumers. Consumers know that if they purchase a product from one of the 50 participating firms, they will have the same basis to refer to, which will allow them to consistently compare the advantages and defaults of each product, thus making a more rational decision in their purchase.

1.4.4. Information

Through the standard, information about production materials are listed, as well as information regarding the product manufacturing, the distribution, the consumption and finally the recycling features of the product. At any stage of the supply chain; it is the manufactures that receive the PCDS from their suppliers, who combine the data into a new PCDS for the product they sell, and then make it available to the consumers, and at a later stage, to the actors in charge of recycling[148].

The consumers can access the PCDS made available by the producers. As such, the consumers can access the data integrated by the producer, itself received from the producer's suppliers[149]. The main concern is the complexity of the information received which can be hard to understand for the consumer.

1.4.5. Conclusions & recommendations

- The collaboration between the private and public sectors is efficient in this situation;
- The creation of a common information-system sharing is essential, just as the fact that it can be modified by only one actor (the producer) and that it is verified by an accredited third-party;
- The progressive development of the technology is also important, by starting with a definite group of 50 private actors, testing the technology and consolidating the network and practices, and then widening it to a wider audience; and
- Such technology is of particular interest, as it covers all the steps of the supply-chain (production), usage (consumer's purchase), and recycling.

[148] Ibid.

[149] Ibid.

1.5. Case 5: The European Secure Cloud label in France and Germany

Note: Because we could not secure any interview, this case study is exclusively based on desk research.

Announced in 2016, but never actually adopted, European Secure Cloud (ESCloud) was the result of the conjoint work of the French National Cybersecurity Agency (ANSSI) and its German counterpart, the Federal Cyber Security Authority (Bundesamt für Sicherheit in der Informationstechnik – BSI). Both governmental agencies aimed at improving IT security, not only in France and Germany but across the European territory. The ESCloud label was the result of the merging of two national initiatives, the SecNumCloud referential in France, and the C5 catalogue in Germany[150].The aim of combining two existing tools was to create a common basis for European cloud computing security[151] by identifying reliable providers of cloud computing services, thanks to a selection of fifteen rules, both technical and organisational, which would have guaranteed consistency across the selected providers. The objective of the initiative was to cover both labelled solutions and data treatment across the European territory.

1.5.1. Development and Management

The agencies involved in the development of the label were ANSSI and BSI as well as the governments of both France and Germany. The two agencies got involved after a years-long collaboration and the decision to align their national programmes in terms of cyber security protection[152].

Both ANSSI and BSI were responsible for the implementation of the label. Being the initiators of the project together with national government agencies provides them with credibility in terms of assessment of the security of the services and distribution of the label. Besides, as national agencies, they both have the IT infrastructure and means necessary to implement the label[153].

By laying the first basis of Franco-German cooperation to foster the improvement of cyber security at the European level, ESCloud would have contributed to the goals of protection of users and citizens in their use of online services.

The label was a pioneer in the creation of a European cooperation system on cyber security. A difficulty is that there already exist many labels on the market, not only from public authorities but also produced by private actors. It may therefore have been challenging to introduce an additional one and face the competition on the market, and for the label to become critical when it comes to calls for tenders. The credibility coming from an alliance between national agencies, as well as the acute knowledge of both BSI and ANSSI should have helped, just as the similarity of the structures of SecNumCloud and catalogue C5 which contributed to the merging process and facilitated the recognition of the label in both countries[154]. However, according to an agent from the Federal Office for Security in the information technology, the technical conditions were not gathered for the label to be properly launched, and insurmountable obstacles prevented its creation[155].

[150] ANSSI, n.d., *ESCLOUD – Un label franco-allemand pour les services d'informatique en nuage de confiance*. Available at: https://www.ssi.gouv.fr/actualite/escloud-un-label-franco-allemand-pour-les-services-informatique-en-nuage-de-confiance/.

[151] Next Inpact, 2016, *Cloud de confiance : l'ANSSI sort son référentiel et lance un label avec l'Allemagne* . G. Pépin., 2016, Available at: https://www.nextinpact.com/article/24782/102493-cloud-confiance-anssi-sort-son-referentiel-et-lance-label-avec-allemagne.

[152] Ibid.

[153] ANSSI, n.d., *ESCLOUD – Un label franco-allemand pour les services d'informatique en nuage de confiance*. Available at: https://www.ssi.gouv.fr/actualite/escloud-un-label-franco-allemand-pour-les-services-informatique-en-nuage-de-confiance/.

[154] Louis Adam. 2015, *'Qui se cache derrière le Label France Cybersecurity ?'*. Louis Adam. February 2015. Available at: www.zdnet.fr/actualites/qui-se-cache-derriere-le-label-france-cybersecurity-39814500.htm.

[155] According to interactions with Anabela da Silva Santos, Federal Office for Information Security (BSI).

1.5.2. Users

ESCloud would have allowed the European actors to have recourse to reliable service providers. Cloud computing technologies are indeed delicate to handle because of the lack of control over data access and confidentiality. Such a problem would have been addressed thanks to the label which allows the identification of safe services[156].

The companies wishing to apply for the label would have found all the necessary documents to be filled, as well as a detailed explanation of the processes to be followed on the website of both ANSSI and BSI[157].

The label would have also directly impacted users of cloud computing services, as they could make a more informed decision by choosing a service already certified by a specialised and trusted national government agency. This therefore would have reduced a consumer's cost of looking for very technical information themselves (both in terms of time and money). To guide them, the list of requirements was available on ANSSI's website[158], as well as the list of qualified products and services[159]. After identifying their needs, they could therefore look for the company that provides the services best fitted.

The label would have improved communication between the product suppliers or service providers and the consumers, and thus increased transparency on the efficiency of security solutions, as well as clarity of information and reliability. The label would save consumers the time to collect information on the reliability of the product they are purchasing. Finally, since the label would have been granted by the two national agencies, an enterprise that had already received the label given by ANSSI and BSI would have neither had to apply to another European label, nor to additional labels at the national level in France and Germany, which would have potentially given companies access to new markets[160].

1.5.3. Information

In case the label had existed and a service had received the label, it would have meant for the consumer that the product was approved and recognised by both the French and the German agency and that it satisfied the fifteen technical and organisational rules laid by the ESCloud team. It, therefore, would have implied that the cloud computing service offers a satisfying level of security, and processes the individual data collected in an accepted way[161]. The service would have then been approved by the ANSSI, and hence the BSI would have made the label available as well.

[156] EuroCloud France, n.d, *ESCLOUD – Un label franco-allemand pour les services cloud de confiance* Available at: https://www.eurocloud.fr/escloud-label-franco-allemand-services-dinformatique-nuage-de-confiance/.

[157] ANSSI, n.d., *Les procédures et formulaires*. Available at: https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/procedures-et-formulaires/.

[158] ANSSI (n.d.) *Prestataires de services de certification électronique (PSCE) et les prestataires de services d'horodatage électronique (PSHE)*. See www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences/.

[159] ANSSI, 2022, *Liste des produits et services qualifiés*. Available at: www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf.

[160] La Tribune, 2017, "*Cyberattaques: que contient le "paquet cyber" que l'Europe veut voter en 2018* ? Available at: https://www.latribune.fr/technos-medias/cyberattaques-que-contient-le-paquet-cyber-que-l-europe-veut-voter-en-2018-751009.html.

[161] ANSSI, n.d, *European Secure Cloud – a new label for cloud service providers*. Available at:www.ssi.gouv.fr/en/actualite/european-secure-cloud-a-new-label-for-cloud-service-providers/.

1.5.4. Conclusions & recommendations

Despite its announcement, the label failed to be launched and was never used in practice. Here are a few recommendations to be applied for next attempts to create a trans-European label for cloud computing security.

- For the label to have gained visibility, it would have been necessary to have a wider marketing campaign across the EU, not only to show the benefits of the label, but also to encourage similar bilateral and multilateral initiatives across the EU Member States;
- The competitiveness of the label, with respect to other private solutions, should be at the forefront of the development and launch to demonstrate the added value for companies to apply for the label; and
- Furthermore, the launching of any similar label should come with clarity when it comes to the new rules and norms that a cloud computing service should fulfil.

1.6. Case 6: The EU Cloud Code of Conduct

The EU Cloud Code of Conduct (Code) aims to secure the trust of cloud customers in Cloud Service Providers (CSPs) and to support CSPs to prove compliance with the General Data Protection Regulation (GDPR). The first pre-GDPR version of the Code was developed by a working group hosted by the European Commission and was handed over to the industry in 2017. Between 2017 and 2021, the Code was re-drafted to reflect the newly introduced requirements of GDPR. The latest version of the code – version 2.11 – was published in May 2021. Following a positive opinion of the European Data Protection Board, this version of the Code received official approval by the Belgian Data Protection Authority. At the same time, the independent monitoring body of the Code – SCOPE Europe – was officially accredited by the Belgian Data Protection Authority (pursuant to Art. 41 GDPR). The Code is a voluntary co-regulatory instrument, allowing a CSP to evaluate and demonstrate its adherence to the Code's requirements.

1.6.1. Development and Management

The foundation of the Code originates from the work of the Cloud Select Industry Group (Data Protection Code of Conduct Subgroup), consisting of representatives of European and multinational companies and organisations, together with authorities of the European Commission (involvement of DG Connect and DG Justice). The Article 29 Working Party - which represented national Data Protection Authorities under the Data Protection Directive – provided feedback to this original version of the Code. When GDPR was introduced, the Code required significant updates to be fit for approval pursuant to Art. 40 GDPR. By that time, in 2017, the mandate of the Cloud Select Industry Group ended, and further development of the Code was handed over to industry. They presented a GDPR compliant version of the Code in 2019 and negotiated with the data protection authorities its official approval in the following two years.

The final approval, which enables the Code to be used as proof of compliance under GDPR, was performed by the Belgian Data Protection Authority in May 2021. All 27 data protection authorities of the European Data Protection Board were involved in the process.

The current governance of the Code consists of a General Assembly, Steering Board and a Monitoring Body:

The General Assembly was founded in 2017 and back then consisted of Alibaba Cloud, Fabasoft, IBM, Oracle, Salesforce and SAP. Over the years, it has steadily grown, including also SMEs. Membership in the Code – and by that, to the General Assembly - is open to everyone, as long as no severe doubts regarding adherence to the Code arise, e.g., in case of a strong and proven track record of GDPR non-compliance. The reasoning behind this is that standard development is a matter where everyone should be able to participate and allowed access to unless this could endanger the overall goal of the initiative.

The Steering Board deals with implementation of the code. Every company with voting rights can send a representative to the steering board.

The independent monitoring body is SCOPE Europe, which scrutinises CSPs that sign up to the Code and monitors services that are verified under the Code. The Monitoring Body checks compliance by an initial assessment, annual recurring assessments and ad-hoc assessments[162] SCOPE Europe also acts as

[162] More information about the assessment procedures can be found here: https://eucoc.cloud/en/public-register/assessment-procedure/.

secretariat to the steering board and general assembly, but there is a strict division of roles and responsibilities to avoid conflicts of interest.

a. The Code membership

To cover the monitoring costs of the independent monitoring body, the Code has a pricing scheme, with different membership options (full membership for large, medium and small enterprises as well as non-voting membership options for medium-sized and small-sized enterprises). Everyone that joins the Code of Conduct directly becomes a member. The full General Assembly Membership Fee costs €10,000 annually. Non-voting membership is €5,000 for medium-sized enterprises or €1,500 for small-sized enterprises. Companies can also become Code of Conduct supporters, for €1,500 (small-sized) up to €5,000 a year[163]. The reason for offering membership options without voting rights, is among others because SMEs often do not have the required resources to participate in the assembly but would still like to sign up for the code and work with it.

Added-value of this membership and ultimately a declaration of adherence to the Code lies with demonstrating that the cloud provider - in its role as a processor - is GDPR compliant to data protection authorities in Europe, but also in front of courts.

The Code provides three levels of compliance that relate to the levels of evidence that are submitted. At each level cloud services have to comply with all provisions of the Code, but a distinction is made in the amount of evidence that is provided. The different levels entail164:

- Level 1: The CSP has performed an internal review and documented its implemented measures proving compliance. Following, the monitoring body performs a compliance check for all provisions of the code, including requesting evidence of implementation of certain provisions;
- Level 2: Additional to Level 1, compliance with the Code is **partially** supported by independent third-party certificates and audits, which were based upon internationally recognised standards; and
- Level 3: Mostly identical to Level 2, however compliance is **fully** supported by independent third-party certificates and audits, which were based upon internationally recognised standards.

b. The Code and its linkages to legislation

The Code is directly linked to the GDPR, as it is a way for companies to ensure compliance with this regulation. For this reason, SCOPE Europe regularly interacts with data protection authorities. Other regulations that deal with data protection are therefore also relevant to the Code, for example the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[165]. Currently, a module of the Code related to third-country data transfer is being developed.

