EUROPEAN
COMMISSION

Brussels, 25.4.2018
SWD(2018) 137 final

COMMISSION STAFF WORKING DOCUMENT

Liability for emerging digital technologies

Accompanying the document

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions

Artificial intelligence for Europe

{COM(2018) 237 final}

TABLE OF CONTENTS

1. INTRODUCTION

Emerging digital technologies, such as the Internet of Things (IoT), Artificial Intelligence, advanced robotics and autonomous systems, lead to the creation of new products and services that allow for new opportunities for our economy and society. These new products and services can create new systems and complex environments that significantly improve our daily life.

An example is the smart home environment. This environment comprises connected and intelligent products (like smart fridges, smart meters, smart doors or smart fire alarms), which collect data through sensors, interact autonomously with each other and with external actors and use cloud services, embedded and non-embedded software for the provision of sophisticated hybrids between products and services.

In order to fully benefit from the opportunities presented by these new products and services, stimulating investment in emerging digital technologies is critical. A clear and stable legal framework will stimulate investment and, in combination with research and innovation, will help bring the benefits of these technologies to every business and citizen.

These new products and services are not inherently less safe than traditional products. Consumers' trust and the uptake of these technologies will depend on whether they are perceived to be safe and on whether the legal framework is considered clear and effective to provide remedies to victims. Clearly, the way in which technologies and tools are used is important for safety and liability aspects. When designing new technologies, it is important to consider also occupational health and safety aspects, in particular, in relation to ergonomics and mental stress. The liability framework that is currently existing in the European Union – as will be described further in this document - is a stable framework that incites investment, innovation and risk-taking.

Nevertheless, a reflection on future needs and developments is needed, not only from the perspective of the victim i.e. in order to ensure equitable remedies, compensation and allocation of responsibility, but also from the perspective of the innovators and companies operating in the EU as legal certainty is a key element for good business development.

In certain cases, when digital technology products or services cause a damage, the allocation of liability[1] may be complex due to their specific characteristics. In addition, ensuring their safety over their lifetime is important, as it can prevent or reduce potential damages and liability issues. It is therefore necessary to examine whether existing rules at EU and national level for safety and for the allocation of liability and the conditions, under which a victim is entitled to obtain compensation for damages caused by products and services stemming from emerging digital technologies, are appropriate and whether, for the producers and services providers, the framework continues to deliver an adequate level of legal certainty.

The Commission has engaged in a series of activities since 2015 which included to look into the issue of liability, also in relation to cybersecurity[2], in various Communications

[1] For the purpose of this document, 'liability' means the responsibility of one party for harm or damage caused to another party, which may be a cause for compensation, financially or otherwise, by the former to the latter.

[2] Joint Communication to the European Parliament and the Council on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final.

and strategic documents, to ensure legal certainty for the rollout and uptake of emerging digital technologies and to fully exploit their potential, as explained in the Communication "Artificial intelligence for Europe"[3].

In particular, the Digital Single Market Strategy (DSM)[4] emphasised the importance of legal certainty for the rollout of the Internet of Things (IoT)[5] and the Communication on "Building a European Data Economy"[6] committed to assess whether the current EU legal rules for product liability are fit for purpose, when damages occur in the context of the use of IoT and autonomous systems. In May 2017, the DSM mid-term review[7] announced that the Commission will consider the possible need to adapt the current legal framework to take account of emerging digital technologies, especially from the angle of civil law liability and taking into account the results of the ongoing evaluation of the Product Liability Directive[8] and the Machinery Directive[9].

The European Parliament issued a Resolution[10] calling for updated civil liability rules that duly take into account the development of autonomous and cognitive features in cars and robots including their safety aspects.

The objective of this document is therefore to provide a first mapping of liability challenges that occur in the context of emerging digital technologies. It builds on preliminary work, such as studies[11], public consultations and internal legal analysis, and provides a basis for the work of an Expert Group on "Liability and New Technologies" which will provide the Commission with expertise on the applicability of the Product Liability Directive to traditional products, new technologies and new societal challenges. The work of this group will also aim at providing the Commission with input relating to the different objectives, as set out in the policy documents referred to above and to consider possible adaptations of the current framework, in order to achieve clarity that would help stimulate investment in emerging digital technologies and to ensure that

[3] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Artificial intelligence for Europe, COM(2018) 237 final.

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A Digital Single Market Strategy for Europe, COM(2015) 192 final.

[5] Commission Staff Working Document on Advancing the Internet of Things in Europe, accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Digitising European Industry - Reaping the full benefits of a Digital Single Market, SWD(2016) 110 final.

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Building a European Data Economy", COM(2017) 9 final.

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All, COM(2017) 228 final.

[8] EU legislation on liability for defective products. Available at: http://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en.

[9] EU Machinery Legislation. Available at: http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_en.

[10] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL).

[11] The publication of the final reports of two relevant studies is envisaged for June 2018.

adequate redress mechanisms are in place in case of damages caused by products and services stemming from them.

As product liability and product safety are closely linked, Chapter 2 of the document outlines both the existing safety and liability frameworks, which are pillars of the internal market. The EU approach to the internal market is based on common safety rules, underpinned by provisions on product liability, while the regime for contractual or extra-contractual liability for services and the regime for specific contractual or extra-contractual liability for products are left to national law. Chapter 3 presents the specific characteristics of emerging digital technologies: increasing level of complexity and variety of ecosystems, actors and value chains; autonomy in decision making and actuating; generation, processing and reliance of big volumes of data; and openness to software extensions, updates and patches after the products have been put into circulation[12]. The document then develops a number of brief theoretical case studies that aim at exemplifying the above specific characteristics, and at discussing the extent to which they could be covered by the existing rules and the impact they may have on the parties involved. Chapter 4 and 5 puts forward a series of questions for further reflection and analysis in relation to the existing elements and concepts and to wider issues, including cybersecurity as well as outlines next steps. The views expressed in this document should be understood as the Commission's services analysis of the matters under discussion, and do not constitute political commitments from the part of the Commission.

2. LANDSCAPE OF EXISTING APPLICABLE RULES AND UNDERLYING PRINCIPLES FROM EXISTING LEGISLATION OR JURISPRUDENCE

Product safety and liability are complementary legal frameworks aiming to provide trust and safety to consumers. EU product safety legislation aims at ensuring that only safe products can be placed on the internal market of the Union. EU product liability legislation[13] provides for liability of producers of defective products that cause damage to natural persons or their property. In addition, various national liability regimes may apply if damage occurs.

2.1. Overview of relevant elements of safety rules applicable in the context of emerging digital technologies at EU level

Emerging digital technologies, such as IoT, AI-powered advanced robots and autonomous self-learning systems, must meet the essential health and safety requirements laid down in the applicable EU safety legislation[14] which ensures a single market for a wide range of equipment and machines, such as for instance Directive (EC) 2006/42[15] on machinery (which is the relevant safety legislation for robots), Directive 2014/53/EU on

[12] A more detailed description of these specific characteristics per technology is given in Annex I.

[13] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29–33).

[14] A more comprehensive list of EU relevant legislation is included in Annex II.

[15] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) (OJ L 157, 9.6.2006, p. 24–86).

radio equipment[16], hereinafter referred to as the "Radio Equipment Directive" (which applies to all products, including embedded software, using the radio frequency spectrum), Council Directive 90/385/EEC on Active Implantable Medical Devices (AIMDD)[17], the Council Directive 93/42/EEC on Medical Devices (MDD)[18], Council Directive 98/79/EC on In Vitro Diagnostic Medical Devices (IVDMD)[19], as well as the Council Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work.[20]

Alongside product harmonisation legislation, Directive 2001/95/EC of the European Parliament and the Council of 3 December 2001 on general product safety aims to ensure that only safe consumer products are placed on the market and acts as a safety net role for products and risks not covered by the harmonisation legislation.

