EUROPEAN
COMMISSION

Brussels, 19.2.2020
COM(2020) 64 final

# REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE

## Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics

# REPORT ON THE SAFETY AND LIABILITY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE, THE INTERNET OF THINGS AND ROBOTICS

## 1. Introduction

Artificial Intelligence (AI)[1], the Internet of Things (IoT)[2] and robotics will create new opportunities and benefits for our society. The Commission has recognised the importance and potential of these technologies and the need for significant investment in these areas.[3] It is committed to making Europe a world-leader in AI, IoT and robotics. In order to achieve this goal, a clear and predictable legal framework addressing the technological challenges is required.

### 1.1. The existing safety and liability framework

The overall objective of the safety and liability legal frameworks is to ensure that all products and services, including those integrating emerging digital technologies, operate safely, reliably and consistently and that damage having occurred is remedied efficiently. High levels of safety for products and systems integrating new digital technologies and robust mechanisms remedying occurred damage (i.e. the liability framework) contribute to better protect consumers. They also create trust in these technologies, a prerequisite for their uptake by industry and users. This in turn will leverage the competitiveness of our industry and contribute to the objectives of the Union[4]. A clear safety and liability framework is particularly important when new technologies like AI, the IoT and robotics emerge, both with a view to ensure consumer protection and legal certainty for businesses.

The Union has a robust and reliable safety and product liability regulatory framework and a robust body of safety standards, complemented by national, non-harmonised liability legislation. Together, they ensure the well-being of our citizens in the Single Market and encourage innovation and technological uptake. However, AI, the IoT and robotics are transforming the characteristics of many products and services.

The Communication on Artificial Intelligence for Europe[5], adopted on 25 April 2018, announced that the Commission would submit a report assessing the implications of the emerging digital technologies on the existing safety and liability frameworks. This report aims to identify and examine the broader implications for and potential gaps in the liability and safety frameworks for AI, the IoT and robotics. The orientations provided in this report accompanying the White Paper on Artificial Intelligence are provided for discussion and are part of the broader consultation of stakeholders. The safety section builds on the evaluation[6]

---

1 The definition on Artificial Intelligence of the High-Level Expert Group (AI HLEG) is available at https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

2 The definition of the Internet of Things provided by the Recommendation ITU-T Y.2060 is available at https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

3 SWD(2016) 110, COM(2017) 9, COM(2018) 237 and COM(2018) 795.

4 http://ec.europa.eu/growth/industry/policy_en

5 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN.
The accompanying Staff Working Document (2018) 137 (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137) provided a first mapping of liability challenges that occur in the context of emerging digital technologies.

6 SWD(2018) 161 final.

of the Machinery Directive[7] and the work with the relevant expert groups[8]. The liability section builds on the evaluation[9] of the Product Liability Directive[10], the input of the relevant experts groups[11] and contacts with stakeholders. This report does not aim to provide an exhaustive overview of the existing rules for safety and liability, but focuses on the key issues identified so far.

## 1.2. Characteristics of AI, IoT and robotics technologies

AI, IoT and robotics share many characteristics. They can combine **connectivity**, **autonomy** and **data dependency** to perform tasks with little or no human control or supervision. AI equipped systems can also improve their own performance by learning from experience. Their **complexity** is reflected in both the plurality of economic operators involved in the **supply chain** and the multiplicity of components, parts, software, systems or services, which together form the new technological ecosystems. Added to this is the **openness** to updates and upgrades after their placement on the market. The vast amounts of data involved, the reliance on algorithms and the **opacity** of AI decision-making, make it more difficult to predict the behaviour of an AI-enabled product and to understand the potential causes of a damage. Finally, connectivity and openness can also expose AI and IoT products to **cyber-threats**.

## 1.3. Opportunities created by AI, IoT and robotics

Increasing users' trust and social acceptance in emerging technologies, improving products, processes and business models and helping European manufacturers to become more efficient are only some of the opportunities created by AI, IoT and robotics.

Beyond productivity and efficiency gains, AI also promises to enable humans to develop intelligence not yet reached, opening the door to new discoveries and helping to solve some of the world's biggest challenges: from treating chronic diseases, predicting disease outbreaks or reducing fatality rates in traffic accidents to fighting climate change or anticipating cybersecurity threats.

These technologies can bring many benefits by improving the safety of products, making them less prone to certain risks. For instance, connected and automated vehicles could improve road safety, as most road accidents are currently caused by human errors[12]. Moreover, IoT systems are designed to receive and process vast amounts of data from

---

7 Directive 2006/42/EC

8 Consumer Safety Network as established in Directive 2001/95/EC on general product safety (GPSD), Machinery Directive 2006/42/EC and Radio Equipment 2014/53/EU Directive expert groups composed of Member States, industry and other stakeholders such as consumer associations.

9 COM(2018) 246 final

10 Directive 85/374/EEC

11 The Expert Group on Liability and New Technologies was created to provide the Commission with expertise on the applicability of the Product Liability Directive and national civil liability rules and with assistance in developing guiding principles for possible adaptations of applicable laws related to new technologies. It consists of two formations, the 'Product Liability Formation' and the 'New Technologies Formation', see http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1.
For the Report of the 'New Technologies Formation' on Liability for Artificial Intelligence and other emerging technologies' see https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

12 It is estimated that around 90% of road accidents are caused by human errors. See Commission's report on Saving Lives: Boosting Car Safety in the EU (COM(2016) 0787 final).

different sources. This increased level of information might be used so that products can self-adapt and consequently become safer. New technologies can contribute to better effectiveness of product recalls as for example products could warn the users to avoid a safety problem[13]. If a safety issue arises during the use of a connected product, producers can directly communicate with users, on the one hand to warn the users about the risks and on the other hand, if possible, to directly fix the problem by providing, for example, a safety update. For instance, during the recall of one of its devices in 2017, a smartphone producer carried out a software update to reduce to zero the battery capacity of the recalled phones[14] so that users would stop using the dangerous devices.

