KOMMERSKOLLEGIUM
NATIONAL BOARD OF TRADE SWEDEN

Innovation, AI, Technical Regulation and Trade

Questioning the Invisible Hand in the Digital Economy

2023

Foreword

The benefits of digitalisation for trade and sustainability 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. However, due to digitalisation, product regulation now 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 contribute to products that are much more difficult to control and monitor, and as result, to regulate. At the same time these new regulatory parameters have a significant and direct effect on international trade and market access.

Digital innovation is currently being addressed by policy makers through a host of many new strategies and regulatory proposals, but the question is whether the approach taken, and regulatory techniques to be applied, are effective the purpose. Ill-adapted or non-coordinated regulatory strategies have a decisive impact for international trade and can result, not only in uncertainty, regulatory gaps or barriers but also affects the Level Playing Field for businesses.

Products with embedded digital technologies have not received special focus within the analysis of technical regulation, regulatory techniques and international regulatory cooperation- another reason why more insight on this topic is needed. This report will address whether the various new policies and available regulatory approaches used are appropriate and fit to address digital innovation in industrial goods.

Evidence-based analysis in the field of technical regulation and International Regulatory Cooperation are an integrated part of the work of the National Board of Trade Sweden and an important element in promoting the free movement of goods in the EU and strengthening a functioning multilateral trading system.[1] Insights from this field feed into our contributions on ongoing trade negotiatioDns, 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.

This 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 and Legal Adviser Felinda Wennerberg and Chief Legal Adviser Christian Finnerman.

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 Sjööker, 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 Adminis-

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

tration; 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 Syvänne, CEO & Senior Consultant – CNB Systems Ltd. The insight and input from the business reality as well as the competence provided by regulators and experts are the key to better trade policy!

Stockholm, December 2022

Anders Ahnlid

Director-General
National Board of Trade Sweden

Summary

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 trade policy frameworks, both in the EU and globally are now being seriously challenged.

This situation is created by several factors. First, new technologies and industries have increasingly moved from mass produced products that can be standardised to more customised solutions that are often supported by services and connected to the Internet. This implies 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).

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. This complicates the regulation where the new digital elements are mostly addressed with horizontal legislation, while the traditional regulatory concerns are addressed in sector specific legislation, these two not necessarily coordinated.

The objective of this study is to analyse 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 study discusses how these trends should be considered when developing technical regulation and regulatory techniques. Improved regulation for products with embedded digital technologies can address regulatory fragmentation, reduce trade barriers and thus effectively promote digital transition and trade on the EU internal market and globally.

The study provides initial insights into the extent to which regulation and regulatory techniques applied today embrace technological changes in industrial goods. The analysis is based on discussions with companies active in the fields where the use of ML and AI is more prevalent, e.g., in vehicles, medical devices and Information and Communications Technology (ICT). 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.

Our findings:

Innovation is boosting trade but may radically challenge traditional trade policy frameworks

Digital products and intelligent product features provide immense possibilities. The core of innovative digital products is software that allows and requires continuous improvements along the product's life cycle. The downside is that the potential vulnerabilities arise, and these need to be monitored. Furthermore, innovative businesses are increasingly manufacturing and delivering customised solutions. These aspects can well challenge the role of static product requirements and trade policy frameworks that refer to the importance of using international standards. Furthermore, the way standards are prepared and designed today - might be too slow to cover the fast pace of technological changes. Prospective regulation aiming to address trade barriers and smooth market access might be unable to grasp the use of products with embedded digital technologies. It should also be noted that, regulatory challenges related to innovation are often sector specific. This implies that when horizontal technologies such as AI are being addressed, much

more effective policy coordination will be needed among policy makers and regulators to avoid gaps that create uncertainty and trade barriers.

Furthermore, the digital economy not only requires a focus on regulatory techniques but also on suitable enforcement mechanisms. As a result, "continuous compliance" in terms of enforcement of "data management and security" (in addition to product safety), i.e., a life-cycle approach to enforcement is likely to become important. This motivates enhanced cross-sectoral collaboration in the field of **market surveillance** and the enforcement of product compliance.

Product or service – does it matter?

The blurring interface between digital products and services is often raised as an important parameter for regulatory uncertainty. This was not the case in our analysis in the three sectors we investigated. Instead, the challenges are often related to data, e.g., access to data (cross border, clinical trials), use of data (GDPR) and considering ML and AI in the managing of software.

The regulatory landscape has changed – Digital innovation increases regulatory complexity

Innovation that makes use of ML and AI in industrial products such as mobile phones, medical devices and vehicles adds to regulatory complexity, particularly when cyber vulnerabilities are considered.

In practice, digital regulation implies that sector specific regulations are being complemented by horizontal ones on AI, data use and cybersecurity. This creates confusion concerning how various, sometimes duplicative or conflicting, legislative instruments will or will not complement each other. Due to lack of guidance this situation results in regulatory uncertainty, but also affects the **Level Playing Field**, which requires that the same regulatory demands apply to all economic operators within the EU.

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 with the horizontal digital legitimate regulatory objectives (like cybersecurity). This could relate to terminology, including definitions of safety and risk. We have not analysed this in more detail 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 (i.e., between various groups, consumers and users).

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

The use of ML and AI in industrial products is not a new phenomenon, at least in the sectors studied in this analysis. 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.

As legal frameworks for AI products are still under development it is not clear to businesses whether their innovation will fall, e.g., under proposed AI Act in the EU. However, the proposed AI Act does not necessarily fully embrace sector-specific aspects, which creates uncertainty as companies are not able to identify their innovation in legislation.

To conclude, the use of ML and AI in products is not a temporary phenomenon. It is driven by business innovation to efficiently solve new customer needs. The constantly evolving new use cases and application areas for ML and AI are the ones that are "new", not the technology itself. However, it is the technology that creates the current regulatory challenge.

Products utilising AI – Safe and secure?

When it comes to the use of digital technology, the objective of this report has not been the identification of risks, safety gaps and other vulnerabilities other than those related specifically to cybersecurity. As result, we have not conducted a specific analysis of risks and safety gaps but instead draw upon the information provided by various stakeholders in the case studies.

The companies and regulators interviewed argued that adding ML or product AI does not automatically equal greater risk - the actual risks are dependent on several variables that are related to the AI use cases. At the same time businesses and regulators were positive towards efforts to grasp and define what "high-risk Artificial Intelligence" is. It is evident from our analysis, however, that defining what high risk AI is requires much more cross sectoral investigation.

In addition, the risk scenarios of products have been extended and broadened due to digitalisation. Vulnerabilities in digital products materialise in cyber vulnerabilities (in terms of greater attack area), privacy and personal integrity concerns (in terms of handling of data) and in effects on resilience (as many products are also used in critical infrastructure). This means that the traditional product safety perspective in regulation needs to expand to cover security (IT security), privacy (GDPR) and resilience, which are currently addressed by a multitude of approaches and regulative proposals, but not necessarily in a coordinated manner, nor with clarity.

The companies, regulators and experts we interviewed argue that the cyberthreats are widely acknowledged and regarded as a major challenge related to digitalisation, and one that is not easily addressed. One of the questions with the most uncertainty is whether there are sufficient resources and tools to truly monitor cybersecurity throughout a product's life cycle. The answer for compliance seems to lie with the policy makers and regulators who need to develop resources necessary to be able to better understand and effectively monitor the digital market.

Regulatory uncertainties and gaps

Regulatory uncertainties identified by the companies interviewed for this study are mostly related to a lack of straight forward guidance on whether their product falls under various digital frameworks (proposal for the EU AI Act), including possible duplicative requirements regarding sector specific and horizontal legislation. Other issues relate to possible contradictory requirements within sector specific and horizontal legislation. Practical examples of uncertainty are related to requirements for software up-dates and a lack of acceptance (licence) of new technology in export markets.

Concerning data, our case studies show that data-related localisation requirements vary and thus affects the terms for market access in various countries.

Businesses also highlight that to address cyber vulnerabilities there should be greater expertise among regulators and that guidance should be made available. Cyber vulnerabilities are seldom sector specific and, as mentioned earlier, 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.

Can the digital market with "virtual" products be regulated ?

The study's underlying questions are: "Who is taking responsibility for the digital market when digital regulatory frameworks are still under development?" Is there a mechanism that covers up eventual failures in terms of non-compliant products, if products are not as tangible as before and thus partly "invisible" to the regulator? What means can be used to control compliance when the tools for efficient market surveillance have been weakened? The concern, in other words is, whether the digital market of industrial goods is left to "the Invisible Hand".

Whether the digital economy "manages to regulate itself", in the absence of complete and all-embracing regulatory frameworks, is a tricky question to answer since possible regulatory failures or unintended outcomes of technological innovation in the market are not necessarily registered due to the lack of appropriate regulations and enforcement mechanisms. This situation is mostly due to product properties being defined by **software** that is constantly changing. Major product safety hazards, accidents or cyberattacks could be made known through accident reporting obligations, and in extreme cases, by the media. Subtle errors in automated driving, medical treatment e.g., related to software bugs and disturbances caused by cyber vulnerabilities or attacks, might never come to daylight but remain invisible for the regulator. In some cases, these errors could have serious consequences. Consequently, regulators need to be aware that digital intelligence can be subjected to constant change and thus be difficult to control. This needs to be considered in regulatory strategies addressing the "virtual" market. As a result, the key question is how to develop digital technical regulation that results in sufficient levels of safety, privacy, security and resilience.

The digital market with "virtual" products

Our approach highlighting the digital market with "virtual" products aims to draw attention to the fact that there is a risk that important aspects are overlooked in the digital regulation by policy makers.

Even if digital products are of course real, it is much more difficult to follow the eventual changes in the properties of these software-based goods, or assess the effects of these products to consumers and users.

Also, it is challenging to control, audit and verify changes in these products compared to traditional goods, that authorities may inspect visually, or subject to documentation control in market surveillance, with greater certainty that the essential characteristics of the products do not change over time.

To take decisions regarding digital product regulation, e.g., on AI, therefore requires that the regulator comprehend how software is used in general - and in specific **use cases**. Here the risks and effects can vary, not only between sectors, but also between specific use cases.

Based on our analysis on digital regulation we have the following policy recommendations:

Invest in mature and evidence-based regulatory frameworks on AI!

The regulation of Artificial Intelligence in industrial products requires more certainty than current legal frameworks present. This is because 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 European Regulation on Artificial Intelligence (AI Act).[2] From the case studies it can be confirmed that there are conflicts between the proposal for the horizontal AI Act and sector-specific legislation. Based on input from business stakeholders and sectoral authorities, regulators need more insight into how specific intelligence is developed, applied and implemented and above all how automated, intelligent and connected product properties can be monitored throughout the product's life cycle. That said, it is evident from our analysis that digital intelligence in the form of AI will always present uncertainties that are more difficult (if not impossible) to regulate and control.

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.

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 me-

2 In practice the definition of AI within the regulation is yet unsettled and thus it is unclear what should be regarded as AI. Until now the definition has been perceived as very broad by many stakeholders.

chanisms 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.

More coordinated regulatory impact assessment will be needed for achieving evidence-based regulation for digital innovations, including security concerns

As highlighted, digitalisation brings several new regulatory concerns. Industrial products are now required to comply with multiple policies and new proposals for regulation are in the pipeline. The analysis has revealed a lack of coordination creating difficulties due to interrelations between various horizontal and sectoral requirements. We see a need to strive for more coordinated, cross-sectoral regulatory impact assessments to identify gaps and to provide guidance to market players. Here new procedures and regulatory tools need to be analysed and developed by policy makers and regulators, including within the EU.

Trade policy frameworks are being challenged — technical regulation requires analysis

Finally, in terms of trade policy we also see that technological developments and digital innovation can 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 cross-border market access. This is because digital frameworks for AI are not yet mature and international standards not necessarily available or adapted to innovation. [3]

Although beyond the scope of this study, the National Board of Trade has observed increased regulatory fragmentation and a lack of international frameworks and timely standards. This results in private regulatory initiatives and standards that do not follow formal standardisation processes continuing to dominate[4], which may affect the Level Playing Field that has until now been supported by a structured system for technical harmonization within the EU. Here policy makers need to step up and coordinate themselves, instead of working in silos.

3 Applying international standards as a basis for technical regulation is considered as one of the corner stones to prevent and abolish Technical Barriers to Trade (TBTs) according to the WTO Agreement on Technical Barriers to Trade.

4 Standards in 5G area are one example. See also Rühlig, 2020 technical-standardisation-china-and-the-future-international-order.pdf (ui.se).

Table of contents

1 Introduction

Innovation results in markets for goods and services that are in constant flux. Digital technologies[5] and advanced materials and manufacturing have already had a major impact on the properties of industrial goods.[6]

Compared to the past, new technologies do not necessarily contribute to growth, efficiency[7] and competitiveness[8], through mass production but instead by the customisation to specific preferences and use cases[9]. Another change is that industrial systems are developed to become increasingly autonomous, following determined processes to a lesser degree or acting without human involvement.

Use case

A use case is a specific situation in which a product or service could potentially be used.

A use case is also a software and system engineering term that describes how a user uses a system to accomplish a particular goal.

Traditionally automation systems, industrial processes, transport systems, and similar systems were controlled manually by mechanical electromagnetic machines. These sys-

5 Digital technologies embrace data analytics and artificial intelligence, machine learning, robotics and automation, blockchain, IoT and interconnectivity. Advanced materials and manufacturing cover **nanomaterials**, **additive manufacturing** (3D printing) and new compounds and **polymers** (National Board of Trade Sweden, *The Fourth Industrial Revolution. Changing the trade as we know it,* 2019).

6 It can be argued that new technologies, materials and processes are starting to blur the lines between the physical, digital and biological spheres. Digital fabrication technologies, meanwhile, interact with the biological world on a daily basis. Engineers, designers, and architects are combining computational design, additive manufacturing, materials engineering, and synthetic biology to pioneer a symbiosis between microorganisms, our bodies, the products we consume, and even the buildings we inhabit. See Schwab, *The Fourth Industrial Revolution: what it means, how to respond,* WEF- 14 January 2016.

7 Emerging technologies such as **Blockchain**, Artificial Intelligence (AI), and the Internet of Things (IoT) have the potential to increase efficiency and inclusivity in global trade and diminishing the economic gap between developed and developing countries. The question is whether there are efficient and functioning regulatory frameworks these for technologies (in this report commonly called Technology) that contribute to efficient and sustainable trade.

8 See e.g., López Gonzales, J and J.Ferenz, *Digital Trade and Market Openness,* 2018.

9 See e.g., European Commission, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, Brussels, 19.2.2020 COM (2020) 64 final.

tems 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 value added in goods is increasingly generated by software, which is in many ways uncontrollable, vulnerable to manipulation and not easily monitored by regulators. As a result, analysis of the relevance of regulatory models and techniques is crucial.

The question is whether the conditions for product regulation have changed to the extent that new regulatory approaches are required, or whether the existing regulatory tools alongside with private– or self-regulation are sufficient to achieve regulatory objectives[10] and a well-functioning market. Although various analyses provide evidence of the potential benefits of new technologies[11], insight into the regulatory frameworks supporting these innovations are still scarce.

Several reports by the National Board of Trade Sweden provide evidence that regulating the digital economy is not straight forward and that the regulation of goods does not necessarily keep up with technological developments or effects generated by the use of digital solutions. Examples include 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.[12] The increasing interconnection means that as new vulnerabilities arise and complexity increases, the traditional methods for analysing risks are no longer sufficient. Furthermore, the current methods for risk analysis have difficulty handling interconnected systems. Often, they also assume that probabilities of events are known, but nowadays reality changes too quickly to collect relevant statistics.[13]

The National Board of Trade has highlighted that tools that are currently applied to address cybersecurity through regulation, such as requirements on cybersecurity certification, do not guarantee cybersecurity but only provide the means to identify cyber vulnerabilities in an ICT product at a given time, i.e., exactly when the certification has been

10 According to the TBT Agreement, WTO members shall ensure that technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade. Therefore, technical regulations shall not be more trade-restrictive than necessary to fulfil a legitimate objective, taking account of the risks that non-fulfilment would create. Such legitimate objectives are, inter alia, national security requirements; the prevention of deceptive practices; and protection of human health or safety, animal or plant life or health, or the environment. In assessing such risks, relevant elements of consideration are, inter alia, available scientific and technical information related to processing technology or intended end-uses of products (Art 2, TBT Agreement).

11 Machine learning (AI) is already used for example to improve health care, increase the efficiency of farming, and improve logistics or the customisation of various services. See: Ailisto, Neuvonen, Nyman, Halen, Seppälä: *En helhetsbild av artificiell intelligens samt en nationell kartläggning av kunnande- slutrapport*, Statsrådets kansli, 2018. Thanks to evolving computing power and ever-growing **big data**, AI promises to provide access to predictive analytics (i.e., what will happen in the future) and prescriptive analytics (i.e., how to do better in the future), meaningful insights not otherwise possible. These insights can have multiple trade applications from predictive maintenance of equipment to routing optimisation and risk management. For instance, AI can contribute to financial crime risk mitigation. Customs also use AI to predict and identify risks, thereby allocating their resources where there is more value added. See WEF & WTO, 2022.

12 See e.g., Cyberhot (msb.se), Nya risker i sammankopplade system (msb.se)

13 This is because they focus on errors in the parts of the systems, rather than problems arising from deficiencies in the interaction of such system.

carried out.[14] This can result in costly and ineffective regulation that does not result in the regulatory objective intended, like product safety or security. Poorly adapted or fragmented regulatory measures can also have a significant effect on trade by creating barriers between markets, especially if uncertainties are addressed with national or regional regulatory solutions.[15]

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[16] 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 ICT - is it possible for public entities to prepare, adopt, implement and enforce[17] regulations and standards that address vulnerabilities when product properties can change over time?

There is therefore a need to provide increase insight into whether the existing policies and main legislative initiatives actually cover essential regulatory interests and investigate whether the digital economy actually manages to regulate itself. Here we refer to the "Invisible Hand" i.e., a situation with the potential absence of regulation or regulatory guidance at the market.[18]

---

14 Many IT security experts are hesitant about the value of comprehensive and costly product certifications. Certifying a product does not make it safe, i.e., a cybersecurity certification does not necessarily remove all vulnerabilities - the risks are to a high degree dependent on where the ICT product is used. For a more comprehensive insight into cybersecurity regulation and trade see; National Board of Trade, The Cyber Effect, 2018.

15 The report *Online Trade-Offline Rules* discussed the fragmentation of the e-commerce landscape in the EU, which failed to contribute to a fully Digital Single Market. It also addresses the challenges with technological developments affecting trade and regulation (National Board of Trade Sweden 2015). *Trade Regulation in a 3D Printed World* (National Board of Trade, 2016) argued that regulation and policy have not always kept up with technological changes making it necessary to upgrade existing trade rules. "*The Cyber Effect*"- report by the Board provided evidence for that cybersecurity regulation do have trade effects and needs to be better regarded in policymaking. It also addressed the fact thar cybersecurity by regulatory measures as not straight-forward but rather complicated due to the fact that it needs to comply with several, sometimes diverging policy objectives (National Board of Trade, *The Cyber Effect — The Implications of IT-security regulation on international trade*, 2019).

16 For example, the transport sector is increasingly connected, digitalised and automated. See: *The path to automated vehicles- an introduction*, SOU 2018:16.

17 The Commission White Paper on AI acknowledges for example that existing methods for showing compliance to legislative frameworks like conformity assessment procedures for high-risk products, like verification through prior conformity assessment, might not be adapted to all AI applications and that such need to be established. As a result, the Commission presented a proposal in April 2021 for a Regulation with harmonised requirements on AI. See also Chapter 3 in this report.

18 Here also the role of self-regulation in the digital economy is particularly interesting. It could well be that the "regulation" of new and fast-moving technologies is to certain extent led by the business themselves, through private initiatives and standards. Although market forces and non-governmental action can provide valuable controls in certain regards, they cannot fully substitute for mandatory requirements. As with regulatory overhaul, there is generally little public support for voluntary or self-regulatory approaches to emerging technologies (Project on Emerging Technologies 2008). An appropriate degree of government oversight is particularly necessary to maintain public confidence in emerging technologies as many people often largely unaware of them. For example, surveys reveal that over 80% of people have heard nothing or only a little about both nanotechnology and synthetic biology. If people learn that technology risk management is substantially voluntary at the same time that they first learn about a technology, public concern would be expected to rapidly increase, as occurred significantly with biotechnology. The combination of low public awareness and polarizing debates present a challenging landscape for the socially appropriate development of nascent technologies (Mandel, G.M.2009) In real-life, however, we see that the regulation of the digital market is a combination self-regulation and public regulatory initiatives (the latter in focus in this report).

Analysing regulation in the digitalised market is not an easy task. Trends in trade including the dependence on **Global Value Chains** (**GVC**) and increased **servicification**[19] have changed the nature of trade. It is justified to say that the market for industrial goods has become less tangible, to some extent invisible. The characteristics of goods have also changed as have the paths and means by which goods are being manufactured and delivered to end-consumers. This also means that it becomes more challenging for regulators to keep track of technologies and their impacts unless there are tools for that allow for a follow-up and market surveillance with traceability, and capabilities for auditability.

Many developers of new technology argue that a change in technology does not require new product requirements but that the same regulatory objectives should apply as for "old technology". This is of course true if the product's properties, foreseeable use and eventual risk remain unchanged. Today however many products and connected services need to be addressed by several interrelated frameworks that are not necessarily coordinated.

These questions can also be analysed in relation to the existing regulatory parameters, as below.[20]

The regulatory outsets in the digital economy

Current regulatory setting	New elements	Effect on regulation?
Harmonised requirements for harmonised goods	Increased customisation?	EFFECT ON REGULATION?
Product properties static during the product life cycle	Product properties can change during product life cycle	EFFECT ON REGULATION?
Products manufactured on-site and product properties not significantly vulnerable to alterations	Products manufactured off-site (remotely), autonomously and connected product properties can be altered by third parties in the supply chain or e.g., manipulated due to cyber vulnerabilities	
Enforcement of product compliance through physical examination, documentation control, testing and certification	The product enforcement of industrial goods is still mainly based on the concept of post market surveillance, although regulatory frameworks have been complemented by requirements that consider life-cycle vulnerabilities related to software and cybersecurity	EFFECT ON REGULATION AND MARKET SURVEILLANCE?

19 Manufacturing firms use and produce more services than ever. They also sell more services, imbedded or as accompanying parts of their goods. The distinction between manufacturing and service companies has become blurred (National Board of Trade, *Everybody is in Services,* 2012, The National Board of Trade, *The Servicification of EU Manufacturing,* 2016.

20 Our baseline for the comparison of regulatory techniques is the model used in European legislation where product requirements are to a high degree harmonised among a large number of industrial products and where the core or technical regulation is made by following parameters comprising essential mandatory requirements in the Regulations (or directives), standards that provide compliance with the regulations, requirements on conformity assessment (e.g., requirements for testing and certification) and post market surveillance by authorities, see European Commission Blue Guide: The Blue Guide on the implementation of the product rules 2022 is published (europa.eu)

As part of the digitalised market, goods have become "virtual" and "invisible" as many product properties constitute of software and data managed by AI. There is thus a need to examine what these innovative technologies might mean for regulatory policy.

Drawing far-reaching conclusions concerning of the digital market constitutes a complex task. This is because the actual regulatory effects of new technologies can be difficult to trace and reveal. At the very same time, it is highly important to map out in what direction the regulation of the innovative technologies is moving. In addition, it is important to draw some tentative conclusions on whether the invisible, digitalised market seems to manage itself.[21]

1.1 Rationale and the method used

The objective of this study is to analyse how the properties of industrial goods are affected by the utilisation of new technologies such as Artificial Intelligence (hereafter AI) and the prevalence of increasing digital vulnerability[22] (especially cyber vulnerabilities). The study discusses how these changes should be considered when developing technical regulation and regulatory techniques[23] of products.

AI

Artificial intelligence (AI) refers to 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).

To achieve this objective, the Board has leaned on case studies covering interviews with businesses and business organisations, regulatory agencies and sector specific experts, complemented by a literature review.

The sectors that have been chosen to exemplify and provide tangible cases of the regulatory reality are ICT (mobiles), medical devices (software, devices for cancer treatment) and vehicles (trucks). The motivation for the choice is that these sectors are known to be advanced in the utilisation of Machine Learning (hereafter ML) and AI and they have also been pointed out as priority areas for the promotion and adoption of AI in, for example, the public sector.[24] Similarly, addressing IT-security and cybersecurity in these sectors is an important regulatory element as connected products containing software present a multitude of vulnerabilities. By this analysis, the Board wishes to generate hands-on expe-

21 The question is whether regulators can pursue the same control and have the same insight into products on the market as new product properties risk being introduced continuously, for example as part of software. It should be noted that this is a gray zone in various sectors with respect to which new product data-based features are to be regarded as "significant"- which complicates the process of determining whether new features affect product safety and security (calling e.g., for new registrations, certifications and approvals dependent on product). See also Chapter 4.

22 The objective of AI is to improve the product's properties and characteristics, but it may also present new vulnerabilities if significant safety- or security-related changes are not monitored.

23 Regulatory measures are primarily prepared, adapted and implemented to address various societal concerns such as the protection of health, safety, environment and security. Regulation also has a crucial role to facilitate trade. Here well-adapted regulatory approaches, e.g., measures that are based on best practices such as international standards and evidence-based regulations are more likely to address both regulatory concerns as well as better trade, than solutions that are limited in scope and/or prepared by a limited number of stakeholders.

24 European Commission, *White Paper- On Artificial Intelligence- A European approach to excellence and trust*, Brussels 19.2.2020

rience regarding in which manner existing regulatory frameworks and tools manage to embrace digital innovation.

It should be mentioned, however, that the main purpose of this report is to identify the eventual need to change the regulatory approaches and techniques for goods, not to evaluate regulatory outcomes, e.g., safety failures created by new technology. The regulatory challenges highlighted in the report can however be used to identify ways forward.

Furthermore, it should be observed that many digital regulatory frameworks and tools related to AI and digitalisation are new, thus not fully implemented. Also, the business perspective of AI regulation has not yet been widely studied in relation to trade and trade policy frameworks, making it an interesting domain for exploration.

1.2 Limitations

In order to draw conclusions on regulatory frameworks this analysis relies mostly on the European legal framework (EU system for technical harmonisation) although some sectors also depend on international agreements and international legal frameworks and standards. [25]

It should be noted that this analysis should not be regarded as an in-depth legal review but is instead based on a business and expert perspective on AI and cybersecurity. This is due to the lack of mature legal frameworks as several of the legal frameworks discussed are still at the draft stage.

Regarding cybersecurity, and how it is addressed in Information and Communications Technology (ICT) products, we refer the reader to our earlier analysis that provides a comprehensive explanation to the concept of cybersecurity (IT security and information security) and the implications of cybersecurity regulation for international trade. [26]

When addressing regulation, we have covered those regulations that are most often mentioned by stakeholders as being decisive for the regulation of their innovation- and the presentation of these frameworks should therefore be regarded as a baseline for understanding the sector and the effects to trade, not as a complete review or analysis of all applicable requirements for products in question. In this report the focus will be on the technical regulation of industrial goods. The discussion of other dimensions of AI, such as ethics within e.g., regulatory frameworks will be excluded.

This analysis is limited to a small number of cases meaning the findings are not necessarily representative for all industrial products. However, by studying the current situation in some sectors where AI is used it is possible to gain insight into regulatory developments and which trade policy measures might need to be taken.

25 One example of this is the vehicle sector that is covered by the UNECE WP.29 framework.

26 National Board of Trade Sweden, *The Cyber Effect. The implications of IT security regulation on international trade*, 2018

1.3 Outline

The outline of this report is as follows:

Chapter 1 provides the outsets for the analysis.

In **Chapter 2** regulatory challenges provided by the digitalised market, digital products and any trends thereof are discussed. As the introduction of AI also raises some regulatory concerns, these challenges are highlighted in Chapter 2.

AI as well as cybersecurity are addressed in many policies and legal frameworks. **Chapter 3** provides an overview of the most relevant policies and regulations (many of them still on proposal stage).