Emerging digital technologies are also being incorporated in other products; therefore, other EU legislative instruments also apply. In the framework of the Union harmonisation legislation on products, manufacturers must ensure that products meet the essential health and safety requirements by following the applicable conformity assessment procedures, involving in some cases a conformity assessment body, and must keep the technical documentation about the products that they place on the market. These rules apply when the products are placed on the market and in some cases during the lifecycle of the product. They must be taken into consideration when a liability problem arises in relation to safety issues during the lifecycle of the product.

Currently, the production of European harmonised standards for IoT, AI-powered advanced robots and autonomous systems is ongoing. European Standardization Organisations draw up these standards in order to offer a level playing field and a competitive advantage to European manufacturers. These standards would offer presumption of conformity with the European safety legislation, under which they are developed, in particular under the Machinery Directive 2006/42/EC and the Radio Equipment Directive 2014/53/EU. The European Standardization Organizations are also working on standards for "combined" products, i.e. where several pieces of EU safety legislation apply.

Potential connectivity issues may arise in products currently on the market. The Commission has already been empowered under the Radio Equipment Directive 2014/53/EU (Article 3(3)) to ensure, for instance, that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software with the applicable safety requirements has been demonstrated (Article 3(3)(i)). The Expert Group on Reconfigurable Radio Systems is currently working to help the Commission to assess the possibility of adopting one or more delegated acts in that

[16] 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 (OJ L 153, 22.5.2014, p. 62–106).

[17] Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (OJ L 189, 20.7.1990, p. 17–36).

[18] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p.1-43).

[19] Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices (OJ L 331, 7.12.1998, p. 1-37).

[20] Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (OJ L 183, 29.06.1989, p. 1-8).

respect. Several stakeholders have already requested to start a similar exercise on other delegated provisions of this Directive, with the aim to specify the categories or classes of radio equipment concerned by the requirement to support certain features ensuring protection from frauds, to incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected, to interwork with other radio equipment or not to misuse network resources.

2.2. Underlying principles of the extra-contractual liability rules applicable in the context of emerging digital technologies at EU and MS level

Extra-contractual liability relates to the civil law responsibility for damage caused outside the context of a contract (the damage being caused by a violation of a right or legitimate interest protected by law). Extra-contractual liability can be imposed by general civil law rules or specific legislation. Product liability is a form of statutory extra-contractual liability referring to the civil liability of manufacturers.

EU level

At EU level, the product liability regime was introduced by the Product Liability Directive. It was conceived around the notion of movable products, most of which are tangible. It puts forward a horizontal approach in relation to assigning liability in the case of defects and is technology neutral. It covers all types of products, ranging from raw materials to complex industrial products, now including emerging digital technology products. It covers Business-to-Consumer (B2C) relations and provides a comparatively simple point of reference for both consumers and producers.

The Product Liability Directive establishes a liability of producers when defective products cause damages to victims (including personal injuries or death or damage to property). This is a strict liability regime, in that the injured person does not have to prove a fault of the producer. The injured person carries the burden of proof of the defect in the product, the actual damage and the causal link between the defect and the damage.

The Product Liability Directive has an all-encompassing definition of producer, against whom the injured party can bring its claim: the manufacturer of the product, the producer of any raw material or the manufacturer of a component part or any person who, by putting its name, trademark or any distinguishing feature on the product presents himself as the producer. Furthermore, without prejudice to the liability of the producer, the importer is deemed to be a producer. Finally, where the producer cannot be identified, each supplier of the product shall be treated as its producer unless he informs the injured person of the identity of the producer.

The Court of Justice indicated that the Directive applies to products used while providing any service but that the liability of a service provider does not fall within the scope of the Directive.[21] However, the Directive does not prevent Member States from applying national rules under which a service provider using a defective product is liable for a damage caused by such use.

[21] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

The Product Liability Directive creates an exhaustive harmonisation for the matters that it explicitly covers[22].

National level

At national level, the rules implementing the Product Liability Directive coexist[23] with other extra-contractual liability rules that could also be invoked by victims of damages. The Product Liability Directive does not preclude the application of other systems of contractual or non-contractual liability based on other grounds, such as fault or a warranty in respect to latent defects[24]. As regards national extra-contractual liability rules, broadly speaking they could be classified into two categories depending on whether the compensation of the victim requires a fault of the person considered liable by the law or not.[25]

Fault-based extra-contractual liability

As a general rule in most jurisdictions, extra-contractual liability regimes are fault-based. This means that the fault of the author of the wrongful behaviour leading to a damage (which could be an act or an omission whether intentional or by negligence) is a necessary element to be proven for the liability claim to be successful.

It is typically up to the victim submitting a claim to provide the evidence needed to support his liability claim. There are situations, however, where national law introduces variations to facilitate the burden of proof of the victim. Such variations may consist in a presumption of fault by the wrongdoer (or a reversal of the burden of proof), whereby the wrongdoer is liable unless he proves that he was not in fault. The variations may respond to the logic that the general rule on the burden of proof needs to be altered so as to increase the possibility of compensation for the victim or at least balance the situation of disadvantage in which the victim would be pursuant to the ordinary regime. These variations may also reflect the circumstance that there may be an imbalance of information between the victim and the wrongdoer. The abovementioned variations may be linked to a diverse set of factual situations generating different types of risks and damages, such as the responsibility of the owner/possessor of the building in case of damages causes by his/her building (unless he/she proves that he/she observed appropriate care for the purpose of avoiding the damage)[26], the responsibility of a person carrying a dangerous activity (unless he/she proves that all appropriate measures to avoid the damage have been taken)[27], the responsibility of the employer/the principal for the act executed on his behalf or interest by his employees/agents (unless he proves that he used

[22] For instance, CJEU. Judgment of 25 April 2002. Case C-52/00. Commission of the European Communities v French Republic.

[23] According to Article 13 of the Product Liability Directive, the "Directive shall not affect any rights which an injured person may have according to the rules of the law of contractual or non-contractual liability or a special liability system existing at the moment when this Directive is notified".

[24] CJEU- Judgement of 25 April 2002. Case C-183/00 María Victoria González Sánchez v Medicina Asturiana SA. and Judgement of 20 November 2014, Case C-310/13, Novo Nordisk Pharma G.

[25] The analysis of relevant elements and underlying principles of national law undertaken in this section is purely illustrative and is not meant to provide a comprehensive or representative portrait of national liability regimes. The analysis is based solely on a limited sample of national legal regimes.

[26] Cf. for example Section 836 German Civil Code, Section 1319 of the Austrian General Civil Code, Article 2053 of the Italian Civil Code or Section 6:560(1) of the Hungarian Civil Code.

[27] Cf. for example Article 2050 Italian Civil Code.

appropriate care in the selection and the management of the agent/employee)[28] or the responsibility of parents/tutors/guardians/teachers for damages caused by a minor, pupil, student/apprentice or mentally impaired person (unless they can prove that they were not able to prevent the damages from happening). [29]

Special regimes of strict liability (extra-contractual)

National legal systems may also provide for special regimes of strict liability. In most jurisdictions, strict liability is often defined as a liability that does not depend on a fault and the claimant needs only to prove the damage and the causal link.

The reversal of the burden of proof in the context of a fault-based extra-contractual liability and the principle of strict liability typically respond to a common rationale. They both aim overall at facilitating the compensation of the victim of damages in situations where the legislator considers it too burdensome or unbalanced to apply the general fault-based liability rule. Some forms of strict liability may go even a step further by linking liability simply to the materialization of a risk and/or making the discharge of liability either impossible or possible only under the proof that the damaging event was caused by an exceptional/unforeseen circumstance that could not be avoided. There may be also other cases where the risk of damage is linked to the unpredictability of behaviour of specific risk groups, like animals or certain persons: in these cases liability may be attributed to the persons that are considered responsible to supervise the animal or the person, because it is them who should normally be in the condition to adopt measures to prevent or reduce the risk of damages. Finally, when the risk of damages is linked to dangerous activities, some jurisdictions may attribute liability to the person that carries out the activity (e.g. the operator of a nuclear power plant or of an aircraft or the driver of a car) or is ultimately responsible for the dangerous activity to happen (e.g. the owner of a vehicle). The rationale typically is that this person has created a risk, which materialises in a damage and at the same time also derives an economic benefit from this activity.