Furthermore, new technologies can contribute to improve the traceability of products. For instance, IoT connectivity features can enable businesses and market surveillance authorities to track dangerous products and identify risks across supply chains[15].

Along with the opportunities that AI, IoT and robotics can bring to the economy and our societies, they can also create a risk of harm to legally protected interests, both material and immaterial ones. The risk of such harm occurring will increase as the field of applications widens. In this context, it is essential to analyse whether and to what extent the current legal framework on safety and liability is still fit to protect users.

## 2. Safety

The Commission Communication on "Building Trust in Human-Centric Artificial Intelligence" states that ***AI systems should integrate safety and security-by-design mechanisms to ensure that they are verifiably safe at every step****, taking at heart the* ***physical and mental safety*** *of all concerned*[16].

The assessment of the Union product safety legislation in this section analyses whether the current Union legislative framework contains the relevant elements to ensure that emerging technologies and AI systems in particular, integrate safety and security-by-design.

This report mainly looks at the General Product Safety Directive[17] as well as at the harmonised product legislation that follows the horizontal rules of the "New Approach"[18] and/or the "New Legislative Framework" (hereafter "Union product safety legislation or framework")[19]. The horizontal rules ensure the coherence among the sectorial rules on product safety.

---

13 For instance, the driver of a car can be warned to slow down in case there is an accident ahead.

14 OECD (2018), "Measuring and maximising the impact of product recalls globally: OECD workshop report", *OECD Science, Technology and Industry Policy Papers*, No. 56, OECD Publishing, Paris, https://doi.org/10.1787/ab757416-en.

15 OECD (2018), "Enhancing product recall effectiveness globally: OECD background report", *OECD Science, Technology and Industry Policy Papers*, No. 58, OECD Publishing, Paris, https://doi.org/10.1787/ef71935c-en.

16 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Building Trust in Human-Centric Artificial Intelligence, Brussels, 8.4.2019 COM(2019) 168 final

17 Directive 2001/95/EC the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4–17).

18 OJ C 136, 4.6.1985, p. 1.

19 Regulation (EC) No. 2008/765 and Decision (EC) No. 2008/768

The Union product safety legislation aims to ensure that products placed on the Union market meet high health, safety and environmental requirements and that such products can circulate freely throughout the Union. The sectorial legislation[20] is complemented by the General Product Safety Directive[21], which requires that all consumer products, even if not regulated by the Union sectorial legislation, need to be safe. Safety rules are complemented with market surveillance and the powers conferred to national authorities under the Market Surveillance Regulation[22] and the General Product Safety Directive[23]. In transport, there are additional Union and national rules for placing a motor vehicle[24], an aircraft or a ship in service and clear rules governing safety during operation, including tasks for operators as well surveillance tasks for authorities.

European standardisation is also an essential element of the Union product safety legislation. Given the global nature of digitisation and emerging digital technologies, international cooperation in standardisation is of particular relevance for the competitiveness of the European Industry.

A big portion of the Union product safety framework was written prior to the emergence of digital technologies such as AI, the IoT or robotics. It therefore does not always contain provisions explicitly addressing the new challenges and risks of these emerging technologies. However, as the existing product safety framework is technology neutral, this does not mean that it would not apply to products incorporating these technologies. Furthermore, subsequent legislative acts which are part of that framework, such as in the medical devices or cars sectors, have already explicitly considered some aspects of the emergence of digital technologies, e.g. automated decisions, software as a separate product and connectivity.

[20] This schema does not include theUnion transport and cars legislation.

