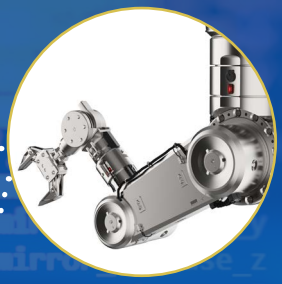
European Commission

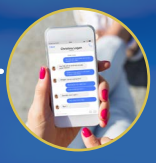
Liability for Artificial Intelligence

and other emerging digital technologies







Report from the Expert Group on Liability and New Technologies – New Technologies Formation

Justice and Consumers

This document was written by the Expert Group on Liability and New Technologies – New Technologies Formation.
It reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. The Expert Group on Liability and New Technologies is an independent expert group which was set up by the European Commission.
Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of the following information.

Cover photograph: Gettyimages - vchal/metamorworks/zhudifeng;/scanrail/PhonlamaiPhoto/grinvalds/PhonlamaiPhoto/South_agency

Print ISBN 978-92-76-12958-5 doi:10.2838/25362 Catalogue number: DS-03-19-853-EN-C
PDF ISBN 978-92-76-12959-2 doi:10.2838/573689 Catalogue number: DS-03-19-853-EN-N

Expert Group on Liability and New Technologies
New Technologies Formation

LIABILITY FOR ARTIFICIAL INTELLIGENCE AND OTHER EMERGING DIGITAL TECHNOLOGIES

Table of Contents

Executive summary

Artificial intelligence and other emerging digital technologies, such as the Internet of Things or distributed ledger technologies, have the potential to transform our societies and economies for the better. However, their rollout must come with sufficient safeguards, to minimise the risk of harm these technologies may cause, such as bodily injury or other harm. In the EU, product safety regulations ensure this is the case. However, such regulations cannot completely exclude the possibility of damage resulting from the operation of these technologies. If this happens, victims will seek compensation. They typically do so on the basis of liability regimes under private law, in particular tort law, possibly in combination with insurance. Only the strict liability of producers for defective products, which constitutes a small part of this kind of liability regimes, is harmonised at EU level by the Product Liability Directive, while all other regimes – apart from some exceptions in specific sectors or under special legislation – are regulated by the Member States themselves.

In its assessment of existing liability regimes in the wake of emerging digital technologies, the New Technologies Formation of the Expert Group has concluded that the liability regimes in force in the Member States ensure at least basic protection of victims whose damage is caused by the operation of such new technologies. However, the specific characteristics of these technologies and their applications – including complexity, modification through updates or self-learning during operation, limited predictability, and vulnerability to cybersecurity threats – may make it more difficult to offer these victims a claim for compensation in all cases where this seems justified. It may also be the case that the allocation of liability is unfair or inefficient. To rectify this, certain adjustments need to be made to EU and national liability regimes.

Below are listed the most important findings of this report on how liability regimes should be designed – and, where necessary, changed – in order to rise to the challenges emerging digital technologies bring with them.

- A person operating a permissible technology that nevertheless carries an increased risk of harm to others, for example AI-driven robots in public spaces, should be subject to strict liability for damage resulting from its operation.
- In situations where a service provider ensuring the necessary technical framework has a higher degree of control than the owner or user of an actual product or service equipped with AI, this should be taken into account in determining who primarily operates the technology.
- A person using a technology that does not pose an increased risk of harm to others should still be required to abide by duties to properly select, operate, monitor and maintain the technology in use and – failing that – should be liable for breach of such duties if at fault.
- A person using a technology which has a certain degree of autonomy should not be less accountable for ensuing harm than if said harm had been caused by a human auxiliary.
- Manufacturers of products or digital content incorporating emerging digital technology should be liable for damage caused by defects in their products, even if the defect was caused

by changes made to the product under the producer's control after it had been placed on the market.

- For situations exposing third parties to an increased risk of harm, compulsory liability insurance could give victims better access to compensation and protect potential tortfeasors against the risk of liability.
- Where a particular technology increases the difficulties of proving the existence of an element of liability beyond what can be reasonably expected, victims should be entitled to facilitation of proof.
- Emerging digital technologies should come with logging features, where appropriate in the circumstances, and failure to log, or to provide reasonable access to logged data, should result in a reversal of the burden of proof in order not be to the detriment of the victim.
- The destruction of the victim's data should be regarded as damage, compensable under specific conditions.
- It is not necessary to give devices or autonomous systems a legal personality, as the harm these may cause can and should be attributable to existing persons or bodies.

Key Findings

[1] Digitalisation brings fundamental changes to our environments, some of which have an impact on liability law. This affects, in particular, the

(a) complexity,

(b) opacity,

(c) openness,

(d) autonomy,

(e) predictability,

(f) data-drivenness, and

(g) vulnerability

of emerging digital technologies.

[2] Each of these changes may be gradual in nature, but the dimension of gradual change, the range and frequency of situations affected, and the combined effect, results in disruption.

[3] While existing rules on liability offer solutions with regard to the risks created by emerging digital technologies, the outcomes may not always seem appropriate, given the failure to achieve:

(a) a fair and efficient allocation of loss, in particular because it could not be attributed to those:

- whose objectionable behaviour caused the damage; or
- who benefitted from the activity that caused the damage; or
- who were in control of the risk that materialised; or
- who were cheapest cost avoiders or cheapest takers of insurance.

(b) a coherent and appropriate response of the legal system to threats to the interests of individuals, in particular because victims of harm caused by the operation of emerging digital technologies receive less or no compensation compared to victims in a functionally equivalent situation involving human conduct and conventional technology;

(c) effective access to justice, in particular because litigation for victims becomes unduly burdensome or expensive.

[4] It is therefore necessary to consider adaptations and amendments to existing liability regimes, bearing in mind that, given the diversity of emerging digital technologies and the correspondingly diverse range of risks these may pose, it is impossible to come up with a single solution suitable for the entire spectrum of risks.

[5] Comparable risks should be addressed by similar liability regimes, existing differences among these should ideally be eliminated. This should also determine which losses are

recoverable to what extent.

[6] Fault liability (whether or not fault is presumed), as well as strict liability for risks and for defective products, should continue to coexist. To the extent these overlap, thereby offering the victim more than one basis to seek compensation against more than one person, the rules on multiple tortfeasors ([31]) govern.

[7] In some digital ecosystems, contractual liability or other compensation regimes will apply alongside or instead of tortious liability. This must be taken into account when determining to what extent the latter needs to be amended.

[8] For the purposes of liability, it is not necessary to give autonomous systems a legal personality

[9] Strict liability is an appropriate response to the risks posed by emerging digital technologies, if, for example, they are operated in non-private environments and may typically cause significant harm.

[10] Strict liability should lie with the person who is in control of the risk connected with the operation of emerging digital technologies and who benefits from their operation (operator).

[11] If there are two or more operators, in particular

(a) the person primarily deciding on and benefitting from the use of the relevant technology (frontend operator) and

(b) the person continuously defining the features of the relevant technology and providing essential and ongoing backend support (backend operator),

strict liability should lie with the one who has more control over the risks of the operation.

[12] Existing defences and statutory exceptions from strict liability may have to be reconsidered in the light of emerging digital technologies, in particular if these defences and exceptions are tailored primarily to traditional notions of control by humans.

[13] Strict liability of the producer should play a key role in indemnifying damage caused by defective products and their components, irrespective of whether they take a tangible or a digital form.

[14] The producer should be strictly liable for defects in emerging digital technologies even if said defects appear after the product was put into circulation, as long as the producer was still in control of updates to, or upgrades on, the technology. A development risk defence should not apply.

[15] If it is proven that an emerging digital technology has caused harm, the burden of proving defect should be reversed if there are disproportionate difficulties or costs pertaining to establishing the relevant level of safety or proving that this level of safety has not been met. This is without prejudice to the reversal of the burden of proof referred to in [22] and [24].

[16] Operators of emerging digital technologies should have to comply with an adapted range of duties of care, including with regard to

(a) choosing the right system for the right task and skills;

(b) monitoring the system; and

(c) maintaining the system.

[17] Producers, whether or not they incidentally also act as operators within the meaning of [10], should have to:

(a) design, describe and market products in a way effectively enabling operators to comply with the duties under [16]; and

(b) adequately monitor the product after putting it into circulation.

[18] If harm is caused by autonomous technology used in a way functionally equivalent to the employment of human auxiliaries, the operator's liability for making use of the technology should correspond to the otherwise existing vicarious liability regime of a principal for such auxiliaries.

[19] The benchmark for assessing performance by autonomous technology in the context of vicarious liability is primarily the one accepted for human auxiliaries. However, once autonomous technology outperforms human auxiliaries, this will be determined by the performance of comparable available technology which the operator could be expected to use, taking into account the operator's duties of care ([16]).

[20] There should be a duty on producers to equip technology with means of recording information about the operation of the technology (logging by design), if such information is typically essential for establishing whether a risk of the technology materialised, and if logging is appropriate and proportionate, taking into account, in particular, the technical feasibility and the costs of logging, the availability of alternative means of gathering such information, the type and magnitude of the risks posed by the technology, and any adverse implications logging may have on the rights of others.

[21] Logging must be done in accordance with otherwise applicable law, in particular data protection law and the rules concerning the protection of trade secrets.

[22] The absence of logged information or failure to give the victim reasonable access to the information should trigger a rebuttable presumption that the condition of liability to be proven by the missing information is fulfilled.

[23] If and to the extent that, as a result of the presumption under [22], the operator were obliged to compensate the damage, the operator should have a recourse claim against the producer who failed to equip the technology with logging facilities.

[24] Where the damage is of a kind that safety rules were meant to avoid, failure to comply with such safety rules, including rules on cybersecurity, should lead to a reversal of the burden of proving

(a) causation, and/or

(b) fault, and/or

(c) the existence of a defect.

[25] As a general rule, the victim should continue to be required to prove what caused her harm.

[26] Without prejudice to the reversal of the burden of proof proposed in [22] and [24](a), the burden of proving causation may be alleviated in light of the challenges of emerging digital technologies if a balancing of the following factors warrants doing so:

(a) the likelihood that the technology at least contributed to the harm;

(b) the likelihood that the harm was caused either by the technology or by some other cause within the same sphere;

(c) the risk of a known defect within the technology, even though its actual causal impact is not self-evident;

(d) the degree of ex-post traceability and intelligibility of processes within the technology that may have contributed to the cause (informational asymmetry);

(e) the degree of ex-post accessibility and comprehensibility of data collected and generated by the technology

(f) the kind and degree of harm potentially and actually caused.

[27] If it is proven that an emerging digital technology caused harm, and liability therefor is conditional upon a person's intent or negligence, the burden of proving fault should be reversed if disproportionate difficulties and costs of establishing the relevant standard of care and of proving their violation justify it. This is without prejudice to the reversal of the burden of proof proposed in [22] and [24](b).

[28] If a cause of harm is attributable to the victim, the reasons for holding another person liable should apply correspondingly when determining if and to what extent the victim's claim for compensation may be reduced.

[29] Where two or more persons cooperate on a contractual or similar basis in the provision of different elements of a commercial and technological unit, and where the victim can demonstrate that at least one element has caused the damage in a way triggering liability but not which element, all potential tortfeasors should be jointly and severally liable vis-à-vis the victim.

[30] In determining what counts as a commercial and technological unit within the meaning of [29] regard is to be had to

(a) any joint or coordinated marketing of the different elements;

(b) the degree of their technical interdependency and interoperation; and

(c) the degree of specificity or exclusivity of their combination.

[31] Where more than one person is liable for the same damage, liability to the victim is usually solidary (joint). Redress claims between tortfeasors should only be for identified shares (several), unless some of them form a commercial and/ or technological unit ([29]-[30]), in which case the members of this unit should be jointly and severally liable for their cumulative share also to the tortfeasor seeking redress.

[32] Damage caused to data may lead to liability where

(a) liability arises from contract; or

(b) liability arises from interference with a property right in the medium on which the data was stored or with another interest protected as a property right under the applicable law; or

(c) the damage was caused by conduct infringing criminal law or other legally binding rules whose purpose is to avoid such damage; or

(d) there was an intention to cause harm.

[33] The more frequent or severe potential harm resulting from emerging digital technology, and the less likely the operator is able to indemnify victims individually, the more suitable mandatory liability insurance for such risks may be.

[34] Compensation funds may be used to protect tort victims who are entitled to compensation according to the applicable liability rules, but whose claims cannot be satisfied.

A. Introduction

I. Context

Artificial intelligence (AI) and other emerging digital technologies,[1] such as the Internet of Things and of Services (IoT/IoS), or distributed ledger technologies (DLT), have extraordinary potential to transform products, services and activities, procedures and practices, in a multitude of economic sectors and in relation to many aspects of society. Although some of these technologies[2] are not new, their increasing application to a growing variety of purposes, and new combinations of a range of different emerging digital technologies, opens up unprecedented possibilities. All this comes with the promise of making the world a safer, fairer, more productive, more convenient place, of helping to fight illness, poverty, crime, discrimination and other forms of injustice, and of connecting people worldwide. Although many of these promises are expected to come true, new or enhanced potential brings new risks with it, or increases existing ones.[3]

Throughout history, legal rules, concepts and principles have risen to the challenges posed by scientific, technical and, more recently, technological progress. In the last few decades, the adaptable principles of technological neutrality and functional equivalence have catered for the impact of digital technologies. These principles have served as the basis for the international response to the advent and first stages of development of the digital economy, and have largely guided the legislative and regulatory initiatives on electronic commerce (and information society services) adopted to date.

The adequacy and completeness of liability regimes in the face of technological challenges are crucially important for society. If the system is inadequate or flawed or has shortcomings in dealing with damages caused by emerging digital technologies, victims may end up totally or partially uncompensated, even though an overall equitable analysis may make the case for indemnifying them. The social impact of a potential inadequacy in existing legal regimes, in addressing new risks created by emerging digital technologies, might compromise the expected benefits. Certain factors, such as the ever-increasing presence of emerging digital technologies in all aspects of social life, and the multiplying effect of automation, can also exacerbate the

---

1 The term ‘emerging digital technologies’ is used with the same meaning as in the Commission Staff Working Document ‘Liability for emerging digital technologies’ (SWD(2018) 137 final).

2 Strictly speaking, it is not so much the technology itself, but a particular product or service making use of the technology, that poses a risk. However, for brevity and simplicity, this report will use the term ‘technology’.

3 This is also acknowledged by key players in this area of technology; for example Microsoft in its 2018 US Securities and Exchange Commission filing stated that
‘As with many disruptive innovations, AI presents risks and challenges that could affect its adoption, and therefore our business. AI algorithms may be flawed. Datasets may be insufficient or contain biased information. Inappropriate or controversial data practices by Microsoft or others could impair the acceptance of AI solutions. These deficiencies could undermine the decisions, predictions, or analysis AI applications produce, subjecting us to competitive harm, legal liability, and brand or reputational harm. Some AI scenarios present ethical issues. If we enable or offer AI solutions that are controversial because of their impact on human rights, privacy, employment, or other social issues, we may experience brand or reputational harm.’
<https://www.sec.gov/Archives/edgar/data/789019/000156459018019062/msft-10k_20180630.htm>.

damage these technologies cause. Damages can easily become viral and rapidly propagate in a densely interconnected society.

II. Background

On 16 February 2017 the European Parliament adopted a Resolution on Civil Law Rules on Robotics with recommendations to the Commission.[4] It proposed a whole range of legislative and non-legislative initiatives in the field of robotics and AI. In particular, it asked the Commission to submit a proposal for a legislative instrument providing civil law rules on the liability of robots and AI. In February 2018, the European Parliamentary Research Service (EPRS) published a study on 'A common EU approach to liability rules and insurance for connected and autonomous vehicles'[5] as a European added value assessment accompanying the Resolution on Civil Law Rules.

The 2018 Commission Work Programme announced that the Commission would be seeking to make the most of AI, since it will increasingly play a role in our economies and societies.[6] On 14 December 2017, in a Joint Declaration,[7] the Presidents of the Commission, Parliament and Council agreed to ensure 'a high level of data protection, digital rights and ethical standards while capturing the benefits and avoiding the risks of developments in artificial intelligence and robotics'. On 25 April 2018, the Commission published a Staff Working Document on 'Liability for emerging digital technologies'[8] accompanying a Communication from the Commission to the other institutions on the same day, on 'Artificial Intelligence for Europe'.[9] This Communication and the Sibiu Communication of May 2019[10] stress that 'a robust regulatory framework should proactively address the ethical and legal questions surrounding AI'. In its 2018 AI Communication the Commission also announced the adoption of a report assessing the implications of emerging digital technologies on existing safety and liability frameworks by mid-2019. In its 2019 Work Programme, it confirmed it would 'continue work on the emerging challenge of Artificial Intelligence by enabling coordinated action across the European Union'.[11]

In March 2018, the Commission set up an Expert Group on Liability and New Technologies,[12] operating in two different formations: the Product Liability Directive formation and the New Technologies formation.