Special regimes of strict liability may apply to a diverse set of factual situations generating different types of risks and damages, such as the liability of the owners of animals for the damages caused by the animals under their custody[30]; the strict liability of the person responsible for carrying out an unspecified[31] or specified dangerous activity (for example the operation of nuclear power plants,[32] aircrafts[33] or motor vehicles[34]) or other cases linked to a legal or factual relationship between two persons or a person and an object, such as when the damages are caused by someone executing a task in the

[28] Cf. for example Section 831 of the German Civil Code; Section 1315 of Austrian General Civil Code; Sections 6:540(1) and 6:542(1) of the Hungarian Civil Code.

[29] Cf. for example Articles 2048 and 2047 of the Italian Civil Code; Section 832 of the German Civil Code.

[30] Cf. for example Article 2052 of the Italian Civil Code; Section 833 of the German Civil Code; Section 6:562 of the Hungarian Civil Code.

[31] Cf. for instance Section 6:535(1) of the Hungarian Civil Code.

[32] Cf. for instance Section 3 of the German Atomic Energy Act, in connection with Article 3 of the Paris Convention on Third Party Liability in the Field of Nuclear Energy.

[33] Cf. for instance Section 33 of the German Air Traffic Act and Section 148 of Austrian Air Traffic Act. Third-party liability insurance is required in those cases.

[34] Cf. for instance Article 2054 of the Italian Civil Code; Section 7 of the German Road Traffic Act; Section 5 of the Austrian Railway and Motor Vehicle Liability Act; Hungarian law considers motor vehicles as dangerous operations. (Cf. in this regard Section 6:535(1) Civil Code.

interest of someone else (employee/employer)[35] or by an object that is under his/her custody.[36]

While none of the above selection of national law provisions are specifically applicable to damages that may potentially be caused by emerging digital technologies, these provisions certainly constitute helpful precedents or points of reference to which one can turn to further a reflection about how to best address, from a normative standpoint, certain distinguishing elements of risks and damages created by the emerging digital technologies.

Several Member States have begun to consider the implications of emerging digital technologies on their national liability regimes. For instance, the Justice Ministers of the German federal states adopted a resolution in June 2017 calling for legislative action, including at EU level as needed, in the area of extra-contractual liability for the operation of autonomous systems. In particular in the area of autonomous cars, some Member States have introduced or proposed sector specific legislation. For example, Germany has amended its Street Traffic Act in order to allow autonomous cars to operate on the streets provided that a human driver is present to take over control at all times. Sweden has introduced a law which allows the testing of autonomous vehicles. In the UK, the government has proposed legislation which would amend insurance legislation in connection with the possible roll-out of autonomous vehicles.[37]

International level

Other countries in the world are also analysing the liability implications of emerging digital technologies. In the US, numerous states are addressing the need for legislation of autonomous vehicles, although laws vary widely among themselves since they address licensing, use or regulation issues. Outstanding concerns include questions of responsibility and liability, as well as data protection and cybersecurity threats. In Japan, the Ministry of Economy, Trade and Industry is discussing legal issues regarding AI from the perspective of rights and responsibilities, including liability.

3. THE SPECIFIC CHARACTERISTICS OF EMERGING DIGITAL TECHNOLOGIES

Emerging digital technologies show certain levels of complexity due to the interdependency between the different components and layers: i) the tangible parts/devices (sensors, actuators, hardware), ii) the different software components and applications, to iii) the data itself, iv) the data services (i.e. collection, processing, curating, analysing), and v) the connectivity features.

As it has also been the case in the past, any interdependency gives rise to a number of questions, among which, who should be held liable in case the technology causes a damage or how to identify the root cause of the problem. Nonetheless, as far as they constitute 'movable' items, IoT devices and any other items containing intangible elements or presenting connectivity features qualify as 'products' and defects in these products are covered by the Product Liability Directive.

[35] Cf. for instance Art. 2049 of the Italian Civil Code.

[36] Cf. for instance Art. 2051 of the Italian Civil Code.

[37] House of Commons Library, Briefing Paper, Automated and Electric Vehicles Bill 2017-19, 28 November 2017. Available at: http://researchbriefings.files.parliament.uk/documents/CBP-8118/CBP-8118.pdf.

Issues relating to liability when products involve third party components are not new. The producer needs to ensure the safety of the final product, and in turn, producers and sellers are responsible for any liability arising from the products placed on the market or sold to customers regardless of whether they include third party components. However, based on the specific characteristics of these emerging digital technologies, it should be examined whether, when products and services are increasingly connected and complex both in the design and the system integration, effective redress mechanisms for victims and legal certainty for producers are still ensured.

Furthermore, these technologies will encompass more and more the feature of autonomy. Advanced robots or devices empowered by AI and IoT will have increased capabilities to interpret the environment (via sensing, actuating, cognitive vision, machine learning, etc.), to interact with humans, to cooperate with other artefacts, to learn new behaviours and execute actions autonomously without human intervention. The more autonomous systems are, the less they depend on other actors (i.e. the manufacturer, the owner, the user, etc.) and the greater is their impact on their environment and on third parties.

Combined with self-learning and autonomy, the behaviour of these technologies may be difficult to predict. This could raise questions regarding liability, in situations where the damage caused by a machine operating with a certain degree of autonomy cannot be linked to a defect or a human wrongdoing (e.g. of the driver; the car manufacturer, etc.), but also in the wider context of safeguards to be introduced to ensure the safety of such technologies (e.g. should machines be allowed to freely learn from their context or should they be prevented from learning inadequate/dangerous behaviours). As a consequence, the question of how to attribute liability where the expected outcome of the technology was not identified either before the market launch or after that launch needs to be examined.

Moreover, digital technology products and services generate (e.g. via sensors) and/or process data (e.g. through actuators, algorithms). The availability and the quality of data is essential for their good functioning. Faulty or corrupted data (e.g. due to connectivity problems or when hacked) may render the system malfunctioning.

Providing data through an IoT system could be considered a service, and thus fall as such, outside the product liability and safety regimes. Therefore, where damage is caused by the supply of erroneous data or by a failure to supply data, allocating liability may become unclear and claims potentially difficult to enforce.

Finally, digital technology products are open to software extensions, updates and patches after they have been put into circulation. Any change to the software of the system may affect the behaviour of the entire system or of individual components or may extend its functionality. Software can be patched, updated or revised, by the producer of the system or of individual system components or by third parties, in a way that can affect the safety of these technologies. Updates would usually close safety holes through patches, but new codes also add or remove features in ways that change the risk profile of these technologies.

Contractual liability of a software provider depends to a large extent on its contractual obligations (e.g. to supply applications which provide a certain level of safety and cybersecurity as well as updates for a certain period of time). A failure to comply with these obligations may trigger contractual liability claims. Such liability claims will aim at remedies in case of non conformity with the contract, e.g. bringing it into conformity, price reduction or termination of the contract, or at damages for breach of contract. The contractual liability of a software provider may be limited to the extent its customer contributed to the actual damage, e.g. because he did not install an available update. The

liability of the software provider may also be limited according to the terms of the contract, to the extent such contractual limitation is permitted by the applicable law. The extent to which extra-contractual liability claims can be raised in parallel with possible contractual liability depends on national law.[38]

3.1. Case studies analysis

Introduction

The potential of AI and IoT powered systems is immense and not yet fully known or predictable at this stage. It is already clear, however, that AI applications and systems can generate autonomous decision-making and autonomous behaviour in the physical environment in which they operate including physical contact with humans and their property. This inevitably carries an inherent risk of causing damage to a third party's physical integrity or property. Damages may also be caused by AI systems that are not embedded in a hardware structure, for example economic damage caused by an autonomous trading algorithm at the stock exchange.

Although fully autonomous systems or IoT devices are not yet part of everyday life for most people, it is possible to anticipate likely realistic scenarios raising civil liability questions based on the current state of technological development and of known testing and pilot projects. The following case studies offer a first, preliminary description of such civil liability questions. As there is not yet a mass roll-out of these new technologies, the analysis that follows cannot yet rely on specific liability cases or court decisions and therefore works with some inevitable assumptions and theoretical considerations. In particular, while being based on existing legal concepts and possible relevant interpretations, the analysis does not specifically target and is not premised upon specific national legal systems. The primary goal of the use cases is to prepare the ground for further reflection. These case studies should not be seen as an exhaustive list, these and other cases will be explored further in the expert group work.