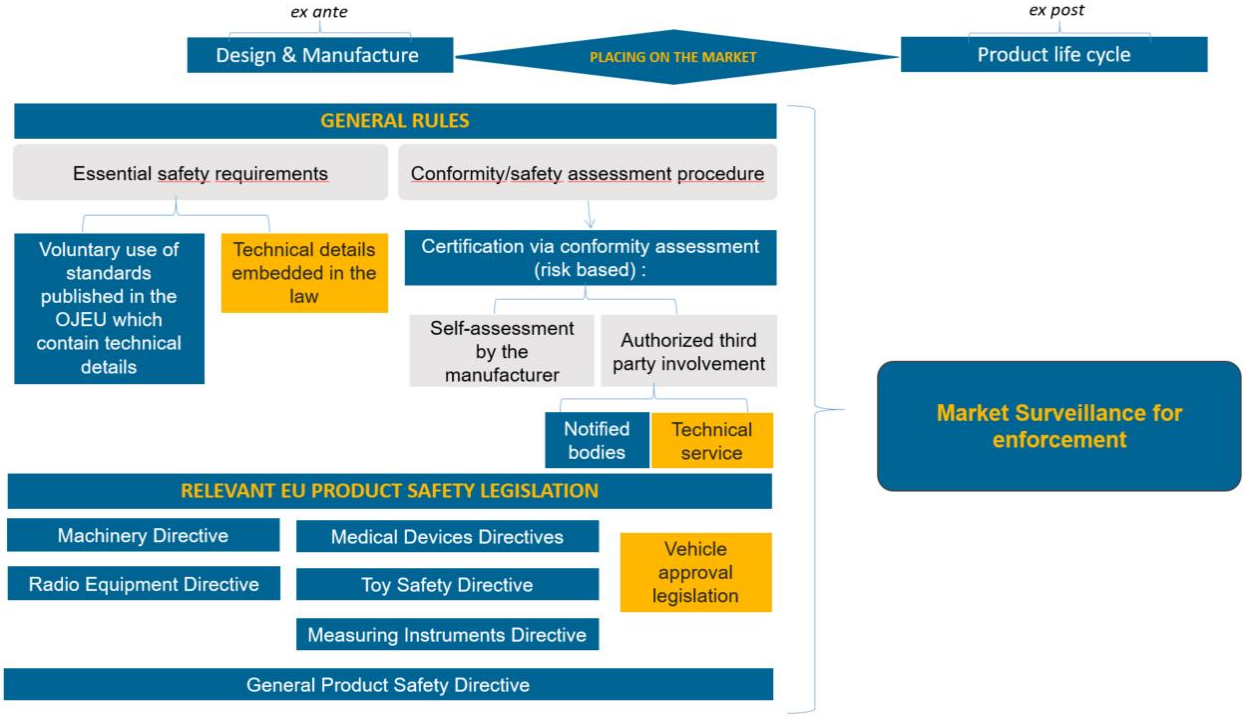
[21] Directive 2001/95/EC the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4–17).

[22] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218, 13.8.2008, p. 30–47, ELI: http://data.europa.eu/eli/reg/2008/765/oj, and, from 2021 onwards, Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/201,1 OJ L 169, 25.6.2019, p. 1–44, ELI: http://data.europa.eu/eli/reg/2019/1020/oj

[23] Article 8 (1) (b) (3) of the General Product safety Directive

[24] For instance, Directive 2007/46/EC — approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, and Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC

**The underlying logic of the current Union product safety legislation**[25]




The challenges brought by the digital emerging technologies to the Union product safety framework are presented hereafter.

**Connectivity** is a core feature in an ever-growing number of products and services. This feature is challenging the traditional concept of safety, as connectivity may directly compromise the safety of the product and indirectly when it can be hacked leading to security threats and affecting the safety of users.

An example is given by an EU Rapid Alert System notification from Iceland concerning a smart watch for children[26]. This product would not cause a direct harm to the child wearing it, but lacking a minimum level of security, it can be easily used as a tool to have access to the child. As one of the product's intended function is to keep children safe through localisation, a consumer would expect that it would not pose security threats to children that may affect their safety by potentially being tracked and/or contacted by anyone.

Another example is indicated in a notification submitted by Germany regarding a passenger car[27]. The radio in the vehicle may have certain software security gaps allowing unauthorised third party access to the interconnected control systems in the vehicle. If these software security gaps were exploited by a third party for malicious purposes, a road accident could occur.

Industrial applications may also be exposed to cyber threats affecting the safety of persons at larger scale when such applications lack the necessary levels of security. This can be the case for example of cyber-attacks on a critical control system of an industrial plant intended to trigger an explosion that might cost lives.

[25] This picture does not include the product lifecycle legislation requirements i.e. use and maintenance and is only presented for general illustration purposes.
[26] RAPEX notification from Iceland published in the EU Safety Gate's website (A12/0157/19)
[27] RAPEX notification from Germany published in the EU Safety Gate (A12/1671/15)

Union product safety legislation does not generally provide for specific mandatory essential requirements against cyber-threats affecting the safety of users. However, there are provisions related to security aspects in the Regulation on Medical Devices[28], the Directive on measuring instruments[29], the Radio Equipment Directive[30], or the vehicle-type approval legislation[31]. The Cybersecurity Act[32] sets up voluntary cybersecurity certification framework for Information and communications technology (ICT) products, services and processes while the relevant Union product safety legislation sets up mandatory requirements.

In addition, the risk of loss of connectivity of emerging digital technologies may also entail risks related to safety. For example, if a connected fire alarm loses connectivity, it might not alert the user in case of a fire.

Safety in the current Union product safety legislation is a public policy objective. The safety concept is linked to the use of the product and the risks, e.g. mechanical, electrical etc., to be addressed to make the product safe. To be noted that depending on the piece of Union safety product legislation, the use of the product covers not only the intended use but also the foreseeable use and in some cases, such as in the Machinery Directive[33], even the reasonably foreseeable misuse.

The safety concept in the current Union product safety legislation is in line with an extended concept of safety in order to protect consumers and users. Thus, the concept of product safety encompasses protection against all kinds of risks arising from the product, including not only mechanical, chemical, electrical risks but also cyber risks and risks related to the loss of connectivity of devices.

Explicit provisions in this respect could be considered for the scope of the relevant Union pieces of legislation in order to provide a better protection of users and more legal certainty.

**Autonomy[34]** is one of the main features of AI. AI based unintended outcomes could cause harm to the users and exposed persons.

As far as the future "behaviour" of AI products can be determined in advance by the risk assessment carried out by the manufacturer before the products are placed on the market, the Union product safety framework already sets obligations for producers to take into account in the risk assessment the "use"[35] of the products throughout their lifetime. It also foresees that manufacturers must provide for instructions and safety information for users or warnings[36]. In

[28] Regulation (EU) 2017/745 on medical devices

[29] Directive 2014/32/EU relating to the making available on the market of measuring instruments

[30] Radio Equipment 2014/53/EU Directive

[31] Directive 2007/46/EC — approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles. The Directive will be repealed and replaced by Regulation (EU) 2018/858 on the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC with effect from 1 September 2020.