---

4 P8_TA(2017)0051.

5 <http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)615635>.

6 <https://ec.europa.eu/info/sites/info/files/cwp_2018_en.pdf>.

7 <https:// ec.europa.eu/ commission/ sites/ beta-political/ files/ joint-declaration-eu-legislative-priorities-2018-19_en.pdf>.

8 SWD(2018) 137 final.

9 COM(2018) 237 final.

10 <https://ec.europa.eu/commission/sites/beta-political/files/comm_sibiu_06-05_en.pdf>.

11 <https://ec.europa.eu/info/sites/info/files/cwp_2019_en.pdf>.

12 <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592>.

In the call for applications,[13] the New Technologies formation (NTF) was asked to assess 'whether and to what extent existing liability schemes are adapted to the emerging market realities following the development of the new technologies such as Artifical Intelligence, advanced robotics, the IoT and cybersecurity issues'. The experts were asked to examine whether the current liability regimes are still 'adequate to facilitate the uptake of … new technologies by fostering investment stability and users' trust'. If there are shortcomings, the NTF should make recommendations for amendments, without being limited to existing national and EU legal instruments. However, recommendations should be limited to matters of extracontractual liability, leaving aside in particular corresponding (and complementary) rules on safety and other technical standards.[14]

The NTF[15] first convened in June 2018 and held nine further meetings up to May 2019. After analysing the relevant national laws and looking at specific use cases,[16] it compares various aspects of existing liability regimes. This report presents the NTF's findings.

13 <http://ec.europa.eu/transparency/regexpert/index.cfm?do=news.open_doc&id=12065>.

14 See the overview in the Commission Staff Working Document (fn 8), 4 ff.

15 See the list of members in the Annex.

16 The following use cases were examined, with the further participation of technical experts in the field in question: autonomous cars, smart home, blockchain and other distributed ledger technologies, autonomous healthcare applications, algorithmic decision making in the financial and other sectors, drones.

B. Liability for emerging digital technologies under existing laws in Europe

I. Overview of existing liability regimes

The law of tort of EU Member States is largely non-harmonised, with the exception of product liability law under Directive 85/374/EC,[17] some aspects of liability for infringing data protection law (Article 82 of the General Data Protection Regulation (GDPR)[18]), and liability for infringing competition law (Directive 2014/104/EU[19]). There is also a well-established regime governing liability insurance with regard to damage caused by the use of motor vehicles (Directive 2009/103/EC[20]), although without touching upon liability for accidents itself. EU law also provides for a conflict of tort laws framework, in the form of the Rome II Regulation.[21]

On a national level, it can generally be observed that the laws of the Member States do not (yet) contain liability rules specifically applicable to damage resulting from the use of emerging digital technologies such as AI. By way of exception, those jurisdictions that already allow the experimental or regular use of highly or fully automated vehicles usually also provide for coverage of any damage caused, be it only by way of insurance[22] or by reference to the general rules.[23]

---

17 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), as amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999, OJ L 141 20 4.6.1999. See also infra B.III.6.

18 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.

19 Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, OJ L 349, 5.12.2014, p. 1.

20 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. The Directive is currently under review, see Proposal COM(2018) 336 final.

21 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199, 31.7.2007, p. 40.

22 For example, Article 19 of the Italian Decree of 28 February 2018 on the testing of connected and automated vehicles on public roads (Modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di Smart Road e di guida connessa e automatica, 18A02619, GU n° 90 of 18 April 2018) provides that the person seeking approval for testing automated vehicles on public roads must give proof of sufficient liability insurance cover. Spain's Directorate-General for Traffic (*Dirección General de Tráfico*) circular of 13 November 2015 (Instrucción 15/V-113) also authorises the testing of automated cars and requires liability insurance to cover compulsory insurance limits for motor vehicles.

23 For example, § 7 of the German Road Traffic Act (*Straßenverkehrsgesetz*) provides for strict liability of the keeper of the vehicle. This rule was deliberately left unchanged when the Road Traffic Act was adapted to the emergence of automated vehicles. Similarly, French Decree n° 2018-211 of 28 March 2018 on experimentation with automated vehicles on public roads relies on the *Loi Badinter* of 5 July 1985 (n°85-677). The most conspicuous example is the recent UK Automated and Electric Vehicles Act 2018 (c 18), Section 2 of

Apart from this legislation, the harmful effects of the operation of emerging digital technologies can be compensated under existing ('traditional') laws on damages in contract and in tort in each Member State. This applies to all fields of application of AI and other emerging digital technologies the NTF of the Expert Group have analysed.

In general, these domestic tort laws include a rule (or rules) introducing fault-based liability with a relatively broad scope of application, accompanied by several more specific rules which either modify the premises of fault-based liability (especially the distribution of the burden of proving fault) or establish liability that is independent of fault (usually called strict liability or risk-based liability), which also takes many forms that vary with regard to the scope of the rule, the conditions of liability and the burden of proof.[24] Most liability regimes contain the notion of liability for others (often called vicarious liability).[25]

However, these regimes may not always lead to satisfactory and adequate results.[26] Furthermore, given the significant differences between the tort laws of all Member States, the outcome of cases will often be different depending on which jurisdiction applies. As experience with the Product Liability Directive has shown, efforts to overcome such differences by harmonising only certain aspects of liability law may not always lead to the desired degree of uniformity of outcomes.

II. Some examples of the application of existing liability regimes to emerging digital technologies

In most jurisdictions, damage caused by motor vehicles is subject to a special liability regime. As mentioned above, there is an EU-wide insurance scheme in place, in the form of the (recodified) Motor Insurance Directive (MID),[27] but the MID only harmonises liability insurance cover, not civil liability itself. Member States therefore continue to regulate tortious liability for accidents involving motor vehicles themselves, limited in their discretion only by the principle of effectiveness of the MID.[28] These rules usually impose liability on the owner/keeper of a vehicle and/or on the driver, although there are systems which introduce direct claims against the insurer regardless of any other person's liability. The appropriateness of existing traffic liability regimes for autonomous vehicles (AV) may be disputed, especially with regard to systems which rely on fault-based liability in general (Malta for example) or in limited circumstances, such as in the case of a collision (Poland for example), or for certain types of damage (Spain for example[29]), or which make the application of the traffic liability regime

which provides that 'the insurer is liable' for damage incurred by the insured or any other person in an accident caused by an automated vehicle. If the vehicle is uninsured, it is the owner of the vehicle who is liable instead.

24 See also infra B.III.5.

25 See also infra B.III.4.

26 See infra B.III.

27 Supra fn 20.

28 CJEU *Delgado Mendes*, C-503/16, EU:C:2017:681, paragraph 48; CJEU *Marques Almeida*, C-300/10, EU:C:2012:656, paragraphs 31, 32, and the case-law cited.

29 Under Spanish law, liability for damage to property caused by motor vehicles remains subject to a fault-based regime.

conditional on the involvement of a driver (Italy). Liability gaps may emerge in the case of a single-vehicle accident in as much as, under existing traffic liability rules, the injured owner/keeper is excluded from compensation. Some legal systems even exclude passengers from protection under strict traffic liability, either in general (Greece[30] or the Netherlands for example[31]) or only in specific circumstances (Poland[32] or Austria for example[33]). This would be hard to accept for accidents involving AVs. Given the complex character of the autonomous driving environment, exclusion of strict liability in the case of a third-party intervention may also prove problematic, particularly in the context of cybersecurity risks, such as where a connected AV has been hacked, or where an accident has been caused because the ICT infrastructure sent the wrong signals. Where damage was caused by a defective vehicle, product liability or producer's liability in tort may apply, but usually become relevant only at the redress stage.[34]

For most technological ecosystems (by which we mean systems with interacting devices or programs), however, no specific liability regimes exist. This means that product liability, general tort law rules (fault-based liability, tort of negligence, breach of statutory duty), and possibly contractual liability, occupy centre stage. The more complex these ecosystems become with emerging digital technologies, the more increasingly difficult it becomes to apply liability frameworks.

An example would be the use case of smart home systems and networks. Where smart home devices were already defective at the point at which they were put into circulation, product liability law applies. In most jurisdictions the producer may also be liable under general tort law, which could go beyond product liability by making the producer liable for, for example, defective ancillary digital services, and for updates as well as for failures in product surveillance or monitoring. In the case of damage caused by the seller of a product, an installing/configuring service provider, internet service provider, energy supplier, cloud operator and others involved in the smart home scenario, both general tort law, and possibly contractual liability, may come into play. Some countries (such as Spain or Greece) can use their special regimes of liability for flawed services, based on a presumed fault on the service provider's part. Other legal systems operate solely or mainly on the basis of their general provisions on fault liability (general clauses) or relatively open tort law concepts (tort of negligence, breach of statutory duty). These

30 Article 12 of Law 3950/1911 on Liability for Automobiles.

31 Article 185, paragraph 1 of the Road Traffic Act (*Wegenverkeerswet* 1994) in the Netherlands. The problem there has recently been solved in a pragmatic way as, per 1 April 2017, the Dutch Association of Insurers declared that motor third-party liability (MTPL) insurers shall compensate passengers of the insured motor vehicle regardless of liability (<https://www.verzekeraars.nl/publicaties/actueel/inzittende-kan-schade-voortaan-direct-regelen>).

32 According to Article 436 § 2 of the Polish Civil Code, strict liability does not apply to passengers transported without any remuneration or other benefit ('out of politeness').

33 According to § 3 of the Austrian Railway and Motor Vehicle Liability Act (EKHG), people transported by the vehicle without the keeper's consent are not covered.

34 Typically, at least in systems with strict liability for motor vehicles, the fact that these were defective does not preclude liability of the vehicles' keeper. It will therefore often be the motor vehicle liability insurer who will pursue the product liability claim.

provisions or legal concepts usually require proof of the defendant's failure to observe the required standard of care.[35]

When the user in the smart home scenario is contractually tied to the actor (seller, installing service providers, internet service provider, energy supplier, cloud operator), the latter may be liable in contract to the user for damage caused by non-performance. Some legal systems (Germany, Austria, or Greece, and to some extent Denmark, for example) extend contractual liability under certain conditions, allowing a third party to invoke a contract they were not a party to themselves. This applies to situations where the contract is deemed to establish duties to also protect such third parties, allowing the latter to sue for compensation in cases of breach.[36] The protected third party must be foreseeably close to the contracting partner, though, confronted in a similar way with the danger stemming from non-performance (such as family members or guests). Any kind of contractual liability is, however, usually subject to contractual (and sometimes also statutory) limitations.

Similarly, complex situations may result in cases where damage was caused by autonomous healthcare applications. Such damage would usually be subject to fault-based liability, either in contract or in tort. Many jurisdictions allow the victim to bring concurrent claims based on contract and on tort alternatively. In some jurisdictions however, this is not possible, in which case it becomes necessary to choose the one or the other. When damage is triggered by a defect present before putting these applications into circulation, product liability may apply, if the application or the device is considered a product for the purpose of product liability law. Further complexities arise from the interplay between these regimes and social insurance and/or healthcare systems.

Damage in connection with the use of algorithms or AI in the financial market is currently subject to reparation under traditional fault-based regimes. Some jurisdictions, however, allow the claimant to invoke administrative law (financial regulations) to establish the benchmark against which the perpetrator's conduct is to be assessed. On the contractual level, information asymmetry resulting from the use of AI may justify the application of a (statutory or case law) pre-contractual liability regime (culpa in contrahendo and similar concepts). It seems more likely, however, that the reaction of the legal system to potential irregularities in contracting with the use of algorithms will rely on contract law tools for assessing and challenging the validity of contracts (vitiated consent, lack of fairness, etc.).[37]

The use of blockchain, in particular cryptocurrencies, is not subject to any particular liability rules, and new legislation already enacted or under discussion in some Member States, related among other things to initial coin offerings, certifications of platforms and cybersecurity, does not extend to compensation for damage. In as much as this legislation provides for the duties

---

35 The standard of care referred to in this document is the model of careful and prudent conduct required from the perpetrator of the damage. It should not be confused with standards of safety or quality of products or services established by law or by certain bodies.

36 This is typically used as a workaround for deficiencies of the tort law regime, whereas other legal systems come to similar solutions via their (at least in some respects such as vicarious liability) more generous law of torts.

37 Cf, e.g., Spanish case law related to swap agreements according to which the infringement of financial regulations and of the duty to inform in the precontractual stage were treated as grounds for vitiated consent.

and responsibilities of the participants in a blockchain or of public authorities, it may be relevant for establishing the standard of care for the purpose of applying fault-based liability rules.

III. Specific challenges to existing tort law regimes posed by emerging digital technologies

It is possible to apply existing liability regimes to emerging digital technologies, but in light of a number of challenges and due to the limitations of existing regimes, doing so may leave victims under- or entirely uncompensated. The adequacy of existing liability rules may therefore be questionable, considering in particular that these rules were formulated decades or even centuries ago, based on even older concepts and incorporating a primarily anthropocentric and monocausal model of inflicting harm.

1. Damage

The main purpose of tort law is to indemnify victims for losses they should not have to bear themselves entirely on the basis of an assessment of all the interests involved. However, only compensable harm will be indemnified, meaning damage to a limited range of interests that a legal system deems worthy of protection.[38]

While there is unanimous accord that injuries to a person or to physical property can trigger tortious liability,[39] this is not universally accepted for pure economic loss.[40] Damage caused by self-learning algorithms on financial markets, for example, will therefore often remain uncompensated, because some legal systems do not provide tort law protection of such interests at all or only if additional requirements are fulfilled, such as a contractual relationship between the parties or the violation of some specific rule of conduct. Nor is it universally accepted throughout Europe that damage to or the destruction of data is a property loss, since in some legal systems the notion of property is limited to corporeal objects and excludes intangibles.[41] Other differences exist when it comes to the recognition of personality rights, which may also be adversely affected by emerging digital technologies, if certain data is released which infringes on the right to privacy for example.[42]

However, generally speaking, AI and other emerging digital technologies do not call into question the existing range of compensable harm per se. Rather, some of the already recognised

---

38 See Article VI-2:101 Draft Common Frame of Reference (DCFR), in particular paragraph 1 lit c; Article 2:101 Principles of European Tort Law (PETL). This range is defined differently at present, with some systems (such as the Romanic systems) being more generous than others, and some of those others setting out only a limited list of protected interests by statute.

39 See Article 2:102 paragraphs 2 and 3 PETL.

40 See Article 2:102 paragraph 4 PETL: 'Protection of pure economic interests … may be more limited in scope.' See for example W van Boom/H Koziol/Ch Witting (eds), *Pure Economic Loss* (2004); and M Bussani/V Palmer, 'The liability regimes of Europe – their façades and interiors', in M Bussani/V Palmer (eds), *Pure Economic Loss in Europe* (2003) p. 120 ff.

41 Compare § 90 German BGB (according to which a 'thing' by definition must be corporeal) with § 285 Austrian ABGB (which does not provide for such a limitation, so that 'things' in Austria may also be intangible).

42 But see Article 82 of the GDPR for a harmonised claim for compensation in cases of data breach.

categories of losses may be more relevant in future cases than in traditional tort scenarios. Damage as a prerequisite for liability is also a flexible concept – the interest at stake may be more or less significant, and the extent of damage to such an interest may also vary. This may in turn have an impact on the overall assessment of whether or not a tort claim seems justified in an individual case.[43]

2. Causation

One of the most essential requirements for establishing liability is a causal link between the victim's harm and the defendant's sphere. As a rule, it is the victim who must prove that their damage originated from some conduct or risk attributable to the defendant. The victim needs to then produce evidence in support of this argument. However, the less evident the sequence of events was that led to the victim's loss, the more complex the interplay of various factors that either jointly or separately contributed to the damage, the more crucial links in the chain of events are within the defendant's control, the more difficult it will be for the victim to succeed in establishing causation without alleviating their burden of proof. If the victim fails to persuade the court, to the required standard of proof,[44] that something for which the defendant has to account for triggered the harm they suffered, they will lose their case, regardless of how strong it would have been against the defendant otherwise (for example, because of evident negligence on the defendant's part).

Hard as it is to prove that some hardware defect was the reason someone was injured, for example, it becomes very difficult to establish that the cause of harm was some flawed algorithm.

> ***Illustration 1.*** *If a smoke detector in a smart home environment fails to trigger an alarm because of flawed wiring, this defect may be identifiable (and in this case is even visible). If, on the other hand, the smoke detector did not go off because of some firmware error, this may not be proven as easily (even though the absence of an alarm per se may be easily proven), if only because it requires a careful analysis of the firmware's code and its suitability for the hardware components of the smoke detector.*

It is even harder if the algorithm suspected of causing harm has been developed or modified by some AI system fuelled by machine learning and deep learning techniques, on the basis of multiple external data collected since the start of its operation. Even without changes to the original software design, the embedded criteria steering the collection and analysis of data and the decision-making process may not be readily explicable and often require costly analysis by experts. This may in itself be a primary practical obstacle to pursuing a claim for compensation, even if those costs should ultimately be recoverable as long as the chances of succeeding are hard to predict for the victim upfront.

