



Innovation, AI, Technical Regulation and Trade

Questioning the Invisible Hand
in the Digital Economy

Key insights

2023



Foreword

The benefits of digitalisation for trade are widely acknowledged. However, the application of technologies and innovative digital solutions such as Artificial Intelligence in industrial products also represent a number of challenges that need to be addressed by regulation.

In the past the main regulatory objective for industrial goods was product safety. Today, due to digitalisation, product regulation also needs to address elements of privacy, cybersecurity and resilience. Furthermore, the fact that many innovative digital products include software, the properties of which can change throughout the products' life cycle means that products are much more difficult to control and monitor, and as result, to regulate. At the same time these new regulatory parameters have a direct and significant effect on trade and market access.

Digital innovation is currently being addressed by policy makers and regulators through a host of new strategies and regulatory proposals, but the question is whether the approaches taken-, and regulatory techniques applied - are effective. Poorly adapted or non-coordinated regulatory strategies can result, not only in uncertainty and regulatory gaps, but also to effects on a Level Playing Field for businesses- another reason why more insight on this topic is needed.

Products with embedded digital technologies have not received focus within the analysis of technical regulation, regulatory techniques and international regulatory cooperation. With insights on regulatory challenges in the fields of Information and Communications Technology, Medical Devices and Vehicles when applying Artificial Intelligence, our analysis highlights that

- There is increased regulatory complexity when addressing digital innovation through technical regulation, risking regulatory fragmentation, effects on a Level Playing Field and new barriers to trade
- Rapidly evolving use cases for digital intelligence in industrial products, such as Artificial Intelligence, means that technical regulation becomes quickly outdated
- Digital risks are about safety, security, privacy and resilience, which require coordinated regulatory approaches. We also see a need to re-evaluate compliance models, e.g., by introducing a life-cycle perspective to enforcement and market surveillance in terms of tools enabling “continuous compliance”
- Policymakers and regulators may need to accept that digital product properties are difficult to control. As result, a new approach on technical regulation of digital products is needed. This is important to boost innovation and trade, and to prepare, adopt and implement technical regulations that are effective
- Due to multiple interconnections, and given horizontal and sector specific digital regulatory concerns, more coordinated regulatory impact assessments will be needed to achieve evidence-based regulation for digital innovation

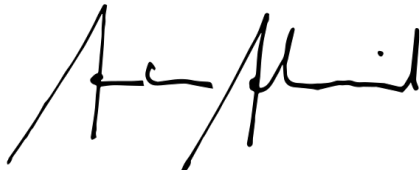
This paper is based on the report “Innovation, AI, Technical Regulation and Trade – Questioning the Invisible Hand in the Digital Economy” by the National Board of Trade Sweden.¹ Read the full report² here:

<https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2023/innovation-ai-technical-regulation-and-trade.pdf>

Insights from this field feed into our contributions on ongoing trade negotiations, negotiations on new digital regulatory frameworks within the EU, initiatives such as the EU-US Trade and Technology Council and processes promoting the digital and green transitions related to trade policy.

We wish to thank all contributors³ that helped us to increase knowledge in the field of digital innovation, regulation and relevant links to trade. The insight and input from the business reality as well as the competence provided by regulators and experts are key to better trade policy!

Stockholm, December 2022



Anders Ahnlid
Director-General
National Board of Trade Sweden

¹ The report is written by Senior Adviser Heidi Lund together with Legal Advisers Sara Emanuelsson and Johanna Nyman. Advice has been provided by a number of colleagues at the National Board of Trade Sweden: Internal Market Adviser Karin Atthoff, Senior Adviser Karolina Zurek, Trade Policy Adviser Neil Swanson, Legal Advisers Ralph Eliasson and Felinda Wennerberg and Chief Legal Adviser Christian Finnerman.

² The findings and policy recommendations in this report are solely those of the National Board of Trade Sweden.

³ For this report contributions from external experts have been crucial. In particular, the National Board of Trade wishes to thank Apple Inc.; Dedalus; Einride; Elekta; Google LLC; Scania; Sandra Sjöåker, Assessor and Rikard Owenius, Assessor- Swedish Medical Products Agency; Mobility Sweden; Swedish Medtech; Bjørn Hesthamar, Process Developer - Swedish Post and Telecom Authority; Anders Gunneriusson, Senior Adviser and Ylva Lidberg, Senior Adviser- Swedish Transport Agency and Volvo Group. The Board further wishes to thank the following experts for their valuable contributions and comments: Kristina Andersson, Senior Researcher/Legal Expert Digital Systems -RISE; Dag Ströman, Head of Cybersecurity Certification Inspectorate - Swedish Defense Materiel Administration; Gustav Söderlind, Executive Officer and Johan Turell, Senior Analyst and Research Coordinator - Swedish Civil Contingencies Agency; Robert Ginsberg, Co-founder and COB – QAdvis; Susanne Lundberg, Director Environmental Product Management - Ericsson and Ari-Pekka Syväne, CEO & Senior Consultant - CNB Systems Ltd.

Table of contents

Foreword	2
1 Setting the scene – what is so special about product regulation for innovative digital products?	5
2 Why technical regulation in digital products need more attention in trade policy	7
3 Addressing digital product intelligence by regulation – the same, but different?	9
4 Emerging tech markets and the application of artificial intelligence	12
4.1 AI technology and regulation in mobile phones – more or less self-regulation?	12
4.2 Medical devices – strict regulatory framework but many challenges for digital innovation	15
4.3 Vehicles – AI technology and regulation in trucks – the access and use of data one of the main issues	18
5 Our conclusions	22
6 Our recommendations.....	28



I Setting the scene – what is so special about product regulation for innovative digital products?

Global trade in industrial goods is facing a new reality, where technological innovation and digitalisation boost trade and growth, but where the basic conditions for regulators and traditional trade policy frameworks and principles both in the EU and globally are being seriously challenged.

This situation is created by several factors. New technologies and industries have increasingly moved from mass produced products, the requirements of which can be standardised to more customised solutions that are often supported by services and connected to the Internet. The increase in product-related interconnections due to cyber-physical systems⁴, brings an additional challenge to regulation, and thereby to international trade.

Another aspect is that digital products are not only affected by the intended use and foreseeable physical and chemical risks, i.e., risks that are typical for non-digital and non-connected goods, but also by aspects that are more difficult to foresee, regulate, monitor and enforce, such as the need to address privacy, cybersecurity and resilience. Vulnerabilities in digital products materialise in cyber vulnerabilities (in terms of greater attack area), privacy and personal integrity concerns (in terms of handling data) and resilience concerns (as many products are also used in critical infrastructure). Risk assessment methodologies also often assume that probabilities of events are known, but the pace of change in digital technologies is often too fast to collect relevant statistics.

An additional element that complicates technical regulation is that digital concerns, related to Artificial Intelligence (AI), cybersecurity and data are currently mainly addressed with new horizontal legislation (much of which is still at proposal stage), while traditional regulatory concerns are addressed in sector specific legislation. There is also often a lack of coordination between horizontal and sector specific legislation. Poorly adapted or fragmented regulatory measures can have a significant negative effect on trade by creating barriers between markets, especially if regulatory uncertainties are addressed with national or regional regulatory solutions.

⁴ Cyber-physical systems are computer-based systems for interacting with machines, vehicles and other equipment, including sensors that can acquire data from the environment.