[32] Regulation (EU) 2019/881

[33] Directive 2006/42/EC on machinery

[34] While AI based products can act autonomously by perceiving their environment and without following a set of pre-determined set of instructions, their behaviour is constrained by the goal they are given and other relevant design choices made by their developers. "

[35] In the Union product safety legislation, producers make the risk assessment based on the intended use of the product, the foreseeable use and/or the reasonably foreseeable misuse.

[36] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC, OJ L 218, 13.8.2008. p. 82–128. Annex I, Article R2.7 reads: "*Manufacturers shall ensure that the product is accompanied by*

this context, for example, the Radio Equipment Directive[37] requires the manufacturer to include instructions with information about how to use the radio equipment in accordance with its intended use.

There may be also situations in the future where the outcomes of the AI systems cannot be fully determined in advance. In such a situation, the risk assessment performed before placing the product on the market may no longer reflect the use, functioning or behaviour of the product. In these cases, insofar as the intended use, initially foreseen by the manufacturer, is modified[38] due to the autonomous behaviour and the compliance with the safety requirements is affected, it could be considered to require a new re-assessment of the self-learning product[39].

Under the current framework, where producers become aware that a product, throughout its lifecycle, poses risks having an impact on safety, they are already required to immediately inform the competent authorities and take actions to prevent the risks for users[40].

Besides the risk assessment performed before placing a product on the market, a new risk assessment procedure could be put in place where the product is subject to important changes during its lifetime, e.g. different product function, not foreseen by the manufacturer in the initial risk assessment. This should focus on the safety impact caused by the autonomous behaviour throughout the product lifetime. The risk assessment should be performed by the appropriate economic operator. In addition, the relevant Union pieces of legislation could include reinforced requirements for manufacturers on instructions and warnings for users.

Similar risk assessments are already required in transport legislation[41]; for example, in railway transport legislation, when a railway vehicle is modified after its certification, a specific procedure is imposed to the author of the modification and clear criteria defined in order to determine if the authority needs to be involved or not.

The self-learning feature of the AI products and systems may enable the machine to take decisions that deviate from what was initially intended by the producers and consequently what is expected by the users. This raises questions about human control, so that humans

---

*instructions and safety information in a language which can be easily understood by consumers and other end-users, as determined by the Member State concerned*."

37 Article 10 (8) referring to the instructions for the end user and Annex VI referring to the EU Declaration of Conformity

38 So far "self-learning" is used in the context of AI mostly to indicate that machines are capable of learning during their training; it is not a requirement yet that AI machines continue learning after they are deployed; on the contrary, especially in healthcare, AI machines normally stop learning after their training has successfully ended. Thus, at this stage, the autonomous behaviour deriving from AI systems does not imply that the product is performing tasks not foreseen by the developers.

39 This is in line with section 2.1 of the 'Blue Guide' on the implementation of EU products rules 2016'

40 Article 5 of Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety.

41 In case of any change to the railway system that may have an impact on safety (e.g. technical, operational change or also organisational change which could impact the operational or maintenance process), the process to follow is described in Annex I to COM Implementing regulation (EU) 2015/1136 (OJ L 185, 14.7.2015, p. 6).
In case of 'significant change' a safety assessment report should be provided to the proposer of the change by an independent 'assessment body' (could be the national safety authority or another technically competent).
Following the risk analysis process, the proposer of the change will apply the appropriate measures to mitigate risks (if the proposer is a railway undertaking or infrastructure manages, the application of the regulation is parts of its safety management system, whose application that is supervised by the NSA).

could choose how and whether delegating decision to AI products and systems, to accomplish human-chosen objectives[42]. The existing Union product safety legislation does not explicitly address the human oversight in the context of AI self-learning products and systems[43].

The relevant Union pieces of legislation may foresee specific requirements for human oversight, as a safeguard, from the product design and throughout the lifecycle of the AI products and systems.

The future "behaviour" of AI applications could generate **mental health risks**[44] for users deriving, for example, from their collaboration with humanoid AI robots and systems, at home or in working environments. In this respect, today, safety is generally used to refer to the user's perceived threat of physical harm that may come from the emerging digital technology. At the same time, safe products are defined in the Union legal framework as products that do not present any risk or just the minimum risks to the safety and health of persons. It is commonly agreed that the definition of health includes both physical and mental wellbeing. Howevermental health risks should be explicitly covered within the concept of product safety in the legislative framework.

For example, the autonomy should not cause excessive stress and discomfort for extended periods and harm mental health. In this regard, the factors that positively affect the sense of safety for older people[45] are considered to be: having secure relationships with health care service staff, having control over daily routines, and being informed about them. Producers of robots interacting with older people should take these factors into consideration to prevent mental health risks.

Explicit obligations for producers of, among others, AI humanoid robots to explicitly consider the immaterial harm their products could cause to users, in particular vulnerable users such as elderly persons in care environments, could be considered for the scope of relevant EU legislation.

Another essential characteristic of AI-based products and systems is **data dependency**. Data accuracy and relevance is essential to ensure that AI based systems and products take the decisions as intended by the producer.

The Union product safety legislation does not explicitly address the risks to safety derived from faulty data. However, according to the "use" of the product, producers should anticipate during the design and testing phases the data accuracy and its relevance for safety functions.