AI powered devices and systems

Autonomous unmanned aircraft (autonomous drones)

Unmanned aircraft[39], or for brevity and for the purposes of this Staff Working Document drones, represent a rapidly developing sector of aviation with great potential to create new jobs and economic growth in the EU. The Commission predicts that by 2035, the European drone sector will directly employ more than 100,000 people and have an economic impact exceeding €10 billion per year, mainly in services. Drones can potentially be used for various civil purposes such as package delivery, surveillance and monitoring, data collection, inspection, search and rescue or even passenger transport. Drones rely on several technological components like for instance sensors, actuators and software that overall enable the drone's operation. While the level of automation may

[38] This issue is demonstrated in the case decided by the Court of Appeal in Ghent (Belgium) in December 2016. De Redactie, Geldboetes voor UZ Gent en 3 bedrijven voor foute hersenbestraling, 7 September 2015. Available at: http://deredactie.be/cm/vrtnieuws/regio/oostvlaanderen/1.2434505.

[39] The notion of unmanned aircraft is defined in Article 3 of the Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council (2016/0277 (COD)) ('Proposal for a new Basic Regulation in the field of aviation safety').

vary depending on the specific application, fully autonomous drones already exist for instance for the delivery of packages.

This use case discusses possible liability scenarios in the context of the use of autonomous drones, to be intended as drones executing a certain activity - such as the delivery of a package - in a completely autonomous manner, from take-off, to selection of the route, avoidance of obstacles, landing, etc.

A parcel delivery drone that is flying autonomously from the seller's warehouse to the customer's dwelling may cause damage in a variety of ways. It may abruptly fall to the ground or collide in-air with another flying vessel or drop the package resulting in property damage or personal injury.

Without prejudice to any possible national legislation addressing the specific liability for autonomous drones, it can be reasonable to argue that autonomous drones are "aircrafts" and could therefore potentially be covered by national laws and international conventions regarding the liability for aircraft. In this respect, typically aircraft are subject to a strict liability regime and the party liable for damage is generally the operator. [40] In the case of autonomous drones, the operator would be the person or entity that, although not remotely or manually steering it, has control on the overall use of the drone. The injured person would therefore have a strict liability claim against the operator if the national law stipulating the liability for aircraft accidents is considered as covering drones. Autonomous features of the drones should not have an impact on the likelihood of success of the victim's claim against the drone operator under strict liability air traffic legislation. The victim should only prove that the damage was caused by the drone without having to substantiate what made the drone fall down or drop the package.[41]

The victim could also have a claim against the operator under general national tort law rules which would require a fault of the operator. Such a fault could be envisaged for example when the drone operated under dangerous weather conditions or when the required maintenance was not performed. Depending on the provisions of national law that is applicable and to the extent the operation of the drone relies on third party service providers (for instance, the provider of GPS mapping, the provider of weather data, etc.) the operator could under certain conditions also be responsible if the accident was caused by malfunctioning of the services provided by the third party.

The victim may also sue the manufacturer under the national law provisions implementing the Product Liability Directive.[42] This would require to demonstrate a defect of the drone and to prove that the damage was caused by that defect.

As the accident of the drone may be a result of a rather large set of unknown circumstances, for instance a defect of the device, exceptional weather conditions or other circumstances such as a cyber-attacker, it will be difficult for the victim to prove the elements of a liability claim.

In most national regimes, a strict liability claim against the operator of the parcel delivery drone exists, and this appears to be an efficient way for the victim to achieve

[40] Steer Davies Gleeve, Study on the Third-Party Liability and Insurance Requirements of Remotely Piloted Aircraft Systems, Final Report, November 2014. Available at: https://www.eurocontrol.int/sites/default/files/ec_rpas_final_report_nov14_steer_davies.pdf.

[41] However, this might not be the case in jurisdictions where a fault-based liability regime applies.

[42] In a situation where the damaged property is not intended for private use, the Product Liability Directive would not apply.

compensation.[43] In the case the operator has compensated the victim and the accident was caused by a defect of the drone or a breach of the obligations of a service provider, the operator could seek redress against the manufacturer or the service provider. If the operation of the parcel delivery drone is subject to (mandatory) insurance coverage, any potential redress claim could under statutory law be transferred to the insurance.

For example, an autonomous drone crashed into a crane in the UK in June 2017[44]. The data programmed into the drone did not include information about the crane which was erected after the programming.

Autonomous cars

Autonomous cars are motor vehicles equipped with systems that allow operating the vehicle without human intervention either partially, or completely (full automation). Autonomous cars are at present one of the most important AI applications. Their announced benefits range from a dramatic drop in the number of road accidents[45] to reduced travelling time, improved traffic flow and environmental benefits.

In the case of partial, conditional automation[46], the car operates under the supervision of the driver, but without human input under specific conditions only (for instance on certain road types or in specific geographic areas). Outside these limited environments, the vehicle requires the control by a human driver or, if the driver does not take control, it may enter into a safe fall-back mode (for instance, park the vehicle). In these cases, the driver has the responsibility to supervise the car and stand ready to re-take control if needed or upon notice. In case of higher levels of automation, the vehicle is capable to operate without any human intervention and with full automation also on any road and in any conditions. There might not even be a human person inside the vehicle and the car might not even be equipped with a steering wheel or pedals.

At the current stage, only few jurisdictions have adopted rules specifically targeting highly automated or fully automated vehicles. As a consequence, the key components of the liability regime for automated vehicles are the national civil liability rules applicable to motor vehicles.

However, under the Motor Insurance Directive[47] all Member States have to ensure that civil liability for the use of vehicles is covered by insurance and that victims of an accident caused by a vehicle enjoy a direct claim against the insurer covering the person

[43] A strict-liability regime of aircraft operators may not however exist in every Member State.

[44] AAIB investigation to Quest Q-200 (UAS, registration n/a), Collision with a crane, Hinkley Point, Somerset, 12 July 2017. Available at: http://www.gov.uk/aaib-reports/aaib-investigation-to-quest-q-200-uas-none.

[45] According to the World Health Organization, every year over 1.2 million people die as a result of car accidents. It is considered that 90% of accidents each year are caused by human error.

[46] SAE International's On-Road Automated Vehicle Standards Committee published the SAE Information Report: (J3016) "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems". The SAE table summarizing the different levels of driving automation defines "conditional automation" (level 3) the situation in which the automated driving system performs all aspects of the dynamic driving task with the expectation that the human driver responds adequately to a request to intervene ("fallback performance"). Available at: https://en.wikipedia.org/wiki/Autonomous_car.

[47] Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 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. This is a minimum harmonisation Directive, so Member States may apply higher levels of protection such as obligatory amounts of insurance cover.

responsible against civil liability. Although the Motor Insurance Directive does not harmonise issues of civil liability, it aims to ensure an effective protection of victims irrespective of the allocation of liability according to the different national civil liability systems.

In case of an accident caused by a fully automated vehicle, liability for a damage may be allocated to the driver/holder of the vehicle under civil law liability rules or to the manufacturer of the automated vehicle under the rules implementing the Product Liability Directive.

Practically, all Member States attribute liability for damages caused by motor vehicles to the holder or the driver of the vehicle. Liability is either fault-based, including cases where the fault can be presumed unless the holder/driver proves the opposite, or risk-based, where the holder/driver is strictly liable for having opened the risk associated with the circulation of a motor vehicle on public streets. In particular, the liability of the holder of the car is typically risk-based.

If the victim claims damages against the holder of a motor vehicle based on strict liability rules, normally there is no need to demonstrate whether the accident was caused by a wrongdoing of the car driver or another person or by any deficiency of the car. If the victim decides to pursue a claim against the manufacturer of the car based on national legislation implementing the Product Liability Directive, he has to identify and prove a defect of the car and the causal link between the defect and the damage. Considerations similar to those made in the previous case study regarding the need for the victim to prove the cause of the damage apply.