---

43 See Article 2:102 paragraph 1 PETL: 'The scope of protection of an interest depends on its nature; the higher its value, the precision of its definition and its obviousness, the more extensive is its protection'.

44 The standard of proof determines the degree to which a court must be persuaded of some assertion in order to hold it as true. This standard is quite different throughout Europe. Most civil law systems traditionally require that the judge be convinced to something equivalent to a certainty, or at least a high degree of probability, to find in favour of the party with the burden of proof. By contrast, common law countries require that there be a probability greater than 50% (or a preponderance of the evidence) to satisfy the burden of proof.

In cases of strict liability,[45] proving causation may be easier for the victim, and not only in those jurisdictions where causation is presumed in such cases.[46] Instead of establishing some misconduct in the sphere of the defendant, the victim only has to prove that the risk triggering strict liability materialised. Depending on how this risk was defined by the legislator, this may be easier, considering that, for example, current motor vehicle liability statutes merely require an 'involvement' of the car or its being 'in operation' when the accident happened.

In addition to the initial complexity of AI systems upon release, they will most likely be subject to more or less frequent updates which are not necessarily supplied by the original producer. Identifying which part of a now flawed code was wrong from the beginning or adversely changed in the course of an update, will at least require (again) significant expert input, but doing so is essential in order to determine whom to sue for compensation.

The operation of AI systems often depends on data and other input collected by the system's own sensors or added by external sources. Not only may such data be flawed in itself, but the processing of otherwise correct data may also be imperfect. The latter may be due to original defects in designing the handling of data, or the consequence of distortions of the system's self-learning abilities due to the bulk of data collected, whose randomness may lead the AI system in question to misperceive and miscategorise subsequent input.

Problems of uncertain causation are of course not new to European legal systems, even though they are posed differently depending on the applicable standard of proof.[47] As long as the uncertainty exceeds that threshold, the victim will remain uncompensated, but as soon as the likelihood of the causation theory on which the victim's case rests meets the standard of proof, they will be fully compensated (subject to the further requirements of liability).

This all-or-nothing dilemma is already being addressed throughout Europe by some modifications that aid the victim in proving causation under certain circumstances. Courts may for instance be willing to accept prima facie evidence in complex scenarios, such as those emerging digital technologies give rise to, where the exact sequence of events may be difficult to prove. While the burden of proving causation is not shifted yet,[48] it is clearly alleviated for the victim, who need not prove every single link in the chain of causation if courts accept that a given outcome is the typical effect of a certain development in that chain. Furthermore, as past medical malpractice cases have shown, courts tend to be willing to place the burden of producing evidence on the party who is or should be in control of the evidence, with failure to bring forward such evidence resulting in a presumption to the disadvantage of that party. If, for example, certain log files cannot be produced or properly read, courts may be prepared to hold this against

---

45 But see the differences between the tort laws of the Member States when it comes to introducing and applying strict liability infra B.III.5.

46 See for example Article 1063 of the Croatian Civil Obligations Act: 'Damage caused in relation to a dangerous thing or dangerous activity shall be considered to result from that thing or activity, unless it has been proved that it did not cause the damage.' (translated by M Baretić in E Karner/K Oliphant/B Steininger (eds), *European Tort Law: Basic Texts* [2nd edition 2019] 48).

47 See fn 44.

48 Unlike in a full reversal of the burden of proof, prima facie evidence is meant to resolve uncertainties rather than bridge *non liquet* situations, and it can be rebutted already if the opponent can prove (again adhering to traditional standards) that there is a (mere) genuine possibility of a turn of events deviating from the one expected according to experience.

the party that was in charge of these recordings (and/or of the technology for analysing them). In some cases, some European legislators have intervened and shifted the burden of proving causation altogether,[49] thereby presuming that the victim's harm was caused by the defendant, though leaving the defendant the possibility to rebut this.[50] It remains to be seen to what extent any of these tools will be used in favour of the victim if their harm may have been caused by emerging digital technologies.

It is already difficult to prove that some conduct or activity was the cause of harm, but it gets even more complex if other alternative causes come into play. This is nothing new, but it will become much more of an issue in the future, given the interconnectedness of emerging digital technologies and their increased dependency on external input and data, making it increasingly doubtful whether the damage at stake was triggered by a single original cause or by the interplay of multiple (actual or potential) causes.

Current tort law regimes in Europe handle such uncertainties in the case of multiple potential sources of harm quite differently. Even if something is proven to have triggered the harm (for example, because an autonomous car collided with a tree), the real reason for it is not always equally evident. The car may have been poorly designed (be it its hardware, pre-installed software, or both), but it may also have either misread correct, or received incorrect, data, or a software update done by the original producer or by some third party may have been flawed, or the user may have failed to install an update which would have prevented the collision, to give just a few examples, not to mention a combination of multiple such factors.

The classic response by existing tort laws in Europe in such cases of alternative causation, if it remains unclear which one of several possible causes was the decisive influence to trigger the harm, is that either no-one is liable (since the victim's evidence fails to reach the threshold to prove causation of one cause), or that all parties are jointly and severally liable, which is the majority view.[51] The former outcome is undesirable for the victim, the latter for those merely possible tortfeasors who in fact did not cause harm, but may still be attractive targets for litigation because of their procedural availability and/or their more promising financial ability to actually pay compensation. The problem of who really caused the harm in question will therefore often not be solved in the first round of litigation initiated by the victim, but on a recourse level, if ever. More modern approaches provide for proportional liability at least in some cases, reducing the victim's claim against each potential tortfeasor to a quota corresponding to the likelihood that each of them in fact caused the harm in question.[52]

---

49 One such example is § 630h of the German BGB in the field of medical malpractice.

50 However, since the reason for shifting the burden of proof has often been the expectation that the victim will not succeed in establishing causation, the burden on the defendant will typically not be lighter.

51 See, e.g., B Winiger et al (eds), *Digest of European Tort Law I: Essential Cases on Natural Causation* (2007), p. 387 ff.

52 See I Gilead/M Green/BA Koch (eds), *Proportional Liability: Analytical and Comparative Perspectives* (2013).

3. Wrongfulness and fault

As already mentioned in the overview above, tort laws in Europe are traditionally fault-based, providing compensation to the victim if the defendant is to blame for the former's damage.[53] Such blame is commonly linked to the deviation from some conduct expected of, but not shown, by the tortfeasor. Whether or not a legal system distinguishes between objective or subjective wrongdoing and/or divides the basis of liability for misconduct into wrongfulness and fault,[54] two things remain crucial: to identify the duties of care the perpetrator should have discharged and to prove that the conduct of the perpetrator of the damage did not discharge those duties.

The duties in question are determined by various factors. Sometimes they are defined beforehand by statutory language prescribing or prohibiting certain specific conduct, but often they must be reconstructed after the fact by the court on the basis of social beliefs about the prudent and reasonable course of action in the circumstances.[55]

Emerging digital technologies make it difficult to apply fault-based liability rules, due to the lack of well established models of proper functioning of these technologies and the possibility of their developing as a result of learning without direct human control.

The processes running in AI systems cannot all be measured according to duties of care designed for human conduct, or not without adjustments that would require further justification. As European legal systems tend to regulate product and safety requirements in advance more than other jurisdictions,[56] it may well be the case that at least certain minimum rules will be introduced (if only, for example, logging requirements alleviating an analysis, after the fact, of what actually happened), to help define and apply the duties of care relevant for tort law should damage occur. A violation of such statutory or regulatory requirements may also trigger liability more easily for the victim, by shifting the burden of proving fault in many systems for example.[57] Still, such requirements will not be present from the beginning, and it may take years for such rules to emerge, either in legislation or in the courts.

Legal requirements have to be distinguished from industry standards (or practices) not yet recognised by the lawmaker. Their relevance in a tort action is necessarily weaker, even though the courts may look at such requirements as well when assessing in retrospect whether or not conduct complied with the duties of care that needed to be discharged under the circumstances.

Taking a step back and shifting the focus onto a software developer who wrote the firmware for some smart gadget, for example, does not resolve the problem entirely, since – as already

---

53 See also the Commission Staff Working Document (fn 8), p. 7.

54 On the range of existing approaches in this regard throughout Europe, see H Koziol, 'Comparative Conclusions', in H Koziol (ed), *Basic Questions of Tort Law from a Comparative Perspective* (2015), p. 685 (782 ff).

55 See the notion of a 'Schutzgesetz' (protective norm) in a comparative overview, see B Winiger et al (eds), *Digest of European Tort Law III: Essential Cases on Misconduct* (2018), p. 696 ff.

56 See *U Magnus*, 'Why is US Tort Law so Different?', JETL 2010, 1 (20).

57 See for example § 2911 Czech Civil Code: 'If a wrongdoer causes damage to the injured party by breaching a legal obligation, he shall be deemed to have caused the damage through negligence.' (translated by J Hradek in *European Tort Law: Basic Texts*² [fn 46] 68). There are also tort law systems where fault is presumed in general (see Article 45(2) of the Bulgarian Law on Obligations and Contracts; § 1050 of the Estonian Law of Obligations Act; § 6:519 of the Hungarian Civil Code; § 420(3) of the Slovak Civil Code).

mentioned – the software may have been designed to adjust itself to unprecedented situations or at least to cope with novel input not matching any pre-installed data. If the operation of some technology that includes AI, for example, is legally permissible, presuming that the developer made use of state-of-the-art knowledge at the time the system was launched, any subsequent choices made by the AI technology independently may not necessarily be attributable to some flaw in its original design. The question therefore arises whether the choice to admit it to the market, or implement the AI system in an environment where harm was subsequently caused, in itself is a breach of the duties of care applicable to such choices.

In addition to the difficulties of determining what constitutes fault in the case of damage caused by an emerging digital technology, there may also be problems with proving fault. Generally, the victim has to prove that the defendant (or someone whose conduct is attributable to them) was at fault. The victim therefore not only needs to identify which duties of care the defendant should have discharged, but also to prove to the court that these duties were breached. Proving the defendant is at fault entails providing the court with evidence that may lead it to believe what the applicable standard of care was and that it has not been met. The second part of this is to provide evidence of how the event giving rise to the damage occurred. The more complex the circumstances leading to the victim's harm are, the harder it is to identify relevant evidence. For example, it can be difficult and costly to identify a bug in a long and complicated software code. In the case of AI, examining the process leading to a specific result (how the input data led to the output data) may be difficult, very time-consuming and expensive.

4. Vicarious liability

Existing tort laws in Europe differ substantially in their approach to holding someone (the principal) liable for the conduct of another (the auxiliary).[58] Some attribute an auxiliary's conduct to the principal without further requirements, other than that the auxiliary acted under the direction of the principal and for the benefit of the principal. Others hold the principal liable in tort law only under very exceptional circumstances, such as known dangerousness of the auxiliary or the auxiliary's complete unsuitability for the assigned task,[59] or if the defendant was at fault in selecting or supervising the auxiliary.[60] There are also jurisdictions which use both approaches.[61]

---

58 See the overview by *H Koziol*, 'Comparative Conclusions' (fn 54), p. 795 ff.

59 The latter is true in Austria for example. See § 1315 ABGB: 'Whosoever, for the conduct of his affairs, avails himself either of an unfit person, or knowingly of a dangerous person, is liable for the harm such a person causes to another in that capacity.' (translated by B Steininger in *European Tort Law: Basic Texts*² [fn 46] 5).

60 See, e.g., the German § 831 BGB, according to which the principal can excuse himself 'where the principal has exercised due care in the selection of the agent and – in so far as he has to provide equipment or tools or has to supervise the performance of the duties – has acted with due care in such provision and supervision, or where the loss would have occurred even if such care had been exercised' (translated by F Wagner von Papp/ J Fedtke in *European Tort Law: Basic Texts*² [fn 46] 144).

61 See, e.g., Article 429 of the Polish Civil Code, according to which the principal is liable for the agent's unlawful (but not necessarily culpable) conduct, unless the principal has chosen the agent carefully or has chosen a professional agent, and Article 430 of the Polish Civil Code, which makes the principal strictly liable for the culpable conduct of the agent if the agent is a subordinate of the principal. See also Article 3-19-2 of Act no 11000 of 15 April 1683, King Christian the Fifth's law of Denmark.

Jurisdictions with a neutral (and therefore broader) definition of strict liability (as liability without fault of the liable person in general) regard vicarious liability as a mere variant of this strict (or no-fault) liability. If the notion of strict liability is equated with liability for some specific risk, dangerous object or activity instead, vicarious liability is rather associated with fault liability, as liability of the principal without personal fault of their own, but for the (passed-on) 'fault' of their auxiliary instead, even though the auxiliary's conduct is then not necessarily evaluated according to the benchmarks applicable to themselves, but to the benchmarks for the principal.[62]

Irrespective of such differences, the concept of vicarious liability is considered by some as a possible catalyst for arguing that operators of machines, computers, robots or similar technologies should also be strictly liable for their operations, based on an analogy to the basis of vicarious liability. If someone can be held liable for the wrongdoing of some human helper, why should the beneficiary of such support not be equally liable if they outsource their duties to a non-human helper instead, considering that they equally benefit from such delegation?[63] The policy argument is quite convincing that using the assistance of a self-learning and autonomous machine should not be treated differently from employing a human auxiliary, if such assistance leads to harm of a third party ('principle of functional equivalence'). However, at least in those jurisdictions which consider vicarious liability a variant of fault liability, holding the principal liable for the wrongdoing of another, it may be challenging to identify the benchmark against which the operations of non-human helpers will be assessed in order to mirror the misconduct element of human auxiliaries. The potential benchmark should take into account that in many areas of application non-human auxiliaries are safer, that is less likely to cause damage to others than human actors, and the law should at least not discourage their use.[64]

5. Strict liability

Particularly from the 19th century onwards, legislators often responded to risks brought about by new technologies by introducing strict liability, replacing the notion of responsibility for misconduct with liability irrespective of fault, attached to specific risks linked to some object or activity which was deemed permissible, though at the expense of a residual risk of harm linked to it.[65] So far, these changes to the law have concerned, for example, means of transport (such as trains or motor vehicles), energy (such as nuclear power, power lines), or pipelines.[66] Even before that, tort laws often responded to increased risks by shifting the burden of proving

---

62 On this divide, see *S Galand-Carval*, 'Comparative Report on Liability for Damage Caused by Others', in J Spier (ed), *Unification of Tort Law: Liability for Damage Caused by Others* (2003), 289 (290).

63 One might even draw support for such a solution from the analogy to a historic precedent – the Roman legal concept of noxal liability for slaves, whom the law at the time treated as property and not as persons, see, e.g., W Buckland/A McNair, *Roman Law and Common Law* (1952), p. 359 ff; AJB Sirks, 'Delicts', in D Johnston (ed), *The Cambridge Companion to Roman Law* (2015), p. 246 (265 ff).

64 R Abbott, 'The Reasonable Computer: Disrupting the Paradigm of Tort Liability', 86 Geo. Wash. L. Rev. 1 (2018).

65 See the contributions to M Martín-Casals (ed), *The Development of Liability in Relation to Technological Change* (2010). See also the Commission Staff Working Document (fn 8) 8 f.

66 See the overview provided by BA Koch/H Koziol, 'Comparative Conclusions', in BA Koch/H Koziol (eds), *Unification of Tort Law: Strict Liability* (2002), p. 395 ff.

fault, making it easier for the victim to succeed if the defendant was in control of particular sources of harm such as animals[67] or defective immovables.[68]

The landscape of strict liability in Europe is quite varied. Some legal systems are restrictive and have made very limited use of such alternative liability regimes (often expanding fault liability instead). Others are more or less generous, while not allowing analogy to individually defined strict liabilities (with the sole exception of Austria[69]). Some Member States have also introduced a (more or less broad) general rule of strict liability, typically for some 'dangerous activity',[70] which the courts in those jurisdictions interpret quite differently.[71] In some jurisdictions, the keeping of a thing triggers strict liability,[72] which is another way to provide for a rather far-reaching deviation from the classic fault requirement.

Existing rules on strict liability for motor vehicles (which can be found in many, but not all EU Member States) or aircrafts may well also be applied to autonomous vehicles or drones, but there are many potential liability gaps.[73]

Strict liability for the operation of computers, software or the like is so far widely unknown in Europe, even though there are some limited examples where countries provide for the liability of the operator of some (typically narrowly defined) computer system, such as databases operated by the state.[74]

The advantage of strict liability for the victim is obvious, as it exempts them from having to prove any wrongdoing within the defendant's sphere, let alone the causal link between such wrongdoing and the victim's loss, allowing the victim to focus instead only on whether the risk brought about by the technology materialised by causing them harm. However, one has to bear in mind that often strict liabilities are coupled with liability caps or other restrictions in order to counterbalance the increased risk of liability of those benefiting from the technology. Such

---

67 See the notes to Article VI-3:202 DCFR, describing the rather diverse landscape in Europe, which sometimes holds the keeper of the animal regardless of fault, or based on a presumption of the keeper's fault (in particular of an omission). Some jurisdictions also distinguish between the types of animal (wild or farm animals).