For example, an AI-based system designed to detect specific objects may have difficulty recognising items in poor lighting conditions, so designers should include data coming from product tests in both typical and poorly lit environments.

Another example relates to agricultural robots such as fruit-picking robots aimed at detecting and locating ripe fruits on trees or on the ground. While the algorithms involved already show success rates for classification of over 90%, a shortcoming in the datasets fuelling those

[42] Policy and Investment Recommendations for Trustworthy AI, High-Level Expert Group on Artificial Intelligence, June 2019.

[43] This does however not exclude that oversight may be necessary in a given situation as a result of some of the existing more general obligations concerning the placing on the market of the product

[44] WHO Constitution, first bullet point: "Health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity." (https://www.who.int/about/who-we-are/constitution)

[45] Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction, pp.237-264, Research, Neziha Akalin, Annica Kristoffersson and Amy Loutfi, July 2019.

algorithms may lead those robots to make a poor decision and as a consequence injure an animal or a person.

The question arises if the Union product safety legislation should contain specific requirements addressing the risks to safety of faulty data at the design stage as well as mechanisms to ensure that quality of data is maintained throughout the use of the AI products and systems.

**Opacity** is another main characteristic of some of the AI based products and systems that may result from the ability to improve their performance by learning from experience. Depending on the methodological approach, AI-based products and systems can be characterised by various degrees of opacity. This may lead to a decision making process of the system difficult to trace ('black box-effect'). Humans may not need to understand every single step of the decision making process, but as AI algorithms grow more advanced and are deployed into critical domains, it is decisive that humans can be able to understand how the algorithmic decisions of the system have been reached. This would be particularly important for the ex-post mechanism of enforcement, as it will allow the enforcement authorities the possibility to trace the responsibility of AI systems behaviours and choices. This is also acknowledged by the Commission Communication on Building Trust in Human-Centric Artificial Intelligence[46].

The Union product safety legislation does not explicitly address the increasing risks derived from the opacity of systems based on algorithms. It is therefore necessary to consider requirements for transparency of algorithms, as well as for robustness, accountability and when relevant, human oversight and unbiased outcomes[47], particularly important for the ex-post mechanism of enforcement and to build trust in the use of those technologies. One way of tackling this challenge would be imposing obligations on developers of the algorithms to disclose the design parameters and metadata of datasets in case accidents occur.

Additional risks that may impact safety are those stemming from the **complexity of the products and systems**, as various components, devices and products can be integrated and have influence on each other's functioning (e.g. products part of a smart home ecosystem).

This complexity is already addressed by the Union safety legal framework referred to at the beginning of this section[48]. In particular, when the producer carries out the risk assessment of the product, he must consider the intended use, foreseeable use and, where applicable, reasonably foreseeable misuse.

In this context, **if the producer envisages that their device will be interconnected and will interact with other devices, this should be considered during the risk assessment.** Use or misuses are determined on the basis of, for example, experience of past use of the same type of product, accident investigations or human behaviour.

The complexity of systems is also more specifically addressed by sectorial safety legislation such as the Medical Devices Regulation and to a certain extent in the General Product Safety

[46] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

[47] Based on the key requirements proposed by the High-Level Expert Group in the Ethics guidelines for trustworthy AI: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

[48] Regulation (EC) No. 2008/765 and Decision (EC) No. 2008/768 and harmonised sectorial product safety legislation e.g. Machinery Directive 2006/42/EC.

legislation[49]. For example, the producer of a connected device, intended to be part of a smart home ecosystem, should be able to reasonably foresee that their products will have an impact on the safety of other products.

In addition, transport legislation addresses this complexity at system level. For cars, trains and airplanes, type-approval and certification takes place for each component as much as for the entire vehicle or aircraft. Road-, air-worthiness and rail interoperability are part of the safety assessment. In transport, "systems" have to be "authorised" by an authority, either on the basis of a third party assessment of conformity against clear technical requirements, or after a demonstration on how risks are being addressed. The solution is in general a combination of "product" and "system" level.

The Union product safety legislation, including transport legislation, already takes into account to a certain extent the complexity of products or systems to tackle the risks that may have an impact on the safety of users.

Complex systems often involve **software,** which is an essential component of an AI based system. Generally, as part of the initial risk assessment, the manufacturer of the final product has obligations to foresee the risks of software integrated in that product at the time of its placing on the market.

Certain pieces of Union product safety legislation refer explicitly to the software integrated in the product. For example, the Machinery Directive[50] requires that a fault in the software of the control system does not lead to hazardous situations.

In the Union product safety legislation, software updates could be compared to maintenance operations for safety reasons provided that they do not significantly modify a product already placed on the market and they do not introduce new risks that were not foreseen in the initial risk assessment. However, if the software update modifies substantially the product in which it is downloaded, the entire product might be considered as a new product and compliance with the relevant safety product legislation must be reassessed at the time the modification is performed[51].

For stand-alone software, placed as it is on the market or uploaded after the product has been placed on the market, the Union sector-specific harmonised product safety legislation does not generally have specific provisions. However, certain pieces of Union legislation address stand-alone software, for example the Regulation on Medical Devices. Furthermore, stand-alone software uploaded in connected products that communicate via certain radio modules[52] can also be regulated by the Radio Equipment Directive via delegated acts. This Directive requires that specific classes or categories of radio equipment support features ensuring that the compliance of that equipment is not compromised when software is uploaded[53].