The case studies presented in **Chapter 4**, constitute the core of this analysis, and have been constructed as follows:

First, general information about the product category in question is presented (i.e., mobile phones, medical devices, vehicles). This background highlights in which manner AI is used in the product. The introduction will also reflect in which manner, if at all, AI changes the properties of goods (i.e., aspects normally covered by technical regulation).

Secondly, a sector specific legal framework for each product is presented on a generic level to provide an enhanced understanding about the product and how it is regulated (**Regulatory outset**).

Then the sector specific cases are presented (Case mobile phones, Case medical devices, Case vehicles).

Each case will start with an introduction of the type of companies and stakeholders that have been interviewed. The case then focuses on three themes:

1) **AI Technology** (i.e., how AI is applied in the sector and in which manner the stakeholders see that current regulatory frameworks address it);

2) **Vulnerabilities and risks identified and approaches to address them** (i.e., how risks related to AI are perceived by various stakeholders); and

3) **Change in regulatory parameters** (i.e., based on the views presented by various stakeholders, eventual challenges and gaps related to the regulatory technique applicable are highlighted).

At the end of the chapter, some **general conclusions are drawn based on all sectors.**

Chapter 5 highlights our conclusions and recommendations.

2 Emerging technologies, trade and regulation – trends

Fast technological development together with **digitalisation** has dramatically changed our trade patterns.

We might drive a vehicle that adjusts itself to the road and traffic flow by taking control and correcting the steering for us. In the near future we will probably more often be able to jump into a self-driving bus or see self-driving trucks operate at a construction site. We will be able to take the benefit from medical devices that can present a diagnosis of eventual health problems or perhaps even treat us independently, under the supervision of a doctor. We are already exposed to online marketing of goods and services based on our search pattern on the Internet. More and more products, systems and interconnected services will also be connected to the Internet and communicate with other products and systems throughout their life cycle.

When taking note of these developments three main issues that seem to constitute the change of play related to product properties and thus the **technical rules** used to address various legitimate regulatory concerns.

The first issue is the fact that software is the key in many innovative tech products. The collection of data managed by a computer makes decisions for us while we are driving or surfing on our mobile phone.

Secondly, many products could be regarded as services, which complicates the evaluation of what types of requirements apply to them and blurs who is legally responsible for a product or service.

Finally, automation, product connectivity and intelligent self-instructing elements result in a situation where product properties are not necessarily static but change over time and, most importantly, increase the vulnerability for unforeseeable manipulation.

In other words, the parameters that normally guide product regulation with respect to the level of protection, and which result in technical regulation and standardised requirements could now be challenged![27] Until now the whole regulatory process was designed to

27 Naturally there are several product groups that need to be monitored throughout their life cycle, like vehicles, foodstuff, machinery and lifts to mention several. The foreseeable use, often referred to in legislation, has earlier resulted in more or less standardised product requirements without the need to acknowledge that hacking may affect a line of products simultaneously.

Product requirements as we know it

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 applied 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 can 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).

be linear and mechanistic, using technical regulation, standards and conformity assessment for compliance and (post) **market surveillance** to verify that products on the market fulfil legal requirements.

It should also be noted that in the past decision-makers and regulators had more time to study a specific issue and thereafter develop the necessary response or appropriate regulatory framework. However, today the development of technology is a constantly moving target. Given the rapid pace of change and broad impacts, legislators and regulators are being challenged to an unprecedented degree. As a result, there is a need to collaborate with businesses and find agile ways to respond to developments on the market without putting the legitimacy of the legislative process at risk. This development can, however, be challenged by private regulation, for example sectoral or regional standards in case the public bodies fail to respond to regulatory needs. This can in turn risk regulatory fragmentation with trade effects, like technical barriers to trade, as a result.[28]

28 See also: WTO/WEF, The Promise of TradeTech- Policy approached to harness trade digitalisation, 2022.

2.1 New technologies — regulative concerns

Emerging technologies are transforming the properties of many products on the market in order to provide customers with both improved features and services. [29]

When analysing new technology from a consumer perspective, products found on the market provide following characteristics:[30]

- They not only contain software but also interact with software located in the cloud (e.g., IoT platform) or with software installed on third-party smart devices (e.g., applications installed on smartphones or tablets).
- They are connected to the Internet and/or to other products.
- They can be used to access services.
- They can be used to process and collect personal and non-personal (meta)data.
- Their software consists partly of adaptive algorithms and their software can be updated (remotely) after their placement on the market.
- They allow a higher degree of human-product interaction.

The most obvious risks that have been identified are[31] related to cybersecurity, personal security and to mental health. In this analysis the focus will be on cybersecurity as only this domain has the strongest link to technical regulation.[32] Cybersecurity vulnerabilities in heavy vehicles/trucks,[33] medical devices and mobile phones are also widely acknowledged by both businesses and regulators. As already mentioned, the emphasis in this report is not on identifying risks in new technology, from a product safety perspective, but rather on examining the regulatory technique - i.e., whether existing regulatory techniques are adapted to products and systems, the properties of which can change over time. Still, the new product properties provided by **digitalisation** and highlighted above can be considered when analysing the regulatory outsets for AI.

---

29 This is, as highlighted in our case studies (see Chapter 4), also the rationale for business to apply intelligence such as AI and ML.

30 The Consumer Product Safety Network has looked into the question of new tech from the consumer perspective and has leaned on the definition of safe products found in the General Product Safety Directive (GPSD) to identify digital characteristics. §2b in the directive defines a safe product as 'any product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular: (i) the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance; (ii) the effect on other products, where it is reasonably foreseeable that it will be used with other products; (iii) 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; (iv) the categories of consumers at risk when using the product, in particular children and the elderly "

31 Opinion of the Sub-Group on Artificial Intelligence, Connected Products and other Challenges in Product Safety to the Consumer Safety Network, European Commission.

32 Personal security and mental health are covered by other domains.

33 The cybersecurity regulation for the transport sector as whole consists of fragmented and complex legislation. Different legal spaces serve different purposes, with requirements that are often directed at different types of actors and activities. While there are no harmonised cybersecurity requirements between different legal spaces, there are a number of recurring measures. These include reporting activities to competent authorities, assessing risks and taking safety measures, as well as reporting safety incidents (Wennberg, Zouave, Jaitner, *Law and cybersecurity in smart road traffic*, FOI 2019-12-31). The fact that risks are increasing especially for heavy vehicles is related to the fact that different third-party superstructures add to the interfaces connecting to the rest of the world. According to recent research, it its estimated that **Denial-of-Service attacks** pose the biggest threat. See e.g., Valassi & Karresand, Cyber Physical Vulnerabilities in Heavy Vehicles, FOI, December 2020.

3. Existing policies and legal frameworks to address artificial intelligence and cyberthreats

3.1 Important legislative initiatives in the EU and beyond

There are many arguments that support **automation** and the intelligence provided by ML and AI as creating benefits for citizens and society. At the same time there seems to be an uncertainty about what AI is and does when it is applied, especially concerning the unpredictability and uncontrollability of its application. The regulation of AI can thus be considered as part of the development of public sector policies and laws for promoting and regulating AI. Regulation is considered necessary to both encourage AI and manage associated risks. Public administration and policy considerations generally focus on the technical and economic implications and on trustworthy and human-centered AI systems.

The development of public sector strategies for the management and regulation of AI is deemed necessary at the local, national, and international levels and in a variety of fields, from public service management and accountability to law enforcement, the financial sector, robotics, **autonomous vehicles** (**AV**), the military and national security, and international law. [34]

AI matters for trade because it can contribute to greater productivity, better supply chain management and lower trade costs. At the same time, trade, and trade policy, matter for the diffusion of AI systems because they enable access to goods, services, people and data.[35]

34 The European Industrial Strategy (2021 250 final) and European Commission Communication on EU Trade Policy (2021 66 final) highlight the importance of addressing digitalisation transition.

35 OECD, *Artificial Intelligence and International Trade: Some Preliminary Implications*, Working Party of the Trade Committee, 15-16 December 2021, TAD/TC/WP (2021)22

Automation, Algorithms, Machine Learning (ML), Deep Learning and AI — defined

Automation is the process of using physical machines, computer software and other technologies to perform tasks that are usually done by humans.

Industrial automation is the process of automating physical processes using physical robots and special control systems. A vivid example of this is a car factory with a very high level of autonomy. On the other hand, when people talk about automation in general, they are usually referring to software automation.

Software automation is using software to perform tasks people do with computers. There are numerous branches (types, trends) of software automation: test automation, robotic process automation, and many others.

How about AI, could it be considered automation?

Artificial Intelligence (AI) is often confused with automation, yet the two are fundamentally different. Automation has been around for some time and is probably so integrated into most business operations that it is not obvious. The main difference is that AI mimics human intelligence decisions and actions, while automation focuses on streamlining repetitive, instructive tasks. As a result, the regulatory challenge for automation is totally different as automation can be standardised. Another way to put it is that automation is an application of technology while AI is a new technology.

AI and **Machine Learning (ML)** 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. **Deep learning** is a subfield of machine learning, and neural networks make up the backbone of deep learning algorithms.

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 can 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.

ML is used in web searches, spam filters, credit scoring, fraud detection, stock trading, drug design and many more applications. ML algorithms may help to solve a wide array of problems, ranging from predicting how capable a credit applicant is of repaying a loan, identifying and labelling objects in images or videos, classifying patterns in human cells, converting written text to spoken forms, classifying malware, etc.

The capabilities of applications relying on algorithms depend, however, on the sophistication of the algorithms (from simple to deep learning systems). Somewhere here we are also able to evaluate the level of complexity, sophistication and unpredictability of the outcomes that are classified as **Artificial Intelligence**.[36] 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 IoT applications.)

36 This in turn is related to an algorithms' decision-making ability and where supervised learning can be evaluated to different degrees by looking into aspects such as data, testing and decision models, identifying errors that may be led to biased or harmful effects.

For the consumer the benefits can mean improved healthcare, and e.g, fewer breakdowns of household machinery. For business, it promises the new generation of products like machinery for transport and farming; regarding public interest, it reduces the cost of providing services in the fields of transport, education, and waste management. Moreover, it also provides sustainability gains[37] in terms of climate change mitigation.[38]

We have also witnessed some poor outcomes of AI in e.g., vehicles.[39] Here it is important to highlight that many such vehicles are characterised as **autonomous**, which is not correct, as fully autonomous vehicles have not been yet put onto the market.[40]

Another example of a poor outcome of AI is that in 2017, Microsoft's chatting bot Tay had to be shut down after 16 hours because it became racist, sexist, and denied the Holocaust.[41] These and other examples have fuelled a variety of concerns about the accountability, fairness, bias, autonomy, and due process of AI systems. Bakardieva Engelbrekt et. al. (2020) e.g., describe the developments in terms of a *technology shift* that the EU needs to address actively via strong collaboration by the Member States, given that the developments are not uniform, but rather spread over a number of policy areas and engage a variety of stakeholders. The technology shift presents several additional challenges. It can be expected to have an uneven impact on different groups in society. Although the technology shift is a global phenomenon, its effects are local which needs to be considered, including by the public sector, especially as authorities and public bodies might find it difficult to manage any potentially negative fallouts.

"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." [42]

Furthermore, there is a connection between AI and cybersecurity. Experts believe that AI and ML have both negative and positive effects on cybersecurity. AI algorithms use training data to learn how to respond to different situations. They learn by copying and adding

37 Naturally digitalisation also has sustainability challenges, in terms of e.g., the growing amount of e-waste and increasing volumes of toxic chemicals released into the environment. Higher interconnectivity leads to more complex security risks.

38 European Commission, White Paper on Artificial Intelligence- A European approach to excellence and trust, Brussels, 19.2.2020 - COM (2020) 65 final. See also Vinuesa & Azizpour ,2020 The role of artificial intelligence in achieving the Sustainable Development Goals | Nature Communications and IPCC Intergovernmental Panel for Climate Changehttps://report.ipcc.ch/ar6wg3/pdf/IPCC_AR6_WGIII_FinalDraft_FullReport.pdf

39 Deamer. K, "What the First Driverless Car Fatality Means for Self-Driving Tech" (*Scientific American*, 1 July 2016) www.scientificamerican.co/rticl/hat-the-first-driverless-car-fatality-means-for-self-driving-tech 14 February 2019; Tesla Motors statement (30 June 2016) www.teslamotors.co/n_G/lo/ragic-loss

40 Manufacturers are often clear about this in the vehicle instructions but not necessarily in marketing. In the disclaimer Tesla has with driver approval it is made clear that it is not a self-driving car, and which responsibilities are the drivers'.

41 Tay was an AI Chat Bot that was originally released by Microsoft Corporation via Twitter on March 23, 2016; it caused subsequent controversy when the bot began to post inflammatory and offensive tweets through its Twitter account, causing Microsoft to shut down the service only 16 hours after its launch.

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

additional information as they go along.[43] AI can be used for threat hunting, vulnerability management, data centres and network security.[44]

The emerging regulatory and policy landscape surrounding artificial intelligence (AI) in jurisdictions around the world is not a totally unexplored field, although the regulation of AI can still be regarded as in its infancy. As Gesley et. al. have explored, AI is regulated in many markets,[45] and they argue that the country surveys look at various legal issues, including data protection and privacy, transparency, human oversight, surveillance, public administration and services, autonomous vehicles, and lethal autonomous weapons systems, with the most advanced regulations being found in the area of autonomous vehicles, in particular the testing of such vehicles.

Regulative initiatives exist also on a more horizontal level internationally:

43 Attacks are becoming more and more dangerous despite the advancements in cybersecurity. The main challenges of cybersecurity include geographically-distant IT systems—geographical distance makes the manual tracking of incidents more difficult. Cybersecurity experts need to overcome differences in infrastructure to successfully monitor incidents across regions. Manual threat hunting—can be expensive and time-consuming, resulting in more unnoticed attacks. The reactive nature of cybersecurity means—companies can resolve problems only after they have already happened. Predicting threats before they occur is a great challenge for security experts. Hackers often hide and change their IP addresses and use different programs like Virtual Private Networks VPN, **Proxy servers** and more. These programs help hackers stay anonymous and undetected.

44 There are also some limitations that prevent AI from becoming a mainstream security tool, e.g., Resources—companies need to invest a lot of time and money in resources like computing power, memory, and data to build and maintain AI systems; and Data sets—AI models are trained with learning data sets. Security teams need to get their hands on many different data sets of malicious codes, **malware** codes, and anomalies. Some companies just do not have the resources and time to obtain all of these accurate data sets; Hackers also use AI—attackers test and improve their malware to make it resistant to AI-based security tools. Hackers also learn from existing AI tools to develop more advanced attacks and attack traditional security systems or even AI-boosted systems. **Neural fuzzing** is the process of testing large amounts of random input data within software to identify its vulnerabilities. It leverages AI to quickly test large amounts of random inputs. However, it has also a constructive side. Hackers can learn about the weaknesses of a target system by gathering information with the power of neural networks. Microsoft developed a method to apply this approach to improve their software, resulting in a more secure code that is harder to exploit.

45 Many countries have developed or are in the process of developing national AI or digital strategies and action plans. Canada was the first country to launch such a national AI strategy in 2017. The strategies and action plans highlight, among other things, the need to develop ethical and legal frameworks to ensure that AI is developed and applied based on the country's values and fundamental rights. Many countries have established specific commissions to investigate these issues. However, apart from the EU, no jurisdiction has yet published such specific ethical or legal frameworks for AI. In December 2018, an expert group from the European Commission released draft AI ethics guidelines that set out a framework for designing trustworthy AI.

The evolvement of AI regulation — Memory Lane

In early 2015, the United Nations Interregional Crime and Justice Research Institute (UNICRI) established a centre on AI and robotics to "help focus expertise on Artificial Intelligence (AI) throughout the UN in a single agency.[46] The International Telecommunication Union (ITU) on the other hand is a specialised agency of the UN for information and communication technologies and has become one of the key UN platforms for exploring the impact of AI.[47]

The development of a global governance board to regulate AI development was suggested as early as 2017. [48] In December 2018, Canada and France announced plans for a G7-backed International Panel on Artificial Intelligence, modelled on the International Panel on Climate Change, to study the global effects of AI on people and economies and to steer AI development. In 2019 the Panel was renamed the Global Partnership on AI, but it is yet to be endorsed by the United States[49]. However on January 7, 2019, following an Executive Order on Maintaining American Leadership in Artificial Intelligence, the White House's Office of Science and Technology Policy released a draft Guidance for the Regulation of Artificial Intelligence Applications, which includes ten principles for United States agencies when deciding whether and how to regulate AI. [50]

When it comes to international initiatives the OECD Recommendations on AI[51] were adopted in May 2019, and the G20 AI Principles in June 2019. In September 2019[52] the World Economic Forum issued ten 'AI Government Procurement Guidelines'. [53] In February 2020, the European Union published its draft strategy paper for promoting and regulating AI. [54] At the United Nations, several entities have begun to promote and discuss aspects of AI regulation and policy, including the UNICRI Center for AI and Robotics.

In Europe a major step forward was taken in 2018 when the European Commission adopted an AI strategy. The Commission also appointed 52 experts to a High-Level Expert Group on AI (AI HLEG) tasked with making policy and investment recommendations and offering guidance on ethical issues related to AI use in Europe.[55]

---

46 UNICRI signed the host country agreement for the opening of its Centre for Artificial Intelligence and Robotics in The Hague, the Netherlands, in September 2017. This Centre is focused on "understanding and addressing the risks and benefits of AI and robotics from the perspective of crime and security through awareness-raising, education, exchange of information, and harmonisation of stakeholders."3 UNICRI has developed a large international network of stakeholders with whom it collaborates, including the International Criminal Police Organisation (INTERPOL), the International Telecommunications Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE), the Foundation for Responsible Robotics, the World Economic Forum, Centre for Future Intelligence, and many more.

47 The ITU website states that it "will provide a neutral platform for government, industry and academia to build a common understanding of the capabilities of emerging AI technologies and consequent needs for technical standardisation and policy guidance".

48 Boyd, Matthew, Willson Nick (2017-11-01) *Rapid developments in Artificial Intelligence: How might the New Zeeland government respond?* Policy Quaterly 13 ④

49 The World Has a Plan to Rein in AI—but the US Doesn't Like It | WIRED

50 Convington- Inside Tech Media, AI Update: White House Issues 10 principles for Artificial Intelligence Regulation, 2020. While there is current no federal regulation of AI in the U.S. regulators have sent a message that AI regulation is on the Horizon, see e.g., U.S. Artificial Intelligence Regulation Takes Shape (orrick.com)

51 OECD Principles on Artificial Intelligence - Organisation for Economic Co-operation and Development

52 G20 ***Ministerial Statement on Trade and Digital Economy*** (PDF). Tsukuba City, Japan: G20. 2019

53 WEF_Guidelines_for_AI_Procurement.pdf (weforum.org) Cologny/Geneva WEF, 2019

54 European Commission, White Paper: On Artificial Intelligence — A European approach to excellence and trust). Brussels. 2020. p. 1

55 In 2019, HLEG published the document "Ethics Guidelines for Trustworthy AI", not meant to provide legal advice or guidance on compliance with applicable laws (Bakardjieva et. al, 2020).

3.2 Specific policies and regulatory initiatives in the EU with a bearing on the regulation of AI

The use of new technologies is well embraced by various policy initiatives that involve regulation. In its White Paper on AI from 2020, the European Commission presents an important outset that outlines the essentials both with respect to activities promoting innovation[56] and measures to create trust in solutions to be used. It highlights, based on the Guidelines of the High-Level Expert Group on AI key requirements for AI, i.e., Human agency and oversight, Technical Robustness and safety, Privacy and governance, Transparency, Diversity, Non-discrimination and fairness, Social and environmental wellbeing, and Accountability. Further the paper, with specific relevance for this study, examines regulatory approaches, clearly pointing out areas where the legislative frameworks could be improved to address risk and situations.

When it comes to cybersecurity, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented in 2019 the new EU Cybersecurity Strategy. As a key component of other policies such as Shaping Europe's Digital Future, the Recovery Plan for Europe and the EU Security Union Strategy, this strategy aims to bolster Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The objective is also for the EU to step up globally with respect for regulation and standards while strengthening international cooperation.[57] The strategy is followed by several legislative tools, e.g., proposals to address both the cyber and physical resilience of critical entities and networks: the Directive on measures for a high common level of cybersecurity access in the Union (revised NIS Directive or 'NIS 2'), and a new Directive on the resilience of critical entities.

Based on our discussions with stakeholders (see Case studies) the most relevant legislative acts and regulatory initiatives for the study are divided into three main areas

I) **Requirements on AI;**

II) **Legislation related to data;**

III) **Legislation related to cybersecurity; and**

IV) **Sector specific regulatory frameworks for products, including software (presented in Chapter 4 of this study).**

As our inventory, below, clearly shows, the existing digital regulatory framework is far from mature – legal proposals in many cases are at the proposal stage or have just been implemented. Consequently, an effort to try to highlight the possible effect of interrelations between frameworks (horizontal and sector specific) is not realistic - in this study we will rely on the perception by experts expressed in the case studies.

56 Examples are actions to work with Members States to foster the development and use of AI, efforts on research and innovation, a Skills Agenda to fill competence shortages, focus on SMEs, promotion the adoption of AI by the public sector (especially in the areas of health care and transport where there are already specific rules within the acquis. Securing access to data and computing infrastructures, Fostering international alliances especially with like-minded countries and identification the elements of an ecosystems of trust by proper regulatory framework for AI.

57 See: New EU Cybersecurity Strategy (europa.eu)

Regulation of Artificial Intelligence

The proposal for a European Regulation of AI

In April 2021 the European Commission put forward a proposal for a regulation of AI that recognises the need to integrate product safety in the existing sector – specifically harmonised with legislation in the EU's **New Legislative Framework** (**NLF**)[58] concerning, for example machinery, medical devices and toys. By this means the Commission has initiated harmonised rules for AI with the aim of strengthening the competitiveness and functioning of the internal market and at the same time addressing risks that new technology can bring. It involves, among other things, risks in connection with the placing on the market, commissioning and the use of systems with AI (AI systems).

The proposal would require providers and users of high-risk AI systems to comply with rules on data and data governance; documentation and record-keeping; transparency and provision of information to users; human oversight; and robustness, accuracy and security. The high-risk list includes systems used for remote biometric identification systems, safety in **critical infrastructure**, educational or employment purposes, eligibility for public benefits, credit scoring, and dispatching emergency services. Some AI systems, such as those used for law enforcement, immigration control and the administration of justice are deemed high risk.

The proposal for an AI Regulation excludes certain components, products and systems from the application of the majority of the provisions in the regulation. High-risk AI systems that are safety components of products or systems, or which are themselves products or systems, and fall within the scope of certain acts, only have to comply with article 84 of the AI Regulation, which concerns evaluation and review. The relevant acts include those related to, for example, motor vehicles, meaning that the AI Regulation would not apply in its entirety to vehicles/cars addressed in this study.[59] However, the ex-ante essential requirements for high-risk AI systems set out in the proposal for a regulation will have to be taken into account when adopting relevant implemented or delegated legislation under those acts. The rationale was supported by a broad consultation that provided the following arguments.

There was a request for a narrow, clear and precise definition of AI. Stakeholders also highlighted that besides the clarification of the term of AI, it is important to define 'risk', 'high-risk', 'low-risk', 'remote biometric identification' and 'harm'. Most of the respondents are explicitly in favour of the risk-based approach. Using a risk-based framework was considered a better option than blanket regulation of all AI systems. The types of risks and threats were to be based on a sector-by-sector and case-by-case approach. Risks should also be calculated considering the impact on rights and product safety.

Concerning the approach, the initial options varied from an EU legislative instrument setting up a voluntary labelling scheme to a Horizontal EU legislative instrument establishing mandatory requirements for all AI systems, irrespective of the risk they pose. However, the Commission settled for an ambitious, middle way approach meaning a horizontal EU legislative instrument following a proportionate risk-based approach + codes of conduct for non-high-risk AI systems.

58 To improve the internal market for goods and strengthen the conditions for placing a wide range of products on the EU market, the New Legislative Framework was adopted in 2008.

59 Article 2 of the proposal for an AI Regulation.

Artificial intelligence system (AI system) as in the proposed Regulation on Artificial Intelligence (AI Act)

Software as developed by using one or more of the techniques and methods listed in Annex I of the proposed Regulation, which can, for a given set of human-defined goals, generate results in the form of content, predictions, recommendations or decisions that influence the environment as the system interacts with.

The techniques listed in Annex I are as follows:

Methods of machine learning, including supervised, unattended and reinforced learning, using a variety of approaches, including deep learning.

Logic and knowledge-based methods, including knowledge representation, inductive (logical) programming, knowledge bases, inference and deduction motors, (symbolic) reasoning and expert systems.

Statistical methods, Bayesian calculation, search and optimisation methods, and thus a very large set of "smart methods" used in software development.

High-risk AI systems include those intended to be used as safety components of products that are already regulated under existing product safety law, including machinery, toys and medical devices. In addition, the legislation specifically defines certain stand-alone AI systems as high risk when they pose special risks to established fundamental rights.

The proposal for the AI Regulation can be seen as a positive initiative for addressing potential risks related to new technology. The approach with harmonised requirements adapted to the risk level of a product also has the potential to promote innovation. However, as the proposal relates to several other legislative acts [60] there is a need for clarity and predictability. For instance, it must be clear for companies when their products fall under the scope of the legislation as well as how the requirement in the regulation relates to other legislative acts, such as, for example, the GDPR. It is also important that initiatives such as the proposed AI Regulation take into account rules and recommendations in third countries and clearly includes an ambition for information exchange and cooperation with third countries in order to facilitate global trade.[61] The jurisdiction of the regulation covers providers of AI systems in the EU irrespective of where the provider is located, as well as users of AI systems located within the EU, and providers and users located outside the EU "where the output produced by the system is used in the Union." This "effects" test potentially extends the law's reach to companies without a market presence in the EU but that use AI systems to process data about EU citizens.

Regulation of Data

General Data Protection Regulation (GDPR)

Another important legislation with regards to AI is the General Data Protection Regulation (GDPR). Although the GDPR does not specifically regulate AI and does not include

60 The Swedish Civil Contingencies Agency has evaluated e.g., that the proposed act has overlaps with GDPR, NIS, NIS 2.0, the Regulation on digital operational resilience for the financial sector (DORA) and the Security Protection Act in Sweden (MSB 2021-06424)

61 National Board of Trade Sweden, 'Remiss av kommissionens förslag till förordning om harmoniserade regler för artificiell intelligens', (2021, Dnr 2021/00825-).

concepts such as AI and autonomous systems[62], the regulation is still highly relevant in the context of AI.

The GDPR has been applicable from 2018 and contains rules relating to the protection of personal data. According to GDPR, the processing of personal data must follow certain principles. These principles include, for example, that personal data must be processed lawfully, fairly and in a transparent manner in relation to the person the data concerns. Moreover, that data must be collected for specified, explicit and legitimate purposes and be limited only to what is necessary. The processing must also have a legal basis. The processing can, for instance, be based on consent from the person the data concerns, necessary for the performance of a contract or necessary for compliance with a legal obligation.

Given the importance of data processing for AI, it is easy to see why the provisions of the GDPR are relevant in the context of AI and can have an impact on the possibility to use it. A study from the European Parliamentary Research Unit (EPRS) concludes that it is possible to use AI in a way that is in accordance with the rules in the GDPR. However, at the same time, the study points out that there is a lack of clarity on the relation between GDPR and AI, and that provisions on AI are often vague and open-ended. This risks difficulties for companies, not least SMEs.[63]

Regulation on the free flow of non-personal data (FFD)

As an integral part of the EU Digital Single Market initiative, the Regulation on the free flow of non-personal data (FFD) aims at removing unjustified barriers to the free movement of non-personal data in the EU. FFD applies to the processing of electronic data other than personal data. The Regulation defines non-personal data in opposition to personal data, as laid down by the GDPR. Examples of non-personal data can be data in the finance sector or data which are aggregated to the extent that individual events are no longer identifiable. The FFD lays down a prohibition against data localisation requirements for non-personal data.