68 See the notes to Article VI-3:202 DCFR, which sets out strict liability 'for damage caused by the unsafe state of an immovable, inspired by existing laws in Europe, which typically either provide for strict liability or liability based on a presumption of flawed maintenance (which may or may not be rebutted).

69 BA Koch/H Koziol, 'Austria', in *Unification of Tort Law: Strict Liability* (fn 66), 14.

70 See Article 1064 of the Croatian Civil Obligations Act (dangerous things and activities); § 2925 of the Czech Civil Code (extraordinarily dangerous operation); § 1056 of the Estonian Law of Obligations Act (major source of danger); § 6:535 of the Hungarian Civil Code (extraordinarily dangerous activity); Article 2050 of the Italian Civil Code (dangerous activity); Article 2347 of Latvian Civil Law (activity associated with increased risk for other persons); § 432 of the Slovakian Civil Code (extremely dangerous operation); Article 149 ff of the Slovenian Obligations Code (dangerous objects or activities). The French liability for things (Article 1242 of the Civil Code) is another peculiar solution not limited to any specific object or risk.

71 See also the variety of causes of action in the Czech Civil Code (<http://obcanskyzakonik.justice.cz/images/pdf/Civil-Code.pdf>): Article 2924 (damage caused by an operating gainful activity unless all reasonable care exercised), Article 2925 (damage caused by a particularly hazardous operation, 'if the possibility of serious damage cannot be reasonably excluded in advance even by exercising due care'), Article 2937 (damage caused by a thing, though with a reversal of the burden of proof that the defendant had properly supervised it).

72 See Article 1242 of the French Civil Code and Article 1384 of the Belgian Civil Code.

73 See supra B.II.

74 See §§ 89e, 91b paragraph 8 of the Austrian *Gerichtsorganisationsgesetz* (Court Organisation Act).

caps are often further justified as contributing to making the risk insurable, as strict liability statutes often require adequate insurance cover for the liability risks.

A factor which any legislator considering the introduction of strict liability will have to take into account is the effect that such introduction may have on the advancement of the technology, as some may be more hesitant to actively promote technological research if the risk of liability is considered a deterrent. On the other hand, this allegedly chilling effect of tort law is even stronger as long as the question of liability is entirely unresolved and therefore unpredictable, whereas the introduction of a specific statutory solution at least more or less clearly delimits the risks and contributes to making them insurable.

6. Product liability

For more than 30 years, the principle of strict producer liability for personal injury and damage to consumer property caused by defective products has been an important part of the European consumer protection system. At the same time, the harmonisation of strict liability rules has helped to achieve a level playing field for producers supplying their products to different countries. However, while all EU Member States have implemented the Product Liability Directive (PLD[75]), liability for defective products is not harmonised entirely. Apart from differences in implementing the directive,[76] Member States also continue to preserve alternative paths to compensation in addition to the strict liability of producers for defective products under the PLD.

The PLD is based on the principle that the producer (broadly defined along the distribution channel) is liable for damage caused by the defect in a product they have put into circulation for economic purposes or in the course of their business.[77] Interests protected by the European product liability regime are limited to life and health and consumer property.

The PLD was drawn up on the basis of the technological neutrality principle. According to the latest evaluation of the directive's performance, its regime continues to serve as an effective tool and contributes to enhancing consumer protection, innovation, and product safety.[78] Nonetheless, some key concepts underpinning the EU regime, as adopted in 1985, are today an inadequate match for the potential risks of emerging digital technologies.[79] The progressive sophistication of the market and the pervasive penetration of emerging digital technologies reveal that some key concepts require clarification. This is because the key aspects of the PLD's lia-

75 Council directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC).

76 Apart from variations allowed by the directive itself (art 15 f PLD), there is, for example, no accord on whether the threshold of 500 ECU in art 9 lit b PLD is a minimum loss (allowing recovery for the entire harm as long as it exceeds this amount) or a deductible (granting only compensation for any loss above the minimum).

77 Art 4 and 7 PLD.

78 Commission Staff Working Document, Evaluation of Council Directive 85/374/EEC, SWD(2018) 157.

79 This was also acknowledged by the (Fifth) 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), COM(2018) 246 final, 8 f.

bility regime have been designed with traditional products and business models in mind – material objects placed on the market by a one-time action of the producer, after which the producer does not maintain control over the product. Emerging digital technologies put the existing product liability regime to the test in several respects concerning notions of product, defect and producer.

The scope of the product liability regime rests on the concept of product. For the purposes of the Directive, products are defined as movable objects, even when incorporated into another movable or immovable object, and include electricity. So far, the distinction of products and services has not encountered insurmountable difficulties. However, emerging digital technologies, especially AI systems, challenge that clear distinction and raise open questions. In AI systems, products and services permanently interact and a sharp separation between them is unfeasible. It is also questionable whether software is covered by the legal concept of product or product component. It is particularly discussed whether the answer should be different for embedded and non-embedded software, including over-the-air software updates or other data feeds. In any case, where such updates or other data feeds are provided from outside the EEA, the victim may not have anybody to turn to within the EEA, as there will typically not be an intermediary importer domiciled within the EEA in the case of direct downloads.

The second key element of the product liability regime is the notion of defect. Defectiveness is assessed on the basis of the safety expectations of an average consumer,[80] taking into account all relevant circumstances. The interconnectivity of products and systems makes it hard to identify defectiveness. Sophisticated AI autonomous systems with self-learning capabilities also raise the question of whether unpredictable deviations in the decision-making path can be treated as defects. Even if they constitute a defect, the state-of-the-art defence may apply. Additionally, the complexity and the opacity of emerging digital technologies complicate chances for the victim to discover and prove the defect and prove causation.

As the PLD focuses on the moment when the product was put into circulation as the key turning point for the producer's liability, this cuts off claims for anything the producer may subsequently add via some update or upgrade. In addition, the PLD does not provide for any duties to monitor the products after putting them into circulation.[81] Highly sophisticated AI systems may not be finished products that are put on the market in a traditional way. The producer may retain some degree of control over the product's further development in the form of additions or updates after circulation. At the same time, the producer's control may be limited and non-exclusive if the product's operation requires data provided by third parties or collected from the environment, and depends on self-learning processes and personalising settings chosen by the user. This dilutes the traditional role of a producer, when a multitude of actors contribute to the design, functioning and use of the AI product/system.

This is related to another limitation of liability – most Member States adopted the so-called development risk defence, which allows the producer to avoid liability if the state of scientific

80 "Safety which a person is entitled to expect" (Article 6 paragraph 1 PLD).

81 On the manifold difficulties with the PLD today, see P Machnikowski, 'Conclusions', in P Machnikowski (ed), *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (2016) 669 (691 ff).

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 (Article 7 lit e PLD). The defence may become much more important practically with regard to sophisticated AI-based products.

It has been mentioned that the PLD regime protects life and health as well as consumer property. With regard to the latter, it is not clear whether it covers damage to data, as data may not be an 'item of property' within the meaning of Article 9 lit b PLD.

7. Contributory conduct

While balancing liability in light of the victim's own conduct contributing to their harm does not raise new problems in the era of emerging digital technologies, one should keep in mind that all challenges listed above with respect to the tortfeasor apply correspondingly to the victim. This is particularly true if the victim was involved in or somehow benefited from the operation of some smart system or other interconnected digitalised device, e.g. by installing (or failing to install) updates, by modifying default system settings, or by adding their own digital content. Apart from collisions of autonomous vehicles, further obvious examples include the home owner who fails to properly install and combine multiple components of a smart home system despite adequate instructions. In the former case, two similar risks meet, whereas in the latter the risks of an emerging digital technology have to be weighed against failure to abide by the expected standard of care.

8. Prescription

While there is a certain trend throughout Europe to reform the laws regarding prescription of tort claims,[82] it is unproblematic to apply these rules to scenarios involving emerging digital technologies. However, one should be aware that particularly in jurisdictions where the prescription period is comparatively short,[83] the complexities of these technologies, which may delay the fact-finding process, may run counter to the interests of the victim by cutting off their claim prematurely, before the technology could be identified as the source of her harm.

9. Procedural challenges

In addition to the problems of substantive tort law already indicated, the application of liability frameworks in practice is also affected by challenges in the field of procedural law. Considering the tendency of case law experience in some Member States to alleviate the burden of proving causation in certain complex matters (such as medical malpractice),[84] one could easily envisage that courts might be similarly supportive of victims of emerging digital technologies who have

82 See, e.g., BA Koch, '15 Years of Tort Law in Europe – 15 Years of European Tort Law?', in E Karner/B Steininger (eds), *European Tort Law 2015* (2016) 704 (719 f).

83 For example, only one year, as in Spain (Article 1968 of the Civil Code), as opposed to, e.g., three to six years elsewhere.

84 See, e.g., BA Koch, 'Medical Liability in Europe: Comparative Analysis', in BA Koch (ed), *Medical Liability in Europe* (2011) 611 (632 ff).

a hard time proving that the technology in question was the actual cause of their harm. However, again this is likely to differ from case to case and most certainly from Member State to Member State. As far as purely procedural issues are concerned, there may equally be problems, as well-established procedural law concepts like prima facie evidence may be difficult to apply to situations involving emerging technological developments.

The ensuing differences in the outcome of cases which result from differences in the procedural laws of the Member States may be alleviated at least in part by harmonising the rules on the burden of proof.

10. Insurance

An obligatory insurance scheme for certain categories of AI/robots has been proposed as a possible solution to the problem of allocating liability for damage caused by such systems (sometimes combined with compensation funds for damage not covered by mandatory insurance policies).[85] However, an obligatory insurance scheme cannot be considered the only answer to the problem of how to allocate liability and cannot completely replace clear and fair liability rules. Insurance companies form a part of the whole social ecosystem and need liability rules to protect their own interests in relation to other entities (redress rights). Moreover, in order to keep emerging digital technologies as safe as possible and, therefore, trustworthy, a duty of care should be affected by insurance as little as possible. Yet, at the same time, cases of very high or catastrophic risks need to be insured in order to secure compensation for potentially serious damage.

Hence, the question relates to whether first-party or third-party insurance, or a combination of both, should be required or at least recommended and in which cases.[86] Currently, EU law requires obligatory liability (third-party) insurance e.g. for the use of motor vehicles,[87] air carriers and aircraft operators,[88] or carriers of passengers by sea.[89] Laws of the Member States require obligatory liability insurance in various other cases, mostly coupled with strict liability schemes, or for practising certain professions.

New optional insurance policies (e.g. cyber-insurance) are offered to those interested in covering both first- and third-party risks. Overall, the insurance market is quite heterogeneous and can adapt to the requirements of all involved parties. However, this heterogeneity, combined with a multiplicity of actors involved in an insurance claim, can lead to high administrative

85 See points 57 et seq. of the EP Resolution cited in fn 4 above.

86 The whole insurance system is a combination of public and private obligatory or optional insurance that takes the form of first-party or third-party insurance.

87 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.

88 Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators.

89 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.

costs both on the side of insurance companies and potential defendants, the lengthy processing of insurance claims, and unpredictability of the final result for the parties involved.

Insurers traditionally use historical claims data to assess risk frequency and severity. In the future, more complex systems, using highly granular risk profiles based on data analytics, including by analysing data logged or streamed in real time, will be gaining ground. In the light of this, the issue of access to data for insurance companies is very pertinent.

The cost efficiency of the claims process is also an important consideration.[90]

[90] F Pütz et al, 'Reasonable, Adequate and Efficient Allocation of Liability Costs for Automated Vehicles: A Case Study of the German Liability and Insurance Framework', European Journal of Risk Regulation (2018) 9.3: 548-563.

C. Perspectives on liability for emerging digital technologies

The promise of benefits and remarkable opportunities for society enabled by a multitude of uses and applications of emerging digital technologies is incontestable. Despite these indisputable gains, the pervasive use of increasingly sophisticated systems and combinations of technologies, in multiple economic sectors and societal contexts, creates risks and can cause losses. The adequacy of current liability legal regimes in Europe to fully compensate damages caused by these technologies is, however, questionable.[91] To that end, certain key concepts underpinning classical liability regimes need legal clarification. Furthermore, to deal with some situations, the formulation of specific rules, principles and concepts might also be necessary to accommodate legal liability regimes to new realities.

1. Challenges of emerging digital technologies for liability law ([1]–[2])

[1] Digitalisation brings fundamental changes to our environments, some of which have an impact on liability law. This affects, in particular, the

(a) complexity,

(b) opacity,

(c) openness,

(d) autonomy,

(e) predictability,

(f) data-drivenness, and

(g) vulnerability

of emerging digital technolgies.

[2] Each of these changes may be gradual in nature, but the dimension of gradual change, the range and frequency of situations affected, and the combined effect, results in disruption.

Digitalisation has changed and is still changing the world. The law of liability in European jurisdictions has evolved over the course of many centuries and has already survived many disruptive developments. It therefore does not come as a surprise that, in principle, the law of liability is able to also cope with emerging digital technologies. However, there are some fundamental changes, each of which may be only gradual in nature, but whose dimension and combined effect results in disruption.[92]

(a) Complexity: Modern-day hardware can be a composite of multiple parts whose interaction requires a high degree of technical sophistication. Combining it with an increasing percentage

91 Supra B.III.

92 See also the Commission Staff Working Document (fn 8) 9 ff, 22 f.

of digital components, including AI, makes such technology even more complex and shifts it far away from the archetypes of potentially harmful sources on which the existing rules of liability are based. Where, for example, an AV interacts with other AVs, a connected road infrastructure and various cloud services, it may be increasingly difficult to find out where a problem has its source and what ultimately caused an accident. The plurality of actors in digital ecosystems makes it increasingly difficult to find out who might be liable for the damage caused. Another dimension of this complexity is the internal complexity of the algorithms involved.

(b) Opacity: The more complex emerging digital technologies become, the less those taking advantage of their functions or being exposed to them can comprehend the processes that may have caused harm to themselves or to others. Algorithms often no longer come as more or less easily readable code, but as a black-box that has evolved through self-learning and which we may be able to test as to its effects, but not so much to understand. It is therefore becoming increasingly difficult for victims to identify such technologies as even a possible source of harm, let alone why they have caused it. Once a victim has successfully claimed damages from a tortfeasor, the tortfeasor may face similar difficulties at the redress level.

(c) Openness: Emerging digital technologies are not completed once put into circulation, but by their nature depend upon subsequent input, in particular more or less frequent updates or upgrades. Often they need to interact with other systems or data sources in order to function properly. They therefore need to remain open by design, i.e. permit external input either via some hardware plug or through some wireless connection, and come as hybrid combinations of hardware, software, continuous software updates, and various continuous services. This shift from the classic notion of a product completed at a certain point in time to a merger of products and ongoing services has a considerable impact on, among other things, product liability.

(d) Autonomy: Emerging new technologies increasingly perform tasks with less, or entirely without, human control or supervision. They are themselves capable of altering the initial algorithms due to self-learning capabilities that process external data collected in the course of the operation. The choice of such data and the degree of impact it has on the outcome is constantly adjusted by the evolving algorithms themselves.

(e) Predictability: Many systems are designed to not only respond to pre-defined stimuli, but to identify and classify new ones and link them to a self-chosen corresponding reaction that has not been pre-programmed as such. The more external data systems are capable of processing, and the more they are equipped with increasingly sophisticated AI, the more difficult it is to foresee the precise impact they will have once in operation.

(f) Data-drivenness: Emerging digital technologies increasingly depend on external information that is not pre-installed, but generated either by built-in sensors or communicated from the outside, either by regular data sources or by ad hoc suppliers. Data necessary for their proper functioning may, however, be flawed or missing altogether, be it due to communication errors or problems of the external data source, due to flaws of the internal sensors or the built-in algorithms designed to analyse, verify and process such data.

(g) Vulnerability: Emerging digital technologies are typically subject to more or less frequent updates and operate in more or less constant interaction with outside information. The built-in

features granting access to such input make these technologies particularly vulnerable to cybersecurity breaches. These may cause the system itself to malfunction and/or modify its features in a way more likely to cause harm.

2. Impact of these challenges and need for action ([3]–[4])

[3] While existing rules on liability offer solutions with regard to the risks created by emerging digital technologies, the outcomes may not always seem appropriate, given the failure to achieve:

(a) a fair and efficient allocation of loss, in particular because it could not be attributed to those:

- **whose objectionable behaviour caused the damage; or**
- **who benefitted from the activity that caused the damage; or**
- **who were in control of the risk that materialised; or**
- **who were cheapest cost avoiders or cheapest takers of insurance.**

(b) a coherent and appropriate response of the legal system to threats to the interests of individuals, in particular because victims of harm caused by the operation of emerging digital technologies receive less or no compensation compared to victims in a functionally equivalent situation involving human conduct and conventional technology;

(c) effective access to justice, in particular because litigation for victims becomes unduly burdensome or expensive.