[49] Article 2 of the General Product Safety Directive specifies that a safe product shall take into account "the effect on other products, where it is reasonably foreseeable that it will be used with other products".

[50] Section 1.2.1 of Annex I of the Machinery Directive

[51] The Blue Guide on the implementation of EU product rules, 2016

[52] Radio modules are electronic device that transmit and/or receive radio signals (WIFI, Bluetooth) between two devices

[53] Article 3 (3) (i) of the Radio Equipment Directive,

While the Union product safety legislation takes into account the safety risks stemming from software integrated in a product at the time of its placing on the market and, potentially subsequent updates foreseen by the manufacturer, specific and/or explicit requirements on standalone software could be needed (e.g. an 'app' that would be downloaded). Particular considerations should be given to the stand-alone software ensuring safety functions in the AI products and systems.

Additional obligations may be needed for manufacturers to ensure that they provide features to prevent the upload of software having an impact on safety during the lifetime of the AI products.

Finally, emerging digital technologies are affected by **complex value chains**. Yet, this complexity is not new, nor exclusively an issue brought by new emerging digital technologies such as AI or the IoT. This is the case for example of products such as computers, service robots, or transport systems.

Under the Union product safety framework, no matter how complex the value chain is, the responsibility for the safety of the product remains with the producer that places the product on the market. Producers are responsible for the safety of the final product including the parts integrated in the product e.g. the software of a computer.

Some pieces of the Union product safety legislation already contain provisions that explicitly refer to situations in which several economic operators intervene on a given product before this product is being placed on the market. For example, the Lifts Directive[54] requires the economic operator, who designs and manufactures the lift to provide the installer[55] with "*all the necessary documents and information to enable the latter to ensure correct and safe installation and testing of the lift*". The Machinery Directive requires manufacturers of equipment to provide information to the operator on how to assembly that equipment with another machinery[56].

The Union product safety legislation takes into account the complexity of the value chains, imposing obligations to several economic operators following the principle of "shared responsibility".

While the producer's responsibility on the final product safety has been proved adequate for current complex value chains, explicit provisions specifically requesting cooperation between the economic operators in the supply chain and the users could provide legal certainty in perhaps even more complex value chains. In particular, each actor in the value chain having an impact on the product safety (e.g. software producers) and users (bymodifying the product) would assume their responsibility and provide the next actor in the chain with the necessary information and measures.

[54] Pursuant to Article 16(2) of Directive 2014/33/EU

[55] In the Lifts Directive 2014/33/EU the installer is the equivalent of the manufacturer and must take the responsibility for the design, manufacture, installation and placing on the market of the lift.

[56] Machinery Directive, Annex I, Article 1.7.4.2 reads *"Each instruction manual must contain, where applicable, at least the following information"* (i) *"assembly, installation and connection instructions, including drawings, diagrams and the means of attachment and the designation of the chassis or installation on which the machinery is to be mounted;"*

# 3. Liability

At Union level, product safety and product liability provisions are two complementary mechanisms to pursue the same policy goal of a functioning single market for goods that ensures high levels of safety, i.e. minimise the risk of harm to users and provides for compensation for damages resulting from defective goods.

At national level, non-harmonised civil liability frameworks complement these Union rules by ensuring compensation for damages from various causes (such as products and services) and by addressing different liable persons (such as owners, operators or service providers).

While optimising Union safety rules for AI can help avoiding accidents, they may nevertheless happen. This is when civil liability intervenes. Civil liability rules play a double role in our society: on the one hand, they ensure that victims of a damage caused by others get compensation and, on the other hand, they provide economic incentives for the liable party to avoid causing such damage. Liability rules always have to strike a balance between protecting citizens from harm while enabling businesses to innovate.

Liability frameworks in the Union have functioned well. They rely on the parallel application of the Product Liability Directive (Directive 85/374/EEC), which harmonised the liability of the producer of defective products, and other non-harmonised national liability regimes.

The Product Liability Directive provides a layer of protection that national fault-based liability alone does not provide. It introduces a system of strict liability of the producer for damage caused by a defect in their products. In case of a physical or material damage, the injured party is entitled to compensation if he or she proves the damage, the defect in the product (i.e. that it did not provide the safety that the public is entitled to expect) and the causal link between the defective product and the damage.

National non-harmonised regimes provide fault-based liability rules, according to which victims of damage need to prove the fault of the liable person, the damage and causality between the fault and the damage in order to establish a successful liability claim. They also provide strict liability regimes where the national legislator has attributed liability for a risk to a specific person, without the need for a victim to prove fault/defect or causality between fault/defect and the damage.

National liability regimes provide victims of damage caused by products and services with several parallel compensation claims, based on fault or strict liability. These claims are directed often against different liable persons and have different conditions.

For instance, a victim involved in a car accident has typically a strict-liability claim against the owner of the car (i.e. the person who takes out motor vehicle liability insurance) and a fault-based liability claim against the driver, both under national civil law, as well as a claim under the Product Liability Directive against the producer if the car had a defect.

In accordance with the harmonised rules on motor vehicle insurance, the use of the vehicle must be insured[57] and the insurer is always in practice the first point of claim for compensation for personal injury or material damage. According to these rules, the obligatory insurance compensates the victim and protects the insured person who is liable under national civil law rules[58] to pay financial damages for the accident involving the motor vehicle.

[57] Harmonised for motor vehicles by Directive 2009/103/EC relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability.