1.6.2. Technologies

The Code covers the full spectrum of cloud services: software (Software-as-a-Service, SaaS) and platform (Platform-as-a-Service, PaaS) as well as infrastructure (Infrastructure-as-a-Service, IaaS).

[163] All prices are excluding VAT. Companies also need to pay for (renewal of) declarations of adherence, complaints fees and fees for additional assessments.

[164] More information on the different levels of compliance can be found here: https://eucoc.cloud/en/public-register/levels-of-compliance/.

[165] The CLOUD Act is a federal law that enables the US government to force technology companies to hand over data from users, even if these are stored on foreign territory.

According to the Code, it is "crucial that customers develop a level of confidence in a Cloud Service Provider (CSP) before they entrust them with their data and applications."[166] Furthermore, the GDPR requires that customers only use CSPs as processors that provide sufficient guarantees to ensure the protection of the rights of the data subject.

While there are codes on the market that only address one layer of cloud, when developing the Code it was considered very often impossible to discern between the different layers when checking for GDPR compliance. Cloud computing is becoming business standard, therefore, CSPs, as well as customers, are facing a steadily increasing amount of requirements. To address the needs of such a changing environment, the Code is intended to be complemented by dedicated modules extending or detailing its requirements. The first new module focuses on the transfer of personal data to third countries.

In terms of the use of new technologies and digital solutions for the Code itself, the Monitoring Body uses a cloud provider to go through the materials that it receives from members of the Code. This is a standard ticketing system that was recommended by a German Data Protection Authority and has been configured in a way that fits with the monitoring activities. The Monitoring Body is also looking for solutions to automatically scan legislative documents, and checking whether parts of the Code are reflected there. Thus far, they have not found a suitable solution for this.

1.6.3. Users

The Code focuses on business-to-business cloud services, where the CSP is acting as a processor167. The added value of the Code for companies is that it is an official tool to prove compliance to GDPR. Furthermore, by outlining clearly what information must be made available to customers, the Code increases transparency and is perceived to create added value to the market. Finally, by covering the full spectrum of cloud services (SaaS, PaaS and IaaS) it is perceived to address the needs of internationally operating providers and small- and medium enterprises (SMEs) at the same time.

Businesses that want to become a member of the Code, usually reach out to the secretariat. SCOPE Europe tries to update the website on an ongoing basis and is currently developing onboarding material for new members.

For consumers, the Code should make it easier and more transparent to analyse whether Cloud Services are appropriate for their use case. If a consumer (or a data subject) thinks something is off, it is possible to file a complaint with the Monitoring Body. This can be done anonymously.

1.6.4. Information

The main aspect of the Code concerning product safety is the adherence to the GDPR, ensuring that consumer data is protected and privacy is maintained. The Code itself is perceived as a way to make the compliance of the cloud provider to the GDPR transparent.

As the Code protects consumers indirectly, it is not perceived as a necessity to inform consumers about it, apart from presenting information on the website. However, in case a consumer wants to file a complaint against a company, this is possible. A consumer in this case can also be a company using the services of a CSP. Adherence to the code is being communicated by the usage of a dedicated trust mark.

[166] EU Cloud COC, 2018, EU Data Protection Code of Conduct for Cloud Service Providers.

[167] It does not apply to business-to-consumer services or any processing activities for which the CSP may act as data controller.

1.6.5. Conclusions & recommendations

- The primary challenge when developing the Code was to get approval, a process that took a total of four years. In particular, the European Data Protection Board and data protection authorities had to develop a common understanding of the Code and its implementation, while at the same time the GDPR was being launched. A topic of discussion was how comprehensively monitoring should already be part of the Code provisions and what should be rather part of the accreditation of the monitoring body pursuant to Art. 41 GDPR. According to interviewees, a benefit from this process was that data protection authorities were forced to understand the feasibility of the Code and its implementation, and in particular understand the perspective of the companies that needed to join the Code;
- A lesson that therefore can be learned from the Code is that when implementing a Code of Conduct type of co-regulation, it is important to think of reasons and legal incentives why a company or other stakeholders should comply with it, would sign up and what added value it brings to these companies. In the case of the Code, this is legal certainty; and
- The Code can be considered a best practice way of ensuring compliance with a regulation (in this case the GDPR). This kind of co-regulation might however only be suitable in the case of a regulation and not a directive, as it involves the set-up of a governance body and independent monitoring body (which also requires financing)[168].

[168] Institut für Verbraucherpolitik, 2015, Key Points of a Digital Regulatory Policy – Recommendations to improve the conditions for effective co-regulation in the information society.

1.7. Case 7: The International Manufacturer Usage Description Specification

The Manufacturer Usage Description Specification (MUD) is "an embedded software standard defined by the Internet Engineering Task Force (IETF)." It allows "Internet of Things (IoT) device makers to advertise device specifications, including the intended communication patterns for their device when it connects to the network"[169].The specification is documented as a proposed standard in Request for Comments (RFC) 8520, which was published in March 2019.

The goal of the MUD is to "provide a means for end devices (the source or destination of data transmitted over a network) to signal to the network what sort of access and network functionality they require to properly function." Specifically, the MUD is intended to[170]:

- Substantially reduce the attack surface on a device to those communications intended by the manufacturer;
- Provide a means to scale network policies to the ever-increasing number of types of devices in the network;
- Provide a means to address at least some vulnerabilities in a way that is faster than the time it might take to update systems. This will particularly be true for systems that are no longer supported;
- Keep the cost of implementation of such a system to the bare minimum; and
- Provide a means for extensibility for manufacturers to express other device capabilities or requirements.

The "manufacturer" is the entity or organisation that will state how a device is intended to be used. There is an assumption that there exists an organisation in the supply chain of the device that will take responsibility for informing the network about the purpose of the device.

1.7.1. Development and Management

The MUD (RFC8520) was developed by the IETF, which is an open international community consisting of network designers, operators, researchers and vendors that aims to make the internet work better[171]. It does this by producing documents such as protocol standards, best current practices and informational documents. Any interested person can participate in the work of the IETF. People participate in the IETF on an individual basis, not as part of an organisation. The technical work of the IETF is done in working groups that are organised in several areas by topic. Each of the areas is managed by Area Directors, that also participate in the Internet Engineering Steering Group (IESG). The latter is responsible for the final review of IETF documents.

The MUD is a Proposed Standard, which means it is less mature compared to an Internet Standard but a stable and well-reviewed specification. It may eventually become an Internet Standard. The MUD Specification represents the consensus of the IETF community and has been approved by the IESG, the only body that can approve Standards Track RFCs. Most specifications approved by the IETF are Proposed Standards.

[169] CISCO, n.d., *What is MUD?* Available at: https://developer.cisco.com/docs/mud/#!what-is-mud/what-is-mud.

[170] Internet Engineering Task Force, 2019, *Manufacturer Usage Description Specification*. Available at: https://datatracker.ietf.org/doc/html/rfc8520.

[171] Alvestrand, 2015, *A Mission Satement for the IETF*. Available at: https://datatracker.ietf.org/doc/rfc3935/.

A challenge when developing the MUD was that it cuts across four to five different IETF working groups. When submitting the draft, it was therefore a challenge to find the right group to submit it to. Furthermore, many stakeholders were involved in the development of the MUD. This included among other interoperability testing, programming an open flow implementation and control function, developing tooling and a reference implementation. After documenting this the document goes through several rounds of review before finally the IESG performs the final review and approval.

a. The MUD and its linkages with legislation

The MUD itself is not linked to specific legislation. On the other hand, there are several legislative initiatives that exist or are currently being developed that could relate to the security of connected devices. So far, most of these focus on the hardening security of the device itself rather than considering the role of the network and the broader ecosystem. At EU level, in the context of the New Legislative Framework, there is a trend towards expanding the concept of product safety to address cybersecurity of the device. The recently published Delegated Act to the Radio Equipment Directive[172] takes such an approach for wireless devices using radio technology, for example. It is also being considered in the context of the revision of the Machinery Directive[173]. Separate from the product compliance framework, the Commission is also considering horizontal baseline security measures in the forthcoming Cyber Resilience Act legislation (to be published Q3 2022).

At the national level, both the draft UK Product Security and Telecommunications Infrastructure Bill (introduced to Parliament 24/11/21) and the Finnish Cybersecurity Label base their requirements on the ETSI consumer IoT security standard, EN 303 645. The German BSI (cybersecurity authority) has recently opened the application process of two categories of product (email services and broadband routers) for its IT Security Label, which has its legal basis in the IT Security Law 2.0 adopted earlier in 2021.

What the MUD adds to this is the focus on the role of the ecosystem around the device – information that the network is able to interpret and act on about the device's security posture and how it should behave. As such, it helps address important issues such as limited capabilities of the devices, the legacy of insecure devices that are already out there, scalability of onboarding and managing devices and how security posture changes over time[174].

1.7.2. Technologies

The MUD solution itself consists of three components:

- A URL that is emitted by an IoT device and that can be used to locate it;
- The Internet hosted file that the URL points to. It contains information on the level of communication access that is needed for the IoT device to perform its intended function; and
- A means for local network management systems to receive the URL from the IoT device and establish the required access controls and visibility to the device.

Furthermore, tooling has been developed to support the MUD. A visualisation tool was built that allows manufacturers to see what communication is allowed according to the MUD file.

[172] European Commission,2021, Commission Delegated Regulation (EU) of 29.10.2021 - C(2021) 7672 final.

[173] European Commission, 2021, Proposal for a regulation of the European Parliament and of the Council on machinery products – COM(2021) 202 final.

[174] An example is the pneumatic press, which is difficult to move and has therefore often been updated with new control systems.

1.7.3. Users

As an embedded software standard, MUD allows IoT device makers to advertise device properties, including the intended communication patterns for their device when it connects to the network. The network can use this information to ensure a context-specific access policy. The device maker is therefore the primary user of the MUD. Furthermore, there are the following intended users:

- The end users who make use of automation (to establish appropriate access control and auditing);
- Manufacturers who would like to efficiently convey product information to their users; and
- Service providers and firewall vendors who would like to make use of this information to limit consumer risk.

In order to accommodate these different users, it was attempted to make the production of MUD files as easy as possible and present the information in a sensible way. On the side of the enterprise, tooling is still needed to then determine what threats should be tackled first.

The benefit the MUD provides to consumers is that it reduces vulnerability of the device and the potential of the device to do harm. However, the MUD focuses on agents on behalf of the consumer that will make an expert decision on what to tell the consumer and how to tell them.

1.7.4. Information

To date, the following pieces of information can be made available via MUD:

- Device manufacturer and model;
- Access control required by the device;
- Furthermore, the IETF is in the process of developing an additional set of information elements:
- A pointer to software bills of materials (SBOMs); and
- A pointer to a current list of security advisory information related to the device.

1.7.5. Conclusions & recommendations

- The benefit of the MUD being developed by the IETF is that this is an international NGO and therefore the MUD is in itself an international standard. This is useful as there are many (regulatory) developments regarding IoT going on outside the EU as well. Furthermore, the MUD tries to take into account the possibility that the software of the device, the vulnerabilities, the access controls, etc, can each change at a different rate and time. This is something many regulations do not account for (yet); and
- A difficulty when it comes to setting IoT standards is that the legislative process to ensure certification of IoT devices is slow. On the other hand, there are already regulations in place or being developed such as the RED that should be considered. Another difficulty is that suppliers are conservative in the changes they want to make in their software. It should be recognised who is doing what and what measures are appropriate. In the case of the Internet of Things, a possibility is regulating the network instead of the product itself.

ANNEX 2 TECHNOLOGY FICHES

A collection of 8 fiches drafted as part of the report aims to deliver the analysis on the state of play of new technologies and digital solutions on safety.