"Artificial Intelligence and cybersecurity could represent opposite forces in the digital realm. While AI provides full potential for digital development without limits and borders, cybersecurity strives to find the means for to how to scope, control and protect data.⁵

The objective of this paper is to demonstrate how the properties of industrial goods are affected by two digital trends: the utilisation of new technologies, such as AI, and the prevalence of increasing digital vulnerability. The paper discusses how these trends should be considered when developing technical regulation and regulatory techniques. This can help us to improve technical regulation and thus boost trade in digital products in the EU and globally, whilst continuing to address essential regulatory concerns.

By discussing with companies active in the fields where the use of AI is more prevalent, e.g., in vehicles, medical devices and Information and Communications Technology (ICT), we wish to provide insight into how well regulation and regulatory techniques applied today embrace some technological changes in industrial goods, with the aim of providing some recommendations for policymakers with the task to promote digital transition and trade.

⁵ As a result, controlling AI by regulation goes against concept of AI — even if the regulatory need can be understood from a societal perspective.



2 Why technical regulation in digital products need attention in trade policy

Technical regulations and standards affect a large part of world trade. Over past decades a lot of trade policy work has been devoted to overcoming challenges in the area. Technical requirements for products such as, requirements on labelling, certification, packaging and quality are most often prepared, adopted and implemented based on various legitimate concerns such as consumer safety, public health and environmental impacts. As such requirements are necessary to meet legitimate policy objectives, they cannot just be abolished. If **technical rules** vary between markets or if product requirements are unclear or various legal frameworks are not coordinated, e.g., creating duplicative requirements, they risk regulatory fragmentation and barriers to trade. However, with the right regulatory approach and technique, these technical rules may facilitate trade.

Today, there are several reasons to have an increased focus on technical regulation and regulatory techniques. Complex trading patterns, Global Value Chains, increased digital vulnerabilities and technological innovation put new demands on how product requirements are prepared, adopted and implemented. Despite international trade policy frameworks such as the WTO Agreement on Technical Barriers to Trade and longstanding fora for international regulatory cooperation, e.g., within OECD, UNECE and trade agreements, we observe an increased regulatory complexity creating new regulatory challenges.

Our perception is that digital intelligence in industrial products, such as the use of AI, combined with increasing cyber vulnerabilities and threats require a re-evaluation of regulatory techniques for industrial goods. This is highly important to effectively address digital innovation whilst avoiding barriers to trade and an uneven playing field for businesses.

Technical rules

Almost all industrial products are regulated in some way. Technical rules cover technical regulations, standards and requirements on conformity assessment.

Technical regulations

Technical regulations refer to mandatory legal documents drafted, adopted and implemented by public authorities that define the specific characteristics that a product should have, such as its size, shape, design, labelling, marking, packaging, functionality or performance.

Standards

In comparison to technical regulations, standards are documents approved by a recognised body that provides rules, guidelines or characteristics for products or related processes and production methods for common and repeated use. Compliance is not mandatory. Standards may also include or deal exclusively with terminology, symbols, packaging, marking or labelling requirements, as they apply to a product, process or production method. Standards are developed in joint ventures by various stakeholders. The development of a standard can be requested by a regulator in a number of areas. If a standard is made mandatory by legislation it becomes in practice a technical regulation. Standards can be divided into formal standards and other standards. Formal standards are developed by recognised bodies that should adhere to the specific criteria of transparency, openness, impartiality and consensus, effectiveness and relevance.

Examples of other standards are the de facto standards that are developed within a business sector or, for example a specific company.

Conformity assessment procedures

Conformity assessment procedures (CAP) are specific procedures used to assess whether a product is in compliance with product requirements. CAPs can include, for example, product testing, inspection and certification procedures.

To avoid unnecessary barriers to trade related to technical regulation, the World Trade Organization (WTO) Agreement on Technical Barriers to Trade (TBT Agreement) stipulates provisions for regulators to follow when preparing, adopting and implementing technical regulation. The agreement also aims to prevent discrimination and protectionism. The provisions of the agreement concern e.g., principles on openness, transparency, equivalence and mutual recognition. To choose the least trade restrictive measure and use international standards are important elements for avoiding technical barriers to trade (TBT).



3 Addressing digital product intelligence by regulation – the same, but different?

Innovation results in markets for goods and services that are in constant flux. Digital technologies and advanced materials and manufacturing have already had a major impact on the properties of industrial goods.

Compared to the past, new technologies do not necessarily contribute to efficiency through mass production but instead increase customisation of specific preferences and use cases.⁶ Another change is that industrial systems have been developed to become increasingly autonomous, following determined processes to a lesser degree or acting without human involvement.

Traditionally, automation systems, industrial processes, transport systems, and similar systems were controlled manually by mechanical electromagnetic machines. These systems have also been physically isolated and built on specially developed technology. In step with technological development, the boundaries between the administrative systems and the industrial information and control systems have become less clear. This has resulted in the industrial information and control systems partly becoming more automated and partly being connected with the organisations' administrative systems, among other things, to obtain information from them. In addition, the industrial information and control systems have increasingly been made available via the Internet and other public networks to achieve greater flexibility.

Furthermore, the actual value in industrial goods is increasingly generated by software, which is in many ways uncontrollable, vulnerable to manipulation and not easily monitored by regulators and agencies responsible for market surveillance. These changes in industrial goods imply also that regulation that focuses on static product requirements does not necessarily embrace the non-static elements provided by a software and intelligence supplied by, e.g., **Machine Learning** (ML) and **Artificial Intelligence** (AI) in industrial products.

⁶ Use case is a specific situation in which a product or service could potentially be used (application area). A use case is also software and system engineering term that describes how a user uses a system to accomplish a particular goal.

Artificial Intelligence and Machine Learning

Artificial Intelligence and Machine Learning are the part of computer science that are correlated with each other but not the same. AI constitutes a bigger concept to create intelligent machines that can simulate human thinking capability and behaviour, whereas Machine Learning is an application or subset of AI that allows machines to learn from data without being programmed explicitly.

Machine Learning is a subfield of Artificial Intelligence.

In its most basic form, an algorithm is a set of instructions or rules given to a computer to follow and implement. A simple, rule-based algorithm is an unambiguous specification of how to solve a class of problems. These may include ordering possible choices (prioritisation), categorising items (classification), finding links between items (association) and removing irrelevant information (filtering), or a combination of these.

More sophisticated Machine Learning algorithms are designed to learn, meaning to modify their programming to account for new data. By applying ML algorithms, a computer, with the help of training data can learn rules and build a decision model. The computer does not merely execute explicit instructions but is programmed to find patterns in the data, turning them into the instructions that programmers would have otherwise had to write themselves.

Concerning vulnerabilities, we have highlighted in our earlier analyses that tools that are currently applied to address **cybersecurity** through regulation, do not guarantee cybersecurity. Complex and costly cyber certification only provide the means to identify cyber vulnerabilities for an ICT product at a given time. I.e., a cyber certification does not necessarily remove all vulnerabilities - the risks are to a high degree dependent on where the ICT product is used. Comprehensive certification with high assurance levels might represent considerable market value; but ultimately, suppliers and consumers will pay the cost.

All these parameters may result in costly and ineffective regulation that does not address the regulatory objective, like product safety or cybersecurity.

Cybersecurity vs. Information Security

Cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its independent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. In this paper, cybersecurity, when used, is not restricted to the protection of (national) information and systems from major (often foreign) cyber threats, such as cyber terrorism, cyber warfare, and cyber espionage; instead, the term embraces the entire area.