[4] It is therefore necessary to consider adaptations and amendments to existing liability regimes, bearing in mind that, given the diversity of emerging digital technologies and the correspondingly diverse range of risks these may pose, it is impossible to come up with a single solution suitable for the entire spectrum of risks.

Existing liability regimes in all Member States already now provide answers to the question of whether the victim of any risk that materialises can seek compensation from another, and under what conditions.[93]

However, these answers may not always be satisfying when harm is caused by emerging digital technologies given the challenges, and for various reasons.

One reason why existing rules on liability may produce unsatisfactory results is that **loss** resulting from emerging digital technologies is **not allocated to the party** who is the **most appropriate to bear that loss**. As a general rule, loss normally falls on the victim themselves (*casum sentit dominus*) unless there is a convincing reason for shifting it to another party to whom the loss can be attributed. Reasons for attributing loss to another party vary depending on which type of liability is at stake. Under fault-based liability, the pivotal point is that the tortfeasor's objectionable and avoidable behaviour caused the damage, which in turn translates both into a

93 B.III.

corrective justice argument and an argument about providing the right incentives to avoid harm. Under many regimes of strict liability, the pivotal points are benefit and control, i.e. that the liable person exposed others to the risks of an activity from which the liable person benefited and which was under their control. This again translates into arguments both of corrective justice and of the right incentives. Economic analysis re-phrased these elements by putting the stress on the cheapest cost avoider or the cheapest taker of insurance, with the cheapest cost avoider usually being precisely the person who could simply desist from objectionable behaviour, or who controls a risk and its extent.

> ***Illustration 2.*** *For traditional road vehicles, it used to be the individual owner (O) who was the most appropriate person to be liable, where damage was caused by the vehicle's operation. Regardless of whether or not the damage was caused by O's intent or negligence, it was definitely O who benefited from the operation in general, who had the highest degree of control of the risk by deciding when, where and how to use, maintain and repair the vehicle, and who was therefore also the cheapest cost avoider and taker of insurance. Where modern autonomous vehicles (AVs) are privately owned, it is still the individual owner who decides when to use the AV and puts the destination into the system, but all other decisions (route, speed etc.) are taken by algorithms provided by the producer (P) of the AV or a third party acting on P's behalf. P is also in charge of maintaining the vehicle. P may therefore be the much more appropriate person to be liable than O.*

Existing rules on liability may also lead to inappropriate results for reasons related more to coherence and consistency, in particular taking into account the principle of **functional equivalence**, such as where compensation is denied in a situation involving emerging digital technologies when there would be compensation in a functionally equivalent situation involving human conduct and conventional technology.

> ***Illustration 3.*** *Hospital H uses an AI-based surgical robot. Despite the fact that H and its staff have discharged all possible duties of care, damage is caused to patient P by way of some malfunctioning of the robot nobody could have foreseen, and which is unrelated to the condition in which the robot was shipped. If P were not indemnified for the ensuing harm, this would be inconsistent with the outcome in the functionally equivalent situation in which H has employed a human doctor and is liable for that doctor's comparable misconduct under national rules of vicarious liability (see C.8).*

The application of traditional liability rules may also lead to unsatisfactory results because, while the victim might theoretically receive compensation, litigation would be unduly burdensome and expensive, leaving them without **effective access to justice.** This may be the case if the liability requirements they would have to prove either are entirely unsuitable for the risk posed by emerging digital technologies or too difficult to establish. Leaving the victim uncompensated or undercompensated in such cases may be undesirable, as it may effectively deprive the victim of basic protection with regard to significant legally protected interests of theirs (such as life, health, bodily integrity and property, or other important rights).

In many situations, a particular outcome is not satisfactory for two or more of the above reasons.

It is clear from the outset that **no one-size-fits-all solution** can (or should) be offered. Instead, it is necessary to consider a range of options, with the choice within that range to be determined by various factors. Various policy arguments have shown that strict liability of the operator of some emerging digital technology may be justified, given the competing interests of said operator and of the victim, as well as the victim's alternatives to getting compensation ([9]-[12]). In the case of a product defect, the manufacturer of that product may be the appropriate addressee of claims arising out of such defects ([13]-[15]). However, adapting the notion of fault liability by specifying further duties of care ([16]-[17]), or by shifting the burden of proving fault ([22](b), [24](b), [27]), for example, may already resolve disruptive effects of emerging digital technologies in the field of tort law, if necessary and appropriate at all. Remaining gaps may often be filled by extending vicarious liability to the use of autonomous technology in lieu of human auxiliaries ([18]). If there are systemic practical difficulties in proving causation and other factors, it may be necessary to make some adjustments in this respect ([22], [24], [25]-[26], [29]-[30]). An insurance requirement may be necessary in some cases, to ensure that victims will get compensation ([33]). Compensation funds can also play a complementary role ([34]).

3. Bases of liability ([5]–[7])

[5] Comparable risks should be addressed by similar liability regimes, existing differences among these should ideally be eliminated. This should also determine which losses are recoverable to what extent.

[6] Fault liability (whether or not fault is presumed), as well as strict liability for risks and for defective products, should continue to coexist. To the extent these overlap, thereby offering the victim more than one basis to seek compensation against more than one person, the rules on multiple tortfeasors ([31]) govern.

[7] In some digital ecosystems, contractual liability or other compensation regimes will apply alongside or instead of tortious liability. This must be taken into account when determining to what extent the latter needs to be amended.

In most cases, also with emerging digital technologies, **more than one basis of liability** may be invoked if the risks they carry with them materialise. These bases of liability may either all or in part be available to the immediate victim, or to the various parties involved. This raises the question of whether the first person who paid compensation to the victim can recover at least part of their compensation payment from another party.

> ***Illustration 4.*** *For example, if the operator of an autonomous vehicle (O) is held strictly liable for any losses caused by its operation, but the producer of the autonomous vehicle (P) is also liable because the accident was caused by a product defect, O may pass on*

some or all of that risk on the recourse level to P, if it is O, or O's insurer, who has paid damages to the victim in the first place.[94]

Drawing the line between liability in tort and contractual liability is often difficult. Doing so becomes all the more important in jurisdictions that do not allow concurrent claims under both regimes, such as France.[95] Jurisdictions that do allow concurrent claims tend to overcome deficiencies of tort law by shifting tort cases into the realm of **contractual liability**, for example by creating quasi-contractual obligations with the prime purpose of allowing the beneficiaries of such obligations to avail themselves of the benefits of a contractual claimant.[96] However, there is always a limited group of victims who benefit from such contract theories, and victims who are outside the scope of application may still face serious difficulties.

To the extent that victims of emerging digital technologies already have claims under such contract theories, the liability gap created by the disruptive effects of these technologies may be narrow or even non-existant, at least with regard to the immediate victims of the risks of the technologies in question. However, those paying compensation to them under contract liability may still want to seek recourse against, for example, the manufacturer of the product they sold, which caused harm to their customers or users.

The availability of a contractual claim of recourse against another party may also come into play in deciding whether or not the party in question may be the appropriate addressee of the victim's tort claim.[97]

In certain damage scenarios, such as healthcare, there may be **other systems** in place to protect the immediate victims. This has to be taken into account when determining to what extent (and where exactly) emerging digital technologies pose challenges to existing liability regimes.

4. Legal personality ([8])

[8] For the purposes of liability, it is not necessary to give autonomous systems a legal personality

Over the years, there have been many proposals for extending some kind of legal personality to emerging digital technologies, some even dating from the last century.[98] In recent times, the EP report on 'Civil Law Rules on Robotics'[99] called on the Commission to create a legislative instrument to deal with liability caused by robots. It also asked the Commission to consider 'a

94 See the choices made in the PLD in this respect.

95 See M Martín-Casals (ed), *The Borderlines of Tort Law: Interactions With Contract Law* (2019).

96 See, for example, the concept of a contract with protective duties in relation to third parties, which was (and is still being) used in Austria to pursue direct claims of the victims of defective products against the manufacturer alongside the strict liability regime of the PLD.

97 This is one reason why the manufacturer of the final product is typically singled out as the primary person to address product liability claims to, because they may have a contractual claim against the producer of a component (or at least have assigned the risk of harm to third parties internally).

98 See, e.g., L Solum, 'Legal Personhood for Artificial Intelligences', 70 NC L Rev 1231 (1992).

99 Footnote 4 above.

specific legal status for robots', 'possibly applying electronic personality', as one liability solution.[100] Even in such a tentative form, this proposal proved highly controversial.[101]

Legal personality comes in many forms, even for natural persons, such as children, who may be treated differently from adults. The best-known class of other-than-natural persons, corporations, have long enjoyed only a limited set of rights and obligations that allows them to sue and be sued, enter into contracts, incur debt, own property, and be convicted of crimes. Giving robots or AI a legal personality would not require including all the rights natural persons, or even companies, have. Theoretically, a legal personality could consist solely of obligations. Such a solution, however, would not be practically useful, since civil liability is a property liability, requiring its bearer to have assets.

Still, the experts believe there is currently **no need to give a legal personality** to emerging digital technologies. Harm caused by even fully autonomous technologies is generally reducible to risks attributable to natural persons or existing categories of legal persons, and where this is not the case, new laws directed at individuals are a better response than creating a new category of legal person.[102] Any sort of legal personality for emerging digital technologies may raise a number of ethical issues. More importantly, it would only make sense to go down that road if it helps legal systems to tackle the challenges of emerging digital technologies.[103] Any additional personality should go hand-in-hand with funds assigned to such electronic persons, so that claims can be effectively brought against them. This would amount to putting a cap on liability and – as experience with corporations has shown – subsequent attempts to circumvent such restrictions by pursuing claims against natural or legal persons to whom electronic persons can be attributed, effectively 'piercing the electronic veil'.[104] In addition, in order to give a real dimension to liability, electronic agents would have to be able to acquire assets on their own. This would require the resolution of several legislative problems related to their legal capacity and how they act when performing legal transactions.

> ***Illustration 5.*** *Imagine liability for a fully autonomous car were on the car instead of its operator. Victims of accidents would receive compensation only if insurance is taken out for the car and someone (who?) pays the premiums, or if someone (who?) provides the car with assets from which damages could be paid. If such assets did not suffice to fully compensate the victims of an accident, said victims would have a strong incentive to seek compensation from the person benefiting from the operation of the car instead. If the*

---

100 Id.

101 See the Open Letter to the European Commission Artificial Intelligence And Robotics (2018), <http://www.robotics-openletter.eu/>

102 R Abbott/A Sarch, 'Punishing Artificial Intelligence: Legal Fiction or Science Fiction', UC Davis Law Review, [forthcoming 2019, http://dx.doi.org/10.2139/ssrn.3327485].

103 U Pagallo, 'Apples, oranges, robots: four misunderstandings in today's debate on the legal status of AI systems', in *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376 (2018), p. 2133. See also G Wagner, 'Roboter als Haftungssubjekte? Konturen eines Haftungsrechts für autonome Systeme', in F Faust/H-B Schäfer (eds), *Zivilrechtliche und rechtsökonomische Probleme des Internets und der künstlichen Intelligenz* (2019) 1.

104 BA Koch, 'Product Liability 2.0 – Mere Update or New Version?' in S Lohsse/R Schulze/D Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things* (2019) 99 (115).

car's assets were sufficient to pay the same level of compensation as under existing liability and insurance regimes, there would not be any cause for discussion, but in that case, giving the car a legal personality would be a mere formality and not really change the situation.

The experts wish to stress, however, that they only look at the liability side of things and do not take any kind of position on the future development of company law – whether an AI could act as a member of a board, for example.

5. Operator's strict liability ([9]–[12])

[9] Strict liability is an appropriate response to the risks posed by emerging digital technologies, if, for example, they are operated in non-private environments and may typically cause significant harm.

[10] Strict liability should lie with the person who is in control of the risk connected with the operation of emerging digital technologies and who benefits from their operation (operator).

[11] If there are two or more operators, in particular

(a) the person primarily deciding on and benefitting from the use of the relevant technology (frontend operator) and

(b) the person continuously defining the features of the relevant technology and providing essential and ongoing backend support (backend operator),

strict liability should lie with the one who has more control over the risks of the operation.

[12] Existing defences and statutory exceptions from strict liability may have to be reconsidered in the light of emerging digital technologies, in particular if these defences and exceptions are tailored primarily to traditional notions of control by humans.

Existing strict liability rules in the Member States may already apply to emerging digital technologies. The best example of this is liability regimes for motorised vehicles that will most likely already apply to autonomous cars, or for aircraft, (that may already include at least some drones). However, the situation in Europe still varies a lot. Some jurisdictions have more or less generous general clauses, or at least allow analogy to existing statutory regimes, whereas others do without the fault requirement in only very few, narrowly defined situations, but often expand the notion of fault. Strict liability typically only applies in cases of physical harm to persons or property, but not for pure economic loss. Even in the same jurisdiction, there can be considerable differences between the various strict liability regimes, as shown by the diverse range of defences available to the liable person, or by the legislator's choice in favour of or against caps.

The mere fact that technology is new is not justification enough for introducing strict liability. Nevertheless, emerging digital technologies that may **typically cause significant harm**[105] comparable to the risks already subject to strict liability should also be subject to strict liability. This is because victims should be treated alike if they are exposed to and ultimately harmed by similar dangers.

For the time being, this applies primarily to emerging digital **technologies which move in public spaces,** such as vehicles, drones, or the like. Smart home appliances will typically not be proper candidates for strict liability. It is in particular objects of a certain minimum weight, moved at a certain minimum speed, that are candidates for additional bases of strict liability, such as AI-driven delivery or cleaning robots, at least if they are operated in areas where others may be exposed to risk. Strict liability may not be appropriate for merely stationary robots (e.g. surgical or industrial robots), even if AI-driven, which are exclusively employed in a confined environment, with a narrow range of people exposed to risk, who in addition are protected by a different – including contractual – regime (in the illustrations below, patients protected by contractual liability or factory staff covered by workmen's compensation schemes).[106]

> ***Illustration 6.*** *The sensors controlling the path of an AI-driven robot transporting heavy component parts in Factory F malfunction, causing the robot to leave its intended path, exit the factory and run into passer-by P on the street. Even if existing rules of strict motor vehicle liability may not apply in this case, P should still be able to seek compensation from F without having to prove that F or of one of its staff is at fault.*

If the relevant risk threshold for an emerging digital technology is reached and it therefore seems appropriate to make the operation of this technology subject to a strict liability regime, said regime should **share the same features as other no-fault liabilities** for comparable risks. This also applies to the question which losses are recoverable to what extent, including whether caps should be introduced and whether non-pecuniary damage is recoverable.

The introduction of strict liability should offer victims easier access to compensation, without excluding, of course, a parallel fault liability claim if its requirements are fulfilled.[107] Furthermore, while strict liability will typically channel liability onto the liable person (for example, the operator of the technology), this person will retain the right to seek recourse from others contributing to the risk, such as the producer.

The experts have discussed extensively whether strict liability for emerging digital technologies should rather be on the owner/user/keeper of the technology than on its producer. It has been pointed out, in particular in the context of autonomous cars, that while the vast majority of accidents used to be caused by human error in the past, most accidents will be caused by the malfunctioning of technology in the future (though not necessarily of the autonomous car itself). This in turn could mean that it would not be appropriate to hold the owner/user/keeper strictly liable in the first place, because it is the producer who is the cheapest cost avoider and who is primarily in a position to control the risk of accidents. On the other hand, it is still the

---

105 The significance being determined by the interplay of the potential frequency and the severity of possible harm.

106 See also Illustration 3 above.

107 See Illustration 9 below.

owner/user/keeper who decides when, where and for which purposes the technology is used, and who directly benefits from its use. Also, if strict liability for operating the technology (besides product liability) were on the producer, the cost of insurance would be passed on to the owners anyway through the price mechanism.

On balance the NTF of the Expert Group does not consider the traditional concepts of owner/user/keeper helpful in the context of emerging digital technologies. Rather, they prefer the more neutral and flexible concept of '**operator**', which refers to the person who is in control of the risk connected with the operation of emerging digital technologies and who benefits from such operation. 'Control' is a variable concept, though, ranging from merely activating the technology, thus exposing third parties to its potential risks, to determining the output or result (such as entering the destination of a vehicle or defining the next tasks of a robot), and may include further steps in between, which affect the details of the operation from start to stop. However, the more sophisticated and more autonomous a system, the less someone exercises actual 'control' over the details of the operation, and defining and influencing the algorithms, for example by continuous updates, may have a greater impact than just starting the system.

With emerging digital technologies, there is often more than just one person who may, in a meaningful way, be considered as 'operating' the technology. The owner/user/keeper may operate the technology on the frontend, but there is often also a **central backend provider** who, on a continuous basis, defines the features of the technology and provides essential backend support services. This backend operator may have a high degree of control over the operational risks others are exposed to. From an economic point of view, the backend operator also benefits from the operation, because that operator profits from data generated by the operation, or that operator's remuneration is directly calculated on the basis of the duration, continuous nature or intensity of the operation, or because a one-off payment this backend operator has received reflects the estimated overall duration, continuous nature and intensity of the operation.