2.1. Fiche 1: Artificial Intelligence (AI)

2.1.1. Regulatory information and definitions of the technology

a. EU Definition

The European Commission defines AI as "systems that display intelligent behaviour by analysing their environment and taking actions with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g., voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g., advanced robots autonomous cars, drones or internet of things applications)"[175].

b. EU Legislation

In April 2021, the European Commission published the Artificial Intelligence Act where harmonised rules for AI-systems are presented while amending some EU legislative acts.

c. Distinctive EU Member States legislation

Members States individually have presented 'National AI strategies', however these do not in particular focus on product safety or durability and consumer awareness. For instance, the 'Strategic Action Plan for Artificial Intelligence'[176] from the Netherlands has a section on ensuring trustworthiness of AI applications (through research investments and setting up a regulatory body that oversees the use of algorithms), and a section on consumer protection laws, but product safety is not explicitly mentioned.

2.1.2. Technical information

a. Technology maturity

Table 7: Technology maturity of AI

Initial	Managed	Defined	Quantitatively managed	Optimising

Source: Authors' own elaboration.

Defined - the technology is refined and launched widely. Further data gathering and work continue to improve the ease-of-use of the technology, efficiency and supporting infrastructure.

- AI is widely used in numerous applications with different 'goals' (e.g., predictive analytics, pattern recognition, autonomous systems, etc.). As a technology it interacts with other emerging technologies such as IoT, Cloud services and Blockchain. For instance, IoT devices can gather data that AI can use as inputs for personalisation of ads or services;
- The full scope of potential application areas of AI technology is not yet fully defined, especially when it comes to interactions with other emerging technologies. The current legislative

[175] European Commission, 2018, Coordinated Plan on Artificial Intelligence.

[176] Ministry of Economic Affairs of the Netherlands, 2019, *Strategisch Actieplan voor Artificiële Intelligentie.* Available at: https://www.rijksoverheid.nl/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificiele-intelligentie.

framework only focuses on so called 'high-risk' applications and sets out a general outline for safe and ethical use of these applications. Applications labelled as high risk are, for instance, those that relate to biometric identification, management of critical infrastructure, law enforcement, employment and worker management and access to essential private and public services. Common standards for non-high-risk applications have not been created so far; and

- The level of consumer familiarity differs per application area. Consumers are not always aware that the products they are using make use of AI technology. This can for instance be the case with personalised advertisements on the internet, or how AI-models are used to improve online shopping experiences.

b. Technology acceptance

Table 8: Technology acceptance of AI

Little/no time investment required Connectivity is not related to product safety features	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Up-front time investment from the consumer to understand product use and safety - limited need for connectivity - products need some maintenance/updates and can change over time.	Large time investment from the consumer to familiarise with changing product conditions and product safety - connectivity is required for device to unction.	Added costs (EUR) seen as benefit - consumers understand that the product they are purchasing have safety features that create additional costs, but the safety benefits outweigh the additional costs	Added costs (EUR) seen as negative - consumers understand that the product they are purchasing have safety features that create additional costs but they do not see the added value. Consumers are likely to look for alternative (and less safe) products as a result

Source: Authors' own elaboration.

- AI technology is often seen as a 'black box' when applied in consumer products. This leads to complex product conditions and most often consumers might not be fully aware of benefits and risks related to the use of such products. A large time investment is required from consumers to familiarise themselves with changing product conditions and product safety;
- As the application areas of the technology are highly diverse, the level of technology acceptance differs significantly. For instance, for healthcare applications, the technology acceptance level might be lower due to higher perceived risks than in marketing applications. The perceived usefulness of AI-applications or the (perceived) level of false-negatives an algorithm could give could have a bigger impact when used for spotting diseases on MRI-scans compared to the impact false negatives could have in the hyper-personalisation of ads on the internet; and

- Research on the technology acceptance of AI systems by German farmers[177] found that the perceived ease of use (e.g., the degree to which individuals perceive how easy it is to use the system) has a significant influence on the acceptance level. The perceived usefulness (e.g., the perception of whether the system can improve the performance of their work) did not affect the acceptance level. This is probably because the respondents have no knowledge on how to assess the usefulness of such systems as these systems are relatively new. In addition, the personal attitude towards AI systems is an important factor in the technology acceptance level. This 'trust building' towards AI applications is also found in online shopping[178], service delivery[179] and the use of virtual assistants[180].

c. Complexity

Table 9: Complexity of AI

Product safety is a result of product marketing	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Product safety is a result of product functions that do not require connectivity	Product safety is a result of product functions that require connectivity for updates	Product safety is a result of product functions that require connectivity to operate

Source: Authors' own elaboration.

- With AI, connectivity is integral to its functionality. AI applications require connectivity to make necessary calculations. This can be to either access a certain database or to do computations in the cloud as most often the needed computing power is not available on hand. Product safety is therefore a result of the product functions that require connectivity to operate;

- AI can increase product safety through the use of more precise models for predictive maintenance by producers of consumers goods. Predictive maintenance uses AI to make predictions about asset malfunction. This can extend the life of production machines and equipment. It also increases the capability of producers to manufacture safer and longer-lasting products.[181] Furthermore, AI has opened the possibility of hyper personalisation of ads. This enables companies to devote more resources to product safety. In addition, AI allows for products to be designed better and in a more personalised manner. Several design options can be 'fed' to an AI algorithm, which will test for, through a process of repetition, the optimal product design[182].This opens up possibilities for producers to design products that are safer

[177] Mohr, S., & Kühl, R., 2021, *Acceptance of artificial intelligence in German agriculture: an application of the technology acceptance model and the theory of planned behavior*. Precision Agriculture, 1-29.

[178] Nagy, S., & Hajdú, N., 2021, *Consumer Acceptance of the Use of Artificial Intelligence in Online Shopping: Evidence from Hungary*. Amfiteatru Economic, 23(56).

[179] Gursoy, D., Chi, O. H., Lu, L., & Nunkoo, R., 2019, *Consumers acceptance of artificially intelligent (AI) device use in service delivery*. International Journal of Information Management, 49, 157-169.

[180] Song, Y. W., 2019, *User acceptance of an artificial intelligence (AI) virtual assistant: an extension of the technology acceptance model* (Doctoral dissertation).

[181] Rue, N., 2019, *How AI Can Improve Product Safety*, Available at: https://becominghuman.ai/how-ai-can-improve-product-safety-820d391775d3.

[182] Oli Batstone, 2017, *What AI means for Designers*. Available at: https://becominghuman.ai/what-ai-means-for-designers-5c27130a5e0e.

and more durable. Another product safety feature of AI is the continuous access to virtual customer service in the form of chatbots and virtual assistants. These assistants can provide 24/7 assistance to consumers if needed and the data gained from consumers safety concerns can be addressed and prevented in future production of the product; and

- Connected products that use AI also foster new risks when it comes to product safety. First there is the risk of cyber safety. Products might lack sufficient evolution of their software, which makes them vulnerable to hacking and other cyber-attacks.[183] Second, there are personal security risks. Smart watches are a great example of design for children safety. If the software running on these watches lack a minimum level of security, it could easily be used to get access to a child and potentially cause harm, as was a concern in Iceland.[184] Third, there are mental health risks related to AI applications and connected products in general. Connected products might have negative effects on cognitive abilities as a result of constant multitasking (e.g., too many distractions due to the use of multiple products). Also, connected products may cause depression and loss of sleep when products are overused.[185]

d. Transferability

Table 10: Transferability of AI

Consumers learn about product safety at the moment of purchase	Consumers learn about product safety during use	Consumers learn about product safety continuously as the product is updated	Consumers learn about product safety at the time of disposal

Source: Authors' own elaboration.

- In general, AI applications are highly untransparent in use. Most often, AI models act on input data with the outputs being either predictions or other types of data. The technical principles of the model (set of conditions, sequence of operations, associated parameters) might not be known to the end-user. While open-source AI models exist (so called 'white-box models), most AI applications act as 'black-box models' where the model is unknown. Hence when consumers retrieve information on product safety features, they most often retrieve information based on the outputs of the model, rather than how to model attains these safety features.

[183] European Commission, 2020, Opinion of the sub-group on artificial intelligence (AI), connected products and other new challenges in product safety to the consumer safety network.

[184] Notification from Iceland on the EU Safety Gate Website: A12/0157/19. Available at: https://ec.europa.eu/safety-gate-alerts/screen/webReport.

[185] European Commission, 2020, Opinion of the sub-group on artificial intelligence (AI), connected products and other new challenges in product safety to the consumer safety network.

2.1.3. Challenges and opportunities along the value chain for product safety and durability

Key words: transparency, marketing, communication and ethics

Strongest impact for product safety in the value chain: manufacturing, distribution, maintenance and repair

a. Opportunities

The main **benefit** of AI lies in its capacity to analyse large quantities of data in short and up to real-time, and act automatically and self-correcting based on the outcome. In conjunction with other technologies, where AI is used for analysing data while other technologies capture and store the data (blockchain) or perform an action (robotics), the technology can be used to shape activities in design, utilization and waste management. It allows for increased efficiency throughout the value chain (ECERA, 2020).

The use of interconnected technology and solutions, particularly with AI at the centre, offers opportunities to make predictions and recommendations for the **product design stage** based on the data input collected from the connected technologies and solutions. Opportunities for a circular economy include:

- Fast, smart and precise prototyping; failure and downtime reduction; material toxicity prediction; testing related cost reduction activities; real time data and related analytics.

Furthermore, AI technology can increase efficiency of the **manufacturing process** in general. This includes reducing the number of faulty products due to predictive maintenance of production lines and visual recognition of production mistakes. This efficiency is transferable across the value chain as AI can optimise value chain **resource allocation** and **inventory management**. In a broader sense, AI can make shipping of products safer and more efficient due to the use of predictive models based on, for instance, weather models. Opportunities for a circular economy include:

- Repair and upkeeping: intelligence in maintenance; remote monitoring; intelligent product life cycle analysis; upkeeping optimization; real time data transformation: smart inventory management; reverse logistics (improving processes to sort and disassemble products, remanufacture components, recycle materials);
- Manufacturing: intelligent inventory management, pricing, demand prediction, predictive maintenance; and
- End of life: sorting and disassembling products, components remanufacturing, recycling materials (reverse logistics).

In terms of **communication** about product safety, AI-based systems can in theory be used to strengthen **consumer** rights, for example ensuring that contracts are tailored to the wishes and needs of individual consumers or that consumers can enforce their rights more quickly, easily and cost-effectively than was the case previously[186]. AI application opportunities for consumer support in general include:

[186] Ebers, M & Navas, S., 2020, *Artficial Intelligence and Consumer Protection*. Available at: http://www.cambridgeblog.org/2020/09/artificial-intelligence-and-consumer-protection/.

- Customer service; digitalization platforms; data-based analysis; extended product lifecycle; use of algorithms to match demand and supply; collaborative decision making; data enabled prediction.

Finally, AI can be used for sustainability, in fact, sustainable AI has received a lot of attention in recent years and there is an AI4Good movement where AI is directed towards reaching the Sustainable Development Goals. When using AI for these purposes it should however be noted that there are large environmental costs to using AI as well (see challenges)[187].

b. Challenges

AI presents unique challenges when it comes to information transparency, marketing, communication and ethics. These challenges are not specifically related to one stage in the value chain process.

- AI presents challenges for data management as the incorporation of the various solutions into the manufacturing process leads to increased data usage and data creation. The challenge then becomes managing the structured and unstructured data being generated and ensuring the data is being used properly;
- Accountability and liability are an issue, when it is unclear who is accountable for the proper functioning of AI systems. Consumers for example need to be protected against risks related to uploaded software and extended functions acquired by machine learning[188].In particular for consumers that have only a limited understanding of how the technology and complex algorithms work. It can be the case that users do not even know that advertising, information, prices or contract terms have been personalised according to their profile or that the technology reaches out to them at a moment when they are particularly vulnerable[189].The biggest concern making sure that the collected data does not breach consumer privacy, that consumers are aware of the data collection and that it happens through their consensus;
- The use of AI also raises specific issues around discrimination, in particular, if AI learns using data that is inherently biased, these biases will likely impact the way it operates and makes decisions. If consumers increasingly rely on AI to make decisions on their behalf, this raises questions about consumer autonomy and choice. A lack of user-friendly privacy control could also make consumers vulnerable to privacy risks online; and
- Finally, there are concerns related to the sustainability of AI as a technology more broadly and its role in increasing carbon emissions. AI may use a lot of energy. The storage, processing or data in data centres or in the cloud across different centres consume energy. For AI to truly promote circularity, it would need to use renewable energy. A study found that training a large AI model to handle human language can lead to emissions of nearly 300,000 kilograms of carbon dioxide equivalent, about five times the emissions of the average car in the US, including its manufacturing[190]. Swedish researcher Anders Andrae has forecast that data centres could account for 10% of total electricity use by 2025[191].Experts are pushing for a

[187] van Wynsberghe, A., 2021, Sustainable AI: AI for sustainability and the sustainability of AI. AI Ethics 1, 213–218.