The aim of Information Security is to protect information so that it will always be available when needed (availability), trustworthy, and not manipulated or destroyed (integrity); hence only authorised persons may access it, and so that it is possible to follow how and when information has been handled and communicated (traceability). Information security covers administrative (e.g., technical regulations and management systems), technical and physical measures to protect information (such as, e.g., physical passage controls and clean desk policies)

As a result, it is extremely important to analyse whether existing regulatory models and techniques are still appropriate for digital innovation and trade. The decisive questions are as follows: Are the outsets for regulation of industrial goods still the same today as in the past? I.e., are existing regulatory frameworks adapted to autonomous, intelligent and interconnected products and systems? Should the same regulatory techniques and rationale to be applied to autonomous, intelligent and connected products and devices and traditional goods and commodities? Does product regulation need to be modified as a result of products using AI? How to deal with aspects beyond one's control, such as cyber vulnerabilities and threats, which affect commercial Information and Communications Technology (ICT) - is it possible for public entities to prepare, adopt, implement and enforce regulations and standards that address vulnerabilities when product properties can change over time?

As digital regulation is still in its infancy, a good approach is to investigate sectors where Artificial Intelligence is applied to boost innovation. This is important to evaluate how the properties of products (that are addressed by technical regulation) could be affected, and to evaluate whether there are functioning regulatory frameworks for digital products using ML and AI.



4 Emerging tech markets and the application of artificial intelligence

To explore the way AI technology is used in industrial goods and to draw conclusions on the possible impact on technical regulation, we have investigated three sectors where AI is being used and where cyber vulnerabilities constitute an issue: ICT (mobiles phones), medical devices and vehicles (trucks). The selection of cases is based on the parameters that the products discussed should be widely known, and that the sector and company involved should have come far in the utilisation of AI.

The cases focus on three themes:

- AI technology and regulation (i.e., how AI is applied in the sector and in which manner the stakeholders see that the current regulatory framework addresses it)
- Vulnerabilities and risks identified and approaches to address them (i.e., how risks related to AI are perceived); and
- Change in regulatory parameters (i.e., based on the views presented by various stakeholders, the eventual challenges and gaps related to the regulatory technique applicable are highlighted).

In the end, some **general conclusions** are drawn based on all sectors.

4.1 AI technology and regulation in mobile phones – more or less self-regulation?

The ability of mobile phones to generalise and determine what might happen next based on previous patterns and datasets – what is known as machine learning – is becoming an “essential part” of users’ experiences. In 2017, specialty microprocessors that enabled AI were used in just 3% of all smartphones. As of 2020, more than one-third of the world’s three billion smartphones were equipped with processors conducting trillions of operations quickly and with less power. ML and AI in mobile phones can concern, e.g., natural language processing and speech- image-, and voice recognition.

The strategic importance of the field has contributed to mobile manufacturers accelerating their investments into the field of AI-based user experiences. This has led to several specially designed microprocessors that can conduct the sort of maths involved in AI and ML calculations faster and more efficiently – the two most critical requirements for mobile phones – as well as, use less power.

AI and Machine Learning also pop up, increasingly, in smartphone software. AI is already a key part of Google’s apps on Pixel 3. ‘Playing now’, for example, is Google’s “always on” music recognition. Moreover, the third-party apps will be able to use the dedicated processors they want, to conduct their AI tasks.

AI technology is sparsely regulated in the mobile sector – the regulatory focus is on data, protecting communication networks and privacy, as well as on preventing fraud. Some standards exist in the field but not necessarily for all AI use cases.

The definition in the proposed EU Regulation on Artificial Intelligence (AI Act) is not considered by companies as decisive - but whether AI use cases are defined in the legislation is. Most of the use cases that use ML in the mobile sector are not deemed high-risk, and depending on the final text, it may not fit into the scope of the proposed act.

There is a certain understanding among companies for the EU stepping up with a legal framework, especially its work in identifying requirements for various risk categories. At the same time a horizontal regulatory package is considered dangerous as the AI technology is used in so many ways in various products, sectors and applications, and is far from a mature technology. As result, it would be better to closely follow the technological developments and evaluate more carefully the eventual safety critical features, as it is not feasible to regulate something that is not yet well and properly defined. It is thus pointed out that what the proposed AI Act is covering now does not necessarily reflect what is happening in the market, nor will it be valid in the near future.

When discussing standards, companies argue that the situation is somewhat similar to AI legislation, i.e., that there are some standards to be used related to AI but not necessarily all use cases (as the technology is not mature). The regulatory situation for AI can also be compared with cybersecurity. The legal framework for cybersecurity is more mature and as a result there exists well-developed international standards and schemes for mutual recognition that are in phase with technological development. When discussing cybersecurity from the regulators’ perspective, experts confirm that all products and services need to be embraced by a life-cycle approach to ensure security.

When it comes to development of regulatory frameworks experts in companies stress that any efforts to regulate new markets or products and services should be in line with better regulation principles. These should be:

- **Principle based and technology neutral, to give space for innovation;**
- **Proportionate to potential consumer harm and based on clear evidence; and**
- **Predictable, legally certain and avoiding duplication of existing regulatory frameworks.**

What makes regulation complicated, though, is the multiple regulatory layers e.g., horizontal acts such as the proposed AI Act and Cybersecurity Act, which need to be adapted to sectoral legislation such as Radio Equipment Directive (RED), and where the interfaces are not yet totally clear.

Also, from the regulators’ perspective AI constitutes a complex regulatory object as it has a bearing on so many other areas that are still not fully developed. As a result, it is regarded as positive to try to scope sensitive, high-risk applications (in line with the proposed AI Act). Much of this has to do with personal integrity and the risk for the systematic discrim-

ination of individual and information systems that directly affect people. When it comes to AI, the pros and cons rarely affect the same group of individuals. This is why discussions about AI more often slip into human rights and related type of risks. For a certain user, AI can only bring benefits, while a few individuals who are exposed to AI treatment could, hypothetically, have their lives ruined. This thus becomes an impact-based approach (similar to safety protection) where risk (probability and consequence) is not a factor.

Concerning cybersecurity in mobile phones, specific requirements for certain product categories under the Radio Equipment Directive (RED) are subject to the issuance of delegated acts by the Commission. In 2021 the European Commission issued a delegated regulation supplementing RED that addresses elements of cybersecurity.

Vulnerabilities and risks identified

When it comes to risk to users and consumers, companies within the mobile phone-sector argue that adding AI technology to mobile devices does not automatically equate increased risk. It is the specific user case and interface between device, platform and a third-party software related to personal data, that provide the parameters for the actual safety and security. A regulatory challenge is also created by how software is defined in the legislation. The actual consumer/customer risks related to AI is seen as mostly related to personal data.

A lack of control in supply chains is pointed out as a major challenge when applying digital product intelligence to mobile phones. It is highlighted that add-ons in software by third parties means that many compliance parameters are out of reach.

Concerning digital vulnerabilities, cybersecurity was pointed out as the main risk in mobile phones. Furthermore, companies highlight that the impacts of risks related to product intelligence (e.g., on consumers) are not easily foreseeable (they may vary) and can impede effective monitoring (traceability, auditability).