> ***Illustration 7.*** *An AV may be privately owned by an individual who decides whether to use the AV for shopping or for going on a business trip, and how often, when and where. This individual is the frontend operator. The producer of the AV or another service provider is likewise controlling the AV on a continuous basis, e.g. by continuously providing cloud navigation services, continuously updating map data or the AV software as a result of supervised fleet machine learning, and deciding when the AV needs what kind of maintenance. This person is the backend operator. Of course frontend and backend operator may also be the same person, such as in a 'mobility as a service' scheme (MaaS), where an AV is operated by a fleet operator who is also the backend operator.*

Where there is more than one operator, such as a frontend and a backend operator, the experts find that strict liability should be on the one who has more control over the risks posed by the operation. While both control and benefit are decisive for qualifying a person as operator, the benefit is often very difficult to quantify, so relying only on benefit as the decisive factor for deciding who, out of two operators, should be liable, would lead to uncertainty.

Very often, the frontend operator will have more control, but where emerging digital technologies become more backend-focused, there may be cases where so much continuous control over the technology remains with the backend operator that – despite the fact that the technology is

sold to individual owners – it **is more convincing to hold the backend operator liable** as the person primarily in a position to control, reduce and insure the risks associated with the use of the technology.

Ideally, in order to avoid uncertainty, the legislator should define which operator is liable under which circumstances, and all other matters that need to be regulated (concerning insurance for example). For instance, the legislator could decide that for AVs with a level of automation of 4 or 5, it is the provider running the system and who enters the AV in the national registry who is liable. This provider would therefore also take out insurance and could pass on the premiums through the fees paid for its services. Where several providers fulfil the function of backend operators, one of them would have to be designated as responsible operator for every AV.

What has been said so far can, in most Member States, largely be implemented by way of a simple extension of existing schemes of strict liability. However, as these schemes stand today in many Member States, they include a range of **defences**, exceptions and exclusions that may not be appropriate for emerging digital technologies, because they reflect a focus on continuous control by humans for example.

> ***Illustration 8.*** *Several national traffic liability schemes focus on the existence of a driver or allow for a defence in case of an unavoidable event or similar notions. These concepts do not translate properly into risk scenarios involving emerging digital technologies because the driver of an AV more resembles a passenger and because liability (or the exclusion of it) can no longer be linked to human control, which is typically missing entirely, at least with level 5 AVs.*

6. Producer's strict liability ([13]–[15])

[13] Strict liability of the producer should play a key role in indemnifying damage caused by defective products and their components, irrespective of whether they take a tangible or a digital form.

[14] The producer should be strictly liable for defects in emerging digital technologies even if said defects appear after the product was put into circulation, as long as the producer was still in control of updates to, or upgrades on, the technology. A development risk defence should not apply.

[15] If it is proven that an emerging digital technology has caused harm, the burden of proving defect should be reversed if there are disproportionate difficulties or costs pertaining to establishing the relevant level of safety or proving that this level of safety has not been met. This is without prejudice to the reversal of the burden of proof referred to in [22] and [24].

In the opinion of the NTF of the Expert Group, the principle of producer responsibility, adopted in relation to traditional products, should also apply to emerging digital technologies. The **motives** behind it, such as a fair distribution of the risks and benefits associated with commercial production, the spreading of the costs of individual harm to all buyers of a given type of product,

and prevention, are fully valid even if the product or one of its essential components is in digital form.

It is in line with the principle of **functional equivalence** (see [3](b)), that damage caused by defective digital content should trigger the producer's liability because digital content fulfils many of the functions tangible movable items used to fulfil when the PLD was drafted and passed. This is all the more true for defective digital elements of other products, some of which come separately from the tangible item (for example, as a control app to be downloaded onto the user's smartphone), or as over-the-air updates after the product has been put into circulation (security updates for example), or as digital services provided on a continuous basis during the time the product is being used (for example, navigation cloud services).

When the defect came into being as a result of the producer's interference with the product already put into circulation (by way of a software update for example), or the producer's failure to interfere, it should be regarded as a defect in the product for which the producer is liable. The point in time **at which a product is placed on the market** should not set a strict limit on the producer's liability for defects where, after that point in time, the producer or a third party acting on behalf of the producer remains in charge of providing updates or digital services. The producer should therefore remain liable where the defect has its origin (i) in a defective digital component or digital ancillary part or in other digital content or services provided for the product with the producer's assent after the product has been put into circulation; or (ii) in the absence of an update of digital content, or of the provision of a digital service which would have been required to maintain the expected level of safety within the time period for which the producer is obliged to provide such updates.

Only recently, the EU has confirmed in Directive (EU) 2019/771 on the sale of goods that a seller is also liable for such digital elements being in conformity with the contract, including for updates provided for as long a period as the consumer may reasonably expect, and Directive (EU 2019/770 establishes a similar regime for digital content and digital services. The proposed features of a producer's strict liability are very much in the same vein and follow very much the same logic, though on different grounds.

As indicated above, emerging digital technologies are characterised by limited predictability. This phenomenon will intensify with the dissemination of machine learning. The interconnectedness of devices, as well as threats to cyber security, also contribute to difficulties in predicting the product's performance. A defect in digital content or in a product with digital elements may therefore result from the impact of the environment in which the product operates or from the product's evolution, for which the manufacturer only created a general framework but which they did not design in detail. In view of the need to share benefits and risks efficiently and fairly, the development risk defence, which allows the producer to avoid liability for unforeseeable defects, should not be available in cases where it was predictable that unforeseen developments might occur.

Features of emerging digital technologies, such as opacity, openness, autonomy and limited predictability (see [1]), may often result in unreasonable difficulties or costs for the victim to establish both what safety an average user is entitled to expect, and the failure to achieve this

level of safety. At the same time, it may be significantly easier for the producer to prove relevant facts. This asymmetry justifies the reversal of the burden of proof.

The victim should also benefit from an alleviation of evidentiary burden with regard to the causal relationship between a defect and the damage (see [26]).

Producers' strict liability for defective products should be supplemented with fault-based liability for failure to discharge monitoring duties (see [17](b)).

7. Fault liability and duties of care ([16]–[17])

[16] Operators of emerging digital technologies should have to comply with an adapted range of duties of care, including with regard to

(a) choosing the right system for the right task and skills;

(b) monitoring the system; and

(c) maintaining the system.

[17] Producers, whether or not they incidentally also act as operators within the meaning of [10], should have to:

(a) design, describe and market products in a way effectively enabling operators to comply with the duties under [16]; and

(b) adequately monitor the product after putting it into circulation.

For the use of more traditional technologies, it is already recognised that their **operators** have to discharge a range of duties of care. They relate to the choice of technology, in particular in light of the tasks to be performed and the operator's own skills and abilities; the organisational framework provided, in particular with regard to proper monitoring; and maintenance, including any safety checks and repair. Failure to comply with such duties may trigger **fault liability** regardless of whether the operator may also be strictly liable for the risk created by the technology.

> ***Illustration 9.*** *Despite adverse weather conditions due to a heavy storm, which were entirely foreseeable, retailer (R) continues to employ drones to deliver goods to customers. One of the drones is hit by a strong wind, falls to the ground and severely injures a passer-by.*[108] *R may not only be strictly liable for the risks inherent in operating drones, but also for its failure to interrupt the use of such drones during the storm.*

In many national legal systems, courts have raised the relevant duty of care to a point where it is difficult to draw the line between fault liability and strict liability. With emerging digital technologies, such duties of care – despite all new opportunities and safety-enhancing technologies these systems may feature – are often magnified even more.

[108] This illustration is inspired by a hypothetical of the Commission Staff Working Document (fn 8) 12.

> ***Illustration 10.*** *Airline A buys a plane from producer P. A new AI element of the auto pilot may, under very exceptional circumstances, cause the plane to crash if the software is not manually disabled by the pilot. Airline A has a duty of care to make itself familiar with the new feature, to monitor the plane and to make sure pilots receive appropriate training and exchange information about and experience of dealing with the new software. If A breaches this duty, A may be liable under fault liability (without prejudice to existing international legal instruments that may limit A's liability).*

The more advanced technologies become, the more difficult it is for operators to develop the right skills and discharge all duties. While the risk of insufficient skills should still be borne by the operators, it would be unfair to leave **producers** entirely out of the equation. Rather, producers have to design, describe and market products in a way effectively enabling operators to discharge their duties.

> ***Illustration 11.*** *In Illustration 10, it is primarily P who has to alert its customer (A) to the particular features and risks of the software in question, and possibly to offer the necessary training courses, and to monitor the system once it is on the market.*

Under many national jurisdictions, a general product monitoring duty on the part of producers has already been developed for the purposes of tort law. In the light of the characteristics of emerging digital technologies, in particular their openness and dependency on the general digital environment, including the emergence of new malware, such a monitoring duty would also be of paramount importance.

8. Vicarious liability for autonomous systems ([18]–[19])

[18] If harm is caused by autonomous technology used in a way functionally equivalent to the employment of human auxiliaries, the operator's liability for making use of the technology should correspond to the otherwise existing vicarious liability regime of a principal for such auxiliaries.

[19] The benchmark for assessing performance by autonomous technology in the context of vicarious liability is primarily the one accepted for human auxiliaries. However, once autonomous technology outperforms human auxiliaries, this will be determined by the performance of comparable available technology which the operator could be expected to use, taking into account the operator's duties of care ([16]).

One option proposed for addressing the risks of emerging digital technology is the potential expansion of the notion of vicarious liability, leaving the respective national regime of liability for others intact, but expanding it (either directly or by way of analogy) to **functionally equiv-**

alent situations where use is made of autonomous technology instead of using a human auxiliary.[109] This may complement strict liability within the meaning of [9]-[12], and fault liability based on the notion of enhanced duties of care within the meaning of [16].[110]

> ***Illustration 12.*** *A hospital uses an AI-driven surgical robot. Despite the fact that the hospital has complied with all possible duties of care, a patient is harmed because the robot malfunctions in a way nobody could have foreseen. The hospital should be liable, in any case, under the principle outlined in [18].*

The scope and conditions for the application of vicarious liability vary from one country to another, as a result of the different ways national legal systems have developed and the resulting broader or narrower scope of application of strict liability they adopted. However, the development of emerging digital technologies, in particular systems with a high degree of decision-making autonomy, requires that the requirements of equivalence be respected (see 2[3](b)). Where the use of a human auxiliary would give rise to the liability of a principal, the use of a digital technology tool instead should not allow the principal to avoid liability. Rather, it should give rise to such liability to the same extent.

However, as the laws stand in many jurisdictions, the notion of vicarious liability at present requires the auxiliary to have **misbehaved** (though as assessed according to the standards applicable to the principal). In the case of a machine or technology, this triggers the question according to which benchmarks such "conduct" should be assessed. The experts discussed this in some depth, but did not come to a final conclusion. However, the most convincing answer seemed to be that the benchmark for assessing performance by autonomous technology should primarily be the benchmark accepted for human auxiliaries, but once autonomous technology outperforms human auxiliaries in terms of preventing harm, the benchmark should be determined by the performance of comparable technology that is available on the market.[111] As there is usually a broad range of technologies available, which may feature very different safety benchmarks, in choosing the appropriate point of comparison, the same principles should apply as with traditional technologies (such as x-ray machines or other equipment), i.e. reference should be made to the operator's duty of care with regard to the choice of system (see [16](a)).

> ***Illustration 13.*** *In the example of the surgical robot (Illustration 12), it is not difficult to establish relevant misconduct where, for example, the cut made by the robot is twice as long as one a human surgeon would have made. If the cut is longer than the best robots on the market would have made, but still shorter than that of a human surgeon, the question of whether the hospital should have bought a better robot must be answered according to the same principles as the question of whether a hospital should have bought a better X-ray machine or employed extra doctors.*

---

109 See B.III.4 above.

110 In many legal systems, some or all types of vicarious liability are in any case considered a subcategory of the former or the latter.

111 R Abbott, 86 Geo Wash L Rev 1 (2018).

9. Logging by design ([20]–[23])

[20] There should be a duty on producers to equip technology with means of recording information about the operation of the technology (logging by design), if such information is typically essential for establishing whether a risk of the technology materialised, and if logging is appropriate and proportionate, taking into account, in particular, the technical feasibility and the costs of logging, the availability of alternative means of gathering such information, the type and magnitude of the risks posed by the technology, and any adverse implications logging may have on the rights of others.

[21] Logging must be done in accordance with otherwise applicable law, in particular data protection law and the rules concerning the protection of trade secrets.

[22] The absence of logged information or failure to give the victim reasonable access to the information should trigger a rebuttable presumption that the condition of liability to be proven by the missing information is fulfilled.

[23] If and to the extent that, as a result of the presumption under [22], the operator were obliged to compensate the damage, the operator should have a recourse claim against the producer who failed to equip the technology with logging facilities.

Emerging digital technologies not only give rise to unprecedented complexity and opacity. They also offer unprecedented possibilities of reliable and detailed **documentation** of events that may enable the identification inter alia of what has caused an accident. This can usually be done using log files, which is why it seems desirable to impose, under certain circumstances, a duty to provide for appropriate logging and to disclose the data to the victim in readable format.

Any **requirements** must definitely be suitable for the goals to be achieved and proportionate, taking into account, in particular, the technical feasibility and costs of logging, the values at stake, the magnitude of the risk, and any adverse implications for the rights of others. Logging would have to be done in such a way that no interested party could manipulate the data and that the victim and/or the person who compensates the victim in the first place, for example an insurance provider, has access to it. Furthermore, it goes without saying that logging must be done **in accordance with otherwise applicable law**, notably on data protection and the protection of trade secrets.

> ***Illustration 14.*** *There would be a logging duty in the case of AVs. Traffic accidents occur rather frequently and often cause severe harm to the life and health of humans. Motor vehicles are very sophisticated and expensive anyway, so adding logging technology should not significantly increase the costs of production. There is a lot of data that can reasonably be logged and will serve to reconstruct events and causal chains that are both essential for allocating liability (for example by finding out which AV has caused the crash by not replying to a signal sent by the other AV) and could hardly be reconstructed otherwise.*

Illustration 15. *Logging would not be advisable, however, in the case of an AI-equipped doll for children. The risks associated with the doll are not of a kind where logging would be a suitable response. With regard to the risk of hidden merchandising, meaning that the doll manipulates the child's mind by mentioning and repeating certain product brands, the negative implications of logging (which would have to include, to a certain extent, the recording of conversations) for data protection would outweigh any possible benefit. With regard to the risk of a stranger hacking into the doll, the proper response is more cybersecurity to prevent this, not a duty to log.*

Failure to comply with a logging and disclosure duty should lead to a **rebuttable presumption** that the information would, if logged and disclosed, have revealed that the relevant element of liability is fulfilled.

Illustration 16. *Take the example of a crash between A's AV and B's AV, injuring B. The traffic situation was one where, normally, the two AVs would exchange data and "negotiate" which AV enters the lane first. When sued by B, A refuses to disclose the data logged in her AV's recordings. It is therefore presumed that her AV sent a signal telling B's AV to enter the lane first, but nevertheless went first itself.*

If a product used by the operator failed to contain a logging option (for example, in violation of mandatory regulatory requirements or in contrast to other products of such kind) and the operator is, for this reason, exposed to liability, the operator should be able to pass on the loss resulting from her inability to comply with the duty of disclosing logged data to the victim (typically resulting in the operator's liability towards the victim) to the producer. This can be achieved in various ways, including by allowing a separate claim, or by subrogation.

Illustration 17. *Imagine that, in Illustration 16, it is not that A refused to disclose the data, but that A's AV failed to log the kind of data in question. If A had to pay damages to B for this reason only, she should also be able to sue the producer.*

10. Safety rules ([24])

[24] Where the damage is of a kind that safety rules were meant to avoid, failure to comply with such safety rules, including rules on cybersecurity, should lead to a reversal of the burden of proving

- **(a) causation, and/or**
- **(b) fault, and/or**
- **(c) the existence of a defect.**

With enhanced complexity, openness and vulnerability, there comes a greater need to introduce new safety rules. Digital product safety differs from product safety in traditional terms in a number of ways, including by taking into account any effect a product may have on the user's digital environment. Even more importantly, cybersecurity has become essential.[112]

[112] Cf the Commission Staff Working Document (fn 8) 20.

As to the consequences of compliance or non-compliance with such rules, the experts considered two different solutions. One solution was that failure to comply with the rules may lead to a **reversal of the burden of proof** concerning key elements of liability, including causation and fault. The other solution was that compliance with the rules leads to a presumption of the absence of causation or fault. The experts decided in favour of the first solution, because it is better suited to addressing the difficulties of victims when it comes to proving the elements of liability in settings that involve emerging digital technologies. It is in particular the pace at which these technologies are evolving, and the necessity of imposing a duty on providers to monitor the market and react more quickly to new threats than any rulemaker could, that made it seem inappropriate to have a presumption of the absence of causation or fault where a provider complied with the rules.