As there is mandatory insurance coverage for the use of motor vehicles under the Motor Insurance Directive and victims of accidents with insured vehicles can approach insurers directly to receive compensation, the damages will usually be paid by the insurer. In situations where an accident occurred due to a defect of a vehicle which falls under the Product Liability Directive, the victim could also have a claim against the producer of the vehicle under the law implementing the Product Liability Directive. In this context, national law could provide for redress possibilities of the insurer who compensated the victim against the producer of the defective vehicle.

Tesla: On May 7, 2016, a semi-automated Tesla Model S struck and passed beneath a truck. At the time of the collision, the truck was making a left turn and impact with the right side of the semitrailer sheared off the roof of the Tesla. The driver of the Tesla died in the crash. System performance data downloaded from the Tesla revealed that the driver was operating the car using automated vehicle control systems: Traffic-Aware Cruise Control and Autosteer lane keeping systems. The investigations revealed that although the autopilot functioned as designed, it did not detect the truck. The truck was cutting across the car's path instead of driving directly in front of it, which the radar is better at detecting, and the camera-based system was not trained to recognize the flat slab of a truck's side as a threat. The Tesla driver’s lack of responsiveness indicated overreliance on automation and the monitoring steering wheel torque was not an effective method of ensuring driver engagement. The competent authority concluded that the crash was not the result of any specific defect in the autopilot system, thus Tesla was not found responsible for the accident. The competent authority noted that Tesla did an adequate job warning its customers that the autopilot system demands their supervision that their hands should remain on the wheel and their eyes on the road. The Terms of Services of the Tesla car included in cause provisions which were clarifying the semi-

autonomous nature of the autopilot and were requiring the driver to take over the control of the car in 4 seconds, if the driver noticed things were not going in the right direction. Since that accident, Tesla has changed the Autopilot system so that, if a driver repeatedly ignores the Autopilot warnings, the system will stop functioning and will be prevented from restarting for the duration of the trip. If the driver never responds, the car will gradually slow down until it stops and the flashing hazard lights will come on.

Google car: On February 14, 2016, a Google self-driving car attempted to pass a municipal bus in Mountain View, California. The bus did not behave as the autonomous car predicted, and the self-driving car crashed into it, while attempting to move back into its lane. The Google car was traveling at the stately speed of 2 mph, and there were no injuries. Google released a statement accepting fault and announcing that it was tweaking its software to avoid this type of collision in the future.

Uber car: On March 19, 2018 a woman in the street in Arizona died when hit by an autonomous Uber car, in what appears to be the first reported fatal crash involving a self-driving vehicle and a pedestrian in the US[48]. Local police reported the self-driving car was in autonomous mode at the time of the crash and that the vehicle hit a woman, who was walking outside of the crosswalk and later died at a hospital. There was a vehicle operator inside the car at the time of the crash. The circumstances of this accident had not been clarified at the moment of drafting of this Staff Working Document.

Internet of Things

Smart home ecosystem

Smart home ecosystems may include appliances, such as smart smoke detectors, smart fridges, smart thermostats, which are connected to the internet and to each other and have the ability to collect information and communicate with each other and with other systems and humans. Their operation relies on various sources of data, such as embedded sensors that automatically measure e.g. environmental parameters or monitor activity and transfer data to databases in an autonomous way, without human intervention. The data are accessed, processed and analysed by applications, which transfer commands to the physical devices in the smart home ecosystem. The various components in this ecosystem (devices, sensors, applications, etc.) may be provided by different suppliers.

For example, a smart smoke detector can be produced by manufacturer A and sold to the homeowner by seller B, a smart thermostat can be produced by manufacturer C and sold to the homeowner by seller D, the data analysis application could be provided by provider E or by one of the manufacturers of the smart appliances and the connectivity dimension is provided by internet provider F. The smart smoke detector can detect a source of fire and alert the homeowner or the fire department. In addition, the smoke detector can also communicate with other smart home appliances in the ecosystem, such as smart doors, instructing them to unlock in order to allow access to the fire fighters.

In case of a fire, not sending an alert to the fire department may ultimately result in the destruction of the house and/or damage to a neighbour's house. This may be due to

[48] The Guardian, Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian, 19 March 2018. Available at: http://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe.

various causes: a malfunctioning of the smoke detector, a faulty data processing by the application, a failure of electronic communication services or an autonomous decision to switch off the smoke detector, e.g. because of high energy consumption levels of the smoke detector. The more sophisticated an ecosystem gets, the more difficult it may be for the home owner to trace back any upcoming problem to its origin.

The home owner could have a contractual claim for damages against the seller of the thermostat or the seller of the smoke detector. This would require that the thermostat or the smoke detector were not in conformity with the sales contract. As the decision to switch off the smoke detector was taken by the application autonomously, a contractual liability of the seller of the smoke detector could be established on the basis that the device had to be designed in a way not to allow a third-party application to switch it off. The application provider would, in general, be contractually liable for the application's harmful decision.

Any claim of the home owner or the neighbour, who suffered damages from the fire, against the manufacturer of the smoke detector or the thermostat under the Product Liability Directive could be established on the basis of a defect of the device. In the above case, the consumer would have to prove the defect, more precisely which part of the smart home ecosystem was not working properly.

The neighbour could probably as well have a claim against the home owner under national tort law. This would require, in general, to prove a wrongdoing of the home owner.

If the home owner has taken out fire insurance, the insurance will probably cover the damage caused by the fire. In turn, any claim for damages which the home owner might have against the person responsible for the fire will be transferred to the insurance. In case of a complex ecosystem, the insurance faces comparable difficulties in identifying the cause for the fire and the responsible actor than the home owner.

Cyber-attacks

Internet of Things (IoT) devices may also constitute targets of cyber-attacks. In the case of smart home devices, poor security measures at design, manufacturing or operation stage may allow cyber-attackers to take control of the device and modify its functioning or the functioning of other smart devices in the same ecosystem.

In the absence of a contractual relationship to cater for cyber-attack damages, courts could impose tort liabilities on businesses (e.g. manufacturers, vendors, etc.) for the harm that a cyber-attack causes to third parties.

If we apply product liability rules to cyber-attack examples, the notions of defect, the level of safety that users are generally “entitled to expect” and the impact of software updates and functionality revisions on the safety of the product are difficult to define. Is a product defective simply because it has no update capabilities? Should the notion of defect include also a security objective, on top of the safety one?

The Product Liability Directive exempts the producer from liabilities if the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered. This exemption may as well be triggered by the manufacturer in a cyber-attack context to justify that at the moment of placing the good on the market no software vulnerability was discovered.

For example, the recent WannaCry ransomware[49] spread throughout the Internet and affected Windows-based computer systems that were running on outdated software. As well, the Mirai virus botnet leading to Distributed-Denial-of-Service attacks (on 21 October) remained under sustained assault for most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US[50]. These attacks caused disruptions in various places, including hospitals, businesses, and universities resulting in multiple types of damages from destruction (or loss) of data, system downtime, lost productivity, disruption to the normal course of business, forensic investigation, restoration and deletion of hostage data and systems, reputational harm, etc. A stream of (potential) extra-contractual and contractual liability could flow from the attack with various parties to blame for it: the programmers of the malware and the attackers' group; potentially the users who failed to install the Windows security patch as the vulnerability was discovered and the patch announced, and the software vendor, which supplied the insecure code in the first place. It is unclear how liability would be allocated (if at all) between such parties in the absence of a specific regime (e.g. the duty to ensure the protection of personal data; the duty to ensure a specific level of safety or (cyber) security resilience.)[51] Most evidently, the attacker would be liable, but most of such cyberattacks are anonymous and it is difficult if not impossible for the victim to identify the attacker(s) and obtain any compensation from them. Particular users (including businesses) that failed to install the Windows security patch could also potentially face legal actions (not limited to civil actions) for the negligent failure to deliver services following the attack. In addition, contractual liability may not apply since standard terms of service frequently do not contain any promise of (cyber) security resilience. On the contrary, vendors, and especially software vendors, typically attempt to minimize or even exclude their civil liability by inserting warranty disclaimers and limitations of liability in their terms of service. That said, it is questionable whether such limitations of liability would be upheld in case of litigation in the event of a cyber-attack, since liability limitations may be deemed null and void in the case of gross negligence.