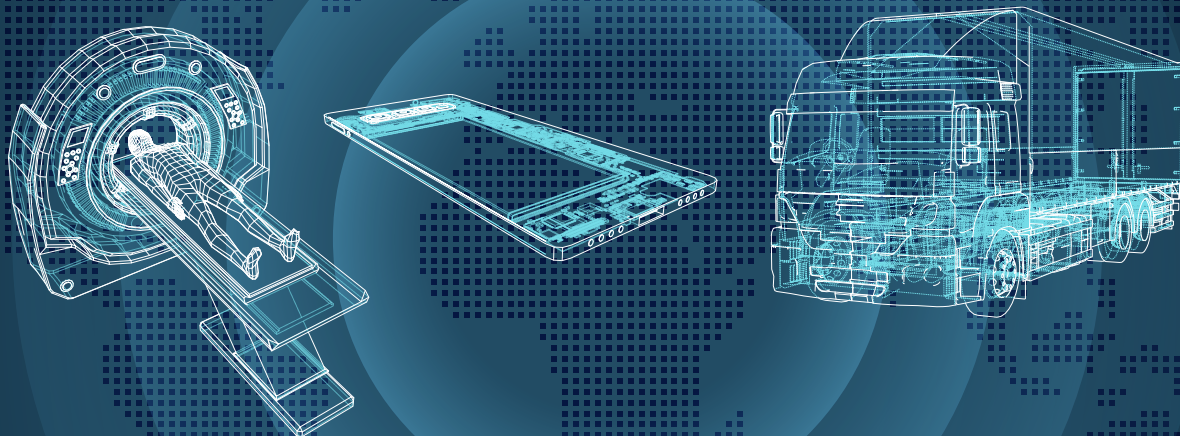
Experiences by companies highlight further that the pros and cons of AI rarely affect the same group of people, which should mean a shift in regulatory strategies from risk (probability and consequence- which is not a factor) to an impact-based approach (similar to safety protection).

Change in regulatory parameters

When discussing whether the current regulatory structure is a good fit for innovation, companies confirm that they can navigate within it but that the increasing regulatory layers are not necessarily compatible and seamless and do create some uncertainties. In addition, regulatory acts such as the Digital Markets Act (DMA), the proposed Cyber Resilience Act and the Implementation of Radio Safety are still not fully evaluated. The lack of overview and coordination is also something that has been brought forward by regulatory bodies. All these regulations are essential for AI in mobiles, and the frameworks need to work together to guarantee that products and services are ethical and safe.

Companies argue further that it is worth nothing that AI and ML encompass a wide range of techniques, from simple to complex. Not all AI and ML is so-called 'deep learning' where it may be unclear how an AI system came to specific decisions.

A regulatory challenge in the mobile sector is materialised in a multitude of regulatory layers that do not necessarily scope in the use cases, which creates uncertainty.



The key take-away from the mobile sector is the effect of often extensive and complex supply chains, that in turn contribute to product properties making traceability and full auditability extremely demanding from a regulatory perspective. The current regulatory challenge materialises in multiple regulatory layers that are not fit to companies AI innovation. Further, the benefits as well as drawbacks, of AI materialise differently for different people- where risk (probability and consequence) may not be the strongest valid parameter, and that should be observed by policy makers and regulators.

4.2 Medical devices — strict regulatory framework but many challenges for digital innovation

AI is being increasingly applied in the pharmaceutical, medical device and healthcare sectors to support various stages of research and development, as well as treat patients the most important application area being “diagnosis and decision support”.

ML and AI are thus important parameters in making health care more efficient e.g. by the analysis of x-rays, cancer screening, prediction of diseases. The utilisation of AI materialises in benefits for society e.g., less expensive screenings after pathological changes, for example in breast cancer and coronary arteries and benefits for patients, e.g., in improved possibilities to predict stroke or newborn sepsis.

Some experts argue that the medical device sector is a late bloomer since today's AI is mostly developed from 2010 onwards embracing applications in medical devices that are frequently used for finding patterns, such as the analysis of images (x-ray, ultrasound) and various apps for medical diagnosis such as those for diabetes that adapt to food intake.

The current (EU) regulatory framework does not address a self-learning AI system specifically but has instead focused on Software as Medical Device (SaMD). SaMD may be used to diagnose, prevent, monitor or treat a disease. It may also provide suggestions for disease mitigation or assist in the diagnosis, screening, monitoring, prediction and determination of a disease.

Artificial Intelligence and Machine Learning technologies differ from software as a medical device in the sense that they have the potential to adapt and optimise device performance in real-time to continuously improve healthcare for patients. AI and ML-based SaMDs inherently change and adapt as more real-world data become available and can be

incorporated. The definition of the use of AI in medical devices is still blurry and understood in a variety of ways - which can range from simpler machine learning based algorithms to sophisticated cognitive computing. AI technologies integrated into medical devices can include big data analytics, deep learning, speech and image recognition, natural language processing, and robotics process automation, among other things. Standard algorithms are sometimes promoted as AI by digital healthcare start-ups but currently they do not represent real computer intelligence.

Several types of AI software can be labelled as a medical device, but manufacturers and authorities are often uncertain as to whether their software can be classified as a medical device under the respective regulations.

Many aspects also impede the use of AI in medical devices, including the parameter of addressing “continuous change” in software-based products, i.e., locked algorithms vs non-locked autonomous systems present a challenge. The strength and advantages with AI/ML are the ability to train and improve the system based on new real-world data. However, the system also needs to be continuously safe for patients and other users, as well as comply with the applicable regulations regarding, for example, validation.

From a trade perspective, the companies highlight that the maturity to accept AI applications varies between countries, also depending on political priorities and data handling. For example, the software application benefits from data storage in a cloud where some countries are more restrictive than others. Using a cloud provides the company with the possibility to scale up infrastructure on demand, but some countries’ cybersecurity concerns have resulted in national requirements, or the introduction of the cloud has taken time.

Concerning the prerequisites for innovation, companies in the sector stress that it should be observed that AI is dependent on qualitative data but that the access to such data is often restricted due to the sensitive nature of the data used in the medical device sector. To test an AI application on a human being, clinical trials are a prerequisite.

Stakeholders interviewed for the analysis argue that the existing sector specific legislation (Medical Devices Regulation (MDR) and In Vitro Diagnostic Regulation (IVDR) are not fully all-embracing when it comes to AI. It is unclear from the MDR when a self-learning and automated adaptive SaMD actually entails a so called “significant change” thus demanding a recertification of additional clinical data. It should be noted that AI and ML are not explicitly mentioned in MDR but enter the regulations by the regulation of software.

The challenges related to medical devices and the proposed regulation on AI are explained also by the European business organisation (COCIR) position paper: The proposed Artificial Intelligence Regulation defines high-risk AI systems so broadly that almost all medical device software may be considered a high-risk AI system. The Medical Device Regulations, especially in combination with the General Data Protection Regulation (GDPR), already include an extensive, often more detailed, set of requirements related to various aspects of the proposed AI Act. However, the proposed Act’s definitions and requirements are not aligned, and the proposal refers to risk and harm in complex and inconsistent ways.

For specific devices, the Act’s requirements conflict with the safety and performance requirements of the Medical Devices Regulations. These misalignments increase complexity, legal uncertainty, and implementation costs, ultimately paid for not only by the manufacturers but also by healthcare systems and patients. Certain requirements may even prevent European patients and citizens’ access to specific state-of-the-art digital health innovations. As a result, the business side strongly supports a targeted, sector-specific, and risk-based approach to the regulation of AI. The other side of the coin is that new

technologies and innovations may always present a risk especially if new products could result in less requirements for health care staff (having also a decisive impact on the use of digital technology).