The proposal for a Data Act

The European Commission has also introduced an initiative called the Data Act, which aims to facilitate the access to end-use of data, including business-to-business and business-to-government, transactions, as well as review the rules on the legal protection of databases. The initiative strives to find a balance between the rights to access data and incentives to invest in data. The Commission has developed an inception impact assessment and held a consultation from June to September 2021.[64]

The initiative aims to increase the access to and further use of data so that more actors, both private and public, can benefit from, for example, Big Data and Machine Learning. This includes both the right to use data in value chains as well as the use of data for public interests. The initiative will, among other things, consider issues related to the ability of the public sector to use privately held data, acquire data and share data between busi-

62 Scientific Foresight Unit (STOA), European Parliamentary Research Unit (EPRS), 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530>, p. 35.

63 Scientific Foresight Unit (STOA), European Parliamentary Research Unit (EPRS), 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020 https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)641530, p. III.

64 European Commission, 'Data Act & amended rules on the legal protection of databases' https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en

nesses, as well as examine how to establish more competitive markets for cloud computing services.[65]

The proposal for the Data Act includes:

- Measures to allow users of connected devices to gain access to data generated by them, which is often exclusively harvested by manufacturers; and to share such data with third parties in order to provide aftermarket or other data-driven innovative services.
- Measures to rebalance negotiation power for SMEs by preventing the abuse of contractual imbalances in data sharing contracts. The Data Act will shield them from unfair contractual terms imposed by a party with a significantly stronger bargaining position.
- Means for public sector bodies to access and use data held by the private sector that is necessary in exceptional circumstances, particularly in the case of a public emergency, such as floods and wildfires, or to implement a legal mandate if data are not otherwise available. Data insights are needed to respond quickly and securely, while minimising the burden on businesses.
- New rules allowing customers to effectively switch between different cloud data-processing services providers and putting in place safeguards against unlawful data transfer.

In addition, the Data Act reviews certain aspects of the Database Directive[66] which was created in the 1990s to protect investments in the structured presentation of data. Notably, it clarifies that databases containing data from Internet-of-Things (IoT) devices and objects should not be subject to separate legal protection. This wi[67]ll ensure they can be accessed and used.

The Proposal for a Regulation on European data governance (Data Governance Act)[68]

The Proposal for a Data Governance Act suggests the first of a set of measures announced in the 2020 European strategy for data. The instrument aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. The initiative is especially important as it supports AI by promoting branch-specific data pools.

It should be noted that while the Data Governance Act (DGA) aims to strengthen the single market's governance mechanism and establishes a framework to facilitate general and sector-specific data-sharing, the Data Act concerns the actual rights concerning the access to and use of data.

65 European Commission, 'Inception Impact Assessment' (Ref. Ares (2021)3527151 - 28/05/2021), p. 1-3.

66 Directive 96/9 on the legal protection of databases.

67 It has been highlighted that several other regulations are on their way which will regulate how data is to be provided, functions and resources in products and that are applicable to specific sectors. The objective of these is to benefit the digital economy by providing third parties access to data and services of manufacturers of products. Here some companies see risks related to existing requirements on safety and cybersecurity and in the development of these techniques. The outcome is still uncertain, however, as the legislation is still under development.

68 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

Cybersecurity vs Information Security

With an increasing number of internet-connected devices and programs in the modern business, combined with the increased deluge of data -- much of which is sensitive or confidential -- the importance of cybersecurity continues to grow. The growing volume and sophistication of **cyberattacks** and attack techniques compound the problem even further.

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 can 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 report, 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)

Cybersecurity regulation

The Directive on the security of network and information systems (NIS-directive) and (NIS2- directive)

The NIS Directive (2016/1148) was the first EU-wide legislation on cybersecurity. The directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring[69]:

- Member States' preparedness, by requiring them to be appropriately equipped. For example, with a competent national NIS authority and a Computer Security Incident Response Team (CSIRT),
- Cooperation among all the Member States, by setting up a **Cooperation Group** to support and facilitate strategic cooperation and the exchange of information among Member States.
- A culture of security across those sectors that are vital for our economy and society and that rely heavily on **Information and Communications Technologies** (**ICTs**), such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the new Directive.

69 The NIS Directive was approved in 2016 and has been directly applicable in EU Member States since 2018.

The aim of the NIS Directive was to create an overall higher level of cybersecurity in the EU. The directive significantly affects digital service providers (DSPs) and operators of essential services (OESs). The directive has three parts:

1. National capabilities: EU Member States must have certain national cybersecurity capabilities, e.g., they must have a national CSIRT, perform cyber exercises, etc.

2. Cross-border collaboration: Cross-border collaboration between EU countries, e.g., the operational EU CSIRT network, the strategic NIS cooperation group, etc.

3. National supervision of critical sectors: EU Member states must supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online marketplaces, cloud and online search engines)

In 2020, the European Commission proposed an expansion of the NIS-directive.[70] The update of the NIS-directive was initiated because of an increasing degree of digitalisation and the rising number of cyber threats at the global level. [71]

The proposed NIS 2 directive obliges more entities and sectors to take measures and increasing the level of cybersecurity in Europe. The objective of the NIS 2 directive is to:

Include more sectors that are critical to the functioning of the internal market;

Harmonise Member States' implementation of the NIS with respect to identification, reporting, safety measures and supervision; and

Expand cooperation between Member States.

On 13 May 2022, the European Parliament and the Council reached a political agreement on NIS2. Once adopted, NIS2, will replace the current NIS directive.[72]

It could be said that the NIS-framework provides a holistic **Information Security** approach on the societal level by targeting critical sectors while the aspects related to the technical regulation of ICT are to be found in the EU Cybersecurity Act, which provides an EU-wide cybersecurity certification, see below.

The EU Cybersecurity Act

The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services and processes and provides a permanent mandate for the EU Agency for cybersecurity ENISA to establish and maintain the European cybersecurity certification framework and to increase operational coordination within cybersecurity in the Union.

Certification plays a crucial role in increasing trust and security in important products and services for the digital world. At the moment, a number of different security certification schemes for ICT products exist in the EU. However, without a common framework for EU-wide valid cybersecurity certificates, there is an increasing risk of fragmentation and barriers between Member States.

70 Directive (EU) 2016/1148 of the European Parliament and of the Council on 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

71 https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985.

72 https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

The certification framework will provide[73] EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. The framework will be based on an agreement at the EU level regarding the evaluation of the security properties of a specific ICT-based product or service. It will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements.

In particular, each European scheme should specify:

- the categories of products and services covered;
- the cybersecurity requirements, such as standards or technical specifications;
- the type of evaluation, such as self-assessment or third party; and
- the intended level of assurance.

The assurance levels are used to inform users of the cybersecurity risk of a product, and can be basic, substantial, and/or high. They are commensurate with the level of risk associated with the intended use of the product, service or process, in terms of probability and the impact of an accident. A high assurance level would mean that the certified product passed the highest security tests.[74]

The resulting certificate will be recognised in all EU Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

The proposal for a Cyber Resilience Act

The European Commission has also in its work programme for 2022 stated that the Commission will develop a Cyber Resilience Act establishing common cybersecurity standards for products. The aim with this legislation is to protect society from increased risks related to for example, the hacking of products as a result of the increased reliance on digital solutions.[75] According to the European Commission, the Cyber Resilience Act will complement product rules under the Radio Equipment Directive and would cover tangible digital products (wireless and wired) and **non-embedded software**, including the whole life cycle of products.[76] The proposal for the Cyber Resilience Act was published in September 2022, together with an impact assessment.[77] A public consultation was held from 16th March to 25th May 2022. The act could be the first step towards requirements concerning responsibility for the whole life-cycle of a product.

73 The European Union aims to develop a framework of cybersecurity certification schemes demonstrating that certified ICT solutions have the right level of cybersecurity protection for the European Digital Market. Several cybersecurity certification schemes are under development: One scheme, covering ICT products, and called "EUCC", is almost ready. It is based on an existing international scheme called "Common Criteria". There is a second scheme covering Cloud services (the "EUCS" scheme) and a third one on 5G networks (the "EU5G").

74 It is important to understand that this applies only for the specific moment, i.e., a snapshot of the situation on a given time.

75 European Commission, Commission Work Programme 2022, COM(2021) 645 final, com2021_645_en.pdf (europa.eu), page 5 and annexes com2021_645-annex_en.pdf (europa.eu).

76 Call for evidence for an impact assessment, Ref. Ares (2022)1955751 - 17/03/2022.

77 Cyber Resilience Act — new cybersecurity rules for digital products and ancillary services (europa.eu)

Remarks

As can be understood from the rough legal inventory there are still only a few established frameworks related to AI, data use and cybersecurity on the horizontal level. GDPR and the NIS-frameworks are the most established. Considering that we have not made a more thorough analysis of the legislation or their interconnections we evaluate that the frameworks that are most decisive for market access are those to be found in sector specific product legislation. These will be presented in the case studies.

Proposals such as the proposed AI Act in the EU – yet to be agreed on and adopted- make it difficult to evaluate the effects and impact at this stage.

Framework legislation (legislation on a horizontal level) such as data and cybersecurity – needs to interact with sector-specific product legislation – but how will this work in practice? There definitely will be a need for clear definitions and guidance (documents) concerning the application of the legislation to avoid ambiguity (in the interpretation).

A major challenge is regulating aspects that are constantly developing and doing so rapidly. It is important for regulators to consult with stakeholders on a regular basis, especially businesses, to avoid trade barriers and additional unintentional regulatory layers.

The long term impact of the horizontal legislation, especially the proposed AI Act, is still unknown – e.g., to avoid a race to regulate, discussions are ongoing.[78]

3.3 The role of standards in supporting innovative technologies

It is impossible to discuss technical regulation without addressing standards. The development of voluntary, industry-led, consensus-based, market-driven global standards for products and technologies are regarded as a key enabler for business to leverage technologies and manufacture products efficiently at economies of scale by reducing the costs that would otherwise be involved in specific variations of products to meet different jurisdictions' standards. The opposite, i.e., nations using mandatory national standards is often used to limit foreign competition and support domestic industries. This naturally provides an opening with which to game the international trading system, but it imposes additional costs that harm consumers as well as the country's own competitiveness.[79] The continued promotion of global standards is therefore a key factor in facilitating trade, especially for digitalised technologies and naturally an approach that is also supported by traditional trade policy frameworks such as the TBT-agreement.

When it comes to new technology, such as AI, an important question is whether there exist global standards that support major policy initiatives and legislative frameworks. Where there is a lack of international or regional formal standards[80] privatisation of regulation occurs, where industry, not the government, leads "regulation" in accordance with its own standards. This becomes interesting both with respect to the level of fragmentation (a number of various normative standards) and the effects on product compliance (the possible lack of insight on the part of regulators).

78 See, e.g., Engler, Alex 2022: https://www.brookings.edu/research/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/

79 According to OECD, compliance with country-specific standards can add as much as 10 per cent to the cost of an imported product.

80 By formal standard we mean standards that are prepared by international standard developing organisations and that have adhered to the principles in the TBT-agreement the Code of Good Practice thus fulfilling the principles of transparency, openness, impartiality consensus, efficiency, relevance and equivalence.

The very outset and rationale concerning why AI standards-related tools are needed are, for example:

- Data sets in standardised formats, including **metadata** for training, validation and testing of AI systems;
- Tools for capturing and representing knowledge and reasoning in AI systems;
- Fully documented use cases;
- Benchmarks;
- Testing methodologies;
- Metrics;
- AI testbeds; and
- Tools for accountability and auditing.[81]

All this relates to the parameters introduced earlier on data, testing and decision making and the need to address these "in a commonly agreed way", which equals to, standardisation.

The question is thus what are the main standardisation initiatives worldwide and in Europe and what does the work tell us about the standardisation maturity in the field of AI.

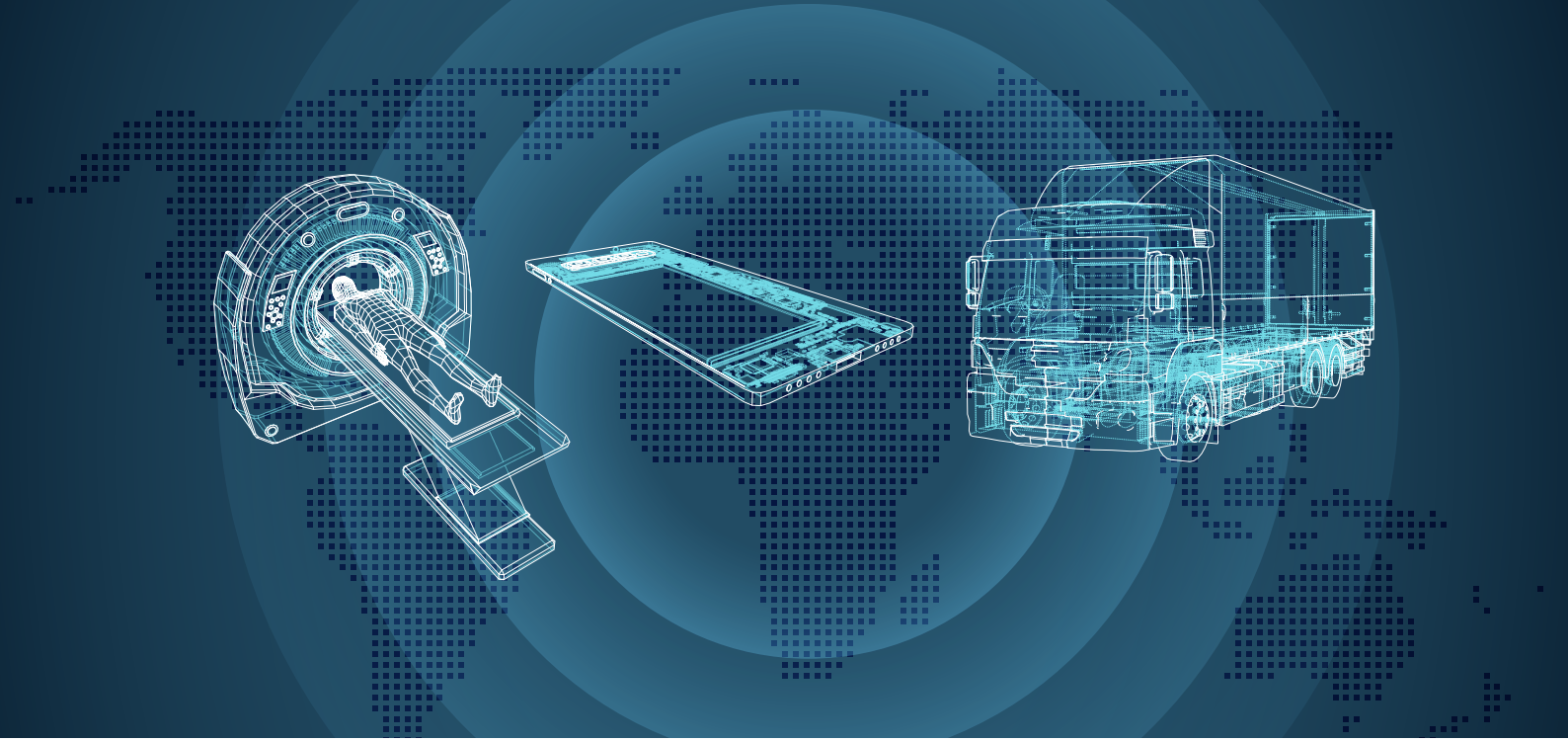
Unfortunately, there is no easy and good way to get a clear overview of all the standardisation work related to AI. There are numerous sector-specific standards addressing various aspects related to AI. In the ISO work programmes.[82] It is however possible to gain insight into ongoing and published standards in the AI field on a horizontal level. These items belong to ISO / IEC JTC 1 / SC 42 which is the ISO Technical Programme on Artificial Intelligence currently chaired by American National Standards Institute - ANSI.

These are the AI standards that have no direct connection to a specific area of use (e.g., self-driving vehicles or medical equipment) and can be applied in most areas where AI can be used. However, this is not all the work that is going on linked to AI, as there are other groups within ISO that run domain-specific projects. These will probably increase in number as the standards in the work programme are published. An example of such a standard is a proposal for a Project Committee (PC) on ISO/NWIP Driver training - Intelligent training system for vehicle driving.

Similarly, it is possible to grasp horizontal standardisation work in the field of cybersecurity (ISO/IEC 27000 series as well as Common Criteria) but much more burdensome to cover specific standards. Within the case studies some companies mention standardisation work relevant for them with respect to AI and cybersecurity but there are also companies who deliberately choose not to comment on their review of or use of standards.

81 See e.g., NIST, *U.S: Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools, 2019*

82 See ISO - ISO/IEC JTC 1/SC 42 - Artificial intelligence



4. Emerging tech markets – case studies

To explore the way AI technology is used in industrial goods and to draw conclusions on the possible impact on regulation, this analysis has looked into 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 are constructed as follows.

First each case chapter will present **general information about the product category in question**) and its relation to the use of Artificial Intelligence (**Case Mobile phones, Medical devices, Vehicles**).

Secondly, a **sector specific legal framework for each product is presented on a generic level** to provide an enhanced understanding of the product and how it is regulated (**Regulatory outset**).

Then the case is presented. Each case will start with an introduction of the type of companies and stakeholders that have been interviewed. The case then focuses on three themes:

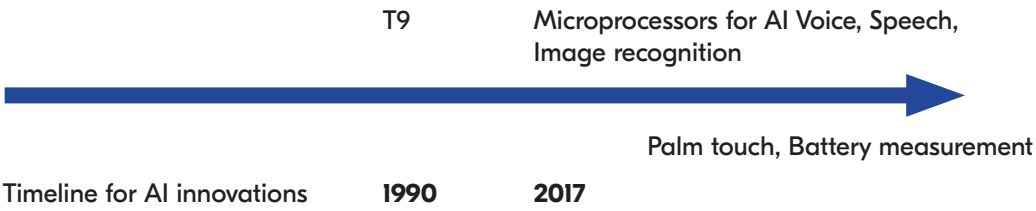
- **AI Technology** (i.e., how AI is applied in the sector and in which manner the stakeholders see that the current regulatory framework addresses it)
- **Vulnerabilities and risks identified and approaches to address them** (i.e., how risks related to AI are perceived); and
- **Change in regulatory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

At the end of the chapter, some general conclusions are drawn based on all sectors.

4.1 Mobile phones

Artificial Intelligence is now increasingly becoming the differentiator for the new generation of smartphones. One of the first very rudimentary applications of Machine Learning

in a mobile phone application is predictive text entry, first in the form of T9[83] developed by Tegic Communications[84] and licenced to manufacturers and integrated into several products in the late 1990s.[85] A more developed system has been in use since 2017 in Apple iPhones and earlier in some Android phones.



Smartphone

A smartphone is a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps. Smartphone intelligence provided by AI can constitute of, e.g., of voice-, speech- and image recognition.

The ability of 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.[86] 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. AI in mobile phones can concern, e.g., natural language processing and speech- image-, and voice recognition as explained below.

83 T9 is a predictive text technology for mobile phones.
84 Tegic is today part of Nuance Communications.
85 These early mobile phones only used the frequency (occurrence) of the entered words to give a priority weight to determine the order with which to suggest words. With the inclusion of special hardware for accelerated machine learning on smart phones the context of the text itself and grammar rules could serve as input data to the model in order to better determine which words to suggest.
86 See: WIRED Brand Lab | Meet the AI Powering Today's Smartest Smartphones | WIRED

Natural Language Processing

Natural Language Processing or NLP is a type of AI technology that is used for text generation. The most common use of NLP is **chatbots**,[87] which allow the user to type a text message to a chatbot application and receive a response in the form of a message. Using natural language processing, mobile applications can speak and understand the users. For instance, a chatbot can interact with the users, and the computer will understand the users' commands and carry out the users' actions. Natural language processing can also be used to develop automated and semi-automated mobile applications. For instance, a mobile application can collect information and then tell a user the weather and the traffic situation. Natural language processing can also be used to develop business solutions. A business solution can be a mobile app that allows users to create a list of appointments and the mobile phone will tell the users whether it is possible to leave earlier.

Speech-, image- and voice- recognition

Speech recognition means converting speech into a language that computers can understand. We use this technology to make people's voices easily understood by computers.

Similarly, image recognition will be used to help computers to understand images. The technology will allow the computers to recognize an object in the photo. This is often used in mobile applications to identify a person or vehicle in a road traffic accident.

Voice recognition is the ability to convert a user's voice into text. Voice recognition has been used in mobile applications to help people speak to their mobile devices without using a keyboard. The mobile devices will understand the user's voice and convert it to text. Voice recognition is used in *several mobile applications such as dictating notes, shopping, or managing personal data.*

Day-to day- operations and Facial Recognition

AI also contributes to day-to-day operations. More fundamentally, AI is behind Google's core search engine, every time you search from your mobile phone and it is being adapted to work behind the scenes in applications such as battery life management and security. AI is also behind the facial recognition customers might use to get into their iPhone which, again, uses images from the onboard cameras.

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.[88]

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

87 A chatbot or chatterbot is a software application used to conduct an on-line chat conversation via text or text-to-speech in lieu of providing direct contact with a live human agent.

88 Huawei's claimed to be the first to insert a Neural Engine into their smartphones last year, which they called their Kirin processor / 970 chipset with 'built-in AI.' At the time, they claimed that their software could process up to 2000 images a minute. The processor was included in their mate range and will stay as part of their upcoming Mate and Mate 10 product releases. Apple, who has also designed one of these AI targeted microprocessors, are opening up their A12 'Bionic' AI chip — which is also designed to conduct AI tasks more efficiently. Apple included its AI chip in the iPhone 8, 8X, and 8 Plus.

music recognition. Moreover, the third-party apps will be able to use the dedicated processors they want, to conduct their AI tasks. [89]

Regulatory outset

Sector-specific requirements for radio equipment on the EU market are provided by the Radio Equipment Directive 2014/53/EU[90] (RED). It applies to the placement and availability of radio equipment on the market and does not as a consequence cover the whole life cycle of the product. Radio equipment includes/is defined as electrical or electronic equipment that intentionally transmits and/or receives radio waves for communication and/or radio determination such as mobile phones, tablet computers, remote controls, drones, radiotelephones and GPS receivers. The essential requirements for all radio equipment, concern the protection of health, an adequate level of electromagnetic compatibility, an effective and efficient use of radio spectrum and the avoidance of harmful interference.

AI in mobiles

Currently there are no specific direct requirements on the use of AI in mobile phones. Mobile intelligence is instead regulated by requirements on data and privacy and, for example, cybersecurity.

Cybersecurity in mobiles

Special requirements for certain product categories under RED are subject to the issuance of delegated acts by the European Commission.[91] In 2021 the Commission issued a delegated regulation supplementing RED that addresses elements of cybersecurity. The objectives of the new requirements are the following:

- To protect communications networks
- Better protect users' privacy and
- Prevent fraud committed using Internet-connected equipment such as toys, childcare equipment and wearables (but not e.g., medical devices). The requirements will be applicable from 1st August 2024.

Case mobile phones

Our mobile case is centred around discussions with two global giants in the field of mobile market- Google and Apple along with reflections from the regulatory body responsible for RED-regulation in Sweden - the Swedish Post and Telecom Authority.

Google LLC is an American multinational technology company founded in 1998 that focuses on AI, search engine technology, online advertising, **cloud** computing computer software, quantum computing, e-commerce and consumer electronics. The company's mission is to organise the world's information and make it universally accessible and useful.

Apple Inc. is an American multinational technology company founded in 1976 that specialises in consumer electronics, software and online services.

89 How AI and Machine Learning are Transforming Mobile Technology | GreenBook

90 Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

91 Article 3(3) Directive 2014/53/EU.

AI technology in mobile phones

Google utilises various types of AI enabled software tools. For example, they are used in "Google Search" to improve the search results by the analysis of language, in mobiles phones cameras for face recognition and in medical/health care applications (Covid diagnostics and apps related to eyes/dermatology (please specify/clarify), of which the latter are classified as Medical Devices. Google is more or less using AI in all Google products on and off mobile devices.

Apple leverages AI and Machine Learning as one set of tools in its software design toolbox to ensure that a product/service/feature works as intended. The company does not necessarily need to market that such product or features are powered by Machine Learning. For example, photo recognition in Apple Photo text translation,[92] voice recognition for virtual assistant (Siri)[93] and text rendition (accessibility features); as well as knowing that the palm touches the iPad rather than the finger,[94] optimise battery charging to lengthen battery life.[95]

Discussions with the two major global mobile manufacturers confirm the result of our legislative review and highlights that mandatory regulatory requirements related to AI are still quite scarce.

For Google there are no regulations that limit the use of AI in mobiles other than those concerning Google applications classified as Medical Devices. AI that is used for improving product and services related to mobile phones also continue learning after they are placed on the market, i.e., they continuously gather data but with the restrictions.

It was also highlighted by the companies that GDPR frames the way personal data can be leveraged for Machine Learning in a way that profiles users.[96]

Whether Google mobile phones fall under the proposed EU AI Act is met with some uncertainty as the AI definition is still under debate. Based on the current formulation several of Google mobile applications seem to fall under the regulation. However, some regulatory requirements in the proposed AI Act do not fit as Google mobile phones do not have facial recognition in public spaces (an example of use cases classified as high-risk). A challenge regarding all these issues and possible specifications is the fact that the phone has a significant amount of software and many applications that are not necessarily related to the phone itself.

It is also highlighted that it is important that the AI Act proposed by the European Commission adheres to already existing privacy principles and other regulatory frameworks, as the industry is seeing an increase in regulations that contradict each other, i.e., different requirements in GDPR and other regulations.

The definition in the proposed EU 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 Machine Learning 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 for the EU stepping up with a legal framework, especially its work in identifying requirements for various risk categories. Google, however, consid-

92 See: Apple Photos Tech Brief: https://www.apple.com/ios/photos/pdf/Photos_Tech_Brief_Sept_2019.pdf

93 See: Siri - Research paper from our Machine Learning Journal: https://machinelearning.apple.com/research/siri-voices

94 See: Face ID: https://support.apple.com/en-us/HT208108

95 See Battery optimisation: https://support.apple.com/en-us/HT210512

96 This is not necessarily relevant for "mobile users" but could be relevant to specific services enjoyed on mobile devices.

ers a horizontal regulatory package dangerous as the AI technology is used in so many ways in various products, sectors and applications and is far from a mature technology. It would be better to closely follow the technological developments and the eventual safety critical features as it is not feasible to regulate something that is not yet well defined. It is thus pointed out that what the EU proposal is scoping now does not necessarily reflect what is happening in the market, nor will it be valid in the near future.

When discussing standards, Google argues 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 are well-developed international standards and schemes for mutual recognition that are in phase with technological development. [97] When discussing cybersecurity from the regulators perspective it can be confirmed that all products and services need to be embraced by a life-cycle approach to ensure security.

On the question regarding whether there are harmonised international standards for AI, there is some further hesitance. From a safety perspective, there is not necessarily a need to standardise Machine Learning or AI as such. Rather, it is a question of standardising various use cases for which AI is applied (like voice recognition, text rendition or battery charging optimisation). [98] Here it was highlighted that it is important to differentiate between potential regulatory requirements (which would only be applicable in specific use cases) and standards, which can be used to demonstrate compliance with those requirements (e.g., standards for risk assessment tools and data quality).[99] The following explanation is provided:

There are good reasons to standardise specific elements of how Machine Learning is used in order to demonstrate compliance with future regulation. Indeed, this should only take place in order to demonstrate compliance with ML uses that are deemed high risk under the future legislation.

Standards target specific processes underlying ML development (like quality assessment etc.) which would be useful for demonstrating compliance in the future. They do not see the standardisation of ML as a tool, or even specific use cases. Existing maturity is relatively low. It will be crucial to ensure that the right standards are available to demonstrate compliance with the oncoming AI Act, but these do not necessarily exist today.

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.

When considering enforcement, regulators should strive to be business model agnostic and independent from politics. The EU should also judge potential standards to be used as harmonised standards to demonstrate compliance on the basis of the solution offered – and always strive to recognise the best solution – rather than take into consideration which stakeholder contributed to the standard or the governance structure of the standard body in question.

