

An analysis on Digital Innovation, AI, Cybersecurity Technical Regulation and Trade

The objective of the analysis is to highlight in which manner the utilisation of technologies and innovations such as AI on one hand, and digital vulnerabilities, especially cyber vulnerabilities on the other, affect the properties of industrial goods and how this should be considered in technical regulation.

In other words, the analysis answers the question whether digital innovation changes the way in which we should regulate industrial goods.



The rationale?

Our earlier study focusing on the trade effects of cybersecurity regulation indicates that regulation of digital elements imply many uncertainties with respect of reaching the set regulatory objectives compared to traditional non-digital and non-connected industrial products.

Also, that efficient regulatory policy making becomes burdensome when different policy areas such as cybersecurity and trade policy do not speak the same language.

If regulations are not adapted to technical innovation companies will face uncertainty and there is a risk for regulatory fragmentation and trade barriers- as a result there is a need to investigate if there are relevant regulatory frameworks for digital innovation, including cybersecurity.

Rationale

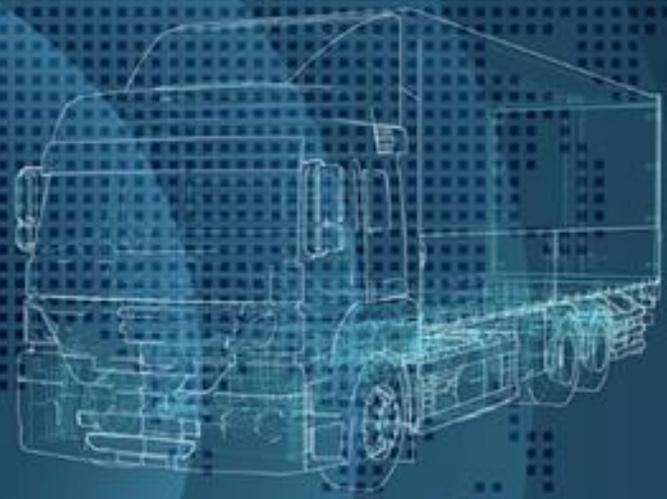
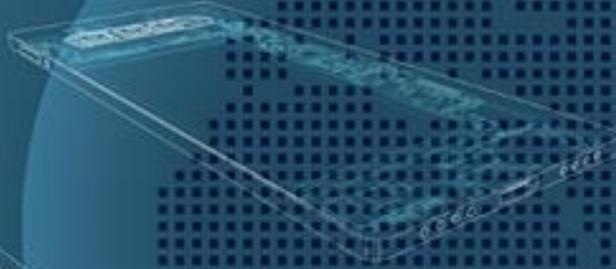
One of the study's underlying questions is “is there anyone that has full insight in and is taking responsibility for the digital market?”

Is there a mechanism that captures eventual “failures” in terms of potentially non-compliant products, if products are not as tangible as before, where digital regulatory frameworks and standards are still under development and where means to verify compliance through market surveillance has been weakened?



Regulatory challenges:

- In contrast to traditional goods, the properties of digital products change throughout their life-cycles (making regulation and standardization more difficult)
- Digital products are less tangible than traditional products (product properties are more difficult to follow and control)
- Regulations and standards are still under development



Case studies

ICT (mobile phones)

Medical devices (software, devices for cancer treatment)

Vehicles (trucks)

COMPANIES	EXPERTS	AUTHORITIES
Vehicles (Trucks)	Vehicles (Trucks)	Vehicles (Trucks)
Einride Scania Volvo	RISE Mobility Sweden	Swedish Transport Agency
Mobile phones	Mobile phones	Mobile phones
Apple Google	Ericsson	The Swedish Post and Telecom Agency
Medical devices	Medical devices	Medical devices
Elekta Dedalus	QAdvis Swedish Medtech	Swedish Medical Products Agency
		Cybersecurity
		Swedish Civil Contingencies Agency Swedish Defence materiel Administration
	Software development	
	CNB Systems Ltd	

Conclusions

- *Innovation is boosting trade but may radically challenge traditional trade policy frameworks.*
- *The regulatory landscape has changed - Digital innovation increases regulatory complexity.*
- *The purpose of the analysis was not to look for vulnerabilities and risks linked to AI. However, the result confirms that the use of digital product intelligence broadens regulatory concerns for industrial goods i.e., regulatory compliance it is not only about product safety but also about cybersecurity, resilience and privacy.*

Conclusions

- *What is most noticeable in the context is that the ability to really control and monitor changes in the properties of digital goods has been significantly weakened.*
- *It is clear, that policymakers still base their regulatory proposals on a sector, while digital innovation and its areas of use are limitless.*
- *Complex supply chains are not sufficiently considered in technical regulation. This is important to observe since the ability to build security into the product from the start (security-by-design) has weakened.*

Conclusions

- *In terms of regulatory gaps and grey zones, the study has identified several cases of overlapping and/or conflicting regulations. Also, that horizontal digital regulations, or proposals, are not necessarily adapted for sector-specific use cases.*
- *It can be confirmed that a good and solid definition of AI is still not available.*
- *Cybersecurity is pointed out as the main regulatory challenge for digital innovation.*
- *There is a risk that regulatory parameters regarding product safety, cybersecurity, personal integrity and resilience are blurred when risks are defined in regulation. All these regulatory concerns can naturally affect parts of a digital product. However, these are currently addressed by a multitude of approaches and various regulative proposals, but not necessarily in a coordinated manner, nor with clarity.*

We are at crossroads..