Vulnerabilities and risks identified

When it comes to risks with AI, stakeholders in the field of medical devices admit that there are risks, but the evaluation of “risk” by the regulator needs to embrace many risk scenarios. For example, is it a great risk to one patient, a smaller risk that applies to a huge number of patients, the risk that a regulation is not being used or the risk that comes from actors not complying with the regulation. An important aspect related to SaMD brought up in the discussions is that new innovative software companies might be especially unaware that they are actually delivering medical devices and need to follow the requirements in the regulation.

Furthermore, stakeholders argue that cyberthreats are one of the greatest challenges and that they are discussing in business fora. Companies address cyber vulnerabilities with e.g., security-by design and vulnerability management processes. Most of the products supplied are “closed” which means that they should function without an online connection behind a firewall and should be protected from attacks. However, this requires a constant monitoring of risk and vulnerabilities. When discussing product safety enforcement and market surveillance the company argues that innovation is much a head of regulation and that, among policy makers and regulators, capacities related to AI must be increased.

It is further stressed that the challenge with AI is not so much related to self-learning algorithms but the concern that - it should not adapt “on-the-job”, that changes to the AI should not be directly implemented and be used in real life on patients (i.e., regarding algorithms that are not locked when the software is in use). Key issues for continuous compliance are change control, traceability and transparency. Another aspect is operation - the operation of medical device software is often produced and managed by third parties. In order to address risk properly, collaboration and clear agreements on the division of responsibilities between parties are essential.

Change in regulatory parameters

Based on the consultation medical devices constitute a strictly regulated area where businesses have limited freedom in the regulatory cycle. As a result, our interpretation is that the introduction of intelligence is made cautiously following carefully existing legal frameworks. That said, it is obvious that proposals for AI regulation as well as cyber vulnerabilities represent a challenge and that there still are many uncertainties with respect to the implementation of digital frameworks. An aspect such as conflicting requirements in the proposed AI Act and Medical Device Regulation is a good example.

The concept of AI is still poorly defined – at the same time product intelligence is applied in a multitude of areas in the sector ranging from simple ML-based algorithms to sophisticated cognitive computing with many various use cases.



The key takeaway from the medical device sector is a perspective of unintended use of software, i.e., that product innovation may result in use cases not covered by a strict legal framework, sometimes even unintentionally (i.e., the businesses not being aware of the applicable legal framework).

The medical devices case also emphasises the important aspect of the risk concerning “false trust” in software updates - which may, but should not, affect the essential requirements defined in legal frameworks.

Further the medical device-case highlights the challenge with cybersecurity. Although the cyber dimension has been strengthened in the sector specific legislation there is the perception that more support is needed from regulatory authorities to address the complexities.

4.3 Vehicles — AI technology and regulation in trucks — the access and use of data one of the main issues

A sector that is evidently benefitting from AI technology, is that of vehicles. The functionalities related to automated driving describes quite well the transformation of a vehicle. In the past, a vehicle was fully managed manually by the driver and could be seen as a “closed system” while it is now partly replaced by vehicle systems that provide transports services and may independently manage both safety-related (ABS/Air bags) and non-safety related critical vehicle features.

In practice this means that new generations of vehicles provide to a greater extent, semi-autonomous, automated and autonomous driving (AD), supported by ML and AI. The term self-driving vehicles, which is frequently used, should be used cautiously as in many cases totally autonomous vehicles are not reality (compare with e.g., lawnmowers that move totally autonomously based on their programming). Automated vehicles (AV), however, include all levels of automation and automated driving. Hence, the most frequently used term internationally is automated driving (AD), which usually includes all levels of automated functions in road vehicles, including advanced driver support, automated functions and fully automatically driven, driver-free vehicles, i.e., the highest levels of automation, where the vehicle’s driving system may in principle completely replace the driver.

It should be highlighted that the common denominator for all companies interviewed for our study is that their use of AI is for the professional market (not for private consumers) and used to a larger extent among customers that need transport over short distances in

defined areas on public roads rather than on all public roads. However, vehicles on general public roads are also in testing.

Trucks in general often represent a customised product – manufactured according to specific buyer requirements, i.e., not to the general public. At large, it can be stated that truck manufacturers type-approve the vehicles and thus conform with the existing requirements (whole vehicle type approval). For automated vehicles there has been a temporary possibility for the European authorities to approve these vehicles by the way of exemption from the present type-approval rules, while the relevant legislation is being developed within the UNECE and in the EU. It was pointed out that if there are no requirements, or if the functionality does not conform with the existing requirements, this creates problems.

Digital intelligence in the vehicle sector is supported by ML and AI, although the concepts do not equal fully autonomous driving. The application of AI in the truck sector is focused on the professional market and the application may concern, e.g., driver assistance systems and automated driving in specific areas such as mines and transport in confined areas.

Autonomous driving systems describe complete automation including the “control tower”, the data flowing from infrastructure and the road users and services. Features such as increasing connectivity and external communication with the vehicle contribute thus to the “openness”, but also to new vulnerabilities.

The Automated Driving System (AD) itself is not fully regulated but validation methods are prepared.

The challenge of explaining the use of AI in the vehicle sector lies in the definitions and what is regarded as AI by different stakeholders. The EU proposal for an AI Act exempts certain high-risk AI systems from most of the requirements in the regulation in case such systems fall within certain already existing legal acts, including vehicle systems under type-approval frameworks that will get receive their own provisions for AI in the type-approval regulation. Companies interviewed for this study say that many of their functions would be regarded as high-risk systems (by definition in the proposed AI Act) and then fall under AI requirements in separate regulations (not yet available). One example of an area where the proposed AI Act may have a role is with regards to liability, as liability is not regulated at the UNECE level.

AI is not in itself much regulated. In the draft European Commission proposal for a regulation of AI it is mentioned that vehicles are excluded but high-risk systems, in particular type-approved functions, are to be regulated by sectoral regulations (i.e., functions rather than the “AI” itself). Here, companies argue that the definition proposed is too broad and may risk creating problems with old, established technology. An airbag, currently not a requirement and not falling under type approval schemes, could fall under the definition and thus be subject to the requirements in the AI regulation.

As one of the companies interviewed pointed out, the new proposal for a European regulation on AI presents a broad definition of AI that may include many existing systems as long as these have sensors, process data and make decisions without active involvement of a human being. It covers products and services that use AI for its development. One company that operates driverless vehicles questions whether the regulation is really about AI (as the regulation puts a focus on human supervision).

The companies interviewed would like to see sectoral legislation instead of harmonised requirements for new technology. Type-approvals for vehicles are considered demanding, but according to the companies interviewed they create predictability.

When it comes to cybersecurity two UN Regulations, have been adopted by the UNECE's World Forum for Harmonisation of Vehicle Regulations. The regulations apply to passenger cars, vans, trucks and buses and entered into force in January 2021.

Vulnerabilities and risks identified

When discussing risks related to new technology, truck manufacturers highlight that more complex systems and more software means more potential vulnerabilities.

Autonomous vehicle systems will be able to control the essential functions of the vehicle, thus they need to be protected against unauthorised access and real cyberattacks. Vehicle manufacturers must be able to guarantee that the access points and functionalities of the vehicle are protected against unintended use or that customer data are only available to those that have a need and agreement with the customer.

AD will change the transport landscape, e.g., with respect to drivers or no driver, or how vehicles are assigned and used in more specialised applications. The possibility to manage a vehicle from distance increases vulnerabilities but companies state that much can be done to increase security by design. Again, it is mentioned that there is no strict requirement on cybersecurity, only an obligation to report incidents.