[188] Fosch-Villaronga, E., & Mahler, T., 2021, *Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots*. Computer Law & Security Review, 41, 105528.

[189] OECD, 2019, *Challenges to consumer policy in the digital age*. Available at: https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf.

[190] European Commission, 2019, *AI can help us fight climate change. But it has an energy problem, too*. Available at: https://ec.europa.eu/research-and-innovation/en/horizon-magazine/ai-can-help-us-fight-climate-change-it-has-energy-problem-too.

[191] Ibid.

reduction of AI carbon emissions and computing power through new innovative technologies. The Ellen MacArthur Foundation also notes that AI raises questions on challenges associated to efficiency, the energy required and the sustainability of the technology[192].

[192] The Ellen MacArthur Foundation, 2019, *Artificial Intelligence and the Circular Economy*. Available at: https://emf.thirdlight.com/link/dl06eujbcbet-wx40o7/@/preview/1?o.

2.2. Fiche 2: Robotics

2.2.1. Regulatory information and definitions of the technology

a. EU Definition

- The European Union's current regulation on robotics is complicated by the absence of a common agreement between EU Member States on what a robot is. An attempt at a definition has been produced by the European Parliament by taking into consideration the below characteristics of an intelligent robot:

○ Its capacity to acquire autonomy through sensor and data exchange;

○ Its capacity for self-learning (optional);

○ Its physical support; and

○ Its capacity to adapt its behaviour and actions to its environment.

- However, this definition is limited as it does not encompass all types of robots (here it refers only to smart autonomous robots[193]).

b. EU Legislation

- In 2016, the European Parliament published the "European Civil Law rules on Robotics", followed by an announcement by the European Commission of a series of regulatory and policy initiatives, in the framework of the RoboLaw project[194], but the EU does not have specific legislation on robotics yet.

c. Distinctive EU Member States Legislation

- Some countries such as Denmark, Sweden, or the Netherlands are taking important steps to include robotics in broader legislative frames of new technologies[195].

2.2.2. Technical information

a. Technology maturity

Table 11: Technology maturity of robotics

Initial	Managed	Defined	Quantitatively managed	Optimising

Source: Authors' own elaboration.

[193] European Parliament, 2015, Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL).

[194] Molyneux, C.C., & Oyarzabal, R., 2017, *What is a Robot under EU law.* Available at: https://www.globalpolicywatch.com/2017/08/what-is-a-robot-under-eu-law/.

[195] For instance, see press releases of SPARC. Available at: https://www.eu-robotics.net/sparc/newsroom/press/smart-robots-for-smart-regions-strategies-to-unleash-the-potential-of-the-digital-economy-in-europe.html.

- Defined - the technology is refined and launched widely. Further data gathering and work continue to improve the ease-of-use of the technology, efficiency, supporting infrastructure;
- Robotics is widely used in the manufacturing context, especially in automotive and electronics, and provide for additional flexibility while fostering the competitiveness of the countries and sectors using such technology. Furthermore, they are used in day-to-day interactions with consumers (cars, health care robots, etc);
- However, if automation of parts of the manufacturing process is underway, applications to other steps of the supply chain process are limited. The potential of robotics application beyond manufacturing is still not fully defined, just as its interaction with other new technologies such as AI; and
- There is still an evident lack of legislation, both at the European and national levels. For instance, if the definition of a robot as a legal person is problematic, the European Parliament is looking for ways to integrate robotics into civil law[196].

b. Technology acceptance

Table 12: Technology acceptance of robotics

Little/no time investment required Connectivity is not related to product safety features	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Up-front time investment from the consumer to understand product use and safety - limited need for connectivity - products need some maintenance/updates and can change over time.	Large time investment from the consumer to familiarise with changing product conditions and product safety - connectivity is required for device to unction.	Added costs (EUR) seen as benefit - consumers understand that the product they are purchasing have safety features that create additional costs, but the safety benefits outweigh the additional costs	Added costs (EUR) seen as negative - consumers understand that the product they are purchasing have safety features that create additional costs but they do not see the added value. Consumers are likely to look for alternative (and less safe) products as a result

Source: Authors' own elaboration.

[196] European Parliament, 2017, *Report with recommendations to the Comission on Civil Law rules on Robotics (2015/2103(INL))*. Available at: https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.pdf.

- The use of robotics, when applied to products such as vehicles, care (robot surgeons, elderly assistants), or maintenance of the public order (Robocop), can raise safety issues, if the robot's code proves to be fallible. In case of hacking or system failure, the robot can put the consumer at risk;

- More generally in Europe, there is a negative perception of the robotic industry, and a fear surrounding the potential lack of control over robots and AI (the idea of all human jobs being substituted by robots, fear of robotic intelligence, etc). As such, it may take a long time for European citizens to acknowledge the economic and safety benefits that robots present for product safety; and

- The use of robotics can also bring privacy and data protection issues with which consumers must get acquainted. This is a two-dimensional problem. First, there are potential privacy and data protection risks when it comes to the "connectivity" aspect of the robot, in the case of a cyberattack. Second, a robot can have an impact on the direct environment and therefore might impact the physical safety of the consumer.

c. Complexity

Table 13: Complexity of robotics

Product safety is a result of product marketing	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Product safety is a result of product functions that do not require connectivity	Product safety is a result of product functions that require connectivity for updates	Product safety is a result of product functions that require connectivity to operate

Source: Authors' own elaboration.

- The connectivity features of robots and the fallibility of their codes can make them vulnerable to cyber threats and manipulation by third parties. For instance, robots used in healthcare should be controlled from disclosing an individual's private information. Updates as part of a broader objective of cybersecurity therefore are necessary;

- According to the common European definition, smart robots have the capacity to recognise events in their environment, and to react and adapt their behaviour to them. It is this decisive feature that enables the creation of smart environments, and therefore the continuous access to product features, by being connected in any place and at any time; and

- In the field of manufacturing, robots have the capacity to collect data massively, as they operate directly with the products' components. This therefore represents an important potential for product safety and components' defaults traceability, especially when these robots also operate with AI systems.

d. Transferability

Table 14: Transferability of robotics

Consumers learn about product safety at the moment of purchase	Consumers learn about product safety during use	Consumers learn about product safety continuously as the product is updated	Consumers learn about product safety at the time of disposal

Source: Authors' own elaboration.

- If robotics are used during the manufacturing process, it is unlikely that the consumer will learn about the added product safety features at the time of purchase. However, if the consumer purchases a good which includes robotic features (like a robot vehicle), he or she will know at the time of purchase what the added safety features of the product are.

2.2.3. Challenges and opportunities along the value chain for product safety and durability

Key words: combination with AI, physical embodiment or cloud service robot, security

Strongest impact for product safety in the value chain: product design, manufacturing, maintenance, reparability & reusability

a. Opportunities

Robotics can allow for the creation of safer working environments and safer products.

- As robots replace human labour in potentially unsafe working conditions. Beyond that, the interlinkage between robotics and other digital solutions (e.g., AI) can allow greater control over the manufacturing process - through such linkages robots could have the capacity to collect data while operating with components;
- If used together with technologies, such as AI and block chain, robotics could help support product traceability, particularly in instances where the robots handle the manufacturing and assembly of components - this data could be collected through AI and support traceability of parts, components;
- Robots can also be used as a form of interactive marketing - providing consumer information about products at the point of purchase. It presents an opportunity for interactive consumer information, though, this would require specialised robotics programable with product information;
- The connectivity of robotics offers the opportunity to present consumers with information about updates, repairability and for manufacturers to ensure consumer goods using robotics stay up to date with the latest safety features. In fact, the use of connectivity could ensure safer products as software becomes more sophisticated allowing consumers to benefit from safer products; and
- Opportunities for using robotics to promote product circularity are primarily focused on the end-of-life stage of the value chain – particularly waste management. Robotics today is still mainly used in industry. Producers are most concerned by their effects. In the waste and recycling industry, the combined use of AI and robotic technologies is rapidly becoming a new

industrial standard[197].AI-powered sorting robots allow material recovery facilities (MRFs) to capture valuable clean materials more efficiently from the waste stream and thereby significantly raise recycling rates[198].The robots create a more structured and predictable sorting environment which helps to mitigate the health and safety risks associated with manual sorting, and thereby create safer working conditions.

An article written by the Ellen MacArthur Foundation[199] points to the combined potential of AI and robotics to continuously improve the identification, categorisation of different waste streams by colour, size, shape, brand and other traits. One technology mentioned, AMPCortex encompasses the largest known real-world dataset of recyclable materials for machine learning, with the ability to classify more than 100 different categories and characteristics of recyclables across single-stream recycling, e-scrap and construction and demolition debris, and reaching an object recognition run rate of more than 10 billion items annually. It could potentially sort recyclables at a rate of 80 items per minute with an accuracy of up to 99%.

There is, nevertheless, an overlooked lacuna in discussions about the environmental impact of robotics[200]. Their critical applications for environmental research, engineering, and remediation have received little attention in the roboethics literature to date.

- The environmental impact of a robot will depend on the nature of the robot considered. At the current state-of-the-art, IR is intrinsically energy intensive, thus contributing to carbon emissions and rising pollution levels. Several innovations are being pursued to reduce the environmental impact of robotics. For instance: energy consumption reduction technologies; IR integrated design and simulation environmental; IR processes optimisation environment; LCA methods to assess and optimise environmental and economic costs. Robotics are also material-intensive, requiring large amounts of minerals and hardware which raises concerns related to sustainable sourcing and end-of-life; and
- The currently emerging forms of soft, biologically inspired electronics and robotics have the unique potential of becoming not only like their natural antitypes in performance and capabilities, but also in terms of their ecological footprint[201].Highly stretchable yet biodegradable polymers, transient sensors and transistors, and easy to recycle batteries assembled in ecofriendly fabrication lines are examples of major interdisciplinary research goals covering diverse fields.

[197] ZenRobotics, 2020, *Circular economy amid the pandemic – how AI-powered sorting robotics lead to better safety and recovery*. Available at: https://zenrobotics.com/blog/circular-economy-amid-the-pandemic-how-ai-powered-sorting-robotics-lead-to-better-safety-and-recovery/.

[198] Ibid.

[199] The Ellen MacArthur Foundation, 2019, *Artificial Intelligence and the Circular Economy*. Available at: https://emf.thirdlight.com/link/dl06eujbcbet-wx40o7/@/preview/1?o.

[200] van Wynsberghe, A., Donhauser, J., 2018, *The Dawning of the Ethics of Environmental Robots*. Sci Eng Ethics 24, 1777–1800. Available at: https://doi.org/10.1007/s11948-017-9990-3.

[201] Hartmann, F., Baumgartner, M., & Kaltenbrunner, M., 2021, *Becoming Sustainable, The New Frontier in Soft Robotics*. Advanced materials (Deerfield Beach, Fla.), 33(19), e2004413. https://doi.org/10.1002/adma.202004413.

b. Challenges

- Robotics is arguably one of the most known or visible new technologies for consumers and manufacturers. Regarding safety, the concerns lie in the capacity to ensure and demonstrate that robotics can provide safe services (whether used for manufacturing or as consumer goods) without the need for human input;
- Some robots depend mainly on physical embodiment to perform a task that directly affects the immediate environment (for example deliver medicines in a hospital) or have a greater reliance on cloud services (for example intelligent speakers that hear and answer questions from a user in real-time and in natural language). The former can cause physical harm while the latter could impact the mental health and emotional wellbeing of users;
- For these reasons, it is important that a product has proper cybersecurity and control measures in place. Uploaded software or extended functions acquired by machine learning play a role here as well, with the possibility for a system to learn undesired behaviour (intentionally or unintentionally);
- Despite the wide use of robotics in manufacturing, the interaction between robotics and other technologies, such as AI, is not well defined. This limits further development and use of robotics to enhance product safety during manufacturing but it also raises the challenges of understanding how robotics can benefit from other technologies and digital solutions that would result in safer products and safer manufacturing;
- The use of robotics in consumer products can raise safety issues, if the robot's code can be corrupted, hacked, or otherwise fail to function properly. This is especially dangerous if the consumer otherwise has no control over the product without the robot (e.g., self-driving cars). As such, the introduction of robotics into consumer goods continues to pose safety challenges for developers, particularly when the robotics are meant to replace human input (and especially if this is argued as a safer alternative to human input);
- A challenge here is that the consumer often disregards security concerns as they place more value on useability, functionality and competitive prices when purchasing this technology; and
- Another challenge is the increased number of entities behind the creation of a product, with responsibilities becoming less clear. Especially with users in a vulnerable position (which for example might be the case with service robots in the healthcare sector[202]) it is crucial to have the right control mechanisms in place.