Old approach

Vertical, detailed product regulation



Vehicles

Food

Chemicals

Straightforward
but detailed product regulation

Policy focus in regulation: Trade/Safety

New Approach

Horizontal regulation combined with vertical generic requirements/NLF
+ Harmonized standards (EN)
+ Global approach to Conformity Assessment (modules)
+ CE marking



GPSD
EMC/LVD

Harmonization
by Structured and Transparent Regulations

Policy focus in regulation: Free movement/Safety

Future approach?

Horizontal regulation combined with horizontal digital regulatory layers together with vertical generic and specific requirements/NLF
+ Harmonized standards (EN) or
+ Common Technical Specifications or
+ industry driven Fora and Consortia Standards
+ Global approach to Conformity Assessment (modules)
+ CE marking
+ Certification scheme for cybersecurity
+ Certification scheme for AI
+ New markings

GPSD

GDPR

Data Act

RED (+ cyber)

Cybersecurity Act

CRA

Product regulation, also regulation of technologies and multitude of regulatory risks and vulnerabilities

Policy focus in regulation: Free movement/Safety but also Resilience, Privacy, Cybersecurity



We are at crossroads..

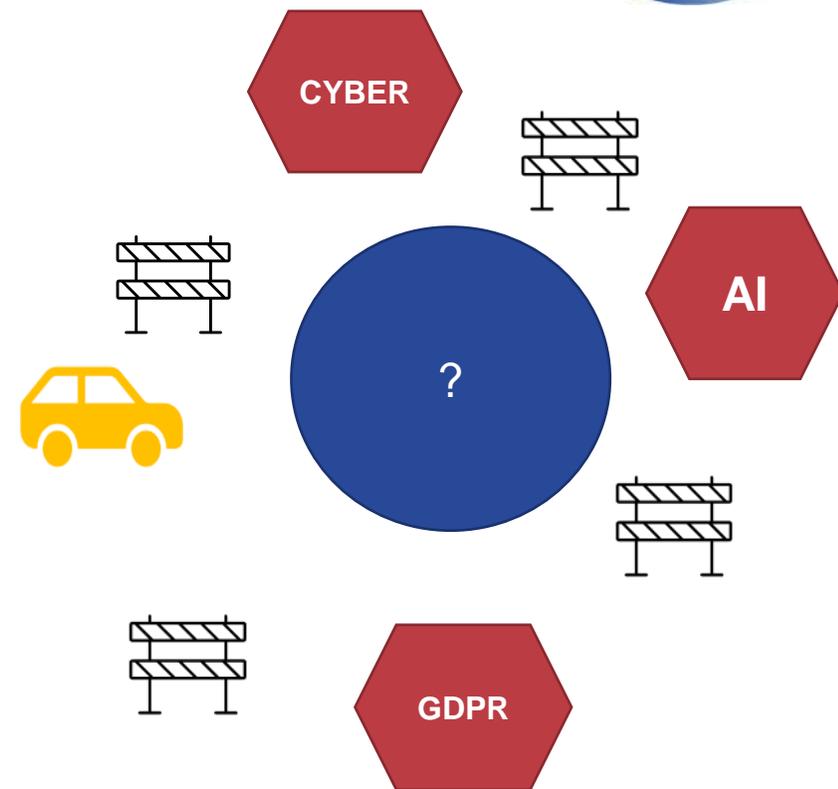
Old Approach



New Approach



Future Approach?



The role of Conformity Assessment in digital transformation?

Extensive and complex supply chains is the main challenge affecting traceability and auditability of digital products.

Still proposals for new digital legal frameworks introduce complex producer responsibilities that cover the whole value chain and that are (more or less) impossible for companies themselves to verify. This will also become a real headache for market surveillance bodies.

Here Conformity Assessment as well as Legal Metrology could have a crucial role in creating better understanding, methodologies and improved tools traceability and auditability.

Policy recommendations

- *The policymakers should invest in more mature regulations! Above all by creating a better understanding of the technology, by analyzing the interrelations of various fields and by coordinating themselves. Furthermore, there is a need to start thinking about regulatory impact analysis across sectors/issues. Particularly, since a large part of digital innovation is very difficult to control.*
- *More focus is needed on **the life cycle perspective in regulation** as the properties of digital goods change over time.*
- *Policymakers and regulators must find new ways to gain better insight in digital products **by improved methods for “continuous compliance”**. Here, new abilities are needed in the form of methods for traceability, auditability, verification in market surveillance/ enforcement of product safety/security. This require both resources and new skills.*

Thank you for your attention!

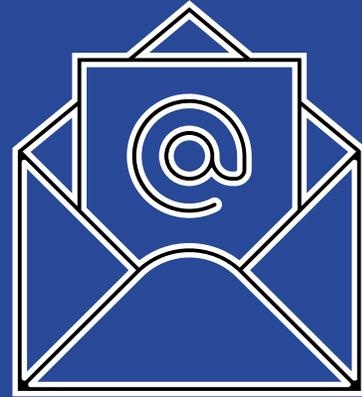


Read the reports!



[innovation-ai-technical-regulation-and-trade.pdf \(kommerskollegium.se\)](https://kommerskollegium.se/innovation-ai-technical-regulation-and-trade.pdf)

[The Cyber Effect \(kommerskollegium.se\)](https://kommerskollegium.se/the-cyber-effect)



Heidi Lund@kommerskollegium.se