Companies argue that complete vulnerability can never be tested (certified) or constructed away. Continuous monitoring, development and updating is required, which is included in the vehicle requirements.

There are also regulatory uncertainties with respect to access to data where there is a conflict between the ambition to promote innovation, on one hand, and the control of data, on the other. Furthermore, there are worry about requirements on openness of data that is perceived as a risk for additional vulnerabilities in the sector, especially given cyberthreats.

In an international perspective it can be stated that the US, China and Asia in general have been more generous in allowing AD testing. The EU wishes to follow but is concerned about efficiency and traffic safety. Here it can be confirmed that there are also differences between Member States (Germany e.g., seen as a frontrunner in the EU).

Change in regulatory parameters

As we have noted, most self-driving vehicles introduced by the industry are not operating totally autonomously, which means that the vehicle drives independently only in specific environments given a number of aspects. In other situations, a human must take control which has implications for safety. A large majority of accidents today are driver related. It is, however, informative to observe that self-driving vehicles will actually increase safety in closed environments like mines and terminals, i.e., in areas where the business is expected first to grow on larger scale.

When it comes to the life cycle perspective of an autonomous vehicle, the question, of continuous compliance arises, i.e., can an intelligent vehicle be fully compliant several years after a type-approval given connectivity, over the air updates and cyberthreats?

Vehicle manufacturers can naturally improve vehicle characteristics to some extent throughout the process. The decisive question is nevertheless when a specific single improvement should be regarded as significant from a traffic safety perspective and thus require a change in the registration of a vehicle or even that it be banned from traffic. Considering software and data, the line between "minor" and "significant" improvement might still be blurry. Based on experts, this is related to regulatory bodies and above all

resources available to keep up and follow the technical developments. Here perhaps consumers and consumer organisations, including experts on accident statistics, might have a new role as whistle-blower in future.

Lack of balance with respect to regulatory definition of AI, on one hand, and the actual use cases on the other result in uncertainty. For trucks, sector-specific framework for type-approval has been highlighted as important as it provides predictability.

The main takeaway from the vehicle sector is the competence around digital intelligence in the sector, developed successively over a longer period – and addressing product safety and security in a more systematic manner related to vehicle functions. This does not, however, imply regulatory certainty as the question of handling data, as a key component of vehicle intelligence, needs much consideration as well as the regulation of AI, which is yet unclear.



5 Our conclusions

Adding horizontal, digital regulatory frameworks on top of existing sector specific regulations, increases regulatory complexity and risk regulatory grey zones, fragmentation and trade barriers

Not surprisingly, our analysis highlights a quite complicated regulatory landscape for the sectors studied when innovation in terms of ML and AI are added to industrial products, especially when cyber vulnerabilities are considered.

For anyone that is familiar with the structure of European harmonised product regulations, the multiple add-on layers presented by horizontal digital frameworks will create confusion!

The current regulatory reality within the EU could be characterised as a “spaghetti bowl” where it is difficult to determine where various pieces of legislation start and end. The proposal for a European AI regulation makes it e.g., burdensome to evaluate whether and to what extent various horizontal and sector-specific frameworks are seamless, and whether there will eventually be additional legal frameworks applicable for a certain digital product. Our analysis has also been able to determine that existing digital frameworks can overlap and create duplicative requirements as well as present requirements that are in contradiction to sector-specific ones.

The main rationale for companies to use intelligence by ML and AI is to improve their products and services. It is clear from our discussions with businesses that the application of AI is not an end in itself, but a means for achieving a competitive edge with one’s own technology for improved product features. For the sectors involved this often means various degrees of customisation. It should be noted that AI is not related to one sector only but a technology that can be utilised in many ways. In practice, the specific use cases for the AI innovation pursued by businesses are not yet completely defined and covered by the legislation, or by standardised requirements.

Based on our analysis, there is a distinct difference between the product sectors though. While heavily regulated medical devices have strict regulatory frameworks, the AI innovation in the sector is introduced more carefully, following the specific openings provided in the established legislation. For automated driving, our perception is that the industry seems to explore the regulatory boundaries a bit more, arguing for exceptions from legis-

lation and testing new use cases in controlled environments. This is because the lack of all-embracing regulatory frameworks for innovations means that things move forward extremely fast. Compared to both medical devices and vehicles our perception is that “AI regulation” in the mobile sector seems more limited and provides more freedom, which is probably connected to the potential risks that are somewhat different in character, being more related to data privacy than product safety.

Generally speaking, the introduction and application of AI technology equals moving from standardised products to more customised ones. It is necessary to highlight, however, that the degree of customisation varies. Customisation alone is not a sufficient parameter for which to take a stance on the eventual need to change regulatory frameworks. An observation we may nevertheless highlight is, that the most important component in innovative digital products is software. Software is not visible, static nor easily controllable from a regulatory point of view. This is quite a change from the past where product regulation was prepared from the point of view of products that have more stable mechanical, electrical or chemical properties.

Digital regulation has developed considerably more slowly than the innovation itself within the sectors studied when it comes to intelligent product properties related to AI. Further, sector-specific regulation does not necessarily cover AI as such. Instead, the regulation addresses software updates and ethical concerns, and are often related to licences for testing (of autonomous vehicles) or clinical trials (medical devices utilising machine learning). It is also often applied under certain conditions (on-off road driving, medical diagnostics) and with requirements on human supervision (by a human/doctor). It should be noted that aspects related to data, software, privacy and cybersecurity are all relevant for AI but often separately regulated. It is these multitude of digital aspects that create a jumble making it extremely difficult to form an understanding of the connections between regulations and a holistic view of how various regulations are to cover data-related properties.

In practice, current digital regulation means that sector-specific regulations are being complemented by horizontal ones on AI, data use and cybersecurity. This creates confusion concerning how various, sometimes possibly duplicative and/or conflicting, legislative instruments will complement each other. A lack of guidance in this situation results in certain regulatory uncertainty, but also risks affecting the Level Playing Field with the same regulatory demands applicable to all economic operators.

In addition, we see that there is a risk in that the regulatory objectives of product safety, privacy, cybersecurity and resilience (and their interconnections) are not yet clearly defined in digital regulation - something that policy makers should be attentive to as this complicates regulation even further.

It should be noted that traditional sector specific product regulations in the EU have a focus on product safety and harmonisation while digital frameworks expand regulatory objectives related to data use, interoperability, privacy, cybersecurity and resilience. As current regulatory processes often work in silos (AI, cybersecurity and sector specific regulation) this could result in horizontal digital legal frameworks, unintentionally mixing sector specific regulatory legitimate objectives (safety and risks) with the horizontal digital legitimate regulatory objectives (cybersecurity). This could relate to terminology including definitions of safety and risk.

The rationale for the importance of distinguishing safety, security and resilience from each other can be explained as follows. When used as intended, a product should not pose any unacceptable risk to human health, property or environment. Values to be safeguarded should be the same irrespective of the implementation techniques as this is how a product can impact its environment. Cyber vulnerabilities, on the other hand “open up”

for “external forces” to influence product performance. It might seem a very thin line between the dimensions, but it may lead to misunderstanding and false approaches in regulation. We have not analysed this in greater depth but note that companies have difficulties navigating the current digital regulatory frameworks. Our analysis also indicates that risks with AI are difficult to address through, e.g., horizontal harmonised legal frameworks on AI as the risk may vary from case to case (various groups, consumers and users).