[58] In most Member States strict liability is applied for the person in whose name the motor vehicle is registered.

Producers are not subject to mandatory insurance under the Product Liability Directive. Autonomous vehicles are not treated in Union legislation any differently from non-autonomous vehicles as regards motor insurance. Such vehicles, like all vehicles, must be covered by the third party motor liability insurance, which is the easiest way for the injured party to get compensation.

Taking out proper insurance can mitigate the negative consequences of accidents by providing for a smooth compensation for the victim. Clear liability rules help insurance companies to calculate their risks and to claim reimbursement from the party ultimately liable for the damage. For example, if an accident is caused by a defect, the motor insurer can claim reimbursement from the manufacturer after compensating the victim.

However, the characteristics of emerging digital technologies like AI, the IoT and robotics challenge aspects of Union and national liability frameworks and could reduce their effectiveness. Some of these characteristics could make it hard to trace the damage back to a human behaviour, which could give grounds for a fault-based claim in accordance with national rules. This means that liability claims based on national tort laws may be difficult or overly costly to prove and consequently victims may not be adequately compensated. It is important that victims of accidents of products and services including emerging digital technologies like AI do not enjoy a lower level of protection compared to similar other products and services, for which they would get compensation under national tort law. This could reduce societal acceptance of those emerging technologies and lead to hesitance to use them.

It will need to be assessed whether challenges of the new technologies to the existing frameworks could also cause legal uncertainty as to how existing laws would apply (e.g. how the concept of fault would apply to damage caused by AI). These could in turn discourage investment as well as increase information and insurance costs for producers and other businesses in the supply chain, especially European SMEs. In addition, should Member States eventually address the challenges to national liability frameworks, it could lead to further fragmentation, thereby increasing the costs of putting innovative AI-solutions and reducing cross-border trade in the Single Market. It is important that companies know their liability risks throughout the value chain and can reduce or prevent them and insure themselves effectively against these risks.

This chapter explains how new technologies challenge the existing frameworks and in what way these challenges could be addressed. Furthermore, specificities of some sectors, for example health care, may deserve additional considerations.

**Complexity of products, services and the value-chain**: Technology and industry have evolved drastically over the last decades. Especially the dividing line between products and services may no longer be as clear-cut as it was. Products and the provision of services are increasingly intertwined. While complex products and value chains are not new to European industry or its regulatory model, software and also AI merit specific attention in respect of product liability. Software is essential to the functioning of a large number of products and may affect their safety. It is integrated into products but it may also be supplied separately to enable the use of the product as intended. Neither a computer nor a smartphone would be of particular use without software. This means that software can make a tangible product defective and lead to physical damage (cf. box on software in the part on safety). This could eventually result in the liability of the producer of the product under the Product Liability Directive.

However, as software comes in many types and forms, answers related to the classification of software as a service or as a product may not always be straightforward. Thus while software steering the operations of a tangible product could be considered part or component of that product, some forms of stand-alone software could be more difficult to classify.

Although the Product Liability Directive's definition of product is broad, its scope could be further clarified to better reflect the complexity of emerging technologies and ensure that compensation is always available for damage caused by products that are defective because of software or other digital features. This would better enable economic actors, such as software developers, to assess whether they could be considered producers according to the Product Liability Directive.

AI applications are often integrated in **complex IoT environments** where many different connected devices and services interact. Combining different digital components in a complex ecosystem and the plurality of actors involved can make it difficult to assess where a potential damage originates and which person is liable for it. Due to the complexity of these technologies, it can be very difficult for victims to identify the liable person and prove all necessary conditions for a successful claim, as required under national law. The costs for this expertise may be economically prohibitive and discourage victims from claiming compensation.

In addition, products and services relying on AI will interact with traditional technologies, leading to added complexity also when it comes to liability. For example, autonomous cars will share the road with traditional ones for a certain time. Similar complexity of interacting actors will arise in some services sectors (such as traffic management and healthcare) where partially automated AI systems will support human decision-making.

According to the Report[59] from the New Technologies formation of the Expert Group on Liability and New Technologies, adaptations of national laws to facilitate the burden of proof for the victims of AI-related damage could be considered. For example, the burden of proof could be linked to the compliance (by a relevant operator) with specific cyber-security or other safety obligations set by law: if one does not comply with these rules, a change to the burden of proof as regards fault and causation could apply.

The Commission is seeking views whether and to what extent it may be needed to mitigate the consequences of complexity by alleviating/reversing the burden of proof required by national liability rules for damage caused by the operation of AI applications, through an appropriate EU initiative.

As regards Union legislation, according to the Product Liability Directive, a product that does not meet mandatory safety rules would be considered defective, regardless of the producers' fault. There may, however, also be reasons to contemplate ways on how to facilitate the burden of proof for victims under the Directive: the Directive relies on national rules on the evidence and the establishment of causation.

**Connectivity and openness**: It is currently not entirely clear what safety expectations may be with regard to damage that results from cybersecurity breaches in the product and whether such damage would be adequately compensated under the Product Liability Directive.

[59] Liability for Artificial Intelligence and other emerging technologies' Report, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

Cybersecurity weaknesses may exist from the outset, when a product is put into circulation, but they may also appear at a later stage, well after the product was put into circulation.

In fault-based liability frameworks, establishing clear cyber-security obligations allows the operators to determine what they have to do in order to avoid the consequences of liability.