4. QUESTIONS FOR FURTHER ANALYSIS

4.1. Product Liability Directive

The Product Liability Directive has provided the EU liability framework for products since 1985. Since its adoption, it has accompanied many technological evolutions remaining a relevant and useful liability framework ensuring legal certainty for all parties involved. In particular, products today already include features relevant to emerging digital technologies, such as embedded software as a component of the product or

[49] CSO online, What is WannaCry ransomware, how does it infect, and who was responsible?, 27 September. Available at: http://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.

[50] The Guardian, DDoS attack that disrupted internet was largest of its kind in history, experts say, 26 October 2016. Available at: http://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[51] Studer, Evelyne and de Werra, Jacques, Regulating Cybersecurity - What Civil Liability in Case of Cyber-Attacks?, 19 August 2017. Expert Focus 8/2017, 511-517. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022522.

connectivity elements, and have so far been adequately covered by the Product Liability Directive.

The Commission has carried out an evaluation of the Product Liability Directive[52] with a specific focus on its continued effectiveness and relevance for emerging digital technologies. The evaluation process included a preliminary assessment of the continued relevance of the Product Liability's concepts, such as product, producer, defect, damage and the burden of proof. The evaluation results as well as the forthcoming Fifth Report on the application of the product Liability Directive highlight that the Directive continues - to some extent - to be adequate for the current state of technological developments.[53]

The Directive defines **products** as movable items. Even though most producers consulted during the evaluation claimed that they did not encounter problems in distinguishing products from services so far, a number of open questions were identified related to software be it embedded or non-embedded, that will have to be further explored.

Concerning the concept of **producer**, the question arises to what extent the producer maintains control over the features of a product in the context of emerging digital technologies and can therefore be held liable for them. While in many cases the final product and producer may be easy to identify, regardless of whether it includes software or other digital elements, or whether different manufacturers have been involved in the production process, other cases may be less straightforward.

The notions of **defectiveness and burden of proof** of the Directive are fairly wide and refer to the safety levels that a consumer is entitled to expect. The defectiveness must be assessed based on an objective analysis of the expectations of an average consumer rather than on subjective expectations or predisposition of one person. The defectiveness of a product is assessed on a case-by-case basis, considering all the relevant circumstances, on the basis of objective criteria, including especially product safety legislation, and all other circumstances, including the presentation of the product, the reasonably expected use and the time when the product was put into circulation. In the context of the emerging digital technologies, it may be difficult to identify whether the damage has been caused by the product itself or by other elements interconnected to it in a digital ecosystem. In this respect, it will be necessary to provide for adequate safety levels for all types of products, taking also account of any new risks that may be posed regarding the emerging digital technologies.

At present, **damages** are limited to either physical or material damages to property that is intended for private use. While this distinction between private and professional use has not appeared to cause major problems in practice, some stakeholders have raised questions as to the continued relevance of this distinction in this day and age. Furthermore, issues related to the infringement of privacy and cybersecurity were also raised.

[52] Forthcoming Commission Staff Working Document on Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[53] Forthcoming Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC).

Finally, the exemptions, notably the **development risk clause** and the **500€ threshold** were contested by some stakeholders and will require further analysis in light of emerging digital technologies.

Thus, while a strict liability regime for producers is uncontested at EU level, the precise effects of new technological developments will have to be more closely analysed, also in light of the provisions of the Product Liability Directive, based on a better practical experience than could be gathered until now.

4.2. Broader challenges posed by emerging digital technologies

A broader and more in-depth analysis of the issues considered in this document should establish whether it is necessary and, if so, how to re-assess concepts and elements of the EU/national liability framework(s) in light of emerging digital technologies. The analysis should also include the economic dimension, including the incentives to invest on the production/provisions of these products and services and to buy them from a consumer perspective.

A first question to assess is **whether concepts like the liability of a guardian** or similar concepts **are appropriate to technologies like AI**. While AI cannot of course be assimilated to humans or animals, the autonomy element is an intrinsic feature that is relevant and very prominent in both cases. Within the limits set by relevant safety frameworks, an AI powered robot can, and actually is supposed to, act autonomously and independently, i.e. without any supervision. The approach on liability for animals is linked to the concept of lack of predictability and therefore interesting to that extent in the context of autonomous behaviour. Safety legislation will have an important role to play in reducing this unpredictability to a socially accepted minimum.

A strict liability concept which is applicable to AI systems in general does not exist. The question whether liability should be fault-based or strict for such systems is a fundamental question to explore. A reflection should be conducted on the substantive conditions for any possible liability claim, in addition to the damage suffered by the victim, for instance whether it matters if the damage could have been avoided.

While fault-based liability is generally justified by the reasoning that a wrongdoer did not respect certain requirements, for instance the reasonable standard of care, the concept of strict liability typically builds on the principle that a person who generated a risk for his own benefit should be responsible for any damage materialised in connection to that risk. Current strict liability provisions could already apply to the use of certain AI powered devices, in particular, in the case of automated cars. Another question is **whether and to what extent it matters for determining liability whether the damage could have been avoided or not**. In the specific national liability schemes regarding the collapse or ruin of buildings, the exercise of dangerous activities and the liability of the employer, any person held liable by law could avoid liability by proving that he/she did everything possible to avoid the damage or that they used reasonable care considering similar circumstances. For instance, if the owner of a building shows that he used reasonable care in the maintenance of the building, and therefore the damage was not caused by poor maintenance, he can avoid liability. By analogy, this could mean that the owner of an advanced robot could avoid liability if, for instance, he had used and maintained the robot properly, respecting the instructions of the producers and updating the software when required. However, as explained above, these technologies might in such scenarios still perform autonomous behaviour and cause damage. The damage might occur even if the use and maintenance of the robot are impeccable. Considering the autonomy aspect, this would raise the question, what actions a person held liable could possibly put in

place in order to avoid the damage caused by the autonomous behaviour of emerging digital technologies.

Questions related to **cybersecurity** are also to be assessed. Security breaches, in particular through cybersecurity attacks, are certainly among the most serious risks posed by these technologies. In most cases, it is likely very difficult, if not impossible, for the victim to identify the attackers and bring a claim for damages against them, meaning that, absent holding someone else liable vis-à-vis the victim, this would likely remain without compensation. If one considers the possibility of holding the operator/owner of the device or the producer liable, such liability would be however of a very different nature. Although the risk inherent in the emerging digital technologies would have been materialised, the existence of an actual wrong-doer at the origin of the damage would have been known, but not his/her identity. If therefore such liability were to be created at all, one would have to consider -at least in such cases- to grant the operator or producer a defence if the operator/owner of the device had used all applicable standards of care and diligence for the use and maintenance/production of the device and yet the cyberattack was successful.

It is also important to assess the issue of the **burden of proof**. National regimes including fault-based liability schemes or different forms of strict liability regimes often include provisions, whereby the burden of proof for a possible fault, defect or other condition is not placed on the victim. Thus, the person held liable by law would need to prove to be discharged from liability, for instance, that the damage was caused as a result of force majeure or an act/behaviour of a third party. Whether the burden of proof should be on the claimant or reversed, what substantive conditions the claimant should demonstrate as well as the impact on the ability of the claimant to obtain compensation are important elements to assess.

The type of damage to be covered should also be assessed.[54] Which type of damage caused by these technologies should be compensated; death, bodily harm, harm to property or also consequential damages in form of purely economic damage? Non-material damage? Especially for the latter, one would also need to consider whether the damage of only natural or also of legal persons should be compensated. In this context, it would also need to be considered whether the liability for the use of AI powered devices should have a threshold and/or be capped, which amount(s) should be chosen and whether they should differ according to sectors. In the context of this set of questions, it would be helpful to consider the damages including non-material damages that could typically materialize in light of the risks connected with the use of AI powered systems taking into account that these technologies may create new types of risks or accentuate existing risks.