[202] Fosch-Villaronga, E., & Mahler, T., 2021, *Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots*. Computer Law & Security Review, 41, 105528.

2.3. Fiche 3: Internet of things (IOT)

2.3.1. Regulatory information and definitions of the technology

a. EU Definition

- Internet of things 'refers to everyday physical devices that are connected to and interconnected with the internet'[203]. These objects are embedded with 'electronics, sensors, software, actuators and network connectivity in such a way that they are able to collect, send and receive data and to connect with other devices'[204]. This allows for data exchange that allows for optimisation of processes, monitoring of environments and performing computations of mathematical calculations.

b. EU Legislation

- Several EU regulations are in place that heavily influence IoT technology[205]. These are:
  - The GDPR is a central part of the EU data protection legislation and was designed to protect users from privacy and data breaches. It controls how IoT devices process personal data;
  - The ePrivay Regulations: legislation that was designed to regulate electronic communication within Europe requires EU Member States to obtain consent before storing cookies on their personal devices; and
  - Under the EU Cybersecurity Act, the EU has designed a cyber security certification scheme for ICT and IoT businesses.

c. Distinctive EU Member States Legislation

- In most EU Member States existing legislation regarding IoT devices fall under the EU Cybersecurity Act. Some countries such as Finland[206] are currently setting up or managing certain labels or certifications that assess the security of connected devices; and

- In a French survey, nearly half of the respondents said that these kinds of labels would increase their trust in these devices[207].

2.3.2. Technical information

a. Technology maturity

Table 15: Technology maturity of IoT

Initial	Managed	[✓ Defined]	Quantitatively managed	Optimising

Source: Authors' own elaboration.

[203] CBI, 2021, *The European market potential for (industrial) internet of things*. Available at: https://www.cbi.eu/market-information/outsourcing-itobpo/industrial-internet-things/market-potential.

[204] Ibid.

[205] Available at: https://www.nabto.com/eu-iot-regulation-guide/.

[206] Available at: https://tietoturvamerkki.fi/en/.

[207] Internet Society, 2019, *Internet Society Advances IoT Security in France*. Available at: https://www.internetsociety.org/news/press-releases/2019/internet-society-advances-iot-security-in-france/.

- IoT has an interesting place in its technology maturity. On the one hand, the widespread use of smart devices (e.g., the smart phone) and wearable devices has resulted in significant consumer familiarity with the technology (or at least its functions). It is arguable that to an average consumer the term IoT itself might mean little, but they would be very familiar with the concepts of connected devices;
- However, despite the widespread use of products that incorporate IoT in their function, IoT itself is influenced by other emerging technologies that can interact with it (e.g., the interplay between IoT and AI that result in connected devices benefiting from data personalisation enabled by AI functions); and
- As such, IoT appears locked in an interesting development cycle where the introduction of new technologies pushes back the maturity level as new technical interactions emerge. Likewise, consumer familiarity with emerging technologies is lower which translates into reduced understanding of how IoT interacts with these technologies (a good example is the lack of awareness of how AI collects and uses personalised data - an interaction that can be enabled through devices utilising IoT).

b. Technology acceptance

Table 16: Technology acceptance of IoT

Little/no time investment required Connectivity is not related to product safety features	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Up-front time investment from the consumer to understand product use and safety - limited need for connectivity - products need some maintenance/updates and can change over time.	Large time investment from the consumer to familiarise with changing product conditions and product safety - connectivity is required for device to unction.	Added costs (EUR) seen as benefit - consumers understand that the product they are purchasing have safety features that create additional costs, but the safety benefits outweigh the additional costs	Added costs (EUR) seen as negative - consumers understand that the product they are purchasing have safety features that create additional costs but they do not see the added value. Consumers are likely to look for alternative (and less safe) products as a result

Source: Authors' own elaboration.

- Devices that use IoT will fall into either of two categories. First are devices that do not require connectivity to function, but connectivity allows the device to be updated. For such devices, the consumer time investment is largest at the start to understand the product safety features enabled by the IoT but the infrequent device updates do not necessitate continuous time investment to keep up to date with constant changes to the device;
- Alternatively, connectivity can be a consumer choice - limiting (or completely ignoring) connectivity means that consumers only benefit from safety features that come with the factory model. Here the important question becomes whether the consumer choice is conscious, and they act with the knowledge that reducing connectivity can affect device functionality; or is it a failure of the manufacturer and the device to properly communicate the need for connectivity to allow updates that translate into safer use for the device; and
- The second category of devices requires connectivity to provide consumers with full product safety benefits (a good example are wearable medical devices that communicate expanded data to the consumer through accompanying smart phone apps or online platforms). Here the interplay between IoT and other technologies, digital solutions lead to new interactions for product safety.

c. Complexity

Table 17: Complexity of IoT

Product safety is a result of product marketing	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Product safety is a result of product functions that do not require connectivity	Product safety is a result of product functions that require connectivity for updates	Product safety is a result of product functions that require connectivity to operate

Source: Authors' own elaboration.

- IoT creates new pathways for manufacturers, developers to integrate safety features into consumer goods. Connectivity enabled by IoT can ensure timely device updates, including software updates/upgrades that remove emerging issues in the product (in extreme cases such connectivity can directly present product recall by fixing software issues that could result in damaged products).

d. Transferability

Table 18: Transferability of IoT

Consumers learn about product safety at the moment of purchase	Consumers learn about product safety during use	Consumers learn about product safety continuously as the product is updated	Consumers learn about product safety at the time of disposal

Source: Authors' own elaboration.

- Using IoT to access consumer goods creates a pathway to provide product upgrades - this, in turn, allows manufacturers to fix issues that can cause harm to the consumer. As such, devices with IoT do ask the consumer to be aware of changing product safety conditions which depends on the frequency of such updates; and
- Connectivity can be used to influence product recall, either through updates/upgrades that prevent malfunctions or by directly informing consumers about recall actions if a remote update/upgrade is not possible. In both cases, the ability to contact consumer to inform them about product concerns becomes a safety feature in and of itself. However, this is only possible if the IoT device is connected to a network and can fail if the consumer does not connect the device (either by choice or due to lack of knowledge).

2.3.3. Challenges and opportunities along the value chain for product safety and durability

Key words: connectivity, new manufacturing, environmental impact

Strongest impact for product safety in the value chain: design, maintenance, and end of life cycles

a. Opportunities

- In the context of industry 4.0 and circular economy, where the goal is to use products and materials to their fullest potential, IOT appears as a digital enabler. Connecting products to the IOT helps to fill important information gaps relating to their lifecycles and boost more agile cooperation along the value chain. The value propositions of integrating IoT into the manufacturing process include: 1) extending the use cycle of an asset; 2) Increasing the utilisation of an asset; 3) Looping/cascading an asset through additional use cycles;
- Across different parts of manufacturing, IoT can help with:
- Tracking: through IoT information is available about a product's identity, location, or unique composition;
- Monitoring: through IoT information is available about a product's use, condition, or environment. This includes alerts and notifications;
- Control: through IoT product functionality can be controlled through software, based on predefined options. This includes pushing regular updates;
- Optimisation: goal-based improvements to operations are supported using advanced algorithms;
- Design evolution: the design of a product or service can be improved based on data feedback from other lifecycle phases. This includes functional upgrades and the development of new products and services; and
- IoT provides particular opportunities for communication on product safety when engaging with the product. IoT devices can receive personalised information about users and can tailor actions towards these users. The technology can be used for communicating important safety information to consumers at the time the product is activated and through the entire lifecycle, from safe installation and setup instructions towards reminders about safe use and product updates. The personalised information that is being collected by the device can also be used for marketing purposes - influencing shopping decisions - or for purchases with automated checkouts.

b. Challenges

- Businesses typically encounter structural, operational, financial, and technological challenges when applying IOT-enabled circular strategies. While IOT can bring environmental savings (raw materials tracing, reduced landfill, boosting repair and remanufacturing), it must be carefully monitored from a resource and environmental point. The sustainability and long-term effects of IOT technologies are not clear and insufficiently investigated to date. As an example, electronic waste is fast becoming one of the major issues caused by the planned rise of IoT products. In light of this, recycling rates and e-waste management are concerns that are increasing;

- Furthermore, a noticeable amount of energy is needed to operate IOT devices. The minimisation of energy consumption in IOT devices is a crucial target as the benefits created by IoT are being outweighed by the environmental impact from the high energy need;

- Challenges relate to the question to what extent the organisation responsible for the development and marketing of the product is also responsible for the ways in which information is communicated, the timing and obligations when unexpected safety issues arise. There are also some ethical challenges. When a product changes user, the company behind it can also still connect to the active user, even if it is not the original purchaser of the product. And if a manufacturer withdraws software support for a device, this could make it vulnerable to security breaches, with subsequent risks to privacy, security or even safety. This is a particular risk as the device is collecting all kinds of information on what the consumer says and does as well as the people (s)he is with, details about his/her home and physiological signs such as sleeping patterns, vital signs and even sexual activity[208,209]; and

- Complications also emerge in terms of legislation as regulations often have to try to catch up with new interactions between IoT and new technologies, decreasing the efficiency of creating common standards for industry to follow and consumers to benefit from.

[208] OECD, 2018, Consumer product safety in the Internet of Things, OECD Digital Economy Papers.

[209] OECD, 2019, *Challenges to consumer policy in the digital age*. Available at: https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf.

2.4. Fiche 4: Cloud computing

2.4.1. Regulatory information and definitions of the technology

a. EU Definition

- The European Commission defines the cloud in simplified terms as 'the storing, processing and use of data on remotely located computers accessed over the internet'.[210] Because cloud computing has a range of features a better definition has been elusive[211]. These features include:
- Hardware is owned by the cloud computing provider, not by the user who interacts with it via the internet. The remote hardware stores and processes data and makes it available, e.g., through applications;
- The use of hardware is dynamically optimised across a network of computers. Organisations and individuals can access their content and use their software when and where they need it, e.g., on desktop computers, laptops, tablets, and smartphones;
- Cloud providers often move their users' workloads around (e.g., from one computer to another or from one data centre to another) to optimise the use of available hardware; and
- Users normally pay by usage, avoiding the large upfront and fixed costs necessary to set up and operate sophisticated computing equipment.

b. EU Legislation

- Legislation on cloud computing is still very much in development. There is a general European strategy on cloud computing dating back to 2012, but no overarching legislation on the safety of cloud exists; and
- There is European legislation that directly relates to cloud services, such as GDPR which sets guidelines on how personal information should be managed and stored in the cloud.

c. Distinctive EU Member States Legislation

No distinctive Member States legislation was found

[210] European Comission, 2020, *Advanced Technologies for Industry – AT WATCH*. Available at: https://ati.ec.europa.eu/reports/technology-watch/technology-focus-cloud-computing.

.[211] European Commission, 2012, *Unleashing the potential of Cloud Computing in Europe*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_1025.

2.4.2. Technical information

a. Technology maturity

Table 19: Technology maturity of cloud computing

Initial	Managed	Defined	Quantitatively managed	Optimising

Source: Authors' own elaboration.

- Cloud computing is nowadays widely used in several applications and products including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). All these models provide a certain part of a needed IT infrastructure 'as a service' that can be accessed through the internet; and
- However, the application areas of cloud computing are not yet exhausted. Recently, we saw the introduction of cloud-based gaming services[212] and even cloud-based quantum computing is being introduced to the market[213]. These new application areas bring new challenges and benefits when it comes to product and consumer safety.

b. Technology acceptance

Table 20: Technology acceptance of cloud computing

Little/no time investment required Connectivity is not related to product safety features	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Up-front time investment from the consumer to understand product use and safety - limited need for connectivity - products need some maintenance/updates and can change over time.	Large time investment from the consumer to familiarise with changing product conditions and product safety - connectivity is required for device to unction.	Added costs (EUR) seen as benefit - consumers understand that the product they are purchasing have safety features that create additional costs, but the safety benefits outweigh the additional costs	Added costs (EUR) seen as negative - consumers understand that the product they are purchasing have safety features that create additional costs but they do not see the added value. Consumers are likely to look for alternative (and less safe) products as a result

Source: Authors' own elaboration.