97 Standards such as the ISO/IEC 27000 series as well as Common Criteria (CC).
98 Each of these can be used separately for practices with very different risks. Syvänne, September, 2022.
99 The actual Machine Learning involved is not standardised, just certain processes leading to their development.

Any move to examine harmonised standards and compliance, predominantly from an industrial policy or digital sovereignty perspective, is likely to lead to sub-par solutions and make it harder for all market actors to demonstrate compliance.

What makes regulation complicated, though, is the multiple regulatory layers e.g., horizontal acts such as the proposed EU 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.

If comparing the regulatory approach taken by the EU and the US, companies interviewed argue that the US has taken a slower approach, waiting before developing a comprehensive AI regulation. Instead focusing on safety and risk within sectors where AI implementation is more mature (compared to the EU's horizontal and more preventive method following a precautionary approach). Asia differs highly from both the EU and the US, and the regulation there is regarded as complicated as since there is a different approach to product safety.

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 EU AI Act proposal). Much of this has to do with personal integrity and the risk for the systematic discrimination of individual and information systems that directly affect people.[100] 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 presented by the technology. For some users, AI will be of benefit, while a few individuals who are exposed to AI- based medical treatment could have their lives ruined.[101] This thus becomes an impact-based approach (similar to safety protection) where risk (probability and consequence) is not a factor.[102]

Vulnerabilities and risks identified and approaches to address them

When it comes to risk to users and consumers, companies argue that adding AI technology to mobile devices does not automatically equate increased risk. It is the specific use 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 are seen by Google as mostly related to personal data.

Vulnerabilities are more related to the interface between device- operating system and third parties which can limit the management control of data. Companies highlighted that there might be output related risk when AI/ML is deployed in high-risk areas (public services, medical devices, or situations where there might be risk to human health and safety, like fully automated cars). Many of those uses cases might already be covered by product safety rules.[103]

---

100 Swedish Post and Telecom Authority July 2022.

101 In the context of mobile devices, it has been highlighted that there are limited risks to users, beyond the risks that are already well mitigated by existing regulations (GDPR, NIS, product safety laws like Radio Equipment Directive).

102 Swedish Post and Telecom Authority July 2022.

103 Apple's approach to security relies on both OS level software design - i.e., by 'sandboxing' apps and managing third party access to functionalities generating personal data - and by reviewing third party apps to ensure they are safe and do not pause security threats. Notably, this helps limit situations where app developers pretend to be something they are not and manipulate users to give them access to data that is not needed for the app but could be leveraged for **ransomware**. See also: Apple Platform Security Website as source. https://support.apple.com/en-gb/guide/security/welcome/web

In general companies are confident in their use of Machine Learning and their knowledge that risks and vulnerabilities are seldom connected with ML as such; safety and risk are more related to the data (use of personal data).[104] The application of security and privacy by design means that data in mobiles devices and apps are encrypted and processed on-device (it does not leave the device).[105]

Vulnerabilities are more related to the interface between device- operating system and third parties which today are mitigated through data minimization principles, users controls and reviewing, how personal data generated by the device is used by third party app developers in order to ensure that such use is proportionate to the intention of the app and that correct information about personal data uses are provided. Here, the uncertainties presented by the Digital Market Act, which will force the sideloading[106] of apps outside of internal review process,[107] might actually make the situation worse by making it harder (or impossible) for a company to act to protect the data and cyber-security of users who decide to side-load apps.[108]

Regarding cybersecurity, Google admits that the cyber vulnerabilities are a major challenge however compared to AI there are far better tools for addressing them. Here security by design is the key. Google argues that there is a great potential for regulators to step up with increased competence indicating that cybersecurity is also a societal concern beyond the sector insofar as it is related to critical infrastructure.[109]

Concerning the role of mobile devices in critical infrastructure, it was highlighted that compliance with the NIS directives' current scope is important, which includes specific digital services like app stores and cloud services (although these are deemed, in the NIS, less risky than other critical infrastructure related to healthcare, connectivity, etc. that need to meet more stringent requirements).

From the regulators point of view, it is too simplified to argue that there is no risk with adding AI to mobile applications.[110] However, it is also highlighted that it is possible to construct processes to deal with AI that have data protection as an opening value.

---

104 It is worthwhile noting that risks to personal data are seen in a broader context about how data are generated and shared with Apple and third parties. This is not necessarily about AI and ML.

105 Experts point out that in case the data leaves the device (messaging, cloud), it should be end-to-end encrypted in-transit and again encrypted at-rest (e.g., in cloud). Also, the **Application Programming Interface (API's)** at both ends (device and cloud) must be adequately protected. API is a way for two or more computers programs to communicate with each other. It is a type of software interface, offering a service to other pieces of software.

106 Sideloading describes the process of transferring of files between two local devices, in particular between a personal computer and a mobile device such as a mobile phone, smart phone, tablet, portable media player or e-reader.

107 See: https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf

108 Up until recently, there were no specific product safety requirements related to cyber-security for mobile devices under RED. One specific requirement related to cybersecurity was recently adopted through a Delegated Act but it does not come into force until August 2024. There is nothing specific to AI/ML in this cybersecurity requirement, although it would cover any embedded AI/ML tool that is used to fulfil that requirement (if any).

109 Defining critical infrastructure is political and depends on national policies and priorities. In general, critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. The U.S. has identified 16 sectors that constitute the critical infrastructure that more or less correspond to the areas pointed out in the directive on the security of network and information systems (NIS Directive) in the European Union: chemicals; commercial facilities; communications; critical manufacturing; dams; defense industrial bases; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials and waste; transportations systems; waste and wastewater systems. When regulating within critical infrastructure, like transportation or financial services, regulators need to regard both the requirements for the platforms that are used for sending data within the sector (IT infrastructure) and the requirements for ICT products that are used within the IT infrastructure (mobiles, computers, equipment, devices, vehicles etc.)

110 It is not, however, just about AI; it is about using data as such.

Change in regulatory parameters and considerations

When discussing whether our current regulatory framework and techniques are effective for dealing with AI Google does not see many problems for its business as such. Nevertheless, the company argues that, from a regulatory point of view, the fast-developing technology, increasing customisation and how data are being used do create regulatory challenges – especially if regulation consists of multiple, possibly duplicate regulatory layers not necessarily grasping the actual risks related to the specific use cases.

Given that standards have an important role for boosting innovation, Google is worried by the tendencies in Europe to change standardisation policy. Instead of supporting consensus-based standards based on the market needs, new structures and regulatory tools are controlled from above – not necessarily delivering expected outcomes. Further there is the worrying tendency for regulation to become industrial politics where again the crucial need for interoperability and international trade are ignored with the risk of fragmentation and trade barriers. Google strongly supports international regulatory cooperation and, e.g., ISO standards instead of allowing for regional and national approaches to flourish.

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,[111] the proposed Cyber Resilience Act and the Implementation of Radio Safety are still not fully evaluated.[112] 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[113] and safe.

Companies argue further that it is worth nothing that AI/ML encompass a wide range of techniques, from simple to complex. Not all AI/ML is so-called 'deep learning' where it may be unclear how an AI system came to specific decisions.[114] There is nearly always an element of control at the conception stage (one designs an AI system to reach a certain output), and other ways to ensure there is human control/oversight over how the AI is used (like an AI power medical diagnostics tool that is reviewed by a medical specialist). Even in cases where it can be hard to trace how an AI system comes to a specific decision, you can test such output to ensure a specific level of quality.

On the question of how to define mobile phones (with software), AI-supported software and third-party delivered software like apps, companies highlight that it is in the end all software. Some might be standalone (an app), others might be embedded in a product (like an operating system or elements of it). In EU law, there is a difference between

111 There is a tension between regulations wanting to open up and create access when it comes to the operating system being the overall responsible for the security of the phone for example. In DMA, there are some challenging proposals with regards to that which affect Google.

112 This is brand new and may provide additional requirements related to SW (embedded and non-embedded) which is likely to cover the use of ML, like any other software tool, where relevant.

113 Here Apple highlights that ethical concerns are only relevant if the use case raise ethical issues - like AI used to determine access to public services, to determine employability, etc. The vast majority of the company's AI use cases does not pose such concerns.

114 This could be considered the ultimate dimension of AI. When can you "cut out" vs. when do you have to "keep in the cuts".

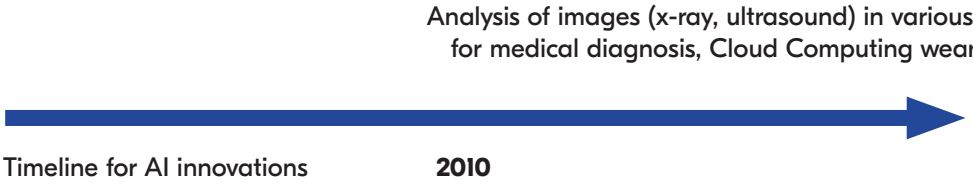
embedded and **non-embedded software**.[115] Product safety laws already covers embedded software when this impacts the safety of the product.

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. 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 regulatory parameter, something that policy makers should be attentive to.

4.2 Medical devices

The medical device sector early on saw the value in making use of innovative and intelligent technologies. First, AI in the form of neural networks were used for the diagnosis of heart problems already in the 1990s, for example, in ECG (electro cardiograms). Some experts argue that the sector is a late bloomer since todays' 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 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.[116]



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[117] the most important application area being "diagnosis and decision support". The implementation of AI essentially relates to the level of adaptability and autonomy. There are two types of AI, defined by their adaptability:

1. Software that is already trained when placed on the market - 'Decision support'; and

2. Software that adapts perpetually and optimises a device in order to continuously improve its outcomes - 'Autonomous decision-making'.

Software as a Medical Device (SaMD) can be used to diagnose, prevent, monitor or treat a disease. It may also provide suggestions for disease mitigation or assist in the diagnosis,

115 Embedded software (in a product) is the property of a product in which the software is embedded in hardware or non-PC devices. Non-embedded software is a service and is classified as either software that was not part of the evice when it was placed on the market, or software in a service to the end user. See also: Safety of non-embedded software, including on safety of health, lifestyle and wellbeing apps | Shaping Europe's digital future (europa.eu)

116 For various application areas see e.g., Artificiell intelligens i praktiken | Bröstcancerförbundet (brostcancerforbundet.se), IRCCS San Raffaele: Identifying the COVID-19 patients at highest risk with AI (microsoft.com), Svensk teknik avslöjar dyslexi med AI — nu ska den erövra USA - Computer Sweden (idg.se) and AI och maskininlärning inom medicinteknik - Zert

117 Tsang et al, 2017

screening, monitoring, prediction and determination of a disease.[118] Artificial Intelligence and Machine Learning (ML) technologies differ from other 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.[119] AI/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.[120]

Figure provides examples of AI in medical devices

AI as a Medical Device	Function in Healthcare	AI technology
AI **image analysis** of CT scans Orthopaedic planning software Skin disease detection AI AI detecting diabetic retinopathy	Radiology diagnosis Cardiac imaging analysis	Image recognition based on Machine Learning and Deep Learning Models
AI in **monitoring** electro-cardiogram (ECG) Medical devices for predictive analysis	Monitoring of disease Early Warning system	Big data analysis, Machine Learning, Deep Learning Algorithm, Neural Networks
AI enhanced **wearables** Glucose monitors equipped with AI	Health monitoring	Computer Vision, Gesture recognition, Natural Language Processing
Medical **robotic** devices enhanced with AI Personal robotic assistant	Surgery Description dispensing Sterilisation Elderly care	Robotics, Natural Language Processing, Speech-and Face recognition, Machine Learning, Neural Networks

Source: Technopolis Group

To use AI/ML technology safely, it needs to be verified and validated in terms of its reliability, accuracy and cost-utility.

Regulatory outset

The concept of medical devices encompasses a large variety of devices used in all fields of healthcare. Examples of medical devices include diagnostics, wound dressings, contact lens products, syringes, needles, implants, and pumps to administer medicinal products. Medical devices are also used by individuals for self-care and to assist daily living with disabilities and functional impairments.[121]

Manufacturers of medical devices have a far-reaching responsibility from the earliest stages of device development to take a responsibility for monitoring the device throughout its lifecycle on the market. Based on the intended use, manufacturers must determine at a very early stage of the device's development whether the device is a medical device;

118 See, Artificial Intelligence in Healthcare – First publication of COCIR AI Use cases
119 SaMD must be CE-marked to be placed on the market and be taken into use.
120 An important aspect of medical technology software is that services are increasingly common. Even if there are parts of the regulations around software, it is primarily adapted for physical products, which can cause difficulties in qualification and classification against MDR/IVDR.
121 Similarly, mobile systems are utilized as medical input.

this is known as 'qualification'. The classification of the device from the perspective of risk is another decision that the manufacturer must make at an early stage of device development, as the risk class of the device determines what type of procedure the **manufacturer** must follow to get its device CE marked.[122]

The responsibilities are governed by the Medical Device Regulation (**MDR**)[123] and the In Vitro Diagnostic Regulation (**IVDR**)[124], both of which replaced in 2017 the former three medical devices directives in the EU.

Rationales for the new regulations were several.

Harmonisation of the legislation across member states was needed. It is obvious that the technological development in the sector has made the earlier legislation outdated such as the increasingly more important software component.

Also, some serious incidents have been reported such as (certain breast implants, hip prosthesis leaking dangerous metals in the body, none of which are on the market today). According to experts, it was not these incidents as such that were the cause for the new legislative package. However, the incident reports resulted in more awareness of vulnerabilities in medical devices, and thus also in a political momentum to address them

Both MDR and IVDR state that quality management systems are mandatory[125] as compared to the situation earlier when quality systems were implemented on a more voluntary basis.[126] Additionally, the requirements for all risk classes have increased when it comes to clinical evaluation and providing scientific evidence for the claims concerning safety and the effect of a device. There are also extended requirements for post-market surveillance.

Reporting adverse events also highlighted a need for attention with respect to the designation and audit of **Notified Bodies**.[127]

With respect to technological development, again, a key issue is the software component, which was not the case in the past. This leads to the need for an updated traceability (on the product level) and appropriate processes, which in turn necessitates more strict requirements on a quality management system[128], including its approval and certification.

One challenge that is also relevant with respect to medical devices is how to treat those devices that have been put on to the market before new regulations have been introduced, i.e., the regulatory outset for so-called legacy devices.

---

122 In practice the manufacturer must first determine the intended purpose and assess whether it qualifies the product as medical technology. Then the classification is made in risk class. Also, it is important to note that qualification and classification can change if the intended purpose changes (which is not entirely uncommon) — i.e., you can have a product that is not a SaMD but happen to add features that push the system over the line. You can also add or change functions in an existing SaMD that change the risk class. So even though it is important to qualify/classify early in the process, you also must continuously monitor this as the system changes.

123 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002.

124 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU.

125 A medical device quality management system (QMS) is a structured system of procedures and processes covering all aspects of design, manufacturing, supplier management, risk management, complaint handling, clinical data, storage, distribution, product labeling, and more. Most medical devices will require some form of a QMS; the complexity of the QMS will vary based on the classification of the device.

126 This applied to devices of class I, not high-risk medical devices.

127 Notified Bodies carry out **conformity assessment** under the harmonised European product regulations. The revised requirements equal with more requirements on conformity assessment bodies that need to be approved by a sectoral authority. The regulations pose a new set of requirements on **accreditation** as well as a new workload for the designating authorities in the member states that supervise these Notified Bodies.

128 According to the legislation each product needs to be covered by a quality system, earlier it was on a voluntary basis/not required.

Legacy devices

A legacy device is a medical device that was legally placed on the market in accordance with the regulations that were applicable at the time, and that continue to be placed on the market after the date of application of new regulations even though they may not comply with the new regulations. Legacy devices are normally managed through transition rules that state certain conditions that apply in order for the manufacturer to continue placing the device on the market. In the transition between the previous medical device directives (MDD/LVFS 2003:11) and the new regulations (MDR), there are transitional rules[129] as follows:

Devices that are CE marked and have a valid EC-certificate according to the old regulations can continue to be placed on the market for as long as the certificate is valid, but no longer than 26 May 2024 (MDR). This includes all devices except those in class I.

Class I medical devices, which a large part of medical device software is classified as, must fully comply with the new regulations from 26 May 2021.

The exception is class I devices which receive a higher classification in the new regulations (and which therefore need assessment by a Notified Body). This applies to the majority of medical device software.

In order to remain under the transitional rules, the manufacturer must not carry out any so-called significant changes to the product. Significant changes lead to the MDR having to be followed. In addition to not making any significant changes, the devices also must comply with some of the requirements in the new regulations, such as post-market surveillance (PMS), vigilance and the collection of post-market clinical follow-up (PMCF) or clinical data.

Several expert opinions from businesses claim that the new regulations will strengthen big established businesses and their market dominance as these companies have the resources to perform the regulative adaptation. For smaller businesses or competitors from some third countries the new requirements might be challenging to meet.[130]

AI in medical device regulation

Medical Device Regulation and the In Vitro Diagnostic Regulation regulate Software as a Medical Device (SaMD) and are applicable and suitable to the AI/ML medical software. However, the current EU regulatory framework does not address a self-learning AI system specifically. It is the intended purpose that determines the risk class of a **SaMD**.[131] The majority of stand-alone software is Class IIa or higher[132] in the MDR. Very few systems will end up in Class I.[133]

Currently, there are few actors that have managed to obtain a CE mark for their decision-making AI system. As is often pointed out, the regulations do not fit the rapid, iterative nature of Artificial Intelligence. As experts point out there seems to be an unfortunate overlap between the proposed AI Act and MDR/IVDS that is still to be clarified.

129 For information see: Transitional regulations MDR | Medicines Agency (lakemedelsverket.se)

130 To provide a practical example the Vigilance-system for incident reporting will be merged with a larger database EUDAMED that require that it must be possible to identify and trace all products individually (or by batch level). This is motivated by many factors, such as better support with product recalls, to be able to exclude counterfeit products and for example to generate better statistics etc.

131 See MDR Appendix 8, rule 11

132 High risk devices such as implantable pacemakers are classified in the most regulated Class III.

133 Swedish Medical Products Agency, September 2022.

The main obstacles using AI in healthcare, and therefore to AI-based medical software, are the following:

- Access to data and data governance AI and ML technologies require secure access to a large amount of high-quality data.[134] The management and access to high-quality data is an important obstacle to the current use of AI/ML software as many healthcare services do not offer publicly available data.[135]
- How to address continuous change i.e., locked algorithms vs non-locked autonomous systems is 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
- Systems interoperability. Achieving the interoperability of systems has become essential. Ensuring the interoperability of systems allows for hospitals to make use of the software on their machines. In a 2019 survey, healthcare and life sciences executives stressed their concerns related to data privacy, data standards, normalisation and disparate software platforms as the main barriers to interoperability.
- Reimbursement of medicine and device expenses. Current reimbursement systems do not recognise AI SaMD as reimbursable expenses, and AI solutions are not covered by health insurance premiums. Reimbursement schemes are country-specific with no clear and unified criteria for AI-based medical software.
- User acceptance of AI. Reluctance to adopt AI by physicians and health professionals, whether in terms of training or accepting to work with AI-enhanced medical devices and robots, is still a significant barrier. A knowledgeable workforce that is comfortable with using AI technologies is key to enabling AI technologies to become more sophisticated.[136]
- Ethical framework. AI tools are developed by humans who may transcribe their own bias to the algorithm and functions of the software and therefore cause unethical outputs. The use of data on which AI is trained has important ethical implications. If the results of AI are generated by biased and skewed datasets, affected stakeholders will not be adequately protected from discriminatory harm.

Cybersecurity in medical device regulation

Among the many novelties introduced by the EU regulatory framework for medical devices, the two Regulations enhance the focus of legislators on ensuring that devices placed on the EU market are fit for the new technological challenges linked to cybersecurity risks. In this respect, the texts lay down certain new essential safety requirements (General Safety and Performance Requirements - GSPR) for all medical devices that incorporate electronic programmable systems and software that are medical devices in themselves. They require manufacturers to develop and manufacture their products in accordance with the state of the art taking into account the principles of risk management, including information security, as well as set out minimum requirements concerning IT security measures, including protection against unauthorised access.[137] The cybersecurity

134 Experts see that sharing of data and AI may be problematic from a GDPR perspective, i.e., to be able to argue that data becomes sufficiently anonymised.

135 The power lies with whoever have such data or access to it.

136 AI development may also result in a dead-end where the perceived performance is not reached and there is a need to discontinue.

137 md_cybersecurity_en.pdf (europa.eu)

requirements listed in Annex I of the Medical Devices Regulations, deal with both premarket and post-market aspects.

Several requirements that are generally associated with cybersecurity are not explicitly mentioned in the Medical Devices Regulations. Of particular relevance are those requirements regarding the privacy and confidentiality of data associated with the use of MDs that can be outside the scope of the Medical Devices Regulations but are subject to other legislations, such as IT security requirements for the operating environment in the NIS directive.[138]

Case medical devices

Our medical device case embraces discussions with two companies. The first company, Dedalus, is a world leading manufacturer of AI-driven medical devices software that is used in hospitals and in ambulances for patient diagnostics, for example to monitor blood pressure and body temperature. The other company, Elekta, manufactures products for the treatment of cancer patients (surgical medical devices and devices with radiation such as the gamma knife and a 3D coordinate system - for open surgery)

AI technology in medical devices

Dedalus is a global company supplying medical devices software, highlighting its AI model validation for the products it incorporates:

- Retrospective data study providing evidence on performance of model accuracy and specificity;
- Literature research to provide evidence on the state of the art of methodologies (e.g., machine learning, models, performance characteristics e.g., accuracy, precision); and
- real-time closed validation of prediction models within the clinical workflow where users are able to provide feedback on the efficacy and relevance of predictions. This feedback loop enables the continuous training and finetuning of the model.

The company's AI platform Clinalytix is based on risk-oriented prediction modelling.[139] It supports three risk prediction AI algorithms:

- Predict the risk of a patient developing delirium during their hospitalisation;
- Predict the risk for a patient developing sepsis during their hospitalisation; and
- Predict the risk for a patient developing acute kidney injury during their hospitalisation.

138 The Directive on the security of network and information systems (the NIS Directive) provides legal measures to boost the overall level of cybersecurity in the EU by ensuring: Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority, cooperation among all the Member States is achieved by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.

139 The underlying AI Deep learning algorithm is based on the Google Transformer AI algorithm using TensorFlow.

The benefit of the AI innovation materialises as follows:

- The Internet of Medical Things[140] based data collection allows clinicians to alleviate 'blind spots';
- A broader range of data collected in the home enables earlier intervention;
- It alleviates the 'worried well' – establishes a normal health baseline;
- Real world data is used for population health management e.g., local service planning and provisioning;
- Risks are captured through a combination of quality systems and clinical reviews. They employ a consistent framework of safety-by-design managed by clinical SMEs that understand the potential risks to patients; and
- Algorithms are developed with SMES/clinicians working together with data scientists. They bring industry and practice experience.

On the question of whether advanced medical software even works without a connection, Dedalus argue as follows: Adapting to operations in Low Communications/No Communications is the default operating model for healthcare meaning that devices must be able to function without connection. The federated nature of care delivery is, however, increasingly dependent on sparsely and geographically dispersed patient populations or services. Increasingly, capabilities, including those listed below, are now commonplace. This means edge-based services (edge appliances) are used to connect data either in the home, hospital or remote care facilities.[141]

Dedalus comments on the evolving regulatory frameworks as follows. When they started to introduce AI based products on one market in the EU their experience indicated that regulators are fully abreast with AI. However, the outset for accepting innovation varies considerably between markets.

In general, the opinion of the company is that regulators tend to be overly cautious and that there is no common application of the ruling even in between Notified Bodies.[142] However, the company argues that the Medical Device Coordination Group (MDCG)[143] established by the MDR provides a good basis for ongoing conversation.[144]

The company highlights itself as the leading provider of healthcare software services in Europe, and while its manufacture of hardware is limited, EU regulations around artificial intelligence, and algorithmic driven care are becoming increasingly important in the

140 IoMT or Internet of Medical Things (IoT in Health Care) is the network of Internet-connected medical devices, hardware infrastructure, and software applications used to connect healthcare information technology.

141 Explanation: Ambulance applications store clinical data locally, before being synced once connections are restored — 'store and forward'. The use of federated machine learning where data stays on the device and the results of the trained model are shared (protecting confidentiality and privacy) is becoming widely adopted today. Where data is captured remotely or in a "disconnected mode", organisations are adopting a mode of operation where the data is in "quarantined state" and clinicians are offered the chance to assess the data against stated quality standards before the information is inserted into the clinical record and used for clinical decisions. This is complemented with: existing access policies in used — role-based access controls (RBAC) and attribute-based access control mechanisms (ABAC)Patient Consent Management for data sharing data is all encrypted at REST and encrypted in flight.

142 A Notified Body is an organisation designated by an EU country to assess the conformity of certain products before being placed on the market. These bodies carry out tasks related to conformity assessment procedures set out in the applicable legislation, when a third party is required. The European Commission publishes a list of such notified bodies. Experts point that it would be advisable to notified bodies to be careful with new technology. The responsibility lies on manufacturers, and it is necessary to have well-grounded arguments for compliance.

143 See:https://ec.europa.eu/health/sites/default/files/md_sector/docs/mdcg_2021-24_en.pdf

144 Article 103 of Regulation (EU) 2017/745.

development of next generation healthcare services.[145] In order to introduce this type of medical devices clinical trials and medical devices software validations naturally apply. Active participation and use require consent from patients. The company explains that AI applications are based on shared responsibility. The company need to follow requirements for MDR regulation and GDPR and indicate the purpose of the device, but the use is the responsibility of the health care provider[146] supervised by health care professionals (i.e., doctors).[147]

From a trade perspective, the company says 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 in some countries' cybersecurity concerns leads to national requirements[148] or the introduction of the cloud has taken time.[149]

Concerning the proposal for a new European regulatory act on AI, the company states that regulation could lead to stunted innovation because of the burden of proof certificates, vigilance, market surveillance, and clinical investigations. Smaller start-ups will have longer GTM (Go-to-Market). While the registration fee is quite nominal, the process can be labour-intensive and can significantly strain on start-ups.[150]

If evaluating connectivity related to cyber threats, the company argues that MedTech without AI or connection[151] does have a smaller attack surface, although it is still susceptible to certain threat vectors. Inappropriate claims can be made about devices irrespective of whether they are connected.

Devices without a means of being (remotely) updated face the additional burden of having to be updated manually when new threats are detected.

Social determinant of healthcare (**SDOH**) and remote monitoring creates an increasing demand that will foster more AI driven capabilities. Closing the blind spots for clinicians (due to additional data) is a good thing particularly as most health systems are struggling with limited resources. Therefore, opportunities to shorten the distance and time to care is a good upside

The company also notes that regulating authorities need to do more. There are a huge number of questions related to customised products and software updates and how to monitor the market, especially as there are multiple policies, but regulators tend to work in silos, i.e., there is a lack of coordination.

The other company, that supplies medical devices for cancer treatment worldwide, Elekta, says that it is questionable whether its products will fall under the proposed EU AI Act, as the definitions are still not confirmed. The company, however, underlines that all its

145 Examples include the Natural Language Processing of clinical notes. Because of the complexities of written language, there are risk factors which must be mitigated — the risk of incorrect entity recognition, and the risk of incorrect coding and recommendation systems; the algorithms are only as good as the training set. A narrow (or biased) training set influences outcome, and remote monitoring of chronic conditions is mainstream in clinical care today. Systems are increasingly demanding that the underlying software go through the rigours of safety-by-design but also the regulatory compliance given the nature-assisted recommendations they offer. The Internet of Medical Things (IoMT) comprises examples of capabilities that fall into this category

146 According to the instructions provided by the manufacturer for the intended purpose.

147 The setup is by no means unique for AI- the manufacturer needs to deliver according to agreement and the health care provided needs to follow guidelines from the manufacturer.

148 For example, in Germany.

149 For example, in the UK. Countries in South America have been more open to cloud-solutions.

150 It should be kept in mind, however, that the safety of products needs to be secure irrespective of the size of a company.