> ***Illustration 18.*** *Imagine there is a new rule on cybersecurity of IoT household equipment, designed to prevent hacking and the resulting harm. The victim's private Wi-Fi is hacked in a way typical of cybersecurity gaps in IoT equipment. Where the victim can show that a water kettle produced by P failed to comply with the standard of safety under adopted safety rules, the victim could sue P, and the onus would be on P to prove that the damage had been caused by a different device.*

It should be stressed that this refers only to rules adopted by the lawmaker, such as those adopted under the "New Regulatory Approach", and not to mere technical standards developing in practice.

The reversal of the burden of proof discussed here is essential in the area of fault-based liability. In the case of producer liability, a similar principle is already applied in many jurisdictions in the context of national PLD implementations. It is assumed that failure to meet a safety standard means that the product does not provide the level of safety that the consumer is entitled to expect. Similar reasoning should apply to the liability of the producer of an emerging digital technology ([13] – [15]).

11. Burden of proving causation ([25]–[26])

[25] As a general rule, the victim should continue to be required to prove what caused her harm.

[26] Without prejudice to the reversal of the burden of proof proposed in [22] and [24](a), the burden of proving causation may be alleviated in light of the challenges of emerging digital technologies if a balancing of the following factors warrants doing so:

- **(a) the likelihood that the technology at least contributed to the harm;**
- **(b) the likelihood that the harm was caused either by the technology or by some other cause within the same sphere;**
- **(c) the risk of a known defect within the technology, even though its actual causal impact is not self-evident;**
- **(d) the degree of ex-post traceability and intelligibility of processes within the technology that may have contributed to the cause (informational asymmetry);**

(e) the degree of ex-post accessibility and comprehensibility of data collected and generated by the technology

(f) the kind and degree of harm potentially and actually caused.

As is already the standard rule in all jurisdictions, whoever demands compensation from another should in general prove all necessary requirements for such a claim, including in particular the causal link between the harm to be indemnified on the one hand and the activities or risks within the sphere of the addressee of the claim may trigger the latter's liability on the other. This **general principle** is supported inter alia by concerns of fairness and results from the need to consider and balance the interests of both sides.

However, given the practical implications of the complexity and opacity of emerging digital technologies in particular, victims may be in a weaker position to establish causation than in other tort cases, where the events leading to the harm can be more easily analysed in retrospect, even from the victim's point of view.

As is true in all jurisdictions, courts have already in the past found ways to **alleviate the burden of proving causation** if the claimant's position is deemed weaker than in typical cases.[113] This includes procedural options such as allowing *prima facie* evidence,[114] applying the theory of *res ipsa loquitur*,[115] or lowering the standard of proof in certain categories of cases.[116] Some jurisdictions are also prepared to even shift the burden of proving causation entirely if the basis for holding the defendant liable can be proven as particularly strong by the claimant (such as the defendant's grave misconduct), but the causal link between such faulty behaviour and the claimant's harm is merely suspected, but not proven, by the evidence available to the claimant.[117] Yet another method of aiding the claimant to prove the cause of harm is by focusing on

---

113 Cf the ruling in CJEU 21.6.2017 C-621/15 *Sanofi Pasteur*, ECLI:EU:C:2017:484, where the Court greenlighted a rather far-reaching presumption of causation in French court practice on vaccine damage, as long as it did not amount to a full-fledged reversal of the burden of proof, which would have infringed Article 4 of the PLD, which was at stake.

114 Unlike in a fully-fledged reversal of the burden of proof, *prima facie* evidence is meant to resolve uncertainties rather than bridge *non liquet* situations. The claimant still has to prove (in compliance with ordinary evidentiary standards) some links in the alleged chain of causation, but is spared proving all of them if experience has shown that the missing link is typically given in other similar cases. The defendant can rebut this by proving (again adhering to traditional standards) that there is a (mere) genuine possibility of a turn of events deviating from the one expected according to said experience, so that the missing link may indeed have not been given in the present case.

115 *Res ipsa loquitur* is the inference of negligence from the very nature of a harmful event, where the known circumstances are such that no other explanation for the accident seems possible than negligence within the sphere of the defendant, who had been in full control of the incident that may have caused the harm, such as a hospital where the patient has some surgical instrument in her body after an operation. Cf the English case of *Byrne v Boadle*, (1863) 2 H & C 722, 159 Eng Repr 299, where a barrel of flour fell out of a warehouse onto a pedestrian passing by, who was not required to prove the negligence of the flourmonger, as barrels do not fall out of such premises in the absence of fault within the latter's sphere. The dealer could in theory have rebutted this by proving some external cause, though.

116 The latter can often be seen in medical malpractice cases. See BA Koch, 'Medical Liability in Europe: Comparative Analysis', in BA Koch (ed), *Medical Liability in Europe* (2011) 611 (nos 46 ff).

117 Again, this is the practice in medical malpractice in countries like Germany, see § 630h paragraph 5 BGB, according to which it is presumed that a treatment error was the cause of the deterioration in the patient's

whoever is in control of key evidence but fails to produce it, for example, if the defendant is or should be able to submit internal evidence such as design blueprints, internal expertise, log files or other recordings, but does not produce such evidence in court, either strategically or because the evidence was lost or never generated.

Promoting any specific measure would run the risk of interfering with national rules of procedure in particular. However, in order to offer guidance on the further development and approximation of laws, and in order to allow for a more coherent and comparable line of reasoning, the experts think that lowering the bar for the claimant to prove causation may be advisable for victims of emerging digital technologies if the following **factors** are at play.

- First, the technology itself may be known to have certain potentially harmful features, which could be taken into account even though it is not (yet) proven that such risks have indeed materialised. If the claimant can prove that there was a defect in a product incorporating emerging digital technologies, thereby creating an extraordinary risk in addition to the ones commonly associated with flawless products, but – again – the harm caused cannot be (fully) traced to said defect, this might still be considered in the overall assessment of how to implement the burden of proving causation.
- If there are multiple possible causes and it remains unclear what exactly triggered the harm (or which combination of potential causes at which percentage of probability), but if the likelihood of all possible causes combined, that are attributable to one party (e.g. the operator) exceeds a certain threshold (e.g. 50% or more), this may also contribute to placing the burden of producing evidence rebutting such first-hand impressions onto that party.

  Illustration 19. *A small delivery robot operated by retailer R injures a pedestrian on the street. It remains unclear which of the following possible causes triggered the accident: the robot may have been defective from the start; R may have failed to install a necessary update that would have prevented the accident; R's employee E may have overloaded the robot; hacker H may have intentionally manipulated the robot; some teenagers may have jumped onto the robot for fun; a roof tile may have fallen off a nearby building, and so on.*[118] *If the likelihood of all possible causes that are attributable to R significantly exceeds the likelihood of all other possible causes, the onus should be on R to prove that none of the causes within its own sphere triggered the accident.*

- Considering further aspects that relate to the analysis of the causal events and who is (or should be) predominantly in control of the expertise and evidence contributing to such analysis, one could consider the **informational asymmetry** typically found between those developing and producing emerging digital technologies on the one hand and third-party victims on the other hand as another argument in the overall assessment of who should bear the burden of proving causation and to what extent. This includes the technology itself, but also **potential evidence generated by such technology** on the occasion of the harmful event. The latter not only considers who can retrieve such data, but also who can read and interpret

condition if such an error was grave and in principle prone to causing such harm. See also the Dutch *omkeringsregel*; cf A Keirse, 'Going Dutch: How to Address Cases of Causal Uncertainty', in I Gilead/M Green/BA Koch (eds), *Proportional Liability: Analytical and Comparative Perspectives* (2013) 227 (232).

118 Cf the hypothetical used by the Commission Staff Working Document (fn 8) 12.

it (particularly if it is encrypted or only intelligible with specific expert knowledge). One specific aspect in this context is if an item that was involved in the harmful event did (or according to industry standards should) have some logging device installed, which could have collected information that is capable of shedding light on what actually happened.[119]

- Finally, as is already commonly used as one weighty argument in the overall balance of interests in tort cases, the **type and extent of harm** may also contribute to deciding to what extent it should still be the victim who proves the cause of her damage.[120]

12. Burden of proving fault ([27])

[27] If it is proven that an emerging digital technology caused harm, and liability therefor is conditional upon a person's intent or negligence, the burden of proving fault should be reversed if disproportionate difficulties and costs of establishing the relevant standard of care and of proving their violation justify it. This is without prejudice to the reversal of the burden of proof proposed in [22] and [24](b).

When the damage results from an activity in which emerging digital technologies play a role, the victim may face significant difficulties in proving facts that substantiate her damages claim based on negligence or fault. This justifies rethinking the traditional approach to proving these conditions of liability.

Adopting any rule concerning the distribution of the burden of proving fault requires explaining fault in the first place. There is a variety of meanings attached to this word in various legal systems, ranging from equating fault with wrongfulness of conduct to understanding fault as purely individual and subjective blameworthiness.[121] Thus fault-based liability requires:

a) always a breach of a certain duty of care (standard of conduct);

b) in some (probably most) jurisdictions, an intent to breach this duty of care or negligence in so doing;

c) in some (probably the minority of) jurisdictions, a negative ethical assessment of the tortfeasor's conduct as subjectively reprehensible.

The **standard of conduct** may be set by the statute or otherwise normatively prescribed in the form of regulatory measures or standards and norms enacted by competent authorities. However, it may also be established ex post by the court, on the basis of general criteria such as reasonableness, diligence, etc.

Emerging digital technologies, in particular the presence of AI, change the structure of fault-based liability. The two most prominent examples of applying fault-based liability to AI-related

119 See also [22].

120 As expressed by Article 2:101 paragraph 1 PETL, '[t]he scope of protection of an interest depends on its nature; the higher its value, the precision of its definition and its obviousness, the more extensive is its protection.'

121 See P Widmer, 'Comparative Report on Fault as a Basis of Liability and Criterion of Imputation (Attribution)', in P Widmer (ed), *Unification of Tort Law: Fault* (2005), 331 ff.

damage are the liability of the producer for damage caused by the product he has produced, should have monitored, etc. (liability outside the scope of a strict liability regime such as the one envisaged under [13]-[15] above) and liability of the user (operator) for damage caused by him while using an AI-driven tool.

In the case of the producer's liability (outside strict product liability), the direct cause of damage is a product, but the damaging features of the product are the effect of the producer's negligence in designing, manufacturing, marketing, monitoring, etc., the product. Thus, proving fault requires proving that the product was not of a required quality and that the producer intentionally or negligently breached an applicable standard of conduct with regard to this product. The advance of emerging digital technologies increases evidentiary difficulties in relation to:

- the quality requirements for the product and details of its actual operation that has led to the damage;
- breach of a duty of care on the part of the producer with regard to the product (including the applicable standard of conduct);
- facts that allow the court to establish that breach of the duty of care was intentional or negligent.

As far as the user's liability is concerned, the overall structure of liability for actions performed using tools is the following:

an actor + the use of a tool an act *[wrongfulness/fault]*	⇨ causation	victim damage *[protected interest]*

The challenge of the fault analysis in the traditional model is the assessment of the actor's behaviour with regard to: (i) his decision to act; (ii) his decision to use a tool at all, (iii) his choice of tool, (iv) his way of using it or controlling or monitoring its operation.

Thus the actor is at fault if: (i) his decision on the action itself is wrong and there is intent or negligence in making this decision, or (ii) his decision about using a tool in the action instead of performing it himself is wrong and there is intent or negligence in making this decision, or (iii) his choice of tool is faulty (he chooses the kind of tool that is unsuitable to the task or the right tool he has chosen subsequently malfunctions) and there was intent or negligence in making this choice, or (iv) he uses his tool or controls/monitors its operation incorrectly and there is intent or negligence in this behaviour.

Under the general rule of liability, the burden of proving both breach of a duty of care and intent or negligence lies with the victim.

In the traditional model, the proper functioning of the tool and the expected outcome of its operation are known and easy to establish and details of the tool's actual performance are usually not too difficult to examine. Because of their fast development and their features, described above (opacity, openness, autonomy and limited predictability), emerging digital technologies used as tools add further layers of complexity to the fault-based liability model, challenging the operation of fault-based liability rules on two levels:

a) a structural level: the autonomy and self-learning capacity of the technology may be seen as breaking the causal link between the actor's conduct and the damage – this is the problem of attribution of the operation and its outcome to a person, which should be solved by legally ascribing all the emerging digital technology's actions and their effects to the operator of the technology (cf [18]).

b) a practical, fact-finding level: facts on which liability is dependent may be hard to discover and communicate to the court. The difficulty may be:

- finding out and explaining to another person how a given set of input data resulted in the outcome of the AI-operated process and that this amounted to a deficiency in the system;
- showing the tortfeasor breached a standard (level) of care in deciding to use this particular emerging digital technology in this concrete situation, or in operating/monitoring it;
- establishing that the breach of this standard was intentional or negligent.

In theory, the claimant has to prove that the defendant breached an applicable standard (level) of care and did so intentionally or negligently. In practice, however, if the standard of care has not been normatively prescribed (by a statute or otherwise), the claimant's burden extends to proving (or persuading) what level of care should apply to the defendant's behaviour. The lack of a clear standard therefore puts the party with the burden of proving the existence of the standard, or its breach, at a disadvantage.

The question is thus whether all these evidentiary difficulties should remain with the victim or all or some of them, in all or in specific circumstances, should affect the defendant.

Items of proof, the burden for which normally is on the claimant, but could be allocated to the defendant are:

- breach of a duty of care by the defendant (the producer, with regard to designing, manufacturing, monitoring, etc., and the user with regard to the choice of technology and operating/monitoring it),
- intention or negligence of the defendant,
- substandard qualities of the technology,
- incorrect functioning of the technology.

In various legal systems, various **factors** are recognised as justifying modification of the burden of proof in favour of the claimant, in particular:

a) high likelihood of fault,

b) the parties' practical ability to prove fault,

c) violation of statutory obligation by the defendant,

d) particular dangerousness of the defendant's activity that resulted in damage,

e) nature and scope of the damage.

There are also various legal techniques for doing this, from the statutory reversal of the burden of proof to all sorts of procedural tools such as *prima facie* evidence, presumptions in fact, adverse inference and so on.

Features of emerging digital technologies such as opacity, openness, autonomy and limited predictability may often result in unreasonable difficulties or costs for the plaintiff to prove facts necessary for the establishment of fault. At the same time, the proof of relevant facts may be much easier for the defendant (producer or operator of the technology). This asymmetry justifies the reversal of the burden of proof. While, as mentioned above, in many cases courts may achieve similar results with various procedural arrangements, the introduction of a clear rule will ensure the desired convergence and predictability in the application of the law.

13. Causes within the victim's own sphere ([28])

[28] If a cause of harm is attributable to the victim, the reasons for holding another person liable should apply correspondingly when determining if and to what extent the victim's claim for compensation may be reduced.

While jurisdictions throughout Europe already now acknowledge that conduct or some other risk within the victim's own sphere may reduce or even exclude her claim for compensation vis-à-vis another, it seems important to state that whatever the NTF of the Expert Group proposes to enhance the rules on liability for emerging digital technologies should apply accordingly if such technologies are being used within the victim's own sphere. This is in line with the so-called "**mirror image**" rule of contributory conduct.[122] Therefore, if two AVs collide, for example, the above-mentioned criteria for identifying the liable operator ([10]-[11]) should apply correspondingly to determining what effect the impact of the victim's own vehicle on her loss has on the liability of the other AV's operator.

14. Commercial and technological units ([29]–[30])

[29] Where two or more persons cooperate on a contractual or similar basis in the provision of different elements of a commercial and technological unit, and where the victim can demonstrate that at least one element has caused the damage in a way triggering liability but not which element, all potential tortfeasors should be jointly and severally liable vis-à-vis the victim.

[122] Cf comment 5 on Article VI-5:102 DCFR (The mirror principle) and M Martín Casals/U Magnus, 'Comparative Conclusions', in M Martín Casals/U Magnus (eds), *Unification of Tort Law: Contributory Negligence* (2004) 259 (263 ff), highlighting that this mirror is quite 'blurred' (at 264).

[30] In determining what counts as a commercial and technological unit within the meaning of [29] regard is to be had to

(a) any joint or coordinated marketing of the different elements;

(b) the degree of their technical interdependency and interoperation; and

(c) the degree of specificity or exclusivity of their combination.

Among the many challenges for victims of emerging digital technologies is the challenge of showing what part of a complex digital ecosystem has caused the damage. This may be particularly hard where different elements have been provided by different parties, creating a significant risk for the victim of suing the wrong party and ending up with no compensation and high litigation costs. It is therefore justified to have special rules for situations where two or more parties cooperate on a contractual or similar basis in the provision of different elements of one and the same digital ecosystem, forming a **commercial and technological unit**. In these situations, all potential tortfeasors should be jointly and severally liable towards the victim where the victim can demonstrate that at least one element has caused the damage in a way triggering liability, but not which element.