Under the Product Liability Directive, the question if a producer could have foreseen certain changes taking account of the product's reasonably foreseeable use may become more prominent. For example, one might see an increase in the use of the 'later defect defence' according to which a producer is not liable if the defect did not exist at the time the product was put into circulation or in the 'development risk defence' (that the state of the art knowledge at the time could not have foreseen the defect). In addition, liability could be reduced where the injured party does not perform safety relevant updates. This could potentially be regarded as contributory negligence by the injured person and therefore reduce a producer's liability. As the notion of foreseeable reasonable use and questions of contributory negligence, such as the failure to download a safety update, may become more prevalent, injured persons might find it more difficult to get compensation for damage caused by a defect in a product.

**Autonomy and opacity:** Where AI applications are able to act autonomously, they perform a task without every step being pre-defined and with less or eventually entirely without immediate human control or supervision. Algorithms based on machine-learning can be difficult, if not impossible, to understand (the so-called 'black-box effect').

In addition to complexity discussed above, due to the black-box effect in some AI, getting compensation could become difficult for damage caused by autonomous AI-applications. The need to understand the algorithm and the data used by the AI requires analytical capacity and technical expertise that victims could find prohibitively costly. In addition, access to the algorithm and the data could be impossible without the cooperation of the potentially liable party. In practice, victims may thus not be able to make a liability claim. In addition, it would be unclear, how to demonstrate the fault of an AI acting autonomously, or what would be considered the fault of a person relying on the use of AI.

National laws have already developed a number of solutions to reduce the burden of proof for victims in similar situations.

A guiding principle for Union product safety and product liability remains that it is for producers to ensure that all products put on the market should be safe, throughout their life-cycle as well as for the use of the product that can reasonably be expected. This means that a manufacturer would have to make sure that a product using AI respects certain safety parameters. The features of AI do not preclude that there is an entitlement to safety expectations for products, whether they are automatic lawnmowers or surgery robots.

Autonomy can affect the safety of the product, because it may alter a product's characteristics substantially, including its safety features. It is a question under what conditions self-learning features prolong liability of the producer and to what extent should the producer have foreseen certain changes.

In close coordination with corresponding changes in the Union safety framework, the notion of 'putting into circulation' that is currently used by the Product Liability Directive could be revisited to take into account that products may change and be altered. This could also help to clarify who is liable for any changes that are made to the product.

According to the Report[60] from the New Technologies formation of the Expert Group on Liability and New Technologies, the operation of some autonomous AI devices and services could have a specific risk profile in terms of liability, because they may cause significant harm to important legal interests like life, health and property, and expose the public at large to risks. This could mainly concern AI devices that move in public spaces (e.g. fully autonomous vehicles, drones[61] and package delivery robots) or AI-based services with similar risks (e.g. traffic management services guiding or controlling vehicles or management of power distribution). The challenges of autonomy and opacity to national tort laws could be addressed following a risk-based approach. Strict liability schemes could ensure that whenever that risk materialises, the victim is compensated regardless of fault. The impact of choosing who should be strictly liable for such operations on the development and uptake of AI would need to be carefully assessed and a risk-based approach be considered.

For the operation of AI applications with a specific risk profile, the Commission is seeking views on whether and to what extent strict liability, as it exists in national laws for similar risks to which the public is exposed (for instance for operating motor vehicles, airplanes or nuclear power plants), may be needed in order to achieve effective compensation of possible victims. The Commission is also seeking views on coupling strict liability with a possible obligation to conclude available insurance, following the example of the Motor Insurance Directive, in order to ensure compensation irrespective of the liable person's solvency and to help reducing the costs of damage.

For the operation of all other AI applications, which would constitute the large majority of AI applications, the Commission is reflecting whether the burden of proof concerning causation and fault needs to be adapted. In this respect, one of the issues flagged by the Report[62] from the New Technologies formation of the Expert Group on Liability and New Technologies is the situation when the potentially liable party has not logged the data relevant for assessing liability or is not willing to share them with the victim.

## 4. Conclusion

The emergence of new digital technologies like AI, the IoT and robotics raise new challenges in terms of product safety and liability like connectivity, autonomy, data dependency, opacity, complexity of products and systems, software updates and more complex safety management and value chains.

The current product safety legislation contains a number of gaps that need to be addressed, in particular in the General Product Safety Directive, Machinery Directive, the Radio-Equipment Directive and the New Legislative Framework. Future work on the adaptation of different pieces of legislation in this framework will be done in a consistent and harmonised manner.

The new challenges in terms of safety create also new challenges in terms of liability. Those liability related challenges need to be addressed to ensure the same level of protection

[60] Liability for Artificial Intelligence and other emerging technologies' Report, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[61] Cf. unmanned aircraft systems referred to in Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

[62] Liability for Artificial Intelligence and other emerging technologies' Report, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

compared to victims of traditional technologies, while maintaining the balance with the needs of technological innovation. This will help create trust in these new emerging digital technologies and create investment stability.

While in principle the existing Union and national liability laws are able to cope with emerging technologies, the dimension and combined effect of the challenges of AI could make it more difficult to offer victims compensation in all cases where this would be justified[63]. Thus, the allocation of the cost when damage occurs may be unfair or inefficient under the current rules. To rectify this and address potential uncertainties in the existing framework, certain adjustments to the Product Liability Directive and national liability regimes through appropriate EU initiatives could be considered on a targeted, risk-based approach, i.e. taking into account that different AI applications pose different risks.

[63] See the Report from the New Technologies formation, p. 3 and the policy recommendation 27.2. of the High Level Expert Group on Artificial Intelligence.