151 Here it is argued by experts that AI vs connection are concepts on a totally different levels from an IT point of view.

devices using Machine Learning are validated according to legislation. The intelligence is above all materialised in software for treatment planning. The rationale with AI in the products is better, safer, and more effective medical devices. This requires, however, good data, and the question is whether the data available is representative for the market.

When it comes to sectoral legislation the company manufacturing medical devices for cancer treatment argues that the European regulatory framework for medical devices may be strict, but the revision of the framework can affect small companies not delivering complex products more, as high-risk products need to address comprehensive requirements through a quality system.[152]

Concerning the prerequisites for innovation in the sector highlights that it should be noted 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.[153] To test an AI application on a human being, clinical trials are a prerequisite. These can currently only be carried out for scientific purposes, ordered and supervised by a doctor. Projects to allow the pooling of large amounts of patient data are currently prepared in Sweden and Finland by universities.[154]

Clinical trials and the validation of a product containing software

For medical devices constituting a (high-risk) product that has a direct impact on human health, extensive quality and risk assurance by the manufacturer is often required. Thus, for the manufacturer to place a medical device on the market, it must demonstrate that it fulfills applicable regulatory requirements. In addition to quality system and risk assessment methodologies clinical trials and medical devices software validation, especially relevant for the application of AI, are required.

Clinical trials are research studies performed on people that are aimed at evaluating a medical, surgical, or behavioural intervention. They are the primary way that researchers find out if a new treatment, like a new drug, or diet or medical device (for example, a pacemaker) is safe and effective for people.

In MDD validation, the medical device manufacturer performs simulated use testing to validate whether all the software functions are executed correctly on the intended hardware platform in the intended use environment by the intended users.

The latest European legislative package for medical devices can be seen as an upgrade, not only with respect to the ambition level from the European perspective, but also internationally. As the package is still fairly new it will take time to evaluate the effects and how foreign approvals will work in practice.

When it comes to new technology the European legislative package addresses important issues such as software updates, AI and cybersecurity in medical devices. The MDR is very much focused on identifying the correct benefit-risk level and is perceived as quite robust

152 It should be pointed out that is not only the strict regulations that need to be taken into account but how the regulations are presented, i.e., the critical regulation mass often consists of numerous overlapping regulations, guidance documents and a multitude of standards.

153 A data federation is a software process that allows multiple databases to function as one. This virtual database takes data from a range of sources and converts them all to a common model. This provides a single source of data for front-end applications. A data federation is part of the data virtualisation framework.

154 An additional challenge is that only doctors providing treatment have access to information and DNA is classified as sensitive information. A possible solution is to use **federated data** to avoid the transport of data. A data federation is a software process that allows multiple databases to function as one.

by Swedish Medtech, the Swedish trade organisation of medical devices companies operating on the Swedish market. Also, the enforcement has been strengthened.

Swedish Medtech argues that the MDR and 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 can be considered a high-risk AI system. The Medical Device Regulations, especially in combination with the 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 Act 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 can 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 Artificial Intelligence.[155] The other side of the coin is that new technologies and innovations can always present a risk especially if new products could result in less requirements for health care staff.

On the positive side, it has been highlighted that AI can be used to detect cyber threats. For evaluating the workability of the regulatory approaches and rationale, it could be argued that it is important to separate between AI, where algorithms are locked at release, and AI applications that continue to learn and autonomously adapt after release. On the other hand, it is (and will probably also in future be) very difficult to achieve regulatory compliance for an AI-based medical device where the algorithms are not locked. There is therefore a need to create a regulatory sandbox[156] for AI[157] and define to which extent it can change from the "release" status.

The outset for regulating AI in medical devices is based on the perception that the requirement profile for a medical device does not change just because AI is used, i.e., the same product requirements apply with no specific classification (within the EU). Nor are there any bans on using AI in medical devices. The decisive issue from the regulatory point of view is that a medical device should be effective and safe.

Transparency related to the safety and performance of medical devices on the market is provided through mechanisms such as Vigilance.[158] The transparency will be further

155 See: COCIR_Feedback_AI_Regulation_-_1_July_2021.pdf

156 The proposed AI Act envisages setting up coordinated AI 'regulatory sandboxes' to foster innovation in artificial intelligence across the EU. A regulatory sandbox is a tool allowing businesses to explore and experiment with new and innovative products, services or businesses under a regulator's supervision. It provides innovators with incentives to test their innovations in a controlled environment, allows regulators to better understand the technology, and fosters consumer choice in the long run.

157 First regulatory sandbox on Artificial Intelligence presented | Shaping Europe's digital future (europa.eu)

158 The Medical Device Vigilance System, based on MDR is for the identification, reporting and trending of serious incidents and the conduct of safety-related corrective action.

increased with the coming implementation of **EUDAMED**.[159] Swedish Medtech argues that the private sector in general reports much more in the system than hospitals which could indicate that the statistics are not complete and there are unrecorded cases.

When it comes to cybersecurity, the main digital vulnerability in focus within this analysis, the European medical device regulations package, puts considerable focus on software with requirements for robustness, usability and fault-tolerance.[160] It should be noted however that especially cyber vulnerabilities create challenges in regulation as the manufacturer needs both to address the functionality of the device (i.e., the parameter that has been decisive in regulation) and connected and intelligent elements that affect the product more today than before. The challenge for regulators is related to the fact that cyber vulnerabilities are more difficult to predict and cannot be regarded as static, harmonised product property elements, as such vulnerabilities have multiple sources and outcomes and are only revealed in real time. It is obvious that legislation is a poorly adapted tool to manoeuvre this change. [161]

There is, nevertheless, considerable knowledge within med-tech businesses to address **security-by-design**. For example, methods on how software and code are developed and analysed at an early stage in product development.

However, there are no mandatory requirements on cybersecurity certification, although this was discussed initially when the European Cybersecurity Act was developed. Instead, there are strong private incentives to use standards.[162] Further, new EU cybersecurity guidance for medical devices is on its way.[163]

Vulnerabilities and risks identified and approaches to address them

When discussing risk, Dedalus in providing medical device software states:

"Digitally native citizens have grown-up with high expectations of health technology with ubiquitous use of mobile devices, web applications and real-time video. Establishing multi-channel digital services - eBooking, eConsultation, eReferral - helps engage and activate citizen wellbeing, and encourages early prevention and intervention through, e.g.

- The democratisation of access to services and education for the population;
- A profound shift towards preventive early diagnosis medicine;
- The expansion of homecare services and the need for fewer acute care services; and

159 The European database on medical devices (EUDAMED) is one of the key aspects of the new rules on medical devices (Regulation (EU) 2017/745) and in vitro diagnostic medical devices (Regulation (EU) 2017/746). EUDAMED provides a picture of the lifecycle of medical devices that are made available in the European Union (EU). It will integrate different electronic systems to collate and process information about medical devices and related companies (e.g., manufacturers). In doing so, EUDAMED aims to enhance overall transparency, including better access to information for the public and healthcare professionals, and the coordination between the different Member States in the EU.
EUDAMED will be composed of six modules related to: actor registration, unique device identification (UDI) and device registration, Notified Bodies and certificates, clinical investigations and performance studies, Vigilance and market surveillance. The use of EUDAMED is not yet mandatory nor required. The mandatory use of the system will start when the entire EUDAMED system (including all 6 modules) has been declared fully functional following an independent audit and a Commission notice to be published in the Official Journal and in accordance with the transitional provisions set out in the medical devices regulations.

160 This could imply, for example, that it is not possible to break a system with a very long password.

161 There are a number of requirements regarding cybersecurity and compliance with the state-of-the-art in the medical technology regulations and also in other regulations. Experts recommend separating between cybersecurity and activities related to clinical functionality.

162 It has been pointed out that it can concern a multitude of standards, e.g., IEC 62366-1 for the Application of usability engineering to medical devices is mentioned in the context.

163 Swedish Medical Products Agency, July 2022. See also: Strengthening Cybersecurity for Medical Devices in the EU (novaleah.com)

- The integration of portable/wearable medical devices and behavioural appliances with healthcare platforms that leverage IoT technology.

Many of these new capabilities will be delivered in a hybrid cloud model, which is expected to be the standard IT landscape for many years to come as healthcare businesses grapple with legacy infrastructure and innovate faster at the same time. The cloud-burst-model[164] is usually a safe-step for businesses to take before full migration to the cloud and the adoption of a cloud-first approach.

The Dedalus Platform approach uses declarative and policy-based infrastructure to provide fine-grained controls to confidently secure workloads, and time-consuming tasks such as reporting, auditing and threat assessment can be streamlined through the use of automated compliance reporting tools.

While healthcare businesses can bootstrap compliance by leveraging the cloud, security and compliance in the Dedalus Platform is underpinned by a shared responsibility model[165] meaning both the organisation and cloud have joint responsibility for security. This shared responsibility model means cloud providers are responsible for the security 'of' the cloud, while businesses are responsible for security 'in' the cloud.[166] For example, while a cloud vendor is responsible for the physical security of its data centres and the services and automations provided to businesses as part of their cloud services, a healthcare system provider is responsible for, e.g., securing secret keys, correctly configuring firewalls and securing their applications, hence limiting the access to the data according to the privacy requirements.

Concerning cybersecurity Dedalus generally argued that the EU's requirement helps improve awareness of the threats, but cyber threats cannot be completely eliminated through testing and certification.

Cyber threats are mitigated through:

- The use of reference models for IoMT – NIST, ISO 30141;
- Post-market surveillance and threat monitoring (out there in the wild);
- Security best practices and risk management including: [167]
    - Authentication
    - Authorisation
    - Access controls
    - Audit
    - End-to-end **encryption** / secure communications.
- Leveraging Enterprise IOT/device management platforms that are optimized against threats (e.g., Azure IoT Hub, AWS Greengrass) – optimized for these types of risks and investments from these companies;
    - Counterfeit and malicious devices; and
    - Exploits/protocol hijacking
- Wrap cyber into the end-to-end clinical process i.e., not in isolation

164 Cloud bursting is a configuration method that uses cloud computing resources whenever on-premises infrastructure reaches peak capacity. When organisations run out of computing resources in their internal data center, they burst the extra workload to external third-party cloud services.

165 Shared Responsibility Model http://amzn.to/3cCpfpb

166 This applies to ALL activities on cloud services. The service provider's responsibilities still include how to enable/limit access to data and with whose permission. Syvänne, September 2022.

167 Here secure processes including safe coding should also be considered.

The company is aligned with a number of international and European bodies and standards (including NIST 800-171, FedRamp, GDPR, HIPAA[168]/HITECH, FIPS 140-2, GAIA-X, TechUK, HIMSS, as well as others).[169]

What concerns incident reporting Dedalus argues that the aspiration of EUDAMED is well founded. As stated by EUDAMED, their objective is to ensure that there is a consistent and verifiable lifecycle picture of medical devices used in the EU. It will integrate different electronic systems to collate and process information about medical devices and related companies (e.g., manufacturers). In doing so, EUDAMED aims to enhance overall transparency, through better access to information for the public and healthcare professionals and improve coordination between the different Member States in the EU.[170] This position aligns with the proven methodology for drugs manufacturing (labelling), adverse drug events and post market surveillance – **Pharmacovigilance**. Hence, EUDAMED should foster the direct reporting of adverse events or risk conditions.

Although not specifically for medical devices, irrespective of industry or business, data incidents and data breaches are today reported to one or more appropriate local regulatory bodies depending on the type of incident, for example, if there is a loss of personal data, a person has been injured or a critical IT system has been affected.[171]

Elekta, which manufactures devices for cancer treatment, argue that cyberthreats are one of the greatest challenges and an issue that is often discussed in business fora. The company addresses cyber vulnerabilities with 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 regulators, capacities related to AI must be increased.

When it comes to risks with AI, the Swedish Medical Products Agency (MPA) admits 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.[172]

It is highlighted 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

168 The HIPAA framework is more or less equivalent with GDPR and e.g., Swedish national legislation that covers privacy within health care (Patient lag 2014:821).

169 For the management of cybersecurity in medical devices there are also new standards such as IEC 81001-5-1 and a technical report (IEC/TR 60101-4-5) and based on standards within automation (62443).

170 https://ec.europa.eu/tools/eudamed/#/screen/home

171 In Sweden data incidents and data breaches concerning IT systems in healthcare, including SaMD, are mainly reported to the Swedish Medical Products Agency in case of a patient safety incident (MDR/IVDR), to the Swedish Authority for Privacy Protection in case of a personal data incident (GDPR, Patient Data Act) and the Swedish Civil Contingencies Agency regarding incidents concerning IT systems and services that are of importance to society (NIS, national regulations). Healthcare providers can also be required to report to the Swedish Health and Social Care Inspectorate that supervises the use of medical devices in healthcare.

172 Such situations could concern the introduction of a health monitoring app that is tested on people but that should be covered by clinical trials under the supervision of a health care provider and follow a quality management system.

compliance are change control, traceability and transparency.[173] 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 and considerations

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 EU AI Act proposal and MDR is a good example.

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

The medical devices case also highlights 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 case study highlights the challenge with cybersecurity. Although the cyber dimension has been strengthened in the sectoral legislation there is the perception that more support is needed to address the complexities.

4.3 Vehicles

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 can independently manage both safety-related (**ABS** /Air bags) and non-safety related critical vehicle features.

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. A concept we often stumble into that describes the vehicle's reality is that of **intelligent transport systems (ITS).**

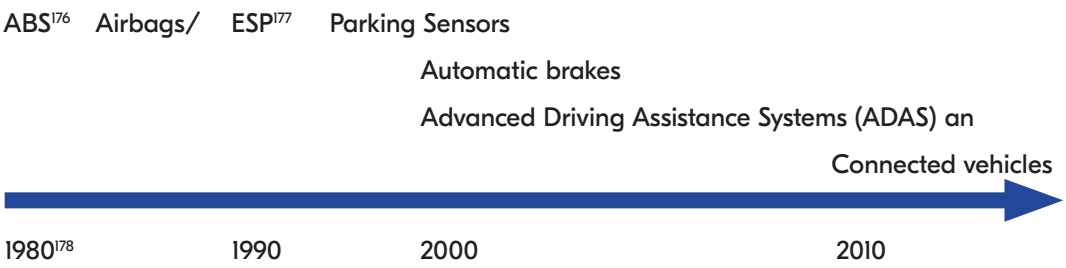
173 There is, in other words no hindrances to updating software, but changes in the software should not update themselves. The software must of course go through all development stages - requirements are set, risk managed, verified, validated and documented etc. If you make significant changes, you of course also need to review whether the intended use is affected and determine the risk class. Substantial changes in a software are in principle seen as a new product from a regulatory perspective.

Intelligent transport systems (ITS)

Intelligent Transport Systems' or 'ITS' means systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as interfaces with other modes of transport.[174]

In practice this means that new generations of vehicles provide to a greater extent, semi-autonomous, automated and autonomous driving (AD),[175] 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 can in principle completely replace the driver.

The intelligence provided by these technologies is not a new but something that has existed for quite some time. One way to put it is that AI within vehicles covers five disruptive technologies that add up to one: electrification, automation, connectivity, sharing economy and digitalisation. Car manufacturers claim that the development started as early as in the 1980s/90s when algorithms were used for the analysis of data to improve vehicle features, as follows:



Timeline for innovation[179]

The first generation of advanced vehicle applications were actually quite simple (brakes, gas and steering- especially cruise control). Often these technologies are regarded to be

174 See Directive 2010/40 on a framework for introducing intelligent transport systems within roads and interfaces with other means of involving transport and national law (2013:315) on intelligent transport systems on road, 3§. Definition agreed upon in UNECE see ECE-TRANS-2021-15_e.pdf

175 Automated for SAE Level 3 (driver ready to take over), and autonomous for Level 4 and 5 where Level 4 indicates that the vehicle is fully autonomous under its ODD, operational design domain, i.e., the conditions (weather, roads, vehicle readiness) under which the vehicle can drive autonomously. In Level 5 there should be no such limitations. See further 5.3.2

176 An antilock brake system (ABS) assists the driver maintain vehicle stability and directional control.

177 Electronic Stability Programme (ESP) is technology that has been mandatory on modern cars in Europe since 2014, though some older cars have it as well.

178 An interesting fact was that California required in the 1980s openness and access to a vehicle's environmental data - a starting point for connected vehicles.

179 The figure highlights the main points concerning the breakthrough into the market, although the actual technology may have been available earlir.

support functions to driving, rather than autonomous driving. Only later were new finesses layered on, e.g., those allowing a vehicle to change lanes, i.e., take steps towards autonomous driving.

The evolution of "intelligent" vehicle properties has developed gradually, since 2000 onwards. It started with measuring and reading fuel consumption (for fuel saving), localisation and traffic information. Each generation of vehicles is more capable with its electronics.[180]

An aspect often not fully acknowledged by general public is that the dominant part of vehicle intelligence based on ML is to a considerable extent concerned with collecting and analysing data (statistics and algorithms) in order to better adjust vehicle features to the environment and improve both safety and the driving experience.

Fully autonomous driving for passenger cars using AI is, according to experts, still quite far away, although the technology receives significant media attention as the testing of such vehicles have been allowed in some countries. Regarding vehicles for professional use, like trucks, however, the use of full automation is more prevalent, as can be demonstrated by our case below. There is a strong business case for using AI as removing the driver decreases the cost of operation considerably and customers are therefore prepared to pay for technology. There is a large shortage of truck drivers both in Europe and on the global level and automated transport with trucks in the most dangerous working environments such as mines, gravels and large terminals will be able to partly solve the driver shortage. Both connected conventional and automated vehicles also have a clear benefit regarding route optimisation and the ability to work with possible driver coaching and predictive maintenance.

Regulatory outset

The compliance requirements for vehicles in the EU are centred around the type-approval systems. Type approval proves that a vehicle or a component type meets the applicable technical requirements. A European type-approval granted by one EU member state is recognised by all EU Member States.

EU type approval applies for whole vehicles, which is relevant to this study on light and heavy trucks (category N).

EU type approval means type approvals in accordance with the following type approval regulations (so-called framework regulations):

- Regulation (EU) 2018/858 on the type-approval of motor vehicles and their trailers
- Regulation (EU) 167/2013 on the type-approval of wheeled agricultural or forestry tractors or in accordance with the separate directive issued under these three framework directives.
- Regulation (EU) 168/2013 on the type-approval of two or three-wheel motor vehicles
- 2016/1628 Non-Road Mobile Machinery[181]

---

180 To provide some examples of the regulation of automated driving it can be mentioned that ESP Electronic Stability System, AEB (automated emergency braking) and LDW (lane departure warning) were required for heavy trucks in the EU General Safety Regulation from 2011 (with implementation a few years later).
ESP was developed during the late 1990s and the other two in the 2000s.. Adaptive cruise control using radar is not regulated but was developed in the early 2000s.
ALKS Automated lane-keep-support was released for cars (as an if-fitted regulation) one or two years and this year for trucks. SAE Level 3. The technology has been available in cars since the mid-2000s, SAE Level 2.

181 ECE type approval refers to the type-approval granted under the provisions of the 1958 Agreement (Geneva, 20 March 1958). The regulations were created in 1958 by the United Nations. See World Forum for Harmonisation of Vehicle Regulations (WP.29) | UNECE

Concerning automated vehicles, e.g., in Sweden, the Swedish Transport Agency issues permits for trial operations with automated vehicles on public roads in accordance with a national ordinance.[182]

Anyone who seeks permission must be able to prove that the operation is conducted in a traffic-safe manner.[183] The purpose of the ordinance is to create better conditions for trial operation with automated vehicles. The ordinance states that when tests are performed with an automated vehicle, there must be a physical driver inside or outside the vehicle and that any person who conducts trial operations without a permit will be fined.

An Automated Vehicle vs. Autonomous vehicle

An Automated Vehicle is a motor vehicle (car, truck or bus) that has technology dedicated to assist the driver so that elements of the driving task can be transferred to a computer system. It is a driving system that observes and understands its environment, makes decisions to safely, smoothly reach a desired location, and takes actions based on these decisions to control the vehicle. A key enabler of this race towards fully AVs are the recent advances in AI, and in particular ML. Designing an AV is a challenging problem that requires tackling a wide range of environmental conditions (lightning, weather, etc.) and multiple complex tasks such as:

- Road-following
- Obstacle avoidance
- Smooth driving style
- Manoeuvre coordination with other elements of the ecosystem (e.g., vehicles, scooters, bikes, pe¬destrians, etc.)
- Control of the commands of the vehicle

An autonomous vehicle is a fully automated vehicle equipped with the technologies capable of performing all driving functions without any human intervention.[184]

Naturally the question of product safety and cybersecurity concerning this technology, which by definition is intended to operate with less human supervision, has emerged. The answers provided by regulatory bodies regarding these issues are likely to play an important role for the adoption of autonomous vehicles (AVs) in society. This is imporatant given that according to ENISA, ML techniques, at the core of AI components developed to mimic human cognitive capabilities, have been proven to be highly vulnerable to a wide range of attacks that could compromise the proper functioning of autonoamous vehicles, and pose serious threats to the safeaty of persons, both inside and outside a vehicle.[185]

182 Regulation 2017:309 on trials for automated vehicles.

183 The Swedish Government has decided on an ordinance concerning trial operation with automated vehicles. The ordinance states that trial operations with automated vehicles may only be carried out with permission from the Swedish Transport Agency. The agency also has the right to assign a permit with terms and conditions. The Swedish Government considers it important that Sweden is a country where new innovative technology for sustainable transport can be tested.

184 See The legal framework for autonomous vehicles in the European Union - Business Going Digital

185 AI components in charge of replicating tasks previously addressed by human drivers, such as making sense of the en¬vironment or taking decisions on the behaviours of the vehicle. By their nature, those AI components do not obey the same rules as traditional software: ML techniques are indeed relying on implicit rules that are grounded on the statistical analysis of large col¬lections of data. While this enables automation to reach unprecedented cognitive capabilities, it opens up at the same time new opportunities for malicious ac¬tors, who can exploit the high complexity of AI sys¬tems to their own advantage (ENISA, 2021).

These findings are however related to *personal cars - analysis and statistics not available for trucks (in focus in this report)*.[186]

Institutional and private actors have been very active into outlining the high-levael principles and standards that should govern the development of AV, either explicitly, with dedicated automotive guidelines, or through the definition of sets of practices driving the expansion of AI and cy-bersecurity. In this respect, it can be concluded that the EU has conducted various initiatives for developing trustworthy AI, where cybersecurity and intelligent transportation play a significant role.

Internationally many countries have themselves taken steps to address AI in vehicles by regulatory measures. Several of them are also contracting parties to the 1968 Vienna Convention on Road Traffic, an international agreement.[187] An amendment to the Convention on Road Traffic in 2016 removed legal obstacles to allow transferring driving tasks to automated technologies.[188]

Countries that have enacted regulations to allow for the testing of autonomous vehicles on public roads.[189] In Sweden e.g., there is no requirement that a driver must be physically present in the vehicle during testing, irrespective of the vehicle category, however, the vehicle must have a driver somewhere capable of taking over driving functions if necessary.[190]

186 Again, the question is "how safe is safe" and what do we expect of autonomous vehicles in terms of accepted accidents in the coming 50 years. The challenge is that if there is a security vulnerability it will appear in all vehicles in the same series (to be compared with a situation with faulty airbags today), implying that all technology creates a new risk that needs to be addressed.

187 The Convention has the objective to "facilitate international road traffic and to increase road safety through the adoption of uniform traffic rules".

188 This provided that the technologies used are in conformity with UN vehicle regulations or can be overridden or switched off by the driver. The USA and China are not parties o the agreement.

189 As an exception, the Netherlands and Lithuania have passed legislation that allows the experimental use of self-driving vehicles without a human driver present in the car on public roads.
Israel passed a regulation and a directive for experimentation in autonomous vehicles. Authorisation to conduct experiments in autonomous vehicles requires, among others, a review by a professional committee. Spain, Qatar, and the United Arab Emirates authorise the testing without a human driver present on a case-by-case basis but have not enacted specific legislation. New Zealand, unlike other countries, has no specific legal requirement for vehicles to have drivers. However, the government has not received any formal requests to test autonomous vehicles on public roads. In Singapore and the Province of Ontario, Canada, it is up to the discretion of the responsible authority to approve driverless testing. Other testing requirements for autonomous vehicles may include insurance, the transmission of certain data to the government, or accident recorders in the vehicle. Finland allows the testing of autonomous vehicles, but one political party has suggested forbidding nonautonomous vehicles as a long-term goal.

190 This is administered differently in different countries. The concept of driver and responsibilities in the market of commercial autonomous vehicles is tricky and has been unregulated the past 100 years but has been settled in court from case to case who is responsible. The outsets for requirements are still under development e.g., in Sweden (Andersson, August 2022).

Autonomous driving — we all know what it implies, or do we?

Contrary to what one could believe autonomous driving is not a simple concept with one definition. The SAE J3016 standard defines **six levels of driving automation for on-road vehicles**, ranging from level with no driving automation at all to level 5 with full driving automation and no need of driver (Figure 1 from ENISA report). Various national and international bodies have adopted the definition of the SAE standard as it is the only one available although it is not based on regulation.

Besides automating driving, another innovation consists of unprecedented levels of connectivity. Connectivity supports the communication of vehicles with all sorts of infrastructures and devices and provides increasing functionalities for drivers, integrating the information needed to enact autonomous driving and enable new driving patterns like vehicle platooning[191] Platooning or flocking is a method for driving a group of vehicles together. It is meant to increase the capacity of roads via an automated highway system. This is also executed on various levels of automation.[192]

Vehicle-to-Network (V2N) connects the vehicle to the Internet and/or to the cloud, to enable the exchange of real-time information about traffic, routes and the road situation. This connection is at the base of infotainment systems and an option available on most current vehicles.

Vehicle-to-Vehicle (V2V) connects vehicles to exchange information comprising their respective location, direction, speed, braking status, and steering wheel position. Since V2V technology en¬ables the sensor outreach of neighbour cars, it may be an enabler of autonomous driving integrating the on-board sensing of the environment.

Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V) technologies allow vehicles to communicate with road infrastructure and vice versa to support a variety of traffic management applications and services.

Vehicle-to-Person (V2P) technology enables vehicle's connection to smartphones and wearable devices, so that pedestrians or any other vulnerable road user (e.g., cyclists, e-scooter users, etc.) can share data with cars. This can be used to share location information and coordinate the operation of the vehicle with pedestrian's behaviour (e.g., alerting drivers if, for instance, they need more time to cross the road.

Vehicle-to-Device (V2D) and Vehicle-to- Everything (V2X) technologies enable the connection of vehicles with any surrounding device, object, and infrastructure connected to the Internet.

The combination of the two trends (toward connected networks and AVs) will eventually result in the full development of **Cooperative, Connected and Automated Mobility (CCAM)**, in which **Connected Autonomous Vehicles (CAVs)** are expected to significantly improve road safety, traffic efficiency and the comfort of driving, by helping the driver to make the right decisions and adapt to the traffic situation in real-time.[193]

In more practical terms, typical high-level automotive functions are presented as specific tasks such as adaptive cruise control, automatic parking, automotive navigation, blind spot/cross traffic/lane change assistance, collision avoidance, automated lane keeping, traffic sign recognition and environmental sound detection.

191 **Vehicle platooning** is part of a suite of features that self-driving cars might employ. A platoon is a group of vehicles that can travel very closely together, safely at high speed. Each vehicle communicates with the other vehicles in the platoon. (ENISA, Cybersecurity *Challenges in the Uptake of Artificial Intelligence in Autonomous Driving*, 2021).

192 The company estimates that L4 platooning with a driver in the truck only is probably the one that has a future.

193 Called V2X — Vehicle-to-Everything, i.e., the vehicle can communicate with everything.

Regulation of AI in vehicles

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 AI Regulation may have a role is with regards to liability, as liability is not regulated at the UNECE level.[194]

The most important forum for harmonising vehicle regulations is The World Forum for the Harmonisation of Vehicle Regulations (UNECE WP.29). It is dedicated to technical regulations applied to the broad automotive sector, addressing the safety and environmental performance of wheeled vehicles, their subsystems and parts.[195] Here it is worthwhile to clarify that EU vehicle regulations are largely based on the horizontal European Framework Regulations (earlier Directives) which are directly applicable in the Member States. The UNECE WP.29 framework[196] that is adopted by the EU supports the technical specifications depending on the needs in various areas.

