Società italiana degli studiosi del diritto civile

15° Convegno Nazionale

"Rapporti civilistici e intelligenze artificiali: attività e responsabilità"

dal 14 al 16 maggio 2020, Napoli.

New reflections on civil liability in the use of artificial intelligence arising from the "Liability for Artificial Intelligence and other Emerging Digital Technologies" report.

Cecilia Celeste Danesi[1]

Index:

---

[1] Attorney at Law. LLM in Damages Law. School of Law, University of Girona (Spain). Scholarship granted by Carolina Foundation (Spain). Thesis: "Damages caused by artificial intelligence: autonomous vehicles." Visiting researcher and professor at the Universities of Oxford, Perugia and Salamanca. Researcher and professor of "Civil and Commercial Obligations" and "Artificial Intelligence and Law", School of Law, University of Buenos Aires. PhD student, University of Perugia (research topic: "Artificial Intelligence and Consumer Law"). Author of the book "Traffic accidents" and publisher of several academic papers. Lecturer in congresses.

I.- Introduction.

Speaking about artificial intelligence does not mean we are keen on futurology. It means we focus on the present and cautiously tackle the immediate future. This phenomenon is here to stay and will indisputably impact and change different spheres of our society, such as medicine, transportation, education, the military, the economy, senior care, to name a few.

This technological irruption calls for the legal experts to critically think over and analyse the core of their foundations with the hopes of determining if the legal system is capable of embracing the peculiarities presented by this new phenomenon.

With this purpose in mind, one of the areas deserving an immediate spotlight is civil liability (as pointed out by the European Union[2],) since AI lands on people's lives with a worrying "damaging potentiality", at least at first sight. This is the reason why our work hopes to go back[3] on the study of damages caused by the use of artificial intelligence, and why we will carefully break down the recent report: "Liability for Artificial Intelligence and other Emerging Digital Technologies"[4] (known as "the report" from now on) written by the Expert Group on Liability and New Technologies from the European Union. Without a doubt this means a milestone in the matter.

II.- Towards a concept of artificial intelligence

Defining "artificial intelligence" proves to be quite hard since there is no consensus surrounding it. We believe this has to do with two factors. On the one hand, it is a technology which is constantly moving forward, and it is, therefore, not easy to find a concept that will comprise this constantly growing phenomenon. On the other, AI poses the peculiar trait of being interdisciplinary. Just as we pointed out during the introduction, it encompasses and performs thousands of roles in diverse fields. Again, it is not easy to find a definition that will fit all of them.

The Report with recommendations to the Commission on Civil Law Rules on Robotics[5] states it is necessary to coin a definition overall accepted for robots and artificial intelligence that will be flexible and not hinder innovation. It additionally stresses the possibility of artificial intelligence outperforming the human intellect in the long run.

John McMarthy, known as the one who coined the term artificial intelligence, defined it as a process consistent in making a machine behave in ways that could be called intelligent if a human being performed them[6]. This is carried out thanks to algorithms constituting a sequence of logical steps, i.e. something similar to a cooking recipe.

It is actually vitally important to understand what an algorithm is. Harari explains that the 21st century will be dominated by them. If we wish to comprehend our lives and future, we must make every possible effort to understand what these are, and how they are connected with our emotions. He defines them as a methodical group of steps that can be employed to make

---

[2] Report with recommendations to the Commission on Civil Law Rules on Robotics, Committee on Legal Affairs (27/01/17), avilable 06/12/19 at http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html.

[3] Danesi, Cecilia C., "Who is responsible for the damages caused by robots? La Ley (Thomson Reuters), Civil Liability and Insurance Publication, November 2018 and "Artificial Intelligence and Tort Law, focusing on autonomous vehicles", LegalTech Special Edition, La Ley (Thomson Reuters), December 2018.

[4] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019.

[5] Report with recommendations to the Commission on Civil Law Rules on Robotics, Committee on Legal Affairs (27/01/17), available Dec 6th, 2019 at http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html.

[6] Kaplan, Jerry, Inteligencia Artificial, lo que todo el mundo debe saber, Oxford University