The regulatory uncertainties and gaps identified by the companies interviewed are mostly related to a lack of straightforward guidance concerning whether their product falls under various legislation (the proposal for EU AI Act) and possible duplicative requirements regarding sector-specific and horizontal legislation. The practical examples of uncertainty are related to requirements concerning software up-dates and a lack of acceptance (licence) of new technology in export markets.

Businesses also highlight that to address cyber vulnerabilities there should be greater expertise among policy makers and that guidance should be available. Cyber vulnerabilities are seldom sector specific and are also related to societal concerns and critical infrastructure. Nevertheless, all stakeholders contributing to this study see the cybersecurity toolbox (regulations, standards and conformity assessment schemes) as more mature than a regulatory toolbox for AI, which is still in its infancy.

It is of upmost importance to address these regulatory complexities to avoid negative effects on the market and international trade.

AI technology is not new but the continuously evolving AI use cases mean that regulation becomes quickly outdated

Based on our analysis, AI as a technology should not be regarded as “new” or non-mature. However, the constantly evolving new use cases and innovative application areas of AI create a huge challenge for policy makers and regulators. Also, the risks, vulnerabilities and other effects generated by the use of AI in various products are not yet fully known. However, many recent regulatory proposals seem to reflect awareness of the need to address the use of AI in regulatory requirements.

The ambition to regulate AI is currently expressed mainly in the EU proposal for an AI Act with horizontal requirements with the view of addressing high-risk AI. However, the proposed Act does not necessarily fully embrace sector-specific aspects, which creates uncertainty as companies are not able to identify their innovation in legislation.

AI is often misunderstood as a feature in products that makes its own decisions without any human supervision. This is something that is not applicable, for example, in trucks and medical devices where the intelligence must be properly set at product launch and where human monitoring is a rule, not an exception.

The actual regulatory challenge is materialised in the effort to scope the various degrees of integration of intelligent properties in products. The very concept of “Artificial Intelligence” is, however, still poorly defined in regulatory frameworks. As a result, innovative businesses are not always comfortable in defining or categorising intelligent products or product features as equal to AI.

Many stakeholders, including industry, accept and even welcome an effort to try to scope in or define “high-risk” AI. At the same time, it should be possible to find various AI use cases in legislation - a scenario that is still far away from reality.

Digital risks in products are about safety and security and privacy and resilience – which require coordinated regulatory approaches

The objective of our analysis has not been the identification of safety gaps or risks in products related to AI, other than those specifically related to cybersecurity. As result we have not conducted a broad analysis of risks and safety gaps but mostly draw upon the information provided by various stakeholders in the case studies. What can be determined, however that digital products equate with several new regulatory concerns.

It can be argued that the companies, especially those that develop medical devices and vehicles, do business in heavily regulated sectors. By introducing of intelligent technologies, with a high degree of automation, ML and AI are thus dependent not only on possible use cases, which is technology that is in demand by the customer, but above all on existing openings to be found in the regulatory frameworks. As consequence, risking safety (e.g., by supplying intelligent medical devices for treatment or providing advanced driving features) would not be an option but would quickly put companies out of business if companies are deemed as delivering safe products.

Adding AI technology in a product might, but does not necessarily need to, increase the risks in industrial products. Our findings also confirm that far from all the effects of AI are yet known. As a result, we could argue that adding intelligence (ML and AI) does not automatically imply risks and safety hazards- but to identify and trace actual effects and vulnerabilities along a product life cycle is and will be a major regulatory challenge.

It is also worthwhile stressing, again, that along with digitalisation the risk scenarios for products are extended and broadened. Vulnerabilities in digital products materialise as cyber vulnerabilities (in terms of greater attack area), privacy and personal integrity concerns (in terms of handling of data) and effects on resilience (as many products are also used in critical infrastructure). This means that the traditional consumer safety perspective in regulation also needs add to cover security (IT security), privacy (GDPR) and resilience which are currently addressed by a multitude of approaches and regulative proposals, although not necessarily in a coordinated manner and with clarity.

As highlighted earlier, a multitude of software-related product features appear in technical legislation and we wonder if regulators are in fact able to distinguish, and be clear about, the aspects of product safety, cybersecurity, privacy and resilience in the regulation of digital products, including with respect to enforcement. It is of great importance that it is possible to understand what specific regulatory objectives are as addressed by various pieces of legislation and any subsequent interconnections.

Consequently, digital regulation requires more certainty that current legal frameworks provide. An absence of clear and harmonised regulatory frameworks, applicable standards that embrace companies' innovation and enforcement that may follow efficiently up compliance there is a great risk of regulatory fragmentation, effects on the Level Playing field and barriers. I.e., there is no use to regulate if the tools and capacities for enforcement are non-existent.

Requirements for data, software updates and cybersecurity are increasingly introduced, as is sector- specific regulation, to address challenges associated with changing product properties. Efficiently monitoring software and creating traceability seems to be challenging, especially related to varying views on data sharing, where there are several proposals on the way in the EU. These have both pros and cons related to innovation safety and security.

When it comes to digital innovation the safety concerns identified by companies themselves are mostly related to data and above all to the cyberthreat.

Unfortunately, there is only a narrow window of opportunity to try to grasp potential risks and hazards related to AI. The visible examples might only be revealed in the media or to be found in vigilance reporting systems by regulators. It should be noted that even those affected by risks or hazards might not always be aware of vulnerabilities (e.g., cyber related or bugs in software). When it comes to regulatory policies for proposals concerning both AI and cybersecurity our perception is that they should be founded on evidence (e.g., based on thoroughgoing regulatory impact assessments) as approaches that try to “scope the unknown” are likely to be costly and inefficient.

Based on our analysis various markets approach the regulatory challenges with AI differently. When deciding and enacting regulation, it should be possible to verify that the actions required by the regulation can also be followed up. Or to put it another way, only aspects that can be verified should be regulated; otherwise, businesses are clueless about what to comply with, and consumers and customers are uncertain of what they have purchased. For example, are there competences and resources that can monitor the changes in software for medical devices? How can the properties of type-approved vehicles be followed up? Vehicle regulation does not allow “changes” after the vehicle has been put on the market, but it is evident that on-vehicle data and updates may change vehicle properties and risk vulnerabilities. Although over-the-air-updates are covered by legislation, the question is whether this can be followed up. As a result, security-by design and data security (in addition to product safety) are likely to become important.

Regulations and standards for AI are still under development so we see that there is potential for policy makers and regulators to evaluate alternatives for best practice. As a result, security-by design, data security (in addition to product safety) and continuous compliance are likely to become important.

The importance of various reporting systems, such as EUDAMED for medical devices, should be highlighted here. The eventual risk scenarios with connected, intelligent and autonomous products are very different when comparing possible hazards related to medical devices or vehicles with those related to personal data (leakages or misuse) in mobile communication. What is quite evident based in our analysis is that there is a need for a new element to be incorporated in regulation, i.e., there is a need for a toolbox for “continuous compliance” that better provides the means required to follow the digital market.

Based on this analysis digital compliance seems to be dependent on the regulators’ next move. Here there is need for serious investments in resources and competence to enable regulatory bodies to find methodologies to track and monitor significant changes in digital product properties (i.e., changes that are decisive for safety, security, privacy and resilience).

Can the digital market with “virtual” products be regulated?

One of the underlying questions of the study is, whether there is anyone having full insight and taking responsibility for the digital market.