Within WP. 29 there is also a Working Group on Automated/Autonomous and Connected Vehicles (GRVA) preparing draft regulations, guidance documents and interpretation documents for adoption by the parent body, WP.29. GRVA deals with safety provisions related to the dynamics of vehicles (braking, steering), Advanced Driver Assistance Systems, Automated Driving Systems and well as Cybersecurity provisions.

The regulation of the digitalisation of vehicles in general have been characterised as "moderate", i.e., not so many requirements. In addition to GDPR, the regulation of platforms[197] and **cyber resilience** does not currently involve many rules.

As highlighted earlier, the approaches to liability vary between markets. In the US it is the manufacturer who guarantees vehicle safety. I.e., the manufacturer needs to control the data to guarantee the functionality, safety and security of the vehicle. Some IP data is also needed for businesses. Companies normally have contracts and agreements with customers and share it with them. The connectivity is in itself a prerequisite for safeguarding that.

Within the European Union it is the Member States type-approval authorities who guarantees vehicle safety. As mentioned earlier, the UNECE framework is a baseline for international harmonisation, but it has not yet been adapted to a driverless scenario even though the guidance based on ISO standards is on its way via so-called safety cases (risks are identified in order to find an approach for how to deal with them).

194 International vehicle harmonisation is based on UNECE WP29 framework: WP29 World Forum for Harmonisation of Vehicle Regulations (WP.29) | UECE

195 See: WP.29 - Presentation | UNECE

196 The ECE regulations that the EU had joined are extensive, but it should be noted that the regulations do not cover all areas regulated within the EU.

197 See Regulation (EU) 2019/1150 of 20 June 2019 on promoting fairness and transparency for business users of online intermediation service.

When it comes to cybersecurity two UN Regulations[198], have been adopted by the UNECE's World Forum for Harmonisation of Vehicle Regulations, which requires that measures be implemented across 4 distinct disciplines:

- Managing vehicle cyberrisks;
- Securing vehicles by design to mitigate risks along the value chain;
- Detecting and responding to security incidents across vehicle fleet; and
- Providing safe and secure software updates, ensuring vehicle safety is not compromised and introducing a legal basis for so-called "Over-the-Air" (O.T.A.) updates to on-board vehicle software.

The regulations apply to passenger cars, vans, trucks and buses and entered into force in January 2021.

Case Trucks

This case deals with trucks, i.e., vehicles that are manufactured for *professional use*, for example to be used in mines or transport various goods in confined areas. Passenger cars for private use are not included in the analysis.

Our case is based on interviews with three companies complemented by information provided by the Swedish Transport Agency and experts. Two of the companies, Scania and Volvo, represent leading traditional manufacturers of vehicles and heavy trucks with business all over the world. The third company, Einride, entered the market in 2016, focuses on electrifying freight transport,[199] with electric, connected and sometimes autonomous trucks. The autonomous trucks are without driving cabins and called Einride Pods. It is necessary to clarify, that although Einride today manufactures autonomous vehicles it is not selling trucks but sells the service of transporting goods for professional use, i.e., to deliver a package, including logistics.[200] Although the vehicle is autonomous a human is always involved in the supervision of the vehicle, but at a distance. The business case with the autonomous vehicle case was initially developed for the Swedish market but today the company also operates in other parts of the EU and in the US in accordance with the legislation for test permits in respective countries.

It should be highlighted again that the common denominator for all three companies 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[201], i.e., not to the general public. By and 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

198 These concern the UN Regulation on Cybersecurity and Cyber Security Management System and UN Regulation on Software Updates and Software Updates Management Systems, see UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles | UNECE

199 All the company's vehicles are electrified.

200 This entails however the responsibility of the product (vehicle) itself.

201 In practice it is various parts that are type-approved that are then assembled in various means.

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.[202]

The companies we interviewed also confirm that the regulation for new innovation, especially considering autonomous driving, is under development. Our cautious interpretation is that the manufacturers are willing to take the lead in introducing technology that is then evaluated by authorities for the approval of new use cases, a picture that is not necessarily shared by regulators who want the industry to engage and be in line with the-type-approval process.[203]

AI technology in trucks

Based on the discussion with manufacturers, the use of intelligence in terms of Machine Learning and AI in trucks cannot be defined by one typical use case as the actual use depends on the definition of AI. For this study the levels identified for automated driving in the internationally applied SAE-standard[204] works as well (see below). Einride, e.g., notes that the US is leading in the development of AI.

It should be noted that all manufacturers are working towards capabilities for full automation, but the use cases are different, and that full automation (no physical driver) is still limited and only applied in limited use cases and defined areas. In some cases, remote surveillance by humans is used. Also, it must be considered that occupational safety and health regulation can restrict the application of certain tech.

The companies we interviewed all use AI today, including driver assistance systems and belt tension systems. The **SAE** levels provided by the standard J30016 (Levels of Driving Automation) are used to identify different levels of automation. It defines six levels of driving automation, from SAE Level Zero - no automation to SAE Level 5 -full vehicle autonomy. Some of the features such as adaptive cruise control system and blind spot monitor reach level 2 of automation in the SAE standards, while companies also have concept vehicles on level 5 (used in cargo terminals, ports- driving, e.g., just between two points - hub to hub). No physical driver is required L4 and higher. Companies and experts interviewed explained that L3[205] and L5-levels are not currently applicable. L3 is not in demand by customers (which is why it is not applied[206], and L5 totally driverless vehicles (i.e., a vehicle that should be able to drive anywhere and applicable in all ODD) is technically very difficult and is thus still very far way (not even under testing) and will not happen within the next couple of years. L4 is the level that are being tested in the near future.

202 EU has proceeded with type-approval for small series (trucks) for automated driving in 2022.

203 A type-approval regulation for ADS (Level 4) will be introduced in the EU (022) and we will thereby gradually start type approving such vehicles. Both business and authorities must learn, so a company argues and estimates that the market should not expect a type-approved ADS for several few years.

204 Standard SAE J30016 (Levels of Driving Automation)

205 Internationally, outside Sweden there are companies that develop L3 but in Sweden there is still hesitation. In L3 the driver is still responsible for the vehicle but maybe needs to intervene about 5% of the time. The question is whether the driver can handle this as people in general are not good in supervising a machine but will be bored and not necessarily observant. Under L4 the computer is responsible without driver supervision. There is a reluctancy to market a L3 as the vehicle could be marketed as autonomous although in practice it is not and could result in bad reputation for the sector (Kristina Andersson, August 2022).

206 Here a company argues that L3 is considered too complex for the additional benefits of trucks since the driver must be there anyway. Cars (e.g., high-end passenger cars) may have L3. L3 need same technology as L4. L5 is even more complex as it must handle all situations (ODDs) which is why L4 is more explored.

Studies also show that busses and heavy trucks are moving the technology forward quicker since they usual ODD with planned traffic from A to B which is more suitable for L4.[207]

SAE J3016 Level of driving automation

	SAE Level 0	SAE Level 1	SAE Level 2	SAE Level 3	SAE Level 4	SAE Level 5
What does the human in the driver´s seat have to do?	You are driving whenever these driver support features are engaged - even if your feet are off pedals and you are not steering			You are driving whenever these driver support features are engaged - even if your feet are off pedals and you are not steering		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature request. You must drive	These automated driving features will not require you to take over driving	
	These are driver support features			**These are automated driving features**		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering **OR** brake/ acceleration support to the driver	These features provide steering **AND** brake/ acceleration support to the driver	These features can drive the vehicleunder limited conditions and will not operate unless all required conditions are met		These features can drive the vehicleunder all conditions
Example features	automatic emergency braking blind spot warning lane departure warning	lane centering **OR** adaptive cruise control	lane centering **AND** adaptive cruise control at the same time	traffic jam chauffeur	local driverless taxi Pedals/steering wheel may or may not be installed	Same as level 4, but feature can drive everywhere in all conditions

[208]One of the companies interviewed uses sensors, software and machine learning to offer trucks with various levels of automation. In certain applications, the vehicles are capable of handling themselves, while in others a number of supporting systems may be needed. All transport assignments for the company are initiated by a person including the prerequisites for automation. In all functions a truck is limited by its **Operational Design Domain** (**ODD**). ODD means the specified conditions for using a vehicle.[209] This could be the surrounding traffic, speed, weather condition, safety case including remote monitoring/control, infrastructure communication or support drivers to take over when needed.[210] On lower levels of automation in vehicles the systems are often designed to enhance safety, add driver comfort services or improve driving functions. The complexity of the ODD determines the AD technology usage, depending on the use case. Based on the SAE scale L5 means for example unrestricted ODD. One company highlighted that they currently put a considerable effort into Level 4 functionality with a far-reaching testing with

207 From a regulator's perspective, the discussion of SAE-levels are avoided. Instead, the automation levels are defined by the regulatory requirements in legislation. Regulators may see that companies do not share the view of whether a certain level is good or bad but communicate in terms of extended level 2 or conditioned level 4 when the actual level will be 3, and this results in a grey zone. The question of liability and who will be responsible becomes very important in these discussions. It may result in that companies wishing stay on the lower levels to avoid liability but simultaneously push the regulatory boundaries to be able to approach autonomous features but keeping the driver responsible (Swedish Transport Agency, August 2022).

208 SAE International Releases Updated Visual Chart for Its "Levels of Driving Automation" Standard for Self-Driving Vehicles.

209 According to experts there is not however a standardised ODD.

210 Technically the smart and autonomous parts of a vehicle are managed by Electronic Control Units (ECU). These types of computers can amount to up 100 for each vehicle!

commercial traffic hub-to-hub in Sweden and driving on closed venues in various parts of the world. Also, that testing in real traffic is key for the company's R&D thus access to nearby R&D facilities is important, even if test is to be carried out in the US or Asia.

The company focusing on electrifying autonomous trucks started with Advanced Automated Driving Assistance (ADAS) and is now concentrating on Level 4 automation. [211]

In addition to the fact that autonomous vehicles may be classified as AI some of the companies interviewed use AI- techniques to develop driving strategies. They also use ML for various driver assistance systems, for example, **ISA**[212] for the identification of road signs.

Concerning vehicles, it is all about data

When it comes to vehicle regulation experts claim that there is a source of conflict, especially when it comes to access to data – an element that stands out especially for intelligent vehicle regulation, which is why the issue deserves attention here.[213] From a business point of view, companies interviewed express that it is important to control data- and the one who controls connectivity is in charge.[214] One company commented that access to data is restricted only to those that are authorised by the customers (unless there is a legal reason). If vehicle data is sent to an **Original Equipment Manufacturer** (**OEM**), the OEM protecting servers and data from unauthorised actors.

Here it is important to differentiate the data obligations between the ITS directive and the Data Act:

In this context the ITS Directive[215] is about sharing data between vehicles and authorities and vehicle to vehicle data. The Data Act is about giving the data generator (user) access (not ownership) to the data they generate and the right to share that data with third parties. One company argues that ITS directive is balanced but that the upcoming access to in-vehicle data and resources are problematic, setting safety and cybersecurity at risk if third parties are given direct access to the vehicle functions.

Further there is the issue of incentive to investment – i.e., finding a balance with investing in data on one hand and letting others use it for innovation. Vehicle data must be stored in the cloud as the capacity to store data in a vehicle is limited.

The oncoming Data Act promotes more data sharing (for improved climate and to address crowding) and aims to grant data to users and third parties (a horizontal act not limited to vehicles or those connected to ITS). Here the representatives of industry that have been consulted for this study are hesitant, especially with respect to security (no control over data access), as factory data constitute a valuable information asset. From a consumer perspec-

211 See: https://en.wikipedia.org/wiki/Advanced_driver-assistance_systems

212 Intelligent Speed Adaptation (ISA) is an in-vehicle system that supports drivers' compliance with the speed limit. ISA is in fact a collective term for various systems. Field trials and driving simulator studies show positive effects on speed behavior and expect significant safety effects. Some studies report negative side effects of ISA, but there is yet insufficient insight into the size of these possible negative side effects and their consequences. Around one quarter of European car drivers considers a speed-limiting device like ISA to be very useful; actual experience with ISA seems to increase acceptance, see Intelligent Speed Adaptation (ISA) | Mobility and transport (europa.eu)

213 There are already problem areas where manufacturers wish to restrict access to data but where third parties claim right to access. This is regulated to some extent in the framework regulation for type approval where manufacturers are obliged to provide information to service stations about reparation and maintenance.

214 The exact data sharing is governed by agreements between manufacturer and suppliers. Some manufacturers share data with suppliers so that they can develop new services while others keep data for themselves.

215 Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

tive, GDPR consent is a basis, but the problem is that it is not verified who the driver is and a question remains about how easy it is to gain access to data compared to before when a car still was a "closed" system.[216] Here authorised garages also have a role to play. To summarise the question of access to data, the industry wishes to remain in control, but policymakers do not share this view.[217] The European Commission e.g., develops new sub areas that result in more data needing to be shared (to address, e.g., climate, crowding and innovation).

With regards to type approval, safety regulations and functional regulations, the companies interviewed see that the regulation of automated driving has increased as a result of some incidents from the early actors in the industry, often related to software used.[218] This has resulted in a revised regulatory outset where new systems cannot be launched on the market without testing. Software updates, a key issue in automated vehicles, are dealt with in UNECE and is also in the EU legislation on type approval of vehicles.

As already mentioned, the Automated Driving System (AD) is itself not fully regulated. Companies interviewed confirm that validation methods (safety cases) are ongoing in UNECE. Companies see a need for the capability to certify AD vehicles, but the regulations should not be too descriptive or inhibit evolution.[219]

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 can 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. The company that operates driverless vehicles questions whether the regulation is really about AI (as the regulation puts a focus on human supervision).

Regulation of AI as well as other aspects related to autonomous vehicles are under development. As a result, manufacturers must apply for exemption from existing (EU and UNECE) regulations for AI use cases, however here the manufacturer must demonstrate how they manage safety.[220] All new applications are approved based on risk assessment. For driverless vehicles type-approval has been decided upon in EU legislation[221], which the businesses expresses is a key issue for present and future development for the European automotive industry.[222] The company also highlights that it is not always the vehicle technique that generates challenges for automated/driverless driving but general traffic rules. E.g., who will place the warning sign on the road, who will communicate with the police or help when an accident has occurred? Currently companies need to innovate solutions

216 In California in the US access to climate data in vehicles has been requested for example.
217 Discussions with Kristina Andersson, RISE, July 2021.
218 It could be stated that the distrust on the part of regulators have increased.
219 The legal framework for autonomous vehicles in the European Union - Business Going Digital
220 In the US it is the manufacturer that provides proof for vehicle safety — in Europe the regulator determines whether a vehicle is safe. It seems that the development is towards more burden of proof by the manufacturer- to show a safety case for regulators (Kristina Andersson, RISE, July 2022).
221 REGULATION (EU) laying down rules for the application of the Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated motor vehicles, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AAres%282022%292667391&qid=1653330410570
222 Type-approval regulation is for small series, 1500 vehicles per type and year.

which become a burden. The company claims that in the Netherlands the authorities have taken a more far-reaching coordination between all parties involved in putting forward test cases.

The companies have furthermore highlighted that there are areas where existing regulations make the implementation of certain automated driving functions cumbersome. There are also areas currently not regulated and the responses reflect that the industry usually takes the "safety first" approach but may use "unregulated" technology to improve products if it is suitable. In these "new" areas, announcements of planned regulations create uncertainties and delay market introductions of technology. For AD there are various approaches in different countries. Concerning the regulation of AI, the EU has been a forerunner, before the Member States.[223] Globally most countries follow the work in UNECE where several proposals are underway that can be used under a type approval process or for self-certification.[224]

Concerning connectivity, it is used for sending data to and from a vehicle. Connectivity is needed for autonomous trucks but if connectivity is lost the vehicles must be able to handle that in a safe way. The vehicle safety systems should not be dependent on remote information, nor should they be dependent on it through regulation. Connectivity is used in AD for non-critical safe operation, although connectivity will be used to ensure that the vehicle remains safe

If analysing connectivity from a broader perspective, one company argued as follows on the various perspectives on connectivity:

"Police and authorities can however require certain "in use" information to be real-time monitored or batched. Customers want "connected" productivity services (and other types of services).

Innovation needs data from "real" applications, data can be extracted remotely or "wired.

Information is not, however, shared with anyone that asks for it, existing information is only shared with respect to customer agreements (or legal obligations), and new data is only created where there is a clear need that outweighs the investment (developments is not only cost, but also priorities over other developments as well). Connectivity and data are in general much in focus and vehicles may need to change to adapt to future regulations that do not always consider the interest of customers or society. Here one company highlighted the upcoming EU Data Act.[225]

Companies stress that the regulations must be written in a manner such that the manufacturer can show evidence that they manage the driving under the relevant boundary conditions within the Operational Design Domain (ODD).

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. Type-approval systems are also harmonised and here the EU has introduced recently a new regulatory framework for the type-approval of the automated driving system (ADS) of fully auto-

223 From a Swedish perspective with a large automotive industry, regulation for the benefit of both development and the use of autonomous vehicles is a key issue for future industrial development.

224 Swedish Transport Agency, August 2022

225 Experts claim that there are larger issues related to mobility data spaces and that legislation that might get importance deal with real-time traffic information that can force data sharing (Kristina Andersson, RISE, July 2022)

mated motor vehicles.[226] Concerning traffic regulations these are national, to some degree harmonised in the Vienna Convention. Here the industry would like to see more harmonisation as some national regulations are not available digitally and still very detailed.

With respect to data, the companies see the objective of GDPR as to protecting data.[227] At the same time the EU work for more access to data , which creates a conflict of interest. As one company pointed out there are two paths concerning software- security or where anyone can alter software in a vehicle. The companies see that the legislators' proposals are alarming and provide parties other than manufacturers to benefit from vehicles. In the end of the day access to many parties contribute to vulnerabilities.[228]

From the view of international trade, it is interesting to highlight that companies also note that they cannot provide connected transport services in some countries that do not allow data leaving the country (like Turkey or Russia with different regulatory settings), which means that the companies need to operate locally.[229] The reasons are that legislation requires local storage and processing, and since other legislations also applies a business decision may be able to not to offer such services in some countries. Also, a local market can be too small for a truck **Original Equipment Manufacturer** (**OEM**) for the development of unique solutions.

Vulnerabilities and risks identified and approaches to address them

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.

UN ECE R155 for cybersecurity[230] will be an explicit requirement also in ADS regulation from the start in addition to R156 for software updates.[231] These two requirements will come into force in the coming years. Both are demanding regulations, but the companies see the benefit they provide.

One of the companies expressed that more advanced cybersecurity results in more advanced ways of hacking them. Certification is a tool for showing that a product is "good enough" at the time it was certified, but no certification can guarantee the unknown (future). As a result, there is a need to look for vulnerabilities outside of regulatory and certification requirements. A part of this is security by design, otherwise known as built-in

226 Adaptation is still required in national law, for example based on criminal responsibility (Kristina Andersson, RISE, October 2022.
227 See, e.g., Chapter 3 and the proposal on the Data Act.
228 At the same time openness to data may be motivated to boost innovation.
229 A means to create trade barriers.
230 UN Regulation No. 155 - Cybersecurity and cybersecurity management system.
231 UN Regulation No. 156 - Software update and software update management system.

security, together with a risk-based approach. Here the companies work together with **AUTO-ISAC**[232], **ISO**[233], **ACEA**[234], **OICA**[235] and a number of other forums.

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. In addition, some heavy vehicles are built in two or more stages, thus systems can be built on a chassis by a bodybuilder.[236] This increases complexity as the vehicle needs to be certified in several steps, which means a shared responsibility and several management systems that coexist for cybersecurity and software updates.

When it comes to transparency and the accidents discussed in the media the companies highlight that there is a system for incident reporting called AUTO-ISAC (intelligence sharing).[237] Further, there will be mandatory reporting through the UNECE regulation into EU type approval.

The most well-known example of an accident involved is the software used by Tesla. An advanced, but not tested software for steering led to accidents, and in practice the problems were created by the software being updated with test versions. This resulted in a situation that it is not allowed to launch new systems on the market without testing. Requirements are to be found in software update -regulations in UNECE and also in type approval requirements within the EU.

Experts claim that established manufacturers take security-by-design very seriously. There is no legislation however that requires full transparency with respect to cyber incidents (i.e., that obliges manufacturers to inform about a hacking attack). Nevertheless, serious safety risks are to be notified to transport authorities in Sweden, which may require a ban on driving according to legislation. Studies carried out to map cybersecurity in intelligent road transport indicate that the cyber frameworks are fragmented and complex. As in any sector, different regulations address various objectives with requirements that apply to many different stakeholders and businesses. The harmonisation of the regulation of data e.g., the integration of data protection in NIS, civil law for robotics and ITS indicate that the integrity of individuals is in focus in cyber regulation within the transport sector. It could also be concluded that the regulative measures focus on organisational aspects of cybersecurity, as the technical measures need to be adapted according to the business and technology development. The key measures concern aspects such as notification and consultation, identification of risks, addressing security and incident reporting.

---

232 Auto-ISAC was formed in August 2015 by automakers to establish a global information sharing community to address vehicle cybersecurity risks. Auto-ISAC operates a central hub for sharing, tracking and analysing intelligence about cyber threats, vulnerabilities and incidents related to the connected vehicle.

233 TF for ISO 21434

234 European Automobile Manufacturers Association.

235 Organisation Internationale des Constructeurs d'Automobiles- International Organisation of Motor Vehicle Manufacturers.

236 A vehicle (any vehicle) can be sent to a body builder for further enhancements (a crane on a truck, fire truck equipment, bodies on a bus chassis), i.e., a manufacturer can deliver a truck without a body and without side and rear underrun protection which means that an "incomplete" vehicle is type-approved. A body builder that builds the body and mounts suitable side and rear protection thereafter only needs to approve the systems added or affected, not the whole vehicle. Each actor is only responsible for their own "builds". For cybersecurity it can be the case that the body builder needs to add some system that needs to communicate with the truck's other systems which the manufacturer needs to secure since the interface becomes and attack vector for cyberthreats.

237 The Automotive Information Sharing and Analysis Center is an industry-driven community to share and analyze intelligence about emerging cybersecurity risks to the vehicle, and to collectively enhance vehicle cybersecurity capabilities across the global automotive industry, including light- and heavy-duty vehicle OEMs, suppliers and the commercial vehicle sector. See Auto-ISAC — Automotive Information Sharing & Analysis Center (automotiveisac.com)

Based on findings there is room for improvement,[238] especially with respect to public private partnerships and collaboration with research.

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).[239]

Change in regulatory parameters and considerations

If we trust the manufacturers' statistics concerning cars that drive on autopilot, we could make the assumption that autonomous driving in general has come far. The miles driven do not, however, provide the whole picture. This does not say that vehicle intelligence provided by AI has not come far – on the contrary more and more sophisticated driving features and automation are being delivered.

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.[240] 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[241] 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.

The main takeaway from the vehicle sector is the competence around digital intelligence in the sector developed successively over a longer period – addressing product safety and security in a more systematic manner related to vehicle functions. This does not, however, equate 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.

238 FOI, *Lag och cybersäkerhet i smart vägtrafik,* december 2019

239 From a Member State perspective representatives of businesses highlight that EU-and global frameworks for technical regulation are the key for maintaining positions on innovation and export- which is why it is important that EU regulatory frameworks are well adapted.

240 As pointed out, there is no type-approved level 4 vehicle and very little on level 3 at least in Europe.

241 This is equal to **Software Development Life Cycle** (SDLC), Serving Mobile Location Centre (SMLC) as well as capabilities for auditing. Syvänne, September 2022.

4. 4 General conclusions on AI innovation and technical regulation

Based on the information presented in the cases, of the use of digital innovation and the utilisation of AI are not regarded as new phenomena by the companies interviewed in the fields of medical devices, mobiles and vehicles. More automated and intelligent products utilising algorithms have already been on the market since the 1990s. The novelty is in the degree of sophistication and new application areas of AI in products. In general, some companies may dodge the concept of whether their products and systems involve AI, which is understandable, as the perception is that AI is still poorly defined in regulatory frameworks. The case also demonstrates that AD and the use of data are addressed differently in various countries.

What differs in earlier AI applications compared to the ones used today is that modern AI solutions make more active choices themselves based on data and can thus support more complex decision making.

Contrary to what could be expected when observing discussions on the need to regulate AI in various forums, AI is rather strictly regulated in the sectors covered by this analysis and to a high degree dependent on human control and intervention. For example, self-driving trucks are authorised for use as test cases when operated in a professional context between working sites and under the full control of a human. The same goes for the application of AI in medical devices that must be preceded by clinical trials, managed by health care providers and the use supervised by doctors.

It is obvious also that the manufacturing and development of AI is not a temporary hype. In the established product sectors, it is driven by the innovation to solve new customer needs and use cases.[242] As one company put it: *"Technology must serve a purpose, be it customers, environment, road users, road operators, enforcers, or vehicle manufacturers. (AI) Technology is seldom the driver or end by itself - we start with a use case and then apply a technology to achieve it."* In the case of trucks, the ambition of AI could be to make transport flows more efficient. As there is a lack of drivers, AI could contribute with resources. Also, traffic safety can benefit from AI.

The regulatory challenges materialise in the access and control of data that is central for AI application and by the fact that the data, including software are regulated or will be regulated in many legislative frameworks at the same time, although sometimes the regulatory objectives are contradictory (openness and access to data vs. closed systems, requirements on protecting data and addressing cybersecurity).

It is evident from this analysis that adding an AI layer on an industrial product is not without any vulnerabilities and risk. When focusing on AI, privacy and personal integrity are the top issues at stake. To systematically identify risks would require more insight into many aspects that existing product reporting systems might not necessarily manage to identify. This is because, much can happen with a digital software-based product that is not visible to the eye, nor easy to control or verify. As the focus of this analysis is not product safety or security gaps, it might suffice to question whether the multitude of digital regulations (or most of the proposals) really will work seamlessly and whether it is clear for all stakeholders which regulatory risks (safety, security, privacy, resilience) they are addressing. Based on this first review we remain puzzled by the regulatory complexity!

242 See also: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises

As a result, we might need to accept that digital innovation may never be fully controllable and will definitely require new regulatory approaches!

An important point that was raised by the experts we interviewed is that generic software and related system components are seldomly designed and used for a single specific purpose (following e.g., a specific sector legislation) but used by industry in "non intended" areas as long as there is a business case (which in itself complicates software auditing from a regulatory point of view). In other words, multi-purpose software can end up in medical devices (both intended and unintended) with various regulatory outcomes. Modern software solutions also typically consist of dozens of individual components, some creating strict dependencies and some being, usually of OSS[243] origin. The AI-layer will complicate the scenario even further as it may be almost impossible to control or regulate. Self-learning algorithms, where the outcomes of innovation can come as a surprise even for the developer. This complicates a regulatory approach that tries to foresee risks as near-impossible or at least near-financially feasible.[244] These factors may challenge the perception that a regulation can guarantee that a product should not change during its life cycle.

243 **Open-source software** (OSS) is computer software that is released under a license in which the copyright holder grants users the rights to use, study, change, and distribute the software and its source code to anyone and for any purpose.

244 Syvänne, September 2022.

Main findings from sectors

	Mobile phones	Medical devices	Vehicles — trucks
AI TECHNOLOGY AND REGULATION	ML and AI are essential part enabling smart phone features such as speech-, image- and voice recognition. AI as technology is sparsely regulated — the regulatory focus is on data, protecting communication networks and privacy as well as on preventing fraud Some standards exist but not necessarily for AI use cases.	ML and AI are important parameters in making health care more efficient e.g, by the analysis of x-rays, cancer screening, prediction of diseases. The current (EU) regulatory framework does not address a self-learning AI system specifically but has instead focused on Software as Medical Device (SaMD). Many aspects also impede the use of AI in medical devices, including the parameter of addressing "continuous change" in products.	AI in the vehicle sector is supported by ML and AI, although the concepts do not equal fully autonomous driving. The application of ML and 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. The Automated Driving System (AD) itself is not fully regulated but validation methods are prepared.
VULNERABILITIES AND RISKS IDENTIFIED	Lack of control in supply chains is pointed out as a major challenge. Add-ons in software by third parties means that many compliance parameters are out of reach. Cybersecurity pointed out as the main risk. Also, the impacts of risks related to AI (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).	In the field of medical devices, the unintended application of software, i.e., businesses not observing existing regulatory framework for medical devices constitutes a challenge. There is a risk that AI adapts changes "on the job" (real life on patients) which is not allowed. Cybersecurity highlighted as an important challenge.	There are 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. Also, there are worry about requirements on openness of data that is perceived as a risk for additional vulnerabilities in the sector, especially given cyberthreats.
CHANGE IN REGULATORY PARAMETERS	The 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 concept of AI is still poorly defined — at the same time AI 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.	A 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.