[212] Kellen Browning, 2021, *'Crucial Time' for Cloud Gaming, which wants to change how you play*. Available at: https://www.nytimes.com/2021/07/01/technology/cloud-gaming-latest-wave.html.

[213] Soeparno, H., & Perbangsa, A. S., 2021, *Cloud Quantum Computing Concept and Development: A Systematic Literature Review*. Procedia Computer Science, 179, 944-954.

- When it comes to cloud computing acceptance, for SME's the adoption of such services is helped by the perceived usefulness which has a positive impact, while the perception of risks has a negative influence[214].The risks can be divided into four classes: organisational, technical, legal and other general risks;
- Organisational risks come from the risks associated with the potential impact of cloud computing on the firm's organisational structure. These include risks such as ICT organisational change and loss of business reputation;
- Technical risks include all possible technical problems including resource sharing problems, data leakage and sharing technology vulnerabilities;
- Legal risks are related to the possible problems that might arise from storing data in different countries with different laws and regulations;
- Other risks include data protection, physical security, and privacy; and
- In a higher education setting, many users are often unclear about the security and privacy information in the cloud.[215] This results in users avoiding these applications.

c. Complexity

Table 21: Complexity of cloud computing

Product safety is a result of product marketing	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Product safety is a result of product functions that do not require connectivity	Product safety is a result of product functions that require connectivity for updates	Product safety is a result of product functions that require connectivity to operate

Source: Authors' own elaboration.

- Product safety functions often arise when cloud computing technology interacts with different technologies. For instance, AI applications often use cloud computing for 'over-the-air' computations. Hence, benefits arising from AI applications thus also relate to cloud computing. Similar overlap can be found with other technologies such as IoT and blockchain.

[214] Ferri, L., Spanò, R., Maffei, M., & Fiondella, C., 2020, *How risk perception influences CEOs' technological decisions: extending the technology acceptance model to small and medium-sized enterprises' technology decision makers*. European Journal of Innovation Management.

[215] Amron, M. T., & Noh, N. H. M. ,2021,. *Technology acceptance model (TAM) for analysing cloud computing acceptance in higher education institution (HEI)*. In IOP Conference Series: Materials Science and Engineering (Vol. 1176, No. 1, p. 012036). IOP Publishing.

d. Transferability

Table 22: Transferability of cloud computing

Consumers learn about product safety at the moment of purchase	Consumers learn about product safety during use	Consumers learn about product safety continuously as the product is updated	Consumers learn about product safety at the time of disposal

Source: Authors' own elaboration.

- As cloud computing is more of service rather than a physical product, consumers are often subjected to changes in terms of service and changes in the services provided. Therefore product safety of cloud services can continuously change.

2.4.3. Challenges and opportunities along the value chain for product safety and durability

Key words: connectivity

Strongest impact for product safety in the value chain: maintenance, reparability, reusability, end-of-life cycle

a. Opportunities

- Cloud computing is the basis for the use of all other digital technologies due to the connectivity enabled through the cloud which provides access to data storage and computing power. Its ability to store large amounts of information on products and processes is an enabler for new manufacturing practices and new products linked to the circular economy;
- As such, cloud computing has the potential to be applied across the value chain, but its full benefits emerge from other technologies connected through the cloud. Cloud computing provides benefits from the different linkages that can be established through it; for example, cloud computing can be used in conjunction with AI to make predictions and recommendations for the product design stage based on the data input collected from device input collected through the cloud;
- The connectivity enabled by cloud computing allows manufacturers and users to benefit from connected technologies while reducing their limitations. For example, manufacturers could make use of connected devices and AI to create a larger data input stream from the devices to the AI to facilitate communication and autonomy of AI that allows it to make better informed decisions, predictions for the manufacturing process; through the incorporation of AI, have predictive manufacturing where the AI collects input across the cloud to analyse the manufacturing process and determine likely fault lines, etc.); and
- For consumers, cloud connectivity likewise provides access to products, services that otherwise would be unavailable to them and help reduce the reliance on high-end hardware for consumers, who could access such services through the cloud. In other words, it can transfer some of the product safety considerations from the consumer on to the service provider who would be responsible for hardware maintenance. Similarly, the use of cloud computing to access remote hardware for services also translates into a reduced need for consumers to worry about product end-of-life cycles as a single connected device can access multiple hardware through the cloud.

b. Challenges

- The challenge of using cloud computing to distribute services (consumers accessing different technologies and solutions across the cloud from their device, effectively eliminating the need for different hardware for consumers) raises the challenge of maintaining the connectivity, network, bandwidth from increased data usage between the consumers on one end and hardware on another. And in relation to this challenge, it should be underlined that data centres today are already very energy-intensive which means that maintaining the connectivity has the added environmental impact due to the energy resources used to maintain the cloud;
- When it comes to cloud computing, major consumer concerns are the vulnerability to attack, with critical business information being stored outside the company's firewall and perhaps even in a different country or continent. In theory, cloud-based storage provides for easy tracking and monitoring of consumers and for sharing this information with third parties for commercial or other purposes. Thus it becomes important for cloud providers to show

customers how they protect an organisation's data and to offer detailed guidance about their security protocols;

- Beyond the subject of cybersecurity (hacking into devices connected through the cloud) there is also the question of services that require constant connection (e.g., to a central server, database). If the connection is disrupted, the device functionality fails - this is especially important as the failure can come from the consumer or the manufacturer, developer; and
- For manufacturers, cloud computing is in many ways the tool that enables connecting different technologies and solutions across the value chain. However, it also presents multiple challenges of ensuring the cloud services can handle the data traffic from consumers, especially as their numbers grow as well as their dependence on cloud services to provide access to technologies and digital services. Likewise, use of the cloud to connect different technologies poses the question of how to ensure these linkages are safe/secure/compatible and consider the possible challenges that emerge from these linkages (e.g., use of AI to collect data through the cloud).

2.5. Fiche 5: Near Field Communication (NFC)

2.5.1. Regulatory information and definitions of the technology

a. EU Definition

- NFC is an acronym for Near Field Communication. According to the NFC Forum, NFC is 'a contact-less communication technology based on a radio frequency (RF) field using a base frequency of 13.56 MHZ. NFC technology is designed to exchange data between two devices through a simple touch gesture'.

b. EU Legislation

- There is no general legislation on NFC; and
- There is, however, recent case law on how NFC is used by big tech companies (Apple, Google) through payment services. The EU Competition authority charged Apple in October 2021 with antitrust concerns over its NFC chip technology. Th EU is currently considering new laws (Digital Market Act) that would require that these companies give access to third parties on the devices' NFC technology.

c. Distinctive EU Member States Legislation

- Recently Germany has introduced a piece of legislation[216] that requires providers of technical infrastructures of NFC (such as Apple), to grant access to those infrastructures to payment service providers. This stands in relation to the investigation of the European Commission to determine if Apple is breaching EU competition laws by refusing this access.

2.5.2. Technical information

a. Technology maturity

Table 23: Technology maturity of NFC

Initial	Managed	Defined	[✓ Quantitatively managed]	Optimising

Source: Authors' own elaboration.

- Quantitatively managed: NFC has been adopted rapidly over the last few years and has some clear use cases. Mostly in the field of mobile payments. Main infrastructure standards have been finalised and mobile device manufacturers have included the technology in their products[217].

[216] Bird & Bird, 2021, *New German legislation allows access to the iPhone's NFC antenna*. Available at: https://www.twobirds.com/en/news/articles/2020/germany/new-german-legislation-allows-access-to-the-iphones-nfc-antenna.

[217] Arcese, G., Campagna, G., Flammini, S., & Martucci, O., 2014, *Near field communication: Technology and market trends*. Technologies, 2(3), 143-163.

b. Technology acceptance

Table 24: Technology acceptance of NFC

Little/no time investment required Connectivity is not related to product safety features	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Up-front time investment from the consumer to understand product use and safety - limited need for connectivity - products need some maintenance/updates and can change over time.	Large time investment from the consumer to familiarise with changing product conditions and product safety - connectivity is required for device to unction.	Added costs (EUR) seen as benefit - consumers understand that the product they are purchasing have safety features that create additional costs, but the safety benefits outweigh the additional costs	Added costs (EUR) seen as negative - consumers understand that the product they are purchasing have safety features that create additional costs but they do not see the added value. Consumers are likely to look for alternative (and less safe) products as a result

Source: Authors' own elaboration.

- In general, the use of NFC in transaction is a relatively accepted technology. One study found that the perceived ease of use is the main driver for this level of acceptance. The perceived security is of much lesser importance[218]; and
- However, there are some countries where the adoption of NFC payments is relatively slow. It is found that in, for instance, Sri Lanka the technology acceptance is relatively low due to limited battery power of Point of Sales device, uncertainty around consumer transaction security, associated initial and recurrent costs, and inadequate government regulations[219].

[218] Luna, I. R. D., Montoro-Ríos, F., Liébana-Cabanillas, F., & Luna, J. G. D., 2017, *NFC technology acceptance for mobile payments: A Brazilian Perspective*. Revista brasileira de gestão de negócios, 19, 82-103.

[219] Kawshalya, K. T. G. D., 2020, *Factors Affecting Slow Adoption of NFC-enabled Payment Services: Sri Lankan Consumers' and Service Providers' Perspective*.

c. Complexity

Table 25: Complexity of NFC

Product safety is a result of product marketing	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Product safety is a result of product functions that do not require connectivity	Product safety is a result of product functions that require connectivity for updates	Product safety is a result of product functions that require connectivity to operate

Source: Authors' own elaboration.

- NFC is considered to be an easy to use technology and users do not need any knowledge about the technology. All a user must do to start communication is bring two devices physically together[220]; and
- The transmission range is generally short. When the user separates two devices the communication is ended. This brings security, as there is no communication between devices when there is no proximity.

[220] Ok, K., Coskun, V., Aydin, M. N., & Ozdenizci, B., 2010, *Current benefits and future directions of NFC services*. In 2010 International Conference on Education and Management Technology (pp. 334-338). IEEE.

d. Transferability

Table 26: Transferability of NFC

Consumers learn about product safety at the moment of purchase	Consumers learn about product safety during use	Consumers learn about product safety continuously as the product is updated	Consumers learn about product safety at the time of disposal

Source: Authors' own elaboration.

- With regard to NFC payments, services are provided by tech companies that have certain terms of use that are susceptible to change.

2.5.3. Challenges and opportunities along the value chain for product safety and durability

Key words: consumer engagement, traceability, marketing

Strongest impact for product safety in the value chain: all main steps of the value chain

a. Opportunities

- NFC tags are standardised worldwide and therefore can be used widely for anything that relies on data exchange, without a particular app. This makes that the technology provides a lot of opportunities for communication with consumers. NFC can take the marketing experience a step further than for example with QR-codes because it allows the merchant to interact with the customer and makes it possible to point the consumer towards future product decisions;

- Next to marketing, NFC also provides opportunities for better information and communication during pre-purchase, purchase and use of the product. An example are healthcare professionals that can stop medicine from going to the wrong patient. NFC also provides possibilities for communication about the sustainability of a product and in itself replaces printed ads, coupons and tickets, enabling customers to load coupons directly to their phone; and

- Product characteristics and can be a helpful tool to help producers along the value chain and consumers check the ethical supply of raw materials and recycling options, communicate with the supplier throughout the product lifecycle, resell it on the secondary market or dispose it in a sustainable way.

b. Challenges

- A challenge is that companies will need infrastructure and staff in place that can incorporate the new flood of customer-specific information that is provided in real-time, and use this data for a better consumer experience;

- NFC technology brings both security gains and security risks. It is no longer necessary for people to carry keys for their home, their office, their car and several credit cards when they can be replaced with an NFC tag. On the other hand, the NFC tag will hold private data that can be stolen by using a card reader when standing close to another person (reading the details on his/her contactless card) without having to physically take the card from the person's wallet. The short-range of the technology and the radio frequency that is used does safeguard transactions against hackers, which makes it safer than Bluetooth or QR-codes; and

- Challenges have been associated with the end-of-life management of NFCs. They are often considered as generic waste and no specific e-waste policy has been identified for them. The paradox is that tags, sometimes used for waste management, are themselves contaminants[221].In theory, NFCs are reusable. It is therefore very important to sort them separately.