Do we have a mechanism that covers eventual failures in terms of potentially non-compliant products, if products are not as tangible as before (and thus partly invisible), where digital regulatory frameworks are still under development and where the means to control compliance during a product’s life cycle has been weakened? The concern, in other words, is whether the digital market of industrial goods is left to “the Invisible Hand”.

Whether the invisible digital economy “manages to regulate itself”, in the absence of complete and all-embracing regulatory frameworks, is a tricky question to answer.

This is because, possible regulatory failures or unintended regulatory outcomes are not necessarily registered and revealed due to fact that the lack of appropriate regulations and enforcement mechanisms. This is mostly since product properties are defined by software that changes constantly. Major product safety hazards, accidents or cyberattacks may be discovered through existing accident reporting obligations, and in extreme cases, through the media. More subtle errors in automated driving and medical treatment, e.g., related to software bugs, disturbances related to cyber vulnerabilities or cyberattacks might never come to light but actually risk remaining invisible both for the businesses and the regulator. Consequently, decision makers and regulators may need to be aware that digital intelligence in products may be subjected to change and will never be fully controllable, taking this into account in the preparation of regulatory strategies addressing the “virtual” market.

6 Our recommendations

Based on this insight into digital regulation of industrial products we have the following policy recommendations.

Invest in mature and evidence-based regulatory frameworks on AI

The regulation of AI in industrial products seems to require more certainty that current legal frameworks provide. This is because, as the use of ML and AI provides multiple scenarios and use cases that do not easily fit into the current definition found in proposals for legislation e.g., in the proposal for the EU AI Act. Based on both the business input as well as reflections from sectoral authorities and experts, more insight needs to be created among policy makers and regulators in general on how specific intelligence is developed, applied and implemented, but above all how automated, intelligent and connected product properties can be monitored throughout the product life cycle. I.e., there is no use to set up far-reaching requirements if use cases are not covered, and if mechanisms and competence for monitoring compliance are not in place. In addition, guidance on the interpretation and application of an AI regulation will be needed. All this said, it is evident from our analysis that digital intelligence in terms of AI will always represent uncertainties which are more difficult to regulate.

Re-evaluate compliance models for products with embedded digital technologies – more focus is needed on security-by-design and approaches taking the whole product life cycle into account

Digital innovation is entirely dependent on access to and use of data. Functioning innovation is also dependent on qualitative data that is representative for the specific use case. As data are the main component of digital products, more insight is needed into data to allow traceability and auditability with respect to product characteristics. Monitoring is required because product characteristics can change with connectivity, algorithms and customisation, and thus be affected by external factors like cyberthreats. This differs from physical, non-digital, non-connected products where the features are relatively stable and where the product's characteristics can be verified more easily according to standardised product requirements.

Therefore, **security-by-design** for products and processes should be discussed to a larger extent in relation to regulatory frameworks. Security-by-design is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through measures such as continuous testing, authentication safeguards and adherence to the best programming practices. In other words, the idea is to “build in” safety and security from the very start.

Security-by-design

Security-by-design is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices

When applying regulatory techniques, it is of utmost importance that technical requirements are prepared, applied and implemented in a manner that can be followed up and verified. Clear technical regulations form the basis for good and effective compliance, both for business and for market surveillance.

New product safety enforcement strategies seem appropriate for products with embedded digital technologies. Post market surveillance needs to be complemented or enhanced by an approach enabling “continuous compliance”

Our analysis shows that the possible use cases for AI may not necessarily be adapted to international harmonisation due to unique product features resulting from increasing customisation and connectivity. This also implies, that product properties could constantly change, due to external factors increasing the risk for unintended consequences.

Many of the regulatory challenges presented in this report are acknowledged by regulatory bodies but the possible regulatory solutions risk becoming obsolete before implantation due to the fast pace of technological change.

Our evaluation is that new strategies and tools for product safety enforcement mechanisms will be needed for digital products to complement or enhance post-market surveillance. The main reason for our recommendation to closely look into this is not the increasing digital vulnerabilities as such – especially, as this has not been the focus of our analysis. Instead, we see that digital frameworks (most of them still in proposal stage) are still vague and do not necessarily provide for effective enforcement and market surveillance of digital products with changing product characteristics. The lack of clear regulatory frameworks is also the cause for uncertainty for businesses.

Based on our analysis, businesses are still confused by complex digital requirements which are hard to interpret in the case of innovative products. The broader scope of more recent regulatory objectives (i.e., more than just product safety) means that preparing, adopting and implementing legal product requirements has become more challenging. Increased regulatory certainty and capabilities for enforcement are thus required, also to address a Level Playing Field. Government bodies need to invest in new competencies covering multiple product related parameters. This means a new approach on enforcement that enables “continuous compliance”- i.e., a life-cycle perspective on the enforcement that facilitates improved capabilities for “data management and security”. The possible methods and tools for achieving a life-cycle approach to enforcement of products with embedded digital technologies depend on sector and product concerned, and should naturally be evaluated, like any other regulatory approach, on parameters such as risks, proportionality, etc., and should be developed by competent agencies.

A more coordinated regulatory impact assessment will be needed for achieving an evidence-based regulation of digital innovations, including security concerns

Finally, in terms of trade policy, we also see that technological developments and digital innovation may challenge traditional regulatory frameworks such as the World Trade Organisation Agreement on Technical Barriers to Trade (TBT-agreement), which promotes harmonisation and the use of international standards and conformity assessments schemes for functioning market access. This is because as regulatory frameworks for AI are not yet mature and international standards are not necessarily available or adapted to innovation. Further, it must be highlighted that digital frameworks differ from traditional sector-specific harmonised legislation that primarily addresses harmonisation. Cross-cutting regulatory impact analysis covering various digital dimensions will be needed to

avoid work in silos and to obtain more control of the digital market. As often pointed out “any horizontal regulation should focus on potential harms that are truly horizontal in nature”.

In general, beyond this analysis, we see a strong trend with regulatory fragmentation with a lack of international frameworks or timely standards. One consequence of this is that private regulatory initiatives (e.g., private branch standards) continue to flourish. This results in effects on a Level Playing Field with the same rules for market actors, in potential regulatory gaps and trade barriers as there is no overview of what is applicable for a certain product. The situation also complicates things for the regulators and surveillance authorities, as there are limited possibilities to gain insight and monitor the developments. Here policy makers and regulators need to step up and coordinate themselves instead of working in silos.

The National Board of Trade Sweden is the government agency for international trade, the EU internal market and trade policy. Our mission is to facilitate free and open trade with transparent rules as well as free movement in the EU internal market.

Our goal is a well-functioning internal market, an external EU trade policy based on free trade and an open and strong multilateral trading system.

We provide the Swedish Government with analyses, reports and policy recommendations. We also participate in international meetings and negotiations.

The National Board of Trade, via SOLVIT, helps businesses and citizens encountering obstacles to free movement. We also host several networks with business organisations and authorities which aim to facilitate trade.

As an expert agency in trade policy issues, we also provide assistance to developing countries through trade-related development cooperation. One example is Open Trade Gate Sweden, a one-stop information centre assisting exporters from developing countries in their trade with Sweden and the EU.

Our analyses and reports aim to increase the knowledge on the importance of trade for the international economy and for global sustainable development. Publications issued by the National Board of Trade only reflect the views of the Board.

The National Board of Trade Sweden, December 2022. ISBN: 978-91-89742-07-9



Kommerskollegium
National Board of Trade Sweden

Box 6803, S-113 86 Stockholm, Sweden
Phone +46 8 690 48 00
E-mail registrator@kommerskollegium.se
www.kommerskollegium.se