5. The Invisible Hand in the digital economy – regulatory impact analysis

This study was initiated to shed light on in which manner the utilisation of technologies such as AI on one hand, and increasing vulnerabilities, especially cyber vulnerabilities on the other, affect the properties of industrial goods and how this should be regarded in the technical regulation.

The key in the analysis lies in an approach where the Board has studied three sectors that make use of AI but that are also affected by cyber vulnerabilities.

By interviewing representatives of business in the three sectors as well as experts and regulatory authorities the Board wished to draw some preliminary conclusions on whether the elements of the current regulatory model and techniques are still valid.

Our findings are as follows:

Innovation is boosting trade but can radically challenge traditional trade policy frameworks

A digitalised market is here to stay. Innovative products respond not only to the needs in our society regarding efficiency, such as new customer features (and well adapted, interoperability), but can also contribute to our commitments towards the green transition and sustainable development.[245]

The core of many innovative digital products is software, that allows and requires continuous improvements along the product's life cycle. The downside is that the potential vulnerabilities arise, and these need to be monitored.

Furthermore, innovative business increasingly involves manufacturing and delivering customised solutions. These aspects may challenge the role of standardised product

245 Digitalisation and AI can specifically contribute to green transition and sustainability. See The role of artificial intelligence in achieving the Sustainable Development Goals | Nature Communications. However, some climate change mitigation gains can also be reduced or counterbalanced by growth in demand for goods and services due to the use of digital devices. See IPCC Intergovernmental Panel for Climate Change- *Climate Change 2022- Mitigation of Climate Change*, Working Group III contribution to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change, WMO-UNEP, 2022

requirements and current trade policy frameworks referring to international standards. This is because, standards - the way they are prepared and designed today - might be too slow to cover the fast technological changes, and the regulations might not be able to grasp the foreseeable use of products. Furthermore, regulatory challenges related to innovation are often sector specific. This implies that when technologies such as AI are being addressed, much more effective cross-sectoral policy coordination as well as common enforcement mechanisms will be needed to avoid regulatory gaps creating uncertainty and trade barriers.[246] Concerning data, our case studies also show that data-related localisation requirements vary, and thus condition business operations in various markets.

Product or Service — does it matter?

Although discussions with companies often bring up the blurring interface between products and services, it is not this product-service interface that is highlighted as the key element for regulatory uncertainty concerning automated, intelligent products and features. Instead, the challenges are often revealed in the multiple aspects that are related to data, e.g., access to data (cross border, clinical trials), use of data (GDPR) and the choice of using (or not) ML and AI managing the software.

The regulatory landscape has changed — Digital innovation increases regulatory complexity!

Not surprisingly, our analysis reveals 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 new (and proposed) 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 Regulation on AI (AI Act) 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 regulatory 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

246 See also: WTO/WEF, The Promise of TradeTech- Policy approached to harness trade digitalisation, 2022.

seems to explore the regulatory boundaries a bit more, arguing for exceptions from legislation 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.[247]

Generally speaking, the introduction and application of AI technology equals moving from standardised products to more customised ones.[248] 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 can 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 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 digital properties.

In practice, current digital regulation means that sector-specific regulations for products 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 a danger in that the concepts and regulatory objectives of product safety, cybersecurity, privacy and resilience (and their interconnections) are not necessary yet clearly defined digital regulation - something that policy makers should be attentive to, as current regulatory processes often mean that various areas and regulators work in silos.

It should be noted that traditional sector-specific product regulations in the EU had focus on product safety and harmonisation while digital frameworks expand regulatory objectives related to data, interoperability, resilience and privacy. 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

247 This does not necessarily cover the whole picture as this can also entail serious risks of other characteristics, but these fall outside the scope of this study.

248 When it comes to the application of AI there might be products that have the same technical execution and performance from the start but can be adaptable in the environment where used.

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 can lead to misunderstanding and false approaches in regulation.

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 technical regulation risks becoming outdated (if it tries to scope in advance the regulatory outcomes of innovation that are not yet fully known)

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 new challenge for regulators. Also, the risks, vulnerabilities and other effects generated by the use of AI in various products are not yet fully known. As a result, we have seen a quick wakening on the regulators side and efforts to address the use of AI by new 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.[249]

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, quickly evolving AI use cases in legislation – a scenario that is still far away from reality.

Products utilising AI — safe and secure?

This analysis has only scratched the surface concerning the use of more mature AI innovation in three sectors.

The objective of this study has not been the identification of safety gaps or risks in products related to AI, other than those specifically related to cybersecurity. Instead, we have focused on the feasibility of regulatory techniques available.

---

249 This perception might be boosted by the discussions of the necessity to address ethics in AI. As Mandel (2009) put it "Emerging technologies, it seems provide an area of significant regulatory sensibility in terms of striking balance between promises of innovation, on one hand, and concerns about risk and a related lack of public confidence on the other. It is critical to industry that the public not lose faith in a technology or its risk-governance system at early stages of technological development. Concern about technological risk and uncertainty about how a technology will be governed can lead investors to be unwilling to invest in the technology and can make it more difficult for firms to know how to proceed with research, development, and commercialization."

It can be argued that the companies embraced by this study, 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 equate risks and safety hazards- but to identify and trace actual effects and vulnerabilities along a product life cycle is, and will be, the major regulatory challenge.

It is also worthwhile mentioning 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. These 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 pop up 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.

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 however, 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 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[250] our perception is that they such should be founded on evidence (e.g., by thoroughgoing regulatory impact assessments), as approaches that try to "scope the unknown" are likely be both costly and inefficient.[251]

Based on our analysis various countries and markets approach the regulatory challenges with AI differently (compare the EU and the US).

250 See; National Board of Trade, The Cyber Effect, 2018.

251 See, however: Office for product safety and standards, *Study on the Impact of Artificial Intelligence on Product Safety Final* Report December 2022.

When designing 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 actually 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 can 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.[252] 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.

Regulatory uncertainties and gaps

The regulatory uncertainties identified by the companies interviewed for this study are mostly related to a lack of straightforward guidance concerning whether their product falls under various legislation (proposal for the 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.

Concerning data, our case studies show that data-related localisation requirements vary and thus set the terms for market access in various countries.

Businesses also highlight that to address cyber vulnerabilities there should be greater expertise among regulators 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.

252 It should be noted however that incident reporting systems are only a complementary source of information, not the only one you can rely on. For example, a company could be unaware of existing problems or unwilling o analyse a problem. A stakeholder could be unwilling to share information about an incident or not prioritise it among other activities. Finally incident reporting systems could lack sophistication which means that benefitting from the information in a system becomes limited.

Can the digital market with "virtual" products be regulated?

The study's underlying questions are: Who is taking responsibility for the digital market when digital regulatory frameworks are still under development? Is there a mechanism that covers up eventual failures in terms of non-compliant products, if products are not as tangible as before and thus partly "invisible" to the regulator? Where are the means to control compliance when market surveillance has been weakened? Is the digital market 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 due to the fact that 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, policy makers and regulators may need to be aware that digital intelligence can be subjected to change and will never be fully controllable, taking this into account in the preparation of regulatory strategies addressing the digital market.

5.1 Policy recommendations

Based on this insight into digital product regulation 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 than 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 European Regulation on AI (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 assessing 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 data-based goods — more focus is needed on security-by-design[253] and approaches taking the whole product life cycle into account

Digital innovation is dependent on the access and use of data. Functioning innovation is also dependent on qualitative data[254] that is representative for the specific use case. As software is the main component of digital products, the regulatory challenge is presented in terms of the degree of insight into data, and capabilities for traceability and auditability (enabling the possibility to monitor product characteristics), as the standardised product requirements are not necessarily applicable to the same extent as before. This differs from physical products where the features are relatively stable and where the product characteristics can be verified more easily and are not, due to a lack of connectivity, algorithms and customisation, as easily affected by external and unforeseen factors like cyberthreats.

As a consequence, security-by-design for products and processes should be discussed to a larger extent in the regulatory frameworks. Security-by-design is an approach to software and hardware development that seeks to make systems as free from vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices. In other words, the idea is to "build in" safety and security in a product from the very start. It should be highlighted, however, that a methodology for this is not straight forward due to complex trade patterns and global value chains, and this requires sectors-specific consideration. To exemplify, modern software is generated by hundreds if not thousands of delivery chains, each of which can involve several stakeholders that are responsible for components. To complicate this even further, when discussing open source, some components might be produced by several companies simultaneously in a decentralised model. Some of these components will in addition constitute the same component in other products that have been used for some time. This makes security-by-design (i.e., building in security from the very start) a challenge but it is definitely something to analyse further!

In addition, the distinction of the role various software plays in industrial goods require special regulatory consideration – it is not only a question of requirements on software updates, but by which means a change in critical product characteristics can be traced after products, processes and related services have been put on the market dependent on ownership and access to data. As mentioned earlier in this report software and system components are not necessarily only used for the specific use case as perceived in sectoral legislation but as suited for any innovative business case. Further, as highlighted before by the Board, cybersecurity has a major impact on trade and regulation, which should be better addressed in regulatory policy coordination.

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

Changes in our society related to technological innovation has led to many new horizontal regulatory layers on top of traditional regulatory frameworks within sectors that address product safety and the environment. The regulatory layers presented in this report related

253 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.

254 Combining datasets and increasing the amount of relevant data to be analysed is the starting point for all AI. The more data, the more conclusions and correlations can be made from it. Syvänne, September, 2022.

to AI and cybersecurity risk creating negative impacts trade through fragmentation, uncertainty and trade barriers if not coordinated properly. With lack of international harmonisation and standards, the frameworks will be extremely difficult to navigate, not to mention enforced, by regulators, which is why these questions need to be addressed now.

Moreover, our analysis shows that the possible use cases for AI may be unique and not necessarily adapted to international harmonisation due to increasing customisation and connectivity, which mean that product properties can change constantly, due in part to vulnerabilities and security threats. Many of the regulatory challenges presented in this report are certainly acknowledged by regulatory bodies but the possible regulatory solutions risk becoming obsolete before the actual regulatory solutions are mature enough to see daylight.

Our evaluation is that for digital products new enforcement mechanisms will be needed to complement or enhance post-market surveillance. The main reason for our recommendation to look into this more closely is that existing digital frameworks are still vague and do not necessarily provide for effective enforcement. 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 of digital products are thus required, also to address a Level Playing Field.

This entails investments in new competences covering multiple product related digital parameters for the government bodies responsible for "product safety". 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 new regulatory parameters such as "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.

This should also entail intensified cross-sectoral market surveillance collaboration.

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 can 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, the National Board of Trade Sweden sees 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. The result is materialised in the lack of a Level Playing Field with the same rules for market actors, potential regulatory gaps and trade barriers as there is no overview of what is applicable for a certain product. The situation also complicates things the regulators, as there are few chances to gain insight and monitor the developments. Here policy makers and regulators need to step up and coordinate themselves!

The regulatory outsets in the digital economy

Current regulatory setting	New elements	Effect on regulation
Harmonised requirements for harmonised goods	Increased customisation? YES, but highly dependent on sectors The main challenge is the multitude of new horizontal digital- and security-related legal frameworks Regulation still follows the scope of well- defined products and sectors while digital innovation applied is driven by multiple possible new use cases.	EFFECT ON REGULATION? More specified requirements requiring sectoral approach will be needed however these can be impossible to "standardise" for regulatory certainty. AI innovation and a multitude of digital vulnerabilities has led to the introduction of new horizontal regulatory layers on top existing sectoral regulation but where there is a risk that regulatory objectives of product safety, security, privacy and resilience are not communicated clearly by the regulator. The trade complexity risk gaps if the various interrelated regulatory proposals are not well coordinated- an aspect to be better integrated in trade policy.
Product properties static during the product life cycle	Product properties can change during product' life cycle? YES. The major game changer is that products are based on software. Also, the safety and risk levels expressed in "essential requirements" in existing sector specific regulation and the new horizontal layers in digital regulation do not necessarily speak the same language. Changing properties are not only related to conscious choices but the complex supply chains and the introduction of AI that is not controllable.	EFFECT ON REGULATION? When addressing technology challenges such as AI and cybersecurity the regulator must, however, regard the sector-specific functionality requirements of a product. The focus should be on specific use cases of software and AI not the technology itself! More focus is needed on "constant change", traceability and auditability.
Products manufactured on-site and product properties not vulnerable to alterations	Products manufactured off-site (remotely), autonomously and connected product properties can be manipulated due to cyber vulnerabilities? YES. The **cyber threat** is the biggest security challenge identified by companies using innovative digital in the study.	EFFECT ON REGULATION? All cyber vulnerabilities cannot be addressed in legislation as the risks materialise in real time. However, there are many tools to enhance cybersecurity by regulatory frameworks such as the requirement for software updates that have a life-cycle approach to products. Based on the analysis the regulatory "cyber toolbox" is currently more solid than the "AI toolbox". This does not however mean that digital safety or security can be fully controlled by regulation.
Enforcement of product compliance through physical examination, documentation control and testing/ certification	Customisation makes traceability and enforcement of product safety and cybersecurity more challenging — many products (or properties) are changing constantly. This does not necessarily mean that safety or security critical properties will do so — however, an identification of high-risk use cases should be prioritised.	EFFECT ON REGULATION AND MARKET SURVEILLANCE? Security-by-design becomes more important, especially in technical regulation. The methodologies to apply security-by design require much more analysis as the methodology is complicated by the complex supply chains (all of which have effect on changes in product properties). New methods and tools for product "safety" enforcement (market surveillance) might be needed in terms of an approach enabling "continuous compliance" i.e., a life-cycle approach to enforcement with improved capabilities for "data management and security" (strengthening traceability and auditability).

References

Ailisto, Neuvonen, Nyman, Halen, Seppälä, *En helhetsbild av artificiell intelligens samt en nationell kartläggning av kunnande- slutrapport*, Statsrådets kansli, 2018

A. Bakardjieva et al., *The European Union and the Technology Shift*, 2021.

Boyd, M., and Willson N., 'Rapid developments in Artificial Intelligence: How might the New Zeeland government respond?' Policy Quarterly, vol. 13, no. 4, 2017.

COCIR, *Artificial Intelligence in Healthcare- First Publication of AI Use cases,* 2020.

Communication from the European Commission to the European Parliament, The Council and the European Economic and Social Committee and the Committee of the Regions *Trade Policy Review - An Open, Sustainable and Assertive Trade Policy,* 2021.

Communication from the European Commission to the European Parliament, The Council and the European Economic and Social Committee and the Committee of the *Regions-Updating the 2020 Industrial Strategy: towards a stronger Single Market for Europe's recovery,* 2021.

Convington, Inside Tech Media, *AI Update: White House Issues 10 Principles for Artificial Intelligence Regulation*, 2020.

Deamer. K, 'What the First Driverless Car Fatality Means for Self-Driving Tech', *Scientific American*, vol. 1, 2019.

Engler, A., *The EU AI Act will have global impact, but a limited Brussels Effect*. Brookings, 2022.

ENISA & European Commission, *Cybersecurity Challenges Challenges in the Uptake of Artificial Intelligence in Autonomous Driving*, 2021.

European Commission, The High-Level Expert Group on Artificial Intelligence, *Opinion of the Sub-group on Artificial Intelligence (AI), Connected Products and Other New Challenges in Product Safety to Consumer Safety Network*, 2020.

European Commission, *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics,* Brussels, 2020.

European Commission, The Blue Guide on the Implementation of EU Product Rules, 2022.

European Commission, *White Paper- On Artificial Intelligence- A European approach to excellence and trust*, Brussels, 2020.

J. Gesley et al., *Regulation of Artificial Intelligence in Selected Jurisdictions, Law Library of Congress,* Global Legal Research Directorate, 2019.

G20 Ministerial Statement on Trade and Digital Economy (PDF). Tsukuba City, Japan, G20, 2019.

López Gonzáles J. and Ferencz, J., *Digital Trade and Market Openness,* OECD Trade Policy Papers, no. 205, OECD Publishing, Paris, 2017.

G. Mandel, D. Braman, and D. Kahan, 'Cultural Cognition and Synthetic Biology Risk Perceptions: A Preliminary Analysis'., 2008.

Mendel, G.M., 2009, 'Regulating Emerging Technologies, Law, Innovation and Technology', vol. 1, no. 1

National Board of Trade, *Online Trade- Offline Rules*. A Review of Barriers to E-commerce in the EU, 2015.

National Board of Trade Sweden, *The Cyber Effect*. The implications of IT security regulation on international trade, 2018.

National Board of Trade, *The Servicification of EU Manufacturing. Building Competitiveness in the Internal Market* 2016:4

National Board of Trade Sweden, *The Fourth Industrial Revolution. Changing the trade as we know it*, 2019.

National Board of Trade, *Trade Regulation in a 3D Printed World- a Primer*, 2016.

National Board of Trade, Statement of opinion on proposal for harmonised rules on artificial intelligence, Dnr 2021/00825-2

NIST, U.S: *Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, Prepared in response to Executive Order 13859, 2019.

Nordea, AI: The dawn of the data age, Nordea Corporate and Investment Banking, 2019.

OECD, *Artificial Intelligence and International Trade: Some Preliminary Implications*, Working Party of the Trade Committee, TAD/TC/WP (2021)22, 2021.

Office for product safety & standards, *Study on the Impact of Artificial Intelligence on Product Safety - Final Report*, 2021

Proposal for a Regulation of the European Parliament and of the Council laying down

Harmonized rules on Artificial Intelligence and amending certain Union legislative acts,

Brussels, 2021.

Rühlig, T.M., 'Technical Standardization, China and the future international order- A European Perspective', *The Swedish Institute of International Affairs*, Brussels, 2020.

S. Wennberg, E. Zouave, and M. Jaitner, *Lag och cybersäkerhet i smart vägtrafik*, FOI-R--4811—SE, 2019.

Schwab, *The Fourth Industrial Revolution: what it means, how to respond*, World Economic Forum, 2016.

Scientific Foresight Unit (STOA), European Parliamentary Research Unit (EPRS), *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, 2020.

Swedish Civil Contingencies Agency, Statement of opinion on NIS 2, MSB 2021-06424

Statens offentliga utredningar från Näringsdepartementet, *Vägen till självkörande fordon – introduktion*, SOU, 2018, p.16

The Law Library of Congress, Global Legal Research Directorate, *Regulation of Artificial Intelligence in Selected Jurisdictions,* 2019.

Tsang, Kracov, Mulryne, Strom, Perkins, Dickinson, Jones, 'The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States', *Intellectual Property & Technology Law Journal*, 2017.

Valassi and Karresand, Cyber Physical Vulnerabilities in Heavy Vehicles, FOI, 2020.

R. Vinuesa et al., 'The role of artificial intelligence in achieving the Sustainable Development Goals', *Nature Communications* vol. 11, no. 233, 2020.

WMO/UNEP, IPCC Intergovernmental Panel for *Climate Change- Climate Change 2022- Mitigation of Climate Change*, Working Group III contribution to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change, 2022.

World Economic Forum & World Trade Organization, *The Promise of TradeTech- Policy approaches to harness trade digitalization*, 2022.

World Economic Forum, *White Paper- Guidelines for AI Procurement*, webforum, 2019.

Glossary

Accreditation

Accreditation is a formal evaluation of competence that is based on regional or international standards. It is a method and tool to evaluate and approve organisations/ bodies that inspect, certify, and verify other parties' products, services, plants or systems. Accreditation is carried out by an accreditation body. Accreditation is used both in mandatory and voluntary areas.

Additive manufacturing

Additive manufacturing or 3D printing is the construction of a three-dimensional objects from a CAD model or a digital 3D model.

Application programming

An application programming interface (API) is a way for two or more computer programmes to communicate with each other. It is a type of software interface, offering a service to other pieces of software.

Artificial Intelligence

Artificial intelligence (AI) is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalise, or learn from past experience.

Artificial Intelligence systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on that knowledge, or processing the information derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.

The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."

A possible means to describe AI is in describing it in various knowledge areas such as Data Analytics, Perception and Situational Awareness, Natural Language Processing (NLP), Interaction with Human Beings, Occupational Digi Competences (like creative computing and problem solving), Machine Learning, Robotics and Machine Automation, and Regulation.

Automation

Automation is the technology by which a process or procedure is performed with minimal human assistance. Automation, or automatic control, is the use of various control systems for operating equipment such as machin-

ery, processes in factories, boilers, heat-treating ovens, switching on telephone networks, steering, the stabilisation of ships, aircraft, and other applications, and vehicles with minimal or reduced human intervention.

Automation covers applications ranging from a household thermostat controlling a boiler, to a large industrial control system with tens of thousands of input measurements and output control signals. In control complexity, it can range from simple on-off control to multi-variable high-level algorithms.

Autonomous vehicle

Autonomous vehicle (AV) is a vehicle capable of sensing its environment and operating without human involvement. Such vehicles can be classified according to several levels of automation.

It is also referred to as a semi-autonomous car, an Automated Driving System-Dedicated Vehicle (ADS-DV).

The J3016 standard defines six levels of driving automation, from SAE Level Zero (no automation) to SAE Level 5 (full vehicle autonomy).

Big Data

Big Data is a field that treats ways to analyse and systematically extract information from, or otherwise deal with, data sets that are too large or complex to be dealt with by traditional data-processing application software.

Blockchain

A blockchain is a type of distributed ledger technology (DTL) that consists of growing lists of records called blocks that are securely linked together using cryptography.

Chatbot

A chatbot or chatterbot is a software application used to conduct an on-line chat conversation via text or text-to-speech in lieu of providing direct contact with a live human agent.

Cloud

Cloud storage is a model of data storage in which the digital data are stored in logical pools. The physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting comapany. These cloud storage providers are responsiable for keeping the data available and accessible and the physical environment protected and operating. People and organisations buy or lease storage capacity from the providers to store user, organisation, or application data.

Conformity Assessment

Conformity assessment (or Conformity Assessment Procedures - CAP) is used to assess whether a product is in compliance with product requirements. It can include, for example, product testing, inspection and certification procedures.

Critical infrastructure

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy.

Cryptography

Cryptography can be described as a discipline, which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification and/or prevent its unauthorised use. A cipher (or cypher) is an algorithm that transforms meaningful data into seemingly random data, and back again, when needed. Encryption is the act of scrambling the data, and decryption is the act of restoring the data to its original form. To encrypt or decrypt a key is needed. The key is the only part of a cipher that should need to be kept secret for the cipher to remain secure (i.e., even if everything else is known about the cipher it should still not be possible to decrypt a text without knowing the key). How strong a cipher is (i.e., how easily it is broken) is usually directly dependent on the length of the key. Applications of cryptography are, for example, used to protect ATM cards, computer passwords and Internet transactions. Cryptographic means are also frequently used in e-id and electronic signatures. Depending on the proliferation of an individual product and its use area, an incident (for example, Heartbleed, vulnerabilities in a program library OpenSSL and Freak, deficiencies in crypto standards) can seriously affect the users involved and be dangerous from a societal point of view. Even if there are flaws in algorithms and protocols, however, many of the failures in cryptographic systems come from implementation errors (e.g., Heartbleed) or an improper use (e.g., Freak) of the system. In economic terms, it could be argued that a cipher key represents the aggregated value of all the information that is protected by it, for example, all bank transactions, the correct status of electricity supply in a given city/country or communication with a ministry. Cybercrime, or computer related crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)". Cybercrime may threaten a person's or a nation's security and financial health. See also Encryption.

Cyber resilience	Cyber resilience refers to an entity's ability to deliver the intended outcome continuously despite an adverse cyber event, even when regular delivery mechanisms have failed, such as during a crisis and after a security breach. The concept also includes the ability to restore regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of new risks. Backups and disaster recovery operations are part of the process of restoring delivery mechanisms.
Cyber threat	Cyber threat means any potential circumstance or event that may damage, disrupt or otherwise adversely influence networks and information systems, their users and affected persons.
Cybersecurity	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 confidentiaality of the information contained therein. In this report, 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. See also: Information security.
Deep learning	Deep learning (also known as deep structured learning) is part of a broader family of machine learning method. Learning can be supervised, semi-supervised or unsupervised. Deep learning is a key technology behind driverless cars, enabling them to recognise a stop sign, or to distinguish a pedestrian from a lamppost
Denial-of-Service Attacks	Denial-of-service attack (DoS attack). In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet. Denial-of-service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack by simply blocking a single source.
Digitalisation	Digitalisation is the process of converting information into a digital (i.e., computer-readable) format. A digitalised society implies a society that is formed as a result of

	the adoption and integration of Information and Communication Technologies (ICT) at home and work, and in education and recreation, and supported by advanced telecommunications and wireless connectivity systems and solutions.
Embedded software	Embedded software (in a product) concerns the properties of a product where the software is embedded in hardware or non-PC devices (compare: Non-embedded software).
Encryption	Encryption is an important parameter in creating IT security. Cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages. See Cryptography.
Federated data	A data federation is a software process that allows multiple databases to function as one. The virtual database takes data from a range of sources and converts them all to a common model. This provides a single source of data for front-end applications. A data federation is a part of the data virtualisation framework.
Firewall	In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external networks, such as the Internet.
Front-end applications	Any web or mobile application divided into two parts. The front-end is what a user sees and interacts with (user interface). The back-end is part of the application that is hidden from the user. This part is responsible for data processing, storing the data, and mathematical operations.
Global Value Chains	International production, trade and investments are increasingly organised within so-called Global Value Chains (GVCs) where the different stages of the production process are located across different countries. Globalisation motivates companies to restructure their operations internationally through outsourcing and offshoring of activities.
Information security	The objective of information security is to protect information so that it will always be available when needed (availability), trustworthy, not manipulated or destroyed (integrity), only accessible by authorised persons, and possible to follow concerning how and when it 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 poliacies). Compare with Cybersecurity.

Internet of Things (IoT)

Internet of Things is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators and network connectivity, which enable these objects to connect and exchange data.

Level Playing Field

In trade policy, a Level Playing Field is a concept about fairness, where each player plays by the same set of rules.

Malware

Malware, short for malicious software, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

Market Surveillance

Market surveillance is the activity carried out by authorities to ensure that products on the market conform to the applicable laws and regulations and comply with the existing EU health and safety requirements. Effective market surveillance should also contribute to a Level Playing Field with the same rules applicable to all companies.

Metadata

Metadata is data that provides information about other data. In other words, it is "data about data". Many distinct types of metadata exist, including descriptive metadata, structural metadata, administrative metadata, reference metadata, statistical metadata and legal metadata.

Nanomaterials

Nanomaterials can be defined as materials possessing, at a minimum, one external dimension measuring 1-100nm. The definition given by the European Commission states that the particle size of at least half of the particles in the number size distribution must measure 100nm or below.

Nanomaterials can occur naturally, be created as the by-products of combustion reactions, or be produced purposefully through engineering to perform a specialised function. These materials can have different physical and chemical properties compared to their bulk-form counterparts.

New Approach

The Council Resolution on the New Approach to Technical Harmonization and Standards was adopted in 1985 in order to address technical barriers to trade and to promote the free movement of goods within the Internal Market. This resolution aims to recast technical harmonisation within the EU on a new basis by only harmonising the essential requirements of products and by applying the "general reference to standards" formula concerning the principle of mutual recognition in order to eliminate technical obstacles to the free movement of goods.