The question of **redress between actors in the value chain**[55] is an important question to be further discussed. While it is not necessarily relevant for the purpose of ensuring that the victim obtains compensation for the damages suffered - which may happen satisfactorily - the question of redress has to be considered from an overall policy standpoint, particularly in situations where a complex ecosystem of market operators

[54] The Product Liability Directive stipulates an obligation of producers to compensate natural persons for damages caused by defective products resulting from death, personal injury or damage to or destruction of an item of property. The Directive is without prejudice to national provisions relating to non-material damage.

[55] Actors in the value chain may include producers, service operators, software providers, traders, conformity assessment bodies and infrastructure providers.

enables the roll-out and functioning of the emerging digital technologies. The redress is indeed crucial for the roll-out emerging digital technologies as the value chain of these technologies present a degree of complexity that is higher than that of other value chains and it will answer the question of who ultimately bears the cost for possible damages. If, for instance, the owner or operator of an AI system is considered strictly liable, even if he has no possibility to control its behaviour or to prevent any associated risks with the adoption of precautionary measures, he should be able to obtain redress for the damages covered, to the extent that the wrongful or undesirable behaviour of the AI system may be attributable to someone else, e.g. the producer. However, this might prove challenging. Although the person held liable under national law does not have to prove the fault of the producer under the Product Liability Directive, this person would still have to prove the defect and the causal link between the defect and the damage.

Conceptually speaking, a strict liability approach to AI powered devices would acknowledge that damages resulting from the use of these devices cannot entirely be avoided. At the same time, it would ensure that potential victims are compensated by the liable person, regardless of any wrongdoing. In order to facilitate the victim's compensation and protecting the victim from the risk of insolvency of the liable person, it could be discussed, among other solutions, whether various actors in the value chain should be required to take out insurance coverage as it is the case today for cars. In case of an accident, the victim would be compensated by the insurance. On their end, although they may still face important difficulties due to the complexity of the technology, insurance companies could use their expertise and assets to assess whether a redress claim against the manufacturer of the AI powered device or any other person can be enforced.

5. NEXT STEPS

The Commission will analyse the above liability questions with the help of the Expert Group on liability, which will consist of two formations: the Product Liability Directive formation and the New Technologies formation.[56] At the same time, it is important to continue analysing what could or should be done to prevent possible damages through an appropriate safety framework.

In the context of the work of the Product Liability Directive formation, questions to be discussed relate, for example, to an update of the concepts of 'producer', 'product' and 'defect', the exemptions and other elements of the Directive, in order to reflect the technological and other developments in the single market and global value chains.

In the context of the analysis of the overall liability regimes and approaches that are or can be relevant to the goal of facilitating the uptake of emerging digital technologies by fostering investment stability and users' trust, the New Technologies formation will analyse other relevant issues, for instance those covered in Section 4.2.

The approaches put forward by the "Building a European Data Economy" Communication based on initial input from stakeholders should also be considered.

If a regulatory intervention on these technologies appears appropriate and necessary (in terms of new rules or an amendment to existing rules), it should be discussed whether that intervention should be developed **in a horizontal or sectorial way and whether new legislation should be enacted at EU level.**

[56] Call for experts for a group on liability and new technologies. Available at: https://ec.europa.eu/digital-single-market/en/news/call-experts-group-liability-and-new-technologies.

6. ANNEX I – SPECIFIC CHARACTERISTICS OF EMERGING DIGITAL TECHNOLOGIES

This annex describes the specific characteristics of the Internet of Things and Artificial Intelligence, which have been used to conduct the analysis in this document. These characteristics are shared to a certain degree by other emerging digital technologies like Blockchain, 3D Printing and cloud computing.

The Internet of Things (IoT)

The Internet of Things (IoT) is about setting up new ecosystems that cut across vertical areas, and create new markets for hardware (connected devices), software (IoT platforms and systems) and services (IoT applications). IoT has a horizontal and cross-cutting character. It should be understood as an ecosystem where areas that have been developed as vertical silos (manufacturing, transport, healthcare, devices, etc.) relate to each other, thanks to common platforms and cross-cutting innovation. IoT ecosystems are, therefore, based on bringing together multiple sectors and a variety of stakeholders to cover an increasingly complex value chain.

IoT is based on various disciplines and technologies like sensors, embedded systems, various communications technologies. It requires a specific configuration for object identification and search, open/closed data sharing, lightweight communication protocols, trade-off between local and networked based information processing, and back-end integration. It also requires specific considerations of data security (e.g. location-based profiling), liability (many service providers involved), seamless identification and authentication mechanisms (including those of persons/entities needed for managing contractual relations, attribution and liability) and trust. All this increases the complexity of the IoT ecosystem.

Connected sensors in private, business or city environments collect data from objects (e.g. a car, a phone, etc.) and these data are analysed either through embedded systems or through cloud-based and Internet systems enabling the creation of new services based on big data analytics.

The data provided by connected sensors and objects allow single and networked objects to take decisions based on the data and actuate or perform specific functions derived from sensing, analysis and intelligence gathered. This takes place normally within the boundaries of given applications but it is expected, with increasing computing power and sophistication, to gain high levels of autonomy in their behaviour and "life". Examples include factory automation, logistics and robotics.

But sensors and smart connected objects are not only designed and optimised to perform certain functions on the basis of vertical business models. They become part of a bigger connectivity network which creates new opportunities to combine more intelligence and actuation across vertical markets and to provide a whole new set of services. Technical and semantic interoperability are the key factor of success. It enables the programming of complex systems to integrate a number of device- and service-providers to deliver complete IoT solutions e.g. at home, in cities, between industries.

Therefore, IoT demonstrates the following specific characteristics:

- Complexity: Given the numerous interdependencies in the value chain and the variety of actors;
- Autonomous behaviour: Many of the operations provided through and by an IoT system can be fully autonomous;

- Data driven: It entails data generation, data gathering, data processing and data analysis;
- Openness due to its digital dimension encompassing tangible and intangible elements (software and data).

In light of these characteristics, it can be concluded that IoT encompasses all of the main specificities that revolve around these technologies: high levels of complexity and high interdependency, the element of autonomy, data generating and/or processing components, and an open dimension.

Artificial Intelligence (AI)

Artificial intelligence (AI) aims to study and develop intelligent machines and software. The associated ICT research includes the development of software that can reason, gather knowledge, plan intelligently, learn, communicate, perceive, and manipulate objects.

AI is used in a variety of ways and can be found across a large number of sectors, from assembly line robots to advanced toys, and from speech recognition systems to medical research. Its most common application is to find patterns in data, which is why it is commonly applied in online search engines and recommendation sites. Another common application is advanced robotics.

AI can allow users of big data to automate and enhance complex descriptive and predictive analytical tasks that would be extremely labour intensive and time consuming, if performed by humans. Unleashing AI on big data can have a significant impact on the role data plays in deciding how we work, how we travel and how we conduct business. More and more aspects of our lives can become predictable, from travel time to customer satisfaction to how long it will take an abled bodied worker to complete a given task.

Also, AI can provide this type of information ahead of time, allowing for improved planning, scheduling, and decision making, providing users with critical information at the right time to make the best opportunities when they present themselves. Moreover, tying the use of artificial intelligence on big data to responsively designed user applications allows for improved user experience that benefits from receiving the required information based on interaction context, without swiping, pinching, scrolling or clicking.

Therefore, we can see that AI combines certain specific characteristics such as:

- Complexity: with machine learning, AI can learn from other AI.
- Autonomous behaviour: Depending on the application, AI software can reason, gather knowledge, plan intelligently, learn, communicate, perceive, and manipulate objects.
- Data driven: AI entails data gathering, data processing and data analysis;
- Openness: AI combined with hardware can create new tangible products and/or deliver services.