> ***Illustration 20.*** *A smart alarm system produced by manufacturer A was added to a smart home environment produced by B and set up and installed by C. This smart home hub runs on an ecosystem developed by provider D. A burglary occurs, but the police is not duly alerted by the alarm system, so significant damage is caused.*[123] *A, B and D are linked by sophisticated contractual arrangements concerning the interoperation of the relevant components each of them supplies and any related marketing. If it can be shown that the malfunctioning was not caused by C (or an external cause), but if it remains unclear what the situation is between A, B and D, the home owner should be able to sue A, B and D jointly. Any one of them is free to prove in proceedings that it was not the commercial and technological unit that caused the malfunctioning, but if not, the home owner can hold them jointly and severally liable.*

The rationale behind this is, on the one hand, that there might be serious undercompensation of victims in an emerging digital technologies scenario as compared with the functionally equivalent situation of the past when alarm systems used to be manufactured by one clearly identifiable producer (and any responsibility on the part of the suppliers of components would have come on top of that) without any significant interaction with the other components of an ecosystem. This may even create false incentives, as providers might be tempted to artificially split up the ecosystems they provide into independent components, thereby obscuring causal links and diluting responsibility. In any case, it should not be the victim who ultimately bears the risk of a particular internal structure on the provider's side in a situation where there could just as well have been one provider. It is also more efficient to hold all potential injurers liable in such cases, as the different providers are in the best position to control risks of interaction and interoperability and to agree upfront on the distribution of the costs of accidents.

[123] Based on the example used in the Commission Staff Working Document (fn 8) 15 f.

It may be difficult, in borderline cases, to define what still qualifies as a commercial and technological unit. **Factors** to be taken into account will be, primarily, any joint or coordinated marketing of the elements, but also the degree of technical interdependency and interoperation between the elements and the degree of specificity or exclusivity of their combination.

> ***Illustration 21.*** *Imagine there was, in Illustration 20, also network provider E who could have caused the problem because of a temporary interruption of the internet connection. However, smart home equipment normally just needs network connectivity, but not network connectivity from a particular provider, and enhanced cooperation between A, B and D on the one hand and E on the other cannot be expected by the consumer. Things might be different in the rather exceptional case that this was in fact offered as a package, with E marketing her services on the strength of their being particularly reliable as a basis for this type of smart home ecosystem.*

Commercial and technological units may also become relevant at the **stage of redress** between multiple tortfeasors, whether or not the notion of commercial and technological units had already been relied on by the victim (see [31]).

15. Redress between multiple tortfeasors ([31])

[31] Where more than one person is liable for the same damage, liability to the victim is usually solidary (joint). Redress claims between tortfeasors should only be for identified shares (several), unless some of them form a commercial and/or technological unit ([29]-[30]), in which case the members of this unit should be jointly and severally liable for their cumulative share also to the tortfeasor seeking redress.

One of the most pressing problems for victims in modern digital ecosystems is that, due to enhanced complexity and opacity, they often cannot find out and prove which of several elements has actually caused an accident (the classic **alternative causation scenario**).

> ***Illustration 22.*** *A patient's artery is cut by an AI-driven surgical robot either due to a failure of the surgeon operating the robot, or due to the wrong execution of the surgeon's movements by the robot. If so, neither of the two potential causes satisfies the* conditio sine qua non *test ('but for' test), because if either one of them is hypothetically disregarded, the damage may still have been caused by the remaining respective other event(s). The consequence would be that neither of these suspected reasons why the victim was harmed could trigger liability, so the victim could – at least in some legal systems – end up without a claim for compensation, despite the known certainty that one of the two or more events was indeed the cause of damage.*

Legal systems in the Member States react very differently to such scenarios, and each solution has its own drawbacks.[124] Where a person caused damage to the victim and the same damage

[124] The PETL have opted for the solution that each of multiple potential tortfeasors should only be held liable for a share of the total loss that corresponds to the probability that it might have been them, which – in cases where this share cannot be determined – typically means per capita: Article 3.103 paragraph 1 PETL provides: 'In case of multiple activities, where each of them alone would have been sufficient to cause the damage, but

is also attributable to another person, the liability of multiple tortfeasors is **normally joint liability**,[125] i.e. the victim may request payment of the full sum or part of the sum from any of the multiple tortfeasors, at the victim's discretion, but the total sum requested may not exceed the full sum due. There may **exceptionally** be situations where there is a reasonable basis for attributing only part of the damage to each of the tortfeasors, in which case liability may also be **several**.[126] At the redress stage, liability of other tortfeasors towards the tortfeasor who has paid damages to the victim is normally several, i.e. other tortfeasors are liable only for their individual share of responsibility for the damage.[127] There is no reason to deviate from these principles in the context of emerging digital technologies, and this is why [31] suggests several liability at the redress stage as a general rule.

However, the complexity and opacity of emerging digital technology settings that already make it difficult for a victim to get relief in the first place also make it difficult for the paying tortfeasor to identify shares and seek redress from the other tortfeasors. However, despite complexity and opacity, it is often possible to identify two or several tortfeasors who form a commercial and/or technological unit (see [29]-[30]). This should be relevant at the redress stage too, i.e. members of that unit should be liable jointly to indemnify another tortfeasor who is not a member of the unit and has paid damages to the victim exceeding his share.

> ***Illustration 23.*** *The producer of hardware has a contract with a software provider and another one with the provider of several cloud services, all of which have caused the damage, and all of which collaborate on a contractual basis. Where another tortfeasor has paid compensation to the victim and seeks redress, the three parties may be seen as a commercial unit, and the paying tortfeasor should be able to request payment of the whole cumulative share from any of the three parties.*

As has been explained in the context of [29]-[30]), this is also in the interests of efficiency, as parties are **incentivised to make contractual arrangements** for tort claims in advance.

---

it remains uncertain which one in fact caused it, each activity is regarded as a cause *to the extent corresponding to the likelihood* that it may have caused the victim's damage.' (emphasis added).

This proportional (or several) liability leads to an overall fairer outcome when looking at all parties involved, but the victim is at least worse off insofar as she will have to collect compensation from all potential injurers and bear the risk of each injurer's insolvency. See the comparative in-depth analysis of this way of dealing with causal uncertainty in I Gilead/MD Green/BA Koch (eds), *Proportional Liability: Analytical and Comparative Perspectives* (2013).

125 Cf Article 9:101 paragraph 1 PETL.

126 Cf Article 9:101 paragraph 3 PETL.

127 Cf Article 9:102 paragraph 4 PETL.

16. Damage to data ([32])

[32] Damage caused to data may lead to liability where

(a) liability arises from contract; or

(b) liability arises from interference with a property right in the medium on which the data was stored or with another interest protected as a property right under the applicable law; or

(c) the damage was caused by conduct infringing criminal law or other legally binding rules whose purpose is to avoid such damage; or

(d) there was an intention to cause harm.

In terms of damage caused, the emergence of digital technologies has brought about some gradual shifts, but only little disruptive change. There is one exception, which is strictly speaking likewise a gradual change, but whose dimension is such that it may be considered disruptive: the significance of damage to data, such as by the deletion, deterioration, contamination, encryption, alteration or suppression of data. With much of our lives and our 'property' becoming digital, it is no longer appropriate to limit liability to the tangible world. However, neither is it appropriate to simply equate data with tangible property for the purposes of liability.

Most legal systems do not have much of an issue when it comes to **contractual liability**, in particular where there was negligence of the contracting partner.

> ***Illustration 24.*** *A stores all her files in cloud space provided by cloud space provider C on the basis of a contract. C has failed to properly secure the cloud space, which is why an unknown hacker deletes all of A's photos. C will normally be liable to A on a contractual basis. Liability would in any case be for the economic loss, e.g. any costs A has to incur for restoring the files. Whether or not A would receive compensation for the non-economic loss associated with the loss of family memories would depend on the national legal system in question.*

Things are less obvious for liability in tort, at least in a number of jurisdictions. For a long time, some jurisdictions have been solving the issue by considering damage to data as damage to the **physical medium** on which the data was stored. This should still be possible.

> ***Illustration 25.*** *Imagine A had stored all her files on her personal computer's hard disk drive at home. Neighbour B negligently damages the computer, making the files illegible. Irrespective of the qualification of damage to data, this was in any case unlawful damage to A's tangible property (the hard disk drive), and already for this reason B would be liable.*

However, this approach does not lead to satisfactory results where the owner of the medium is not identical with the person who has a protected legal interest in the data.

The most difficult question is what amounts to a protected legal interest that is sufficiently akin to property. The NTF of the Expert Group discussed in some depth whether there should also be liability in tort where the relevant data was protected by **intellectual property** law or a

similar regime, such as database protection or trade secret protection. However, at the end of the day it does not seem to make sense to focus on IP protection, because the reasons the legislator introduces IP rights for intellectual achievement have little to do with the reasons a particular copy on a particular medium should be protected.

> ***Illustration 26.*** *A has all her files stored in cloud space provided by C. Without any negligence on C's part, B negligently damages C's servers and all of A's files are deleted. It is not clear why it should make a difference to B's liability whether (a) the files contained text or photos to which A held the copyright, (b) the files contained text or photos to which third parties held the copyright, or (c) the files contained machine data of great economic value, to which nobody held any copyright or other IP right.*

Depending on the applicable legal system, there may, however, be other legal interests that are protected with third-party effect (not only against a contracting party or other particular party), such as possession.

Data being sufficiently akin to property is just one of the justifications for recognising tort liability where data has been damaged. Alternatively, there should be liability where the damage has been caused by conduct amounting to a criminal act, in particular an **activity that is unlawful** under international law such as the Budapest Convention on Cybercrime,[128] or where it has infringed other conduct-related rules such as product safety legislation whose purpose is to avoid such damage.

> ***Illustration 27.*** *If B in Illustration 26 hacks the cloud space and deletes A's files, this normally qualifies as criminal conduct and B should be liable.*

This purpose should ideally be expressed by the language of such legislation. One example, where it has been made very clear, is the General Data Protection Regulation (GDPR). Article 82 explicitly states that there is liability where damage has been caused by infringing the requirements of the GDPR.

In defining such **conduct-related rules** the law should give due consideration, in particular, to the ubiquity of data and its significance as an asset. While it would theoretically be possible to introduce, for example, a standard stating very broadly that it is generally prohibited to access, modify etc. any data controlled by another person and to attach liability if this standard is breached, this might result in excessive liability risks because all of us are, in one way or another, constantly accessing and modifying data controlled by others.

Last but not least, most jurisdictions would agree that damage to data should lead to liability where the tortfeasor was acting with an **intention** to cause harm.

[128] Convention on Cybercrime, Council of Europe Treaty No. 185, 23 November 2001 ('Budapest Convention').

17. Insurance ([33])

[33] The more frequent or severe potential harm resulting from emerging digital technology, and the less likely the operator is able to indemnify victims individually, the more suitable mandatory liability insurance for such risks may be.

Statutory strict liability regimes in particular[129] often come with a requirement that the person to whom the risk is attributable must take out **insurance** cover against her risk of liability. This is typically explained with a need to protect future victims against the **risk of the liable person's insolvency**.[130] However, from an economic analysis point of view, the insurance requirement rather fosters the internalisation of the costs of the activities that the liable person (permissibly) pursues.[131]

Either way, compulsory liability insurance should not be introduced without a careful analysis of whether it is really needed, rather than automatically linked to a certain activity. After all, the tortfeasor may be able to compensate victims of her activities out of her own funds if the overall losses to be expected can be covered even without insurance. Also, the market may simply not offer insurance cover for a certain risk, particularly if it is difficult to calculate due to missing experience, which is quite likely with new technologies (and may therefore also be a problem with emerging digital technologies). Requiring insurance in the latter situation may effectively prevent the deployment of the technology, if this requires proof of insurance despite the fact that no-one on the market is willing to underwrite such yet unknown risks.

This may in part be remedied by **capping liability** for certain risks at a pre-determined (though regularly adjusted) amount, as is often the case with statutory strict liability regimes. One could also imagine a less specific requirement to provide cover (so not necessarily by taking out insurance, but also other financial securities).[132]

Nevertheless, as experience in at least some fields (mostly motorised traffic) has shown, mandatory liability insurance can work well and is indeed appropriate under certain conditions. From an insurance perspective, certain sectors are the most suited to **compulsory insurance**

---

129 Mandatory liability insurance is by no means exclusively linked to strict liability; see the extensive list of statutory insurance requirements for both strict and fault liability in A Fenyves et al (eds), *Compulsory Liability Insurance from a European Perspective* (2016) 445 ff.

130 D Rubin, 'Conclusions', in Fenyves (fn 129) 431. Cf also the Commission Staff Working Document (fn 8) 21: '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.'

131 M Faure, 'Economic Criteria for Compulsory Insurance', The Geneva Papers on Risk and Insurance 31 (2006) 149, who also highlights at 158 'that lawyers often view especially third-party insurance as an instrument of victim protection, whereas economists would stress the fact that insurance is an instrument to remove risk from the risk-averse injurer or to cure the risk of underdeterrence'.

132 D Rubin (fn 130) 436; M Faure (fn 131) 162 f.

schemes, including transportation, industries with a high potential for personal injury and/or environmental harm, hazardous activities and certain professional sectors.[133]

Therefore, it may indeed be advisable to make liability insurance cover compulsory for certain emerging digital technologies. This is particularly true for highly significant risks (which may either lead to substantial harm[134] and/or cause frequent losses), where it seems unlikely that potential injurers will be capable of compensating all victims themselves (either out of their own funds, with the help of alternative financial securities, or through voluntary self-insurance).

If mandatory liability insurance is introduced, the insurer should have a recourse claim against the tortfeasor. In risk scenarios comparable to those of motorised traffic, a direct action of victims against the insurer may also be advisable.[135]

18. Compensation funds ([34])

[34] Compensation funds may be used to protect tort victims who are entitled to compensation according to the applicable liability rules, but whose claims cannot be satisfied.

If liability regimes described above (producer's and operator's strict liability and wrongdoer's fault-based liability) function properly, there is no need to establish new kinds of compensation funds, funded and operated by the state or other institutions and aiming to compensate victims for losses suffered as a result of operating emerging digital technologies. It is advisable, however, to ensure that in the areas where compulsory liability insurance is introduced, a compensation fund is also in place to redress damage caused by an **unidentified or uninsured technology**.[136] Article 10 of the Motor Insurance Directive may serve as a model for such a scheme.

As hacking is a serious threat to users of software-based technologies and traditional tort law rules may often prove insufficient because of the victim's **inability to identify the tortfeasor**, it may be advisable to introduce a non-fault compensation scheme equivalent to that applicable to victims of violent crimes,[137] if and to the extent that a cybercrime constitutes an offence

---

133 B Tettamanti/H Bär/J-C Werz, 'Compulsory Liability Insurance in a Changing Legal Environment – An Insurance and Reinsurance Perspective', in Fenyves (fn 129) 343 (359).

134 However, one should keep in mind that the risk of extremely high or even catastrophic losses may not be (fully) insurable and require, for example, a public-private partnership, as experience in the US has shown with covering the risks of nuclear power plants (<https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/nuclear-insurance.html>).

135 Cf Article 15:101 Principles of European Insurance Contract Law (PEICL).

136 This is also supported by the EP Resolution on 'Civil Law Rules on Robotics' (fn 4), no 59 lit b. However, Parliament also suggests to expand the scope of a compensation fund in lit c, combining it with limited liability of those contributing to such a fund. In lit d, Parliament considers 'to create a general fund for all smart autonomous robots' or individual funds per category of robots. Such proposals are also put forward in academic writing, see, for example, K Abraham/R Rabin, 'Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era', <https://papers.ssrn.com/sol3/papers. cfm? abstract_id= 3151133>.

137 Under national implementations of Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims.

equivalent to the latter. Persons who have suffered serious personal injuries as a result of cybercrime could therefore be treated the same way as victims of violent crime.

Annex: The New Technologies Formation of the Expert Group on Liability for New Technologies

Members

- Ryan ABBOTT (United Kingdom/United States of America)
- Georg BORGES (Germany)
- Eugenia DACORONIA (Greece)
- Nathalie DEVILLIER (France)
- Marlena JANKOWSKA-AUGUSTYN (Poland)
- Ernst KARNER (Austria)
- Bernhard Alexander KOCH (Austria)
- Alžběta KRAUSOVA (Czech Republic)
- Piotr MACHNIKOWSKI (Poland)
- Maria Lillà MONTAGNANI (Italy)
- Marie MOTZFELDT (Denmark)
- Finbarr MURPHY (Ireland)
- Ugo PAGALLO (Italy)
- Teresa RODRIGUEZ DE LAS HERAS BALLELL (Spain)
- Gerald SPINDLER (Germany)
- Christiane WENDEHORST (Austria/Germany)

Institutional Observers from the Product Liability Formation

- Cooley (UK) LLP (United Kingdom)
- Universidad Carlos III de Madrid (Spain)

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

DS-03-19-853-EN-N

Publications Office
of the European Union

ISBN 978-92-76-12959-2
doi: 10.2838/573689