Notified Bodies

In the EU, an important part of conformity assessment is based on Notified Bodies, which carry out conformity assessment against certain EU Directives and harmonised standards according to the New Approach (see New Approach). Organisations that are accredited and notified

	by Member States may test and verify products in competition with each other in a free market.
Neural Fuzzing	Neural fuzzing is a process that invokes neural networks to generate random input data to find vulnerabilities in software. It is a method for the automated security testing of software.
Non-embedded software	Non-embedded software is a service and is classified as software not being part of a devices when it was placed on the market or software in a service to the end user.
Open-source software	Open-source software (OSS) is computer software that is released under a license in which the copyright holder grants users the rights to use, study, change, and distribute the software and its source code to anyone and for any purpose.
Operational Design Domain	Operational Design Domain or ODD indicates the physical, digital, and atmospheric environments in which autonomous vehicles with their Automated Driving Systems (ADS) can operate safely. By definition, according to SAE standard J3016, an ODD defines where the ADS is designed to operate.
Original Equipment Manufacturer	A company that manufactures parts for use in new vehicles — or the parts themselves.
Pharmacovigilance	Pharmacovigilance is the science and activities relating to the detection, assessment, understanding and prevention of adverse effects or any other medicine/vaccine related problem.
Polymers	A polymer is a substance or material consisting of very large molecules called macromolecules, composed of many repeating subunits.
Proxy server	In computer networking, a proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource. Instead of connecting directly to a server that can fulfil a request for a resource, such as a file or web page, the client directs the request to the proxy server, which evaluates the request and performs the required network transactions.
Ransomware	Ransomware is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim.
Regulatory Impact Assessment	Regulatory Impact Assessment (RIA) is a systemic approach to critically assessing the positive and negative effects of proposed and existing regulations and non-regulatory alternatives. In this report "Regulatory Impact Analysis" is used to describe the effort to summarise the findings in the end of the report.

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, i.e., by building security from the very start.
Servicification	Servicification means that manufacturing increasingly depends on being able to buy service inputs, hire service professionals and sell service outputs.
Social Determinants of Health (SDOH)	Social Determinants of Health are conditions in the places where people live, learn, work, and play that affect a wide range of health risks and outcomes.
Software interface	Computer software, or simply software, is a part of a computer system that consists of data or computer instructions, in contrast to the physical hardware from which the system is built. In computer science and software engineering, computer software is all the information processed by computer systems, programs and data. Computer software includes computer programs, libraries and related non-executable data, such as online documentation or digital media. Computer hardware and software require each other, and neither can be realistically used on its own.
Software Development Life Cycle (SDLC)	Software Development Life Cycle is a process used by the software industry to design, develop and test high quality software. The SDLC aims to produce a high-quality software that meets or exceeds customer expectations and reaches completion within times and cost estimates.
Standards	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.
Technical regulation	Technical regulation refers to mandatory legal documents drafted, adopted and applied 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.

Technical rules	Technical rules is a generic name comprising technical regulations by authorities, requirements on conformity assessment (by authorities) and standards (voluntary).
Technology	Technology refers in this report to the use of technology, innovation, and software to support and digitally transform industry.
Use case	Use case is a specific situation in which a product or service could potentially be used (i.e., application area). In software and system engineering the term use case describes how a user uses a system to accomplish a particular goal.
Vehicle Platooning	Vehicle platooning is part of a suite of features that a self-driving car might employ. A platoon is a group of vehicles that can travel very closely together, safely at high speed. Each vehicle communicates with the other vehicles in the platoon. There is a lead vehicle that controls the speed and direction, and all following vehicles (which have precisely matched braking and acceleration) respond to the lead vehicle's movement. Original ideas for vehicle platoons involved some kind of mechanical coupling, as with a train. Modern communication such as Bluetooth and wireless, GPS, radar-sensing systems plus drive-by-wire steering and throttle allows for computers to take control of cars. 5G communications may assist in terms of the volume of data that needs to be processed in order to make platooning a safe option.
Vigilance systems	Vigilance systems are alert systems (often incident reporting mechanisms within a sector like EUDAMED for Medical Devices).
Virtual Private Networks	Virtual Private Networks (VPN) extend a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. ("In the simplest terms, it creates a secure, encrypted connection, which can be thought of as a tunnel, between your computer and a server operated by the VPN service.") Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

Acronyms and Abbreviations

ABS	Anti-lock Braking System
ACEA	European Automobile Manufacturers Association
AD	Autonomous Driving
ADAS	Advanced Autonomous Driving Systems
AI	Artificial Intelligence
API	Application Programming Interface
AUTO-ISAC	Automotive Information Sharing and Analysis Center
AV	Autonomous Vehicle
CAP	Conformity Assessment Procedures
CAV	Connected Autonomous Vehicles
CCAM	Cooperative, Connected and Automated Moability
COCIR	European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries
GVC	Global Value Chains
ESP	Electronic Stability Programme
ENISA	The European Union Agency for Cybersecurity
EU	European Union
EUDAMED	European database on medical devices
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IoMT	IoMT or Internet of Medical Things (IoT in Health Care)
INTERPOL	International Criminal Police Organization
IVDR	In Vitro Diagnostic Regulation
ITU	International Telecommunication Union
MDR	Medical Devices Regulation
ML	Machine Learning
NLF	New Legislative Framework
OEM	Original Equipment Manufacturer
ODD	Operational Design Domain
OSS	Open-source Software
RED	Radio Equipment Directive
SAE	Society of Automotive Engineers
SaMD	Software as a Medical Device
SDHC	Social Determinants of Health

SDLC	Software Development Life Cycle
SMLC	Serving Mobile Location Centre
TBT	Technical Barriers to Trade
UNICRI	United Nations Interregional Crime and Justice Research Institute
WTO	World Trade Organization
3D	3D printing or Additive manufacturing is the construction of a three-dimensional object from a CAD model or a digital 3D model

Sammanfattning på svenska

Summary in Swedish

Den globala handeln med varor står inför en ny verklighet där teknisk innovation [255] och digitalisering[256] stärker handeln. Samtidigt utmanas grundförutsättningarna för beslutsfattare, regelgivande myndigheter och de handelspolitiska regelverk vi är vana att förlita oss på. I förlängningen ökar riskerna för regulativ fragmentering och nya handelshinder.

Nya teknologier och industrier har i allt större utsträckning gått från massproducerade produkter som kan standardiseras, till mer kundanpassade lösningar. Det handlar om produkter som ofta stöds av tjänster och är anslutna till internet. Varureglering som fokuserar på statiska produktkrav fångar därför inte nödvändigtvis upp de icke-statiska elementen som tillhandahålls av en programvara, eller av produktintelligens, som t.ex. maskininlärning och artificiell intelligens.

Vidare påverkas digitala produkter inte endast av den avsedda användningen och förutsägbara risker (t.ex. fysiska och kemiska risker som ofta är fallet för icke-digital, icke-uppkopplade varor). De påverkas nämligen också av faktorer som är svårare att förutse och därmed också svårare att reglera, övervaka och utöva tillsyn över: frågor om exempelvis personlig integritet, cybersäkerhet och motståndskraft. Det regulativa landskapet blir därmed alltmer komplext. Här är det viktigt att uppmärksamma att produktspecifik reglering traditionellt är vertikal (sakområdes-specifik) medan digital reglering mestadels är horisontell (sektorsövergripande); och att dessa två ofta inte är tillräckligt samordnade.

Syftet med denna analys är att belysa på vilket sätt innovationer som maskininlärning (ML) och artificiell intelligens (AI) och relaterade digitala sårbarheter, särskilt cybersårbarheter, påverkar egenskaperna hos industrivaror och hur detta bör beaktas i teknisk reglering. Detta för att effektivt stödja digital omställning och handel såväl inom EU som internationellt.

Genom att föra en dialog med företag som är verksamma inom de områden där användningen av maskininlärning och AI har kommit långt, som fordon (lastbilar), medicintekniska produkter och informations- och kommunikationsteknik (mobiltelefoner), vill Kommerskollegium i denna rapport bidra med förståelse för hur väl den reglering och regleringsteknik som idag tillämpas för industriella varor passar de digitala förändringar som pågår. Vår bedömning är att digital intelligens i industriprodukter, såsom användningen av AI, i kombination med ökande cybersårbarheter och hot kräver en omvärdering av regleringstekniker för industrivaror. Vår förhoppning är att underlaget ska kunna bidra till rekommendationer för de beslutfattare som har att hantera denna utveckling.

Våra slutsatser:

Digital innovation stärker handeln men kan radikalt utmana traditionella handelspolitiska regelverk

Digitala produkter och intelligenta produktfunktioner medför oändliga nya möjligheter. Kärnan i innovativa digitala produkter är mjukvara som också skapar förutsättningar för ständiga förbättringar i produkters egenskaper under hela produktlivscykeln. Nackdelen av detta är olika sårbarheter, som många gånger är oavsiktliga, som i sin tur också kräver

255 Vår analys om additiv tillverkning (3D printing) se: National Board of Trade Sweden, Trade Regulation in a 3D Printed World — a Primer, 2016:1.

256 Kommerskollegium, The Cyber Effect. The implications of IT security regulation on international trade, 2018.

uppföljning.[257] Dessutom tillverkar och levererar innovativa företag i allt större utsträckning skräddarsydda varor. Dessa aspekter kan mycket väl utmana standardiserade produktkrav och våra traditionella handelspolitiska ramverk för teknisk reglering som pekar på vikten av att använda internationella standarder. Detta, eftersom standarder – på det sätt som de är framtagna och utformade idag – kan vara för långsamma för att kunna fånga in den snabba tekniska utvecklingen.

Utöver detta finns det risk att den reglering vi har inte förmår att hantera den förutsedda användningen av uppkopplade produkter med integrerade digitala delar. Det bör vidare noteras att regelutmaningar relaterade till digital innovation ofta är sektorspecifika. Detta betyder att när horisontell teknologi som artificiell intelligens introduceras kommer det också behövas en mer effektiv regulativ samordning för att undvika eventuella regelmässiga luckor som skapar osäkerhet och kan ge uppkomst till handelshinder.[258] Utöver detta visar våra fallstudier att datarelaterade lokaliseringskrav också villkorar utnyttjandet av produktintelligens i form av AI på olika marknader.

Vår bedömning är att den digitala ekonomin även kräver ett nytt fokus på lämpliga mekanismer för produkttillsyn och marknadskontroll, det vill säga inte endast fokus på regleringsteknik. Som ett resultat av detta kommer ”kontinuerlig efterlevnad” dvs. ett livscykelperspektiv på tillsyn (utöver marknadskontroll av produktsäkerhet) sannolikt att bli mycket viktigt. Allt detta motiverar också att det tvärsektoriella samarbetet inom marknadskontroll och produkttillsyn förstärks.

Produkt eller tjänst – spelar det någon roll?

Det suddiga gränssnittet mellan digitala produkter och tjänster lyfts ofta som en fråga som kan skapa osäkerhet och regulativa utmaningar – dock inte i våra fallstudier. I stället lyfts det att utmaningarna ofta är kopplade till de mångfacetterade aspekterna som är relaterade till data, till exempel tillgång till data (gränsöverskridande, kliniska prövningar), användning av data (GDPR) och avvägningar gällande maskininlärning och artificiell intelligens som programvara.

Landskapet för teknisk reglering har förändrats – digital innovation ökar den regulativa komplexiteten

Föga förvånande visar vår studie på att ett komplext regulativt landskap uppstår när innovation i termer av maskininlärning och artificiell intelligens integreras i industriella produkter som mobiler, medicinsk utrustning och fordon, inte minst när cybersårbarhet ska beaktas.

I praktiken innebär digital teknisk reglering att sektorspecifika krav kompletteras med horisontella regler om artificiell intelligens, dataanvändning och cybersäkerhet. Detta leder till förvirring om hur olika, ibland till och med duplicerade eller motstridiga, rättsakter kommer att komplettera varandra. På grund av bristande vägledning bidrar detta till osäkerhet om vad företagen ska uppfylla och vilka regler som ska följas. Komplexiteten kan också bidra till en ojämn spelplan för företagen (idealt ska ju samma regelverk och krav gälla för alla ekonomiska aktörer på marknaden).

Utifrån vår analys vill vi också lyfta att det finns en risk att legitima skyddskrav och aspekter gällande exempelvis produktsäkerhet, integritet, cybersäkerhet och motståndskraft blandas in i digital reglering – något som beslutsfattare bör vara uppmärksamma på, då det kan bidra till ett ännu mer komplext regelverk.

---

257 Syftet med digital intelligens är att förbättra produkters egenskaper men detta kan också innebära nya sårbarheter om inte viktiga säkerhetsrelaterade ändringar inte följs upp.

258 Se även: WTO/WEF, *The Promise of TradeTech- Policy approached to harness trade digitalisation, 2022.*

Det bör noteras att traditionella sektorspecifika produktförordningar i EU främst har haft fokus på aspekter som produktsäkerhet och regelharmonisering, medan digitala regelverk även adresserar dataanvändning, interoperabilitet, integritet, cybersäkerhet och motståndskraft. Eftersom nuvarande regulativa processer ofta innebär att olika regelområden (AI, cybersäkerhet och sektorreglering) arbetar i silon kan konsekvensen bli att de digitala regelverken, eventuellt omedvetet, blandar ihop sektoriella regulativa mål (t.ex. säkerhet och risk) med horisontella digitala skyddshänsyn (t.ex. cybersäkerhet) terminologimässigt, också när säkerhet och risk definieras. Vi har inte gjort någon djupare analys i denna fråga men ser att företagen har stora svårigheter att tolka digitala regelverk. Analysen pekar också på att eventuella risker med AI är svåra att adressera genom harmoniserade horisontella regelverk då riskerna kan materialiseras olika för olika grupper, konsumenter och användare.

AI-teknik är inte ny, men tekniska regler riskerar att bli föråldrade

Användningen av maskininlärning och artificiell intelligens i industriella produkter är inte ett nytt fenomen, åtminstone inte i de sektorer som har inkluderats i denna analys. Trots detta är det först nu som vi ser ett stort antal nya lagstiftningsförslag med syfte att ta itu med användningen av AI och/eller data.

Eftersom de rättsliga ramarna för AI fortfarande är under utveckling är det inte heller klart för företag vilka regler som kommer att gälla och om deras befintliga innovation kommer att falla under till exempel den föreslagna AI-förordningen från EU.

Vi kan konstatera att användning av ML och AI i produkter inte en tillfällig trend, utan det drivs av affärsinnovation med syftet att lösa nya kundbehov. De ständigt föränderliga användarområdena för ML och AI är det som är det ″nya″, inte själva tekniken. Det är dock tekniken som materialiserar den nuvarande regelutmaningen.

Produkter som utnyttjar artificiell intelligens – säkra?

När det gäller användningen av AI-teknik är syftet med denna rapport inte att identifiera säkerhetsluckor eller andra sårbarheter i produkter relaterade till artificiell intelligens, förutom relaterat särskilt till cybersäkerhet. Vi har därmed inte gjort en djupare inventering av säkerhetsaspekter eller sårbarheter utan stödjer oss huvudsakligen på den information som företag, experter och myndigheter lämnat till fallstudierna. Dock ser vi tydligt att digital innovation bidar till ett ökat antal parametrar som måste beaktas i reglering, och som kan ha en direkt och betydande effekt på internationell handel.

Både företag och tillsynsmyndigheter som intervjuats menar dock på att ML eller AI-produkter inte automatiskt innebär en högre risk i produkterna - de faktiska riskerna är beroende av flera variabler som relaterar till hur AI används. Samtidigt är både företag och tillsynsmyndigheter positiva till ett försök att försöka förstå och definiera vad ″högrisk AI″ handlar om – även om vi utifrån vår analys ser att detta skulle kräva mycket mer tvärsektoriell analys.

Det är också viktigt att nämna att riskscenarion för industriella produkter har utökats och breddats genom digitaliseringen. Sårbarheter i digitala produkter materialiseras genom cybersårbarheter (i termer av ett större attackområde), i risker som rör personlig integritet (hantering av data) och i effekter på motståndskraft (eftersom många digitala produkter också används inom kritisk infrastruktur). Det här innebär att det traditionella produktsäkerhetsperspektivet inom teknisk reglering behöver utvidgas till att också omfatta säkerhet (IT-säkerhet och cybersäkerhet), integritet (GDPR) och motståndskraft, dvs. aspekter som för närvarande hanteras av en mängd olika tillvägagångssätt och regelverk, och på ett sätt som inte heller nödvändigtvis är samordnat eller tydligt.

Företag, regelgivare och experter som intervjuats för analysen påpekar att cyberhotet är allmänt erkänt och betraktas som en stor, om inte den största, utmaningen relaterad till digital innovation. Dessutom är det en fråga som är svår att hantera. En av de frågor där mest osäkerhet råder är om det finns tillräckliga resurser och verktyg för att verkligen kunna uppnå verifierad spårbarhet avseende cybersäkerhet under en produkts livscykel. Frågan för hur sådana krav ska adresseras tycks åligga beslutsfattare och regelgivarna och det här är det viktigt att faktiskt generera nödvändiga resurser för att bättre kunna förstå och effektivt övervaka den digitala marknaden.

Osäkerheter och luckor i regelverken

När det gäller osäkerheter i lagstiftning har de företag som intervjuats flaggat för att det i huvudsak gäller en brist på vägledning om vilken lagstiftning deras produkt faller inom (t. ex. förslaget till europeisk AI reglering) och eventuella duplicerade krav mellan sektorsspecifik och horisontell lagstiftning. Några av de praktiska exemplen kring denna otydlighet är relaterade till krav på mjukvaruuppdateringar och bristande acceptans (licens) av ny teknologi på exportmarknaderna.

När det gäller data visar våra fallstudier att datarelaterade lokaliseringskrav varierar och därmed villkorar marknadstillträde i olika länder.

Företag betonar också att det bör finnas mer vägledning och expertis bland regelgivare för att hantera cybersårbarheter eftersom dessa sällan är sektorspecifika utan, som påtalats tidigare, också är relaterade till samhället i stort och i kritisk infrastruktur. De intressenter som intervjuats i denna studie ser dock att den befintliga ″cybersäkerhetsverktygslådan″ (inklusive förordningar, standarder och system för bedömning av överensstämmelse) som mer mogen än den tillgängliga ″regulatoriska verktygslådan för AI″, som fortfarande är i sin linda.

Kan den digitala marknaden med ”virtuella varor” regleras?

En av de grundläggande frågorna i denna utredning är ″Vem tar ansvar för den digitala varumarknaden?″ Finns det någon mekanism som fångar upp eventuella ”misslyckanden” dvs. fel eller sårbarheter i digitala produkter när produkternas egenskaper inte längre är lika ”fysiska” som tidigare och därmed delvis ”osynliga” för beslutsfattare och regelgivare. Detta gäller särskilt på områden där de digitala regelverken fortfarande är under utveck-

Den digitala marknaden med "virtuella" varor

Vår ansats med digitala marknaden med "virtuella" varor" i rapporten syftar till att uppmärksamma att det finns en risk att beslutsfattare förbiser viktiga aspekter i regleringen av digitala produkter.

Även om digitala produkter naturligtvis är konkreta, är det mycket svårare att följa förändringar i egenskaperna hos dessa mjukvarubaserade varor, eller utvärdera vilka effekter de har för konsumenter och användare.

Likaså är det svårt att kontrollera, granska och verifiera förändringar i dessa varor, jämfört med traditionella varor som myndigheter kan inspektera visuellt, genom dokumentationskontroll eller provning i marknadskontrollen, med en större säkerhet om att varors grundläggande egenskaper inte förändras över tid.

Att fatta beslut om reglering av digitala varor, t.ex. för AI, krävs därför att beslutsfattare och regelgivare förstår hur programvara används både i allmänhet, och i specifika användningsfall. Här kan riskerna och effekterna variera, inte bara mellan sektorer utan mellan specifika användningsområden.

ling och där verktygen för att kontrollera efterlevnad genom marknadskontroll kan ha försvagats? Med andra ord är frågan huruvida den digitala marknaden är lämnad till en ”osynlig hand ″.

Huruvida den digitala ekonomin ″klarar att reglera sig själv″, i brist på kompletta och heltäckande regelverk, är en svår fråga att svara på. Detta eftersom eventuella regulativa misslyckanden eller oavsiktliga negativa effekter av teknisk innovation inte nödvändigtvis upptäcks på grund av bristande regler och tillämpningsmekanismer. Denna situation beror huvudsakligen på att många produktegenskaper definieras av mjukvara som förändras hela tiden. Större produktsäkerhetsrisker, olyckor eller cyberattacker kan, men behöver ej, komma till kännedom genom befintliga olycksrapporteringsskyldigheter och i extrema fall av media. Mer subtila fel, som också kan vara allvarliga, exempelvis vid självkörande fordon, medicinsk behandling, såsom programvarubuggar eller störningar relaterade till cybersårbarheter eller attacker, kanske aldrig kommer fram i dagsljuset utan förblir faktiskt osynliga för beslutsfattare, regelgivare och tillsynsmyndigheter. Beslutsfattare måste således i högre grad vara medvetna om att digital intelligens i produkter karakteriseras av ständig förändring och att den därmed kan vara svår att kontrollera. Detta måste beaktas i regleringsstrategier för den ”virtuella” marknaden. Som ett resultat är nyckelfrågan hur kan regelgivare ta fram en teknisk reglering som resulterar i tillräcklig nivå av säkerhet, integritet och motståndskraft för digitala varor.

Baserat på denna analys av digital varureglering har vi följande policyrekommendationer:

Investera i utvecklade och evidensbaserade regelverk för AI!

Regleringen av artificiell intelligens i industriprodukter tycks ställa större krav på tydlighet och säkerhet än nuvarande regelverk levererar. Detta eftersom användningen av maskininlärning och artificiell intelligens skapar flera scenarier och användarmöjligheter som inte passar in i den nuvarande föreslagna definitionen av AI.[259] Från våra intervjuer kan det bekräftas att det redan nu verkar finnas vissa konflikter mellan förslaget till den horisontella AI-förordningen och befintlig sektorslagstiftning. Baserat på såväl företagsutsagor som reflektioner från sektorsmyndigheter ser vi att mer insikt behövs hos regelgivare om hur specifik produktintelligens utvecklas, tillämpas och implementeras, men framför allt hur automatiserade, intelligenta och uppkopplade produktegenskaper kan övervakas under produktens livscykel. Med andra ord finns det ingen anledning att ställa upp långtgående krav om mekanismer och kompetens för att bedöma efterlevnad inte finns på plats. Som vår analys påvisar är det uppenbart att digital produktintelligens i form av AI alltid kommer att kunna medföra osäkerheter som är svårare (om inte omöjliga) att reglera och kontrollera.

Omvärdera efterlevnadsmodeller för produkter med inbyggd digital teknologi – det behövs större fokus på inbyggd säkerhet och metoder som täcker hela produktens livscykel

Digital innovation är helt beroende av tillgång och användning av data. Fungerande innovation är också beroende av kvalitativa data som är representativ för det specifika användarfallet. Eftersom mjukvara är huvudkomponenten i digitala produkter blir den regulativa utmaningen möjligheterna till insyn i data och förmågan till spårbarhet och verifierbarhet när det gäller varuegenskaper. Detta eftersom de standardiserade produktkraven inte nödvändigtvis är tillämpliga i samma utsträckning som tidigare. Detta

259 I praktiken har man inte ännu enats om definitionen för AI I förslaget och vad som ska betraktas som AI. Fram till nu har definitionen betraktats som mycket vid av intressenter.

skiljer sig från fysiska produkter där funktionerna är relativt stabila - produktens egenskaper kan där lättare verifieras och de påverkas inte heller av anslutning, algoritmer och anpassning. O-uppkopplade varor påverkas inte heller av externa och oförutsedda faktorer som cyberhot.

Som en konsekvens ser vi att inbyggd säkerhet för produkter och processer diskuteras i större utsträckning i relation till reglering. Inbyggd säkerhet är ett tillvägagångssätt inom mjukvaru- och hårdvaruutveckling som genom åtgärder som kontinuerliga tester, autentiseringsskydd och efterlevnad av programmeringspraxis, strävar efter att göra system så fria från sårbarheter och så ogenomträngliga för attacker som möjligt. Tanken är således att ”bygga in” säkerhet och trygghet i en produkt redan från början. När det gäller digital kravställning måste de tekniska kraven också kunna följas upp, och verifieras — i annat fall fallerar både grunden till vad företagen ska uppfylla och hur regelefterlevnad ska kontrolleras.

Nya strategier kan behövas för tillsyn av produkter med inbyggd digital teknologi. Marknadskontrollen av varor måste kompletteras eller förstärkas genom ett angreppssätt som möjliggör ”kontinuerlig efterlevnad”

Vår analys att användningen av artificiell intelligens kan vara unik och inte nödvändigtvis anpassad till internationell harmonisering, vilket innebär att produktegenskaper ständigt kan förändras, framför allt på grund av externa och/eller oavsiktliga faktorer.

Många av de regulativa utmaningarna som presenteras i denna rapport är förvisso erkända av regelgivare, men de möjliga regelverken riskerar att bli föråldrade redan innan de introduceras.

Vår bedömning är att det kommer att behövas en ändring i produkttillsyn för att komplettera eller förstärka myndigheters marknadskontroll för digitala produkter. Skälet till att vi ser ett behov av att utvärdera tillsynsmodellen är inte de ökade digitala sårbarheterna, särskilt då utvärdering av sårbarheter inte varit i fokus i analysen. Däremot ser vi att digitala varuregelverk fortfarande är vaga och medger nödvändigtvis inte en effektiv marknadskontroll av föränderliga egenskaper i digitala produkter.

Baserat på vår initiala analys skapar komplexa digitala regelverk förvirring och företagen har svårt att hitta sin innovation i regelmassan. Utarbetande, framtagandet och implementering av varuregelverk, som idag måste ta ombord flera legitima skyddshänsyn (inte endast produktsäkerhet) synes kräva mer säkerhet, och framför allt nya förmågor för tillsyn. Detta kräver investering i ny kompetens som täcker flera produktrelaterade parametrar för myndigheter som ansvarar för "produktsäkerhet". Detta kommer att kräva en ny ansats som omfattar "kontinuerlig efterlevnad" — dvs. ett livscykelperspektiv i tillsynen som möjliggör förbättrad förmåga till ”datahantering och säkerhet”. Vilka metoder och verktyg som skulle kunna användas i tillsynen av digitala produkter lär bero på sektor och produkt i fråga, och bör naturligtvis utvärderas, såsom alla regulativa åtgärder, utifrån flera parametrar t.ex., risk, proportionalitet m.m. och bör tas fram av ansvariga myndigheter.

Handelspolitiska regelverk utmanas — teknisk reglering för digitala produkter måste utvärderas

Slutligen, i termer av handelspolitik ser vi också att teknisk utveckling och digital innovation kan utmana traditionella regelverk som Världshandelsorganisationens avtal för tekniska handelshinder (TBT-avtalet) som främjar harmonisering och användning av internationella standarder och system för bedömning av överensstämmelse för fungerande gränsöverskridande marknadstillträde. Detta eftersom digitala ramverk för artificiell intelligens ännu inte är mogna, och genom att internationella standarder inte nödvändigtvis är tillgängliga eller anpassade till innovationen.[260]

260 Att utgå från internationella standarder i teknisk reglering har beaktats som kärnan i att förebygga och avveckla tekniska handelshinder (TBT) enligt Världshandelsorganisationens (WTO) Avtal om tekniska handelshinder (TBT-avtalet).

Även bortom denna studie, ser Kommerskollegium en stark trend med regulativ fragmentering. Bristen på internationella ramverk och aktuella standarder samt ändat säkerhetsläge globalt resulterar i att privata reglerings initiativ och standarder som inte följer den formella standardiseringsprocessen fortsätter blomstra, vilket leder till ojämna spelregler på marknaden.[261] Här måste beslutsfattare och regelgivare intensifiera arbetet och samordna sig!

261 Standarder inom 5G är ett exempel. Se även Rühlig, 2020 technical-standardisation-china-and-the-future-international-order.pdf (ui.se).

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.

Kommerskollegium, December 2022. ISBN: 978-91-89742-08-6

Kommerskollegium
National Board of Trade Sweden

Box 6803, 113 86 Stockholm
Telefon 08 690 48 00
E-post registrator@kommerskollegium.se
www.kommerskollegium.se