[221] Condemi, Alessia & Cucchiella, Federica & Schettini, Domenico., 2019, *Circular Economy and E-Waste: An Opportunity from RFID TAGs*. Applied Sciences. 9. 3422. 10.3390/app9163422.

2.6. Fiche 6: Quick Response (QR) codes

2.6.1. Regulatory information and definitions of the technology

a. EU Definition

- There is no common official definition of this technology among the EU Member States;
- One EU Agency classifies such Quick Response (QR) codes as one type of mobile scanning technology (just as two-dimensional barcodes and Near-Field Communication[222]); and
- This agency defines QR codes as a data matrix "used to provide information through electronic format to users[223]. In general, QR codes can guarantee the authenticity of products, and allow their traceability[224].

b. EU Legislation

- According to Article 62 of Directive 2001/83/EC[225], a product's packaging can include "symbols or pictograms designed to clarify certain information" which can be useful to the consumer. This excludes any advertising content;
- In the draft report from the European Parliament on General Product Safety Regulations[226] an amendment was proposed so that economic operators have the possibility to provide product safety information by printing a QR code on their products; and
- The IMCO Committee also welcomed the Commission's intention to develop a digital product passport for the increased traceability and circularity of products in the framework of the Circular Economy Action Plan[227].

c. Distinctive EU Member States legislation

- No distinctive EU Member States legislation was found.

[222] European Medicine Agency, 2018, *Mobile scanning and other technologies in the labelling and package leaflet of centrally authorised medicinal products*. Available at: https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/mobile-scanning-other-technologies-labelling-package-leaflet-centrally-authorised-medicinal-products_en.pdf.

[223] European Medicine Agency, 2017, *Quick Response (QR) codes in the labelling and/or package leaflet of veterinary medicinal products authorised via the centralised (CP), mutual recognition (MRP), decentralised procedures (DCP) and national procedures* Available at: https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/quick-response-qr-codes-labelling/package-leaflet-veterinary-medicinal-products-authorised-centralised-cp-mutual-recognition-mrp_en.pdf.

[224] QRcode Tiger, 2022, *How QR codes are used in Europe?* Available at: www.qrcode-tiger.com/how-qr-codes-are-emerging-in-europe-now-that-they-have-utilized-them-in-almost-every-field.

[225] European Parliament, 2001, *Directive 2001/83/EC of the European Parliament and of the Council*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02001L0083-20121116&qid=1472567249742&from=EN.

[226] European Parliament, 2021, Draft report on the proposal for a regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council (COM(2021)0346 – C9-0245/2021 – 2021/0170(COD)). Available at: https://www.europarl.europa.eu/doceo/document/IMCO-PR-702956_EN.pdf.

[227] European Parliament, 2020, Opinion of IMCO for the Committee on the Environment, Public Health and Food Safety on the new Circular Economy Action Plan (2020/2077(INI)). Available at: https://www.europarl.europa.eu/doceo/document/IMCO-AD-652282_EN.pdf.

2.6.2 Technical information

a. Technology maturity

Table 27: Technology maturity of QR codes

Initial	Managed	Defined	Quantitatively managed	Optimising

Source: Authors' own elaboration.

- **Initial:** Progressive use across Europe. As of now, this mobile technology has mainly been used for medicinal and medical products by firms in Canada, the EU, or the United States[228]. In Europe it is currently gaining more attention as a format to provide product safety information on general products; and
- Because of the COVID-19 pandemic, the QR codes technology has however gained recognition thanks to their widespread use for sanitary passport purposes. Their rapid adoption thus shows the potential of such technology, given the number of people that own a smartphone and the ease of use.

b. Technological acceptance

Table 28: Technological acceptance of QR codes

Little/no time investment required Connectivity is not related to product safety features	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Up-front time investment from the consumer to understand product use and safety - limited need for connectivity - products need some maintenance/updates and can change over time.	Large time investment from the consumer to familiarise with changing product conditions and product safety - connectivity is required for device to unction.	Added costs (EUR) seen as benefit - consumers understand that the product they are purchasing have safety features that create additional costs, but the safety benefits outweigh the additional costs	Added costs (EUR) seen as negative - consumers understand that the product they are purchasing have safety features that create additional costs but they do not see the added value. Consumers are likely to look for alternative (and less safe) products as a result

Source: Authors' own elaboration.

[228] Nigel Cory, 2021, *How E-labels Can Support Trade and Innovation in ICT, Medical, and Other Products*. Available at: https://itif.org/publications/2021/10/27/how-e-labels-can-support-trade-and-innovation-ict-medical-and-other-products.

- Consumers are expected to scan the QR codes and read the products' information on their smartphones, which reduces the time needed for information searching and makes the information readily available, at any time and place; and
- The money and time needed to collect product information, therefore, is minimal.

c. Complexity

Table 29: Complexity of QR codes

Product safety is a result of product marketing	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Product safety is a result of product functions that do not require connectivity	Product safety is a result of product functions that require connectivity for updates	Product safety is a result of product functions that require connectivity to operate

Source: Authors' own elaboration.

- QR codes are considered as "dynamic" as they can be modified, updated, and traced[229];
- The access to the products' information is preconditioned by the use of a smartphone or connected device, and by the access to the Internet; and
- This same connectivity feature however poses issues on the safety of use, as QR codes are vulnerable to hacking and can be modified if their code is accessed.

d. Transferability

Table 30: Transferability of QR codes

Consumers learn about product safety at the moment of purchase	Consumers learn about product safety during use	Consumers learn about product safety continuously as the product is updated	Consumers learn about product safety at the time of disposal

Source: Authors' own elaboration.

- Consumers can scan the QR code with their smartphone at the moment of purchase, and thus learn about the product's characteristics then. This can influence their purchasing decision (use of specific components, geographic origin of components, etc.);
- QR codes can be updated as they are considered a "dynamic" technology; and
- At the time of disposal, the QR code and the information it provides about components can guide the consumer, in terms of proper disposal recycling possibilities for instance.

[229] QRcode Tiger, 2022, *How QR codes are used in Europe?* Available at: www.qrcode-tiger.com/how-qr-codes-are-emerging-in-europe-now-that-they-have-utilized-them-in-almost-every-field.

2.6.3. Challenges and opportunities along the value chain for product safety and durability

Key words: accessibility, awareness, consumer engagement

Strongest impact for product safety in the value chain: distribution, maintenance, reparability

a. Opportunities

- QR codes represent arguably an underutilised method of providing consumers with product safety technology, particularly in light of the availability of smart devices and familiarity with the technology by the consumers;
- QR codes could be used to support purchasing decisions by scanning and seeing detailed product information, including safety concerns, in a digital form that would be available to consumers at the store, rather than presented in a manual after purchase;
- QR codes could help support product maintenance for goods that are otherwise unconnected and do not benefit from manufacturer or developer updates. The digital information available via the QR code would only need to be updated, ensuring that consumers always have access to up-to-date information about the product characteristics and safety features; and
- At the end of a product's lifecycle, QR codes can help maintain accountability and advance the circular economy as they can for example be used by recyclers to be confident about the composition of a garment. To eliminate fraud the QR code should however be backed up by a secure digital system.

b. Challenges

- If QR codes are widely adopted to provide up-to-date information for products (especially for unconnected products), it is necessary for manufacturers and developers to contribute towards encouraging consumer behaviour where the QR code is used to repeatedly check-up on information as opposed to a single use or rare uses. This way when the information provided through the QR is updated consumers would have a higher likelihood of being notified about renewed product safety information;
- A challenge in terms of consumer vulnerability is that when QR codes are used for mobile payments and in-app transactions, this is often done 'on the go' and via small screens. Limited authentication controls can provide risks.[230] This way, for example children may be able to make purchases without the consent or knowledge of their parents. Furthermore, QR-codes can easily be duplicated and shared, so are typically not a good solution for sensitive applications; and
- There are also challenges associated with the increased development of electronic devices to read QR codes. The production and sustainable disposal of electronic equipment is still a major challenge in Europe, where less than 40% of all e-waste is recycled (European Parliament, 2020). As QR codes develop, it is thus a major challenge to ensure that e-waste management is improved.

[230] OECD, 2019, *Challenges to consumer policy in the digital age*. Available at: https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf.

2.7. Fiche 7: Blockchain

2.7.1. Regulatory information and definitions of the technology

a. EU Definition

Blockchain is often described as 'distributed ledger technology' (DLT) which 'means a type of technology that supports the distributed recording of encrypted data'[231]. Blockchain is used in a wide array of application areas such as smart contracts, NFT's and cryptocurrencies. For the latter the European Commission has recently proposed a regulatory sandbox for 'financial products based on distributed ledger technology'[232] .For other application areas, regulations are not yet fully developed.

b. EU Legislation

- The European Commission has embraced the importance of blockchain technology and wants the EU 'to be a leader in blockchain technology, becoming an innovator in blockchain and a home to significant platforms, applications and companies'[233];
- The EC wants to support a 'gold standard' for blockchain technology that embraces European values in its legal and regulatory framework. This framework will include environmental sustainability, data protection, digital identity, cybersecurity and interoperability. This includes:
- A European Blockchain Services Infrastructure[234] ;
- Developing regulations on digital assets[235] and smart contracts[236]; and
- Supporting interoperability and standards.

c. Distinctive EU Member States Legislation

- Within EU Member States most discussions on (to be developed) blockchain legislation focusses on the application area of cryptocurrencies. In general, the majority of Europeans want their countries to regulate cryptocurrencies[237]; and
- In some of the EU Member States, such as The Netherlands, several studies on the social and ethical impacts of blockchain are currently performed[238], as well as studies on the need for blockchain regulation[239].

[231] European Commission, 2020, Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.

[232] Ibid.

[233] European Commision, 2021, *Shaping Europe's digital future*. Available at: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy.

[234] European Commission, 2021, *European Blockchain Services Infrastructure.* Available at: https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure.

[235] European Commission, 2020, *Digital Finance package*. Available at: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

[236] Schrepel, T., 2021, *Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3947174.

[237] David Walsh, 2021, *Majority of Europeans want their countries to regulate crypto, not the EU.* Available at: https://www.euronews.com/next/2021/09/01/majority-of-europeans-want-their-countries-to-regulate-crypto-not-the-eu-exclusive-euronew.

[238] See: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/blockchain/relevante-documenten/.

[239] Schellekens et al., 2019, *Blockchain en het recht*. Available at: https://repository.wodc.nl/handle/20.500.12832/2336.

2.7.2. Technical information

a. Technology maturity

Table 31: Technology maturity of blockchain

Initial	[✓ Managed]	Defined	Quantitatively managed	Optimising

Source: Authors' own elaboration.

- Managed - the technology has been launched and is piloted; data is being collected to support wider deployment. Results of piloting contribute directly to a wider launch;
- Blockchain technology is still in rapid development and use cases are still being tested and slowly adopted. It is argued that the technology may bring opportunities such as reducing transaction costs and increasing transparency of transactions[240]; and
- Across sectors, the technology development and adoption levels remain low[241], mainly due to lack of technical knowledge and legislative barriers.

b. Technology acceptance

Table 32: Technology acceptance of blockchain

Little/no time investment required Connectivity is not related to product safety features	[✓ Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment]	Up-front time investment from the consumer to understand product use and safety - limited need for connectivity - products need some maintenance/updates and can change over time.	Large time investment from the consumer to familiarise with changing product conditions and product safety - connectivity is required for device to unction.	Added costs (EUR) seen as benefit - consumers understand that the product they are purchasing have safety features that create additional costs, but the safety benefits outweigh the additional costs	Added costs (EUR) seen as negative - consumers understand that the product they are purchasing have safety features that create additional costs but they do not see the added value. Consumers are likely to look for alternative (and less safe) products as a result

Source: Authors' own elaboration.

[240] Bazaeea, G., Hassanib, M., & Shahmansouric, A., 2020, *Identifying Blockchain Technology Maturity's Levels in the Oil and Gas Industry*.

[241] Civitta, 2020, *Blockchain in SMEs Maturity Report 2020*.