7. ANNEX II – LIST OF EU LEGISLATION

1. Council Directive 70/157/EEC of 6 February 1970 on the approximation of the laws of the Member States relating to the permissible sound level and the exhaust system of motor vehicles (OJ L 042 , 23.02.1970, p. 16-20);

2. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29–33);

3. Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (OJ L 183, 29.06.1989, p. 1-8);

4. Council Directive 92/42/EEC of 21 May 1992 on efficiency requirements for new hot-water boilers fired with liquid or gaseous fuels (OJ L 167, 22.6.1992, p. 17–28);

5. Directive 2000/14/EC of the European Parliament and of the Council of 8 May 2000 on the approximation of the laws of the Member States relating to the noise emission in the environment by equipment for use outdoors (OJ L 162, 3.7.2000, p. 1–78);

6. Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 011, 15.01.2002, p. 4-17);

7. Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation) (OJ L 96, 31.3.2004, p. 26–42);

8. Directive 2004/52/EC of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community (OJ L 200, 7.6.2004, p. 50–57);

9. Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation) (OJ L 96, 31.3.2004, p. 26–42);

10. Directive 2005/64/EC of the European Parliament and of the Council of 26 October 2005 on the type-approval of motor vehicles with regard to their reusability, recyclability and recoverability and amending Council Directive 70/156/EEC (OJ L 310, 25.11.2005, p. 10–27);

11. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery (OJ L 157, 9.6.2006, p. 24–86);

12. Directive 2006/40/EC of the European Parliament and of the Council of 17 May 2006 relating to emissions from air conditioning systems in motor vehicles and amending Council Directive 70/156/EEC (OJ L 161, 14.6.2006, p. 12–18);

13. Directive 2006/66/EC of the European Parliament and of the Council of 6 September 2006 on batteries and accumulators and waste batteries and accumulators and repealing Directive 91/157/EEC (OJ L 266, 26.9.2006, p. 1–14);

14. Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information (OJ L 171, 29.6.2007, p. 1–16);

15. Directive 2007/46/EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (OJ L 263, 9.10.2007, p. 1–160);

16. Directive 2008/2/EC of the European Parliament and of the Council of 15 January 2008 on the field of vision and windscreen wipers for wheeled agricultural or forestry tractors (Codified version) (OJ L 24, 29.1.2008, p. 30–38);

17. Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005 (OJ L 141, 31.5.2008, p. 5–10);

18. Regulation (EC) No 78/2009 of the European Parliament and of the Council of 14 January 2009 on the type-approval of motor vehicles with regard to the protection of pedestrians and other vulnerable road users, amending Directive 2007/46/EC and repealing Directives 2003/102/EC and 2005/66/EC (OJ L 35, 4.2.2009, p. 1–31);

19. Regulation (EC) No 79/2009 of the European Parliament and of the Council of 14 January 2009 on type-approval of hydrogen-powered motor vehicles, and amending Directive 2007/46/EC (OJ L 35, 4.2.2009, p. 32–46);

20. Directive 2009/20/EC of the European Parliament and of the Council of 23 April 2009 on the insurance of ship-owners for maritime claims (OJ L 131, 28.5.2009, p. 128–131);

21. Directive 2009/34/EC of the European Parliament and of the Council of 23 April 2009 relating to common provisions for both measuring instruments and methods of metrological control (OJ L 106, 28.4.2009, p. 7–24);

22. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1–37);

23. Regulation (EC) No 392/2009 of the European Parliament and of the Council of 23 April 2009 on the liability of carriers of passengers by sea in the event of accidents (OJ L 131, 28.5.2009, p. 24–46);

24. Regulation (EC) No 595/2009 of the European Parliament and of the Council of 18 June 2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information and amending Regulation (EC) No 715/2007 and

Directive 2007/46/EC and repealing Directives 80/1269/EEC, 2005/55/EC and 2005/78/EC (OJ L 188, 18.7.2009, p. 1–13);

25. Regulation (EC) No 661/2009 of the European Parliament and of the Council of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor (OJ L 200, 31.7.2009, p. 1–24);

26. Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity (OJ L211, 14.08.2009, p.55-93), to be repealed by the outcome of negotiations of the Commission Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast / COM/2016/0864 final/2 - 2016/0380 (COD);

27. Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 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 (OJ L 263, 7.10.2009, p. 11–31);

28. Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of eco-design requirements for energy-related products (OJ L 285, 31.10.2009, p. 10–35);

29. Implementing acts to the Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of eco-design requirements for energy-related products (OJ L 285, 31.10.2009, p. 10–35);

30. Regulation (EC) No 1005/2009 of the European Parliament and of the Council of 16 September 2009 on substances that deplete the ozone layer (OJ L 286, 31.10.2009, p. 1–30);

31. Directive 2010/31/EU of the European Parliament and of the Council of 19 May 2010 on the energy performance of buildings (OJ L 153, 18.6.2010, p.13-35);

32. Directive 2010/35/EU of the European Parliament and of the Council of 16 June 2010 on transportable pressure equipment (OJ L 165, 30.6.2010, p. 1–18);

33. 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 (OJ L 207, 6.8.2010, p. 1–13);

34. 2012/23/EU: Council Decision of 12 December 2011 concerning the accession of the European Union to the Protocol of 2002 to the Athens Convention relating to the Carriage of Passengers and their Luggage by Sea, 1974, as regards Articles 10 and 11 thereof (OJ L 8, 12.1.2012, p. 13–16);

35. Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC (OJ L 315, 14.11.2012, p. 1–56);

36. Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1–51);

37. Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52–128);

38. Directive 2013/29/EU of the European Parliament and of the Council of 12 June 2013 on the harmonisation of the laws of the Member States relating to the making available on the market of pyrotechnic articles (OJ L 178, 28.6.2013, p. 27–65);

39. Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC (OJ L 354, 28.12.2013, p. 90–131);

40. Commission Delegated Regulation (EU) No 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an interoperable EU-wide eCall (OJ L 91, 3.4.2013, p. 1–4);

41. Directive 2014/28/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market and supervision of explosives for civil uses (OJ L 96, 29.3.2014, p. 1–44);

42. Directive 2014/29/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of simple pressure vessels (OJ L 96, 29.3.2014, p. 45–78);

43. Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (OJ L 96, 29.3.2014, p. 79–106);

44. Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments (OJ L 96, 29.3.2014, p. 107–148);

45. Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (OJ L 96, 29.3.2014, p. 149–250);

46. Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts (OJ L 96, 29.3.2014, p. 251–308);

47. Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to

equipment and protective systems intended for use in potentially explosive atmospheres (OJ L 96, 29.3.2014, p. 309–356);

48. Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits (OJ L 96, 29.3.2014, p. 357–374);

49. 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 (OJ L 153, 22.5.2014, p. 62–106);

50. Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment (OJ L 189, 27.6.2014, p. 164–259);

51. Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146–185);

52. Regulation (EU) No 517/2014 of the European Parliament and of the Council of 16 April 2014 on fluorinated greenhouse gases and repealing Regulation (EC) No 842/2006 (OJ L 150, 20.5.2014, p. 195–230);

53. Regulation (EU) No 540/2014 of the European Parliament and of the Council of 16 April 2014 on the sound level of motor vehicles and of replacement silencing systems, and amending Directive 2007/46/EC and repealing Directive 70/157/EEC (OJ L 158, 27.5.2014, p. 131–195);

54. Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC (OJ L 81, 31.3.2016, p. 1–50);

55. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (OJ L 81, 31.3.2016, p. 51–98);

56. Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC (OJ L 81, 31.3.2016, p. 99–147);

57. Directive (EU) 2016/798 of the European Parliament and the Council of 11 May 2016 on railway safety (OJ L 138, 26.5.2016, p. 102–149);

58. Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44–101);

59. Council Directive of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (90/385/EEC) (OJ L 189, 20.7.1990, p.17);

60. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p.1);

61. Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices (OJ L 331, 7.12.1998, p. 1);

62. Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU (OJ L 198, 28.7.2017, p. 1–23);

63. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88);

64. Delegated acts to the Regulation (EU) 2017/1369 of the European Parliament and of the Council of 4 July 2017 setting a framework for energy labelling and repealing Directive 2010/30/EU (OJ L 198, 28.7.2017, p. 1–23).