- From a twitter discussion analysis[242] it is found that twitter users perceive blockchain to have increased security, privacy, traceability, trust and transparency and reduced costs. Discussed use cases indicate that blockchain, and more specifically smart contracts, minimise uncertainty in transactions, reduce monitoring expenses and are self-enforceable;
- From this study, research shows that benefits are more often discussed than drawbacks. Discussed drawbacks include power consumption, and the users' multiple identities; and
- Research on the acceptance of blockchain in electronic medical record systems showed that the most influential factor affecting to accept Blockchain is the performance expectancy which includes the recognition of technological benefits. In addition, the system is perceived to be low risk. There is, however, a trust factor that relates to the ability, integrity and security and privacy of the application that reduces the acceptance.[243].

c. Complexity

Table 33: Complexity of blockchain

Product safety is a result of product marketing	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Product safety is a result of product functions that do not require connectivity	Product safety is a result of product functions that require connectivity for updates	Product safety is a result of product functions that require connectivity to operate

Source: Authors' own elaboration.

- Product safety features such as increased transparency and traceability of transactions require connectivity per definition as blockchain makes use of decentralised network.

d. Transferability

Table 34: Transferability of blockchain

Consumers learn about product safety at the moment of purchase	Consumers learn about product safety during use	Consumers learn about product safety continuously as the product is updated	Consumers learn about product safety at the time of disposal

Source: Authors' own elaboration.

- As the main product safety benefits and risks of blockchain are related to the core structure of how blockchain operates (through a decentralised network), consumers are not always aware of these risks when a blockchain product is purchased.

[242] Grover, P., Kar, A. K., Janssen, M., & Ilavarasan, P. V., 2019, Perceived usefulness, ease of use and user acceptance of blockchain technology for digital transactions–insights from user-generated content on Twitter. Enterprise Information Systems, 13(6), 771-800.

[243] Wanitcharakkhakul, L., & Rotchanakitumnuai, S., 2017, Blockchain technology acceptance in electronic medical record system. In The 17th International Conference on Electronic Business, Dubai, UAE.

2.7.3. Challenges and opportunities along the value chain for product safety and durability

Key words: traceability, cooperation, authenticity, interoperability, standardization, data privacy

Strongest impact for product safety in the value chain: manufacturing, distribution, maintenance and repair

a. Opportunities

- Increasing product traceability for improved product safety and durability across the value chain:

- Market surveillance can adopt blockchain to manage risk, enhance compliance with product safety regulations, and protect consumers from counterfeit items. These blockchain technologies may readily expand to other applications, such as tracking things at customs ports or providing early warnings of delivery delays. The entry of counterfeit products onto the market can be blocked (for example, using blockchain and embedding smart tags in its footwear to thwart counterfeiting);

- Source tracking using blockchain mitigates risk and increases the bar for real-time quality monitoring in manufacturing and distribution. Once blockchain is adopted, enterprises may enhance visibility with systems that monitor regulatory compliance or maintain a product's lifecycle through warranties; and

- By building up a shared information infrastructure on a blockchain, the technology can enable the circular sourcing of renewable inputs and support resource efficiency. It can also aid in the recovery of the materials, in particular refurbishing and recycling from manufacturers and consumers, via tracking of material and resource flows through different supply chains and consumption steps.

b. Challenges

- As blockchain technology is still evolving, several challenges are emerging;

- The complexity of the technology, data protection and privacy, cyber risk, integration with legacy infrastructures, or interoperability and standardisation between different blockchains. While the present regulatory and supervisory structure is primarily successful at mitigating developing risks, particular challenges should be examined as blockchain technology evolves and its applications in business operations expand. For instance, each blockchain is self-contained, and there is currently no agreement on how and what data should be recorded. Without industry standards, chains cannot interact freely with one another. Each may use a variety of various data kinds and formats and may even store a variety of different types of information;

- There is a risk of exclusion for clients who prefer more conventional modes of communication or who have a poor degree of technical knowledge or aptitude. From a legal and data privacy standpoint, there is a danger that combining vast volumes of historical data on a single consumer or a group of consumers would result in the indirect use of sensitive data that is not permitted under applicable laws. Given the essentially tamper-resistant and unchangeable nature of blockchain records, the unfavourable effect on compliance with the GDPR obligations, such as the right to be forgotten and data deletion requirements, must also be carefully evaluated; and

- A holistic and systemic approach to the sustainability of blockchain is needed. Blockchain is an energy-intensive technology, and some researchers question its efficiency overall in terms of energy consumption. New protocols are emerging and proving to be less energy-dependent.

2.8. Fiche 8: Digital Product Passport (DPP)

2.8.1. Regulatory information and definitions of the technology

a. EU Definition

- There is still no common definition of the DPP. However, the EU Green Deal states that "an electronic product passport with information on the composition, repair and dismantling possibilities" could be introduced as part of the New Circular Economy Action Plan, presented in March 2020[244]. In a later document, the Parliament further specifies that the DPP is a combination of:

○ A unique product identifier

○ Data collected by different value chain actors related to this unique specifier

○ A physical link between the product and the data[245]

b. EU Legislation

- As of now, the Ecodesign Directive 2009/125/EC is the main legal framework related to material efficiency requirements. Even if its scope was widened in March 2020, to include instructions on disassembly and repair operations[246], it still needs to be updated for further inclusion of recyclability and traceability criteria. Similarly, the EU's Battery Directive (2006/66/EC), in force since September 2008, is going to be updated to create a legal framework to allow for the sustainability, traceability as well as the circularity of the production of batteries within the EU[247].

c. Distinctive EU Member States Legislation

- In Belgium, there currently is a provision amendment that is being proposed to include durability and repairability information. The digital product passport is an alternative idea to this one and is also under assessment[248].

[244] European Parliament, 2021, *Legislative Train*. Available at: https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/a-european-green-deal/file/new-circular-economy-action-plan.

[245] European Parliament, 2021, *Committee on Petitions. Notice to Members*. Available at: https://www.europarl.europa.eu/doceo/document/PETI-CM-692920_EN.pdf.

[246] European Parliament, 2020, *Sustainable Consumption and Consumer Protection Legislation. How can sustainable consumption and longer lifetime of products be promoted through consumer protection legislation?*.

[247] EU Battery Proposal released to replace the Battery Directive. Available at: https://www.sgs.com/en/news/2021/03/safeguards-04121-eu-battery-regulation-proposal-released-to-replace-the-battery-directive-2006-66-ec.

[248] European Parliament, 2020, Notice to members: Petition No 0952/2020 by E.D. (German) on improving the labelling of plastic packaging to allow automatic sorting for recycling. Available at: https://www.europarl.europa.eu/doceo/document/PETI-CM-692920_EN.pdf.

2.8.2. Technical information

a. Technology maturity

Table 35: Technology maturity of DPP

Initial	Managed	Defined	Quantitatively managed	Optimising

Source: Authors' own elaboration.

- **Initial** - The technology is still under evaluation to understand what its best use could be; and
- Its benefits (traceability and recyclability) are still being debated against its limits (the DPP would not be able to take contamination into account, it would have to be coupled with another technology – such as blockchain[249] or a registration database[250] – to be efficient, etc.)

b. Technology acceptance

Table 36: Technology acceptance of DPP

Little/no time investment required Connectivity is not related to product safety features	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Up-front time investment from the consumer to understand product use and safety - limited need for connectivity - products need some maintenance/updates and can change over time.	Large time investment from the consumer to familiarise with changing product conditions and product safety - connectivity is required for device to unction.	Added costs (EUR) seen as benefit - consumers understand that the product they are purchasing have safety features that create additional costs, but the safety benefits outweigh the additional costs	Added costs (EUR) seen as negative - consumers understand that the product they are purchasing have safety features that create additional costs but they do not see the added value. Consumers are likely to look for alternative (and less safe) products as a result

Source: Authors' own elaboration.

Added costs (EUR) seen as a benefit:

- For the consumer's health (knowing the chemical components of products for example); and
- For recyclability and the promotion of the circular economy.

[249] Alaranta et al., 2021, *How to Reach a Safe Circular Economy? Perspectives on Reconciliating the Waste, Product, and Chemicals Regulation*.

[250] T. de Romph., 2018, *The legal transition towards a circular economy – EU environmental law examined. Dissertation Thesis*. KU Leuven University.

c. Complexity

Table 37: Complexity of DPP

Product safety is a result of product marketing	Little/no time investment required Connectivity is required but technologies work to reduce consumer time investment	Product safety is a result of product functions that do not require connectivity	Product safety is a result of product functions that require connectivity for updates	Product safety is a result of product functions that require connectivity to operate

Source: Authors' own elaboration.

- **Product safety is a result of product functions that require connectivity to operate:** For different actors to access the DPP (supply chain actors, recycling actors, consumers), the DPP would need to be made available online – both so that the producers can register the information relative to the product, and so that the other actors intervening later in the life cycle can look at this information.

d. Transferability

Table 38: Transferability of DPP

Consumers learn about product safety at the moment of purchase	Consumers learn about product safety during use	Consumers learn about product safety continuously as the product is updated	Consumers learn about product safety at the time of disposal

Source: Authors' own elaboration.

Consumers learn about product safety at the moment of purchase:

- It depends on the actors to whom the DPP is made available: whether it is only to the people intervening in the supply chain, or also to the consumers; and
- If access to the DPP is guaranteed at the time of purchase, the composition and recycling possibilities of the product could influence the buyer's decision, by helping him make a more informed choice.

Consumers learn about product safety at the time of disposal:

- The DPP includes information on the components of a product (for instance the type of plastics used, or the chemical components), which can help promote proper sorting and recycling of waste.

2.8.3. Challenges and opportunities along the value chain for product safety and durability

Key words: traceability, cooperation, transparency, compliance and audit tool

Strongest impact for product safety in the value chain: product design, manufacturing, distribution, maintenance, reparability

a. Opportunities

- The use of DPPs could greatly enhance product traceability as different actors would provide input to the DPP across the value chain, from development to distribution;
- For consumers, if included, a DPP would provide consumers with enhanced product information - digital product information is not limited by the space available on packaging and, unlike documents that can come with products, DPPs can be updated by the manufacturers, developer. PP allows for multidirectional information flows along the value chain which could enable more efficient information exchange between different stakeholders (e.g., repair shops and waste operators);
- In terms of marketing and communication about product safety, a product passport can be seen as a compliance and audit tool, demonstrating to a consumer that the product is the right choice and therefore informing the consumer at the moment of purchase. It is also possible to make privacy-law-compliant direct contact with the end consumer to enable direct customer service during the product use. The availability of DPP would allow making better purchasing decisions, particularly accounting for product recyclability, the composition and the origin of product components;
- As and if the DPP becomes more widespread, the importance for consumers will grow as DPP has the potential to become one of the most important sources of information about the product to guide consumer purchasing decisions (it could even facilitate other technologies, such as AI-driven shopping assistants that quickly scan DPPs to determine whether the products match consumer preferences); and
- Policy makers will also benefit from the information exchanges to regulate compliance and adapt policy making if necessary.

b. Challenges

- Right now, DPPs appear to be a concern for policy makers to achieve a common definition for DPP and manufacturer developers in implementing DPP into the value chain and ensuring its usage. All actors along the supply chain should agree on standards and measures should be taken so that smaller economic actors are not excluded. Producers should be able to build their own solution to access the product passport without having to depend on one technology provider[251].
- In order to contribute to product traceability (and maintenance, reparability, end of life cycle) the DPP needs:
  - To be accessible online to the different value chain actors. This means establishing a database that is accessible for the actors and likewise ensuring that the actors update product information of the DPP.

[251] Guth-Orlowski, S., 2021, *The digital product passport and its technical implementation.* Available at: https://medium.com/@susi.guth/the-digital-product-passport-and-its-technical-implementation-efdd09a4ed75.

- To be efficient in providing information, the DPP needs to be connected to other technologies and digital solutions (e.g., blockchain) which means increased complexity and infrastructure necessary for DPP to provide the relevant consumer information.
- Certain information about the composition of a product or the supply chain is a company secret. For this reason, secrecy should be part of the access control mechanisms of the system that implements the digital product passport.

The General Product Safety Directive is a cornerstone of the EU product safety legislative framework. Issues and emerging trends have however impacted the effectiveness of the current Directive. This study examines how new technologies and digital solutions can help improve consumers' awareness, while also guaranteeing a better safety of the products placed on the Single Market. The study formulates recommendations that provide a framework for the better alignment of existing legislation on product safety and digital services, as well as the European Community sustainability objectives.

This document was provided by the Policy Department for Economic, Scientific and Quality of Life Policies for the committee on Internal Market and Consumer Protection (IMCO).

PE 703.348

IP/A/IMCO/2021-05

Print ISBN 978-92-846-9582-9 | doi:10.2861/02705 | QA-07-22-503-EN-C
PDF ISBN 978-92-846-9581-2 | doi:10.2861/807825 | QA-07-22-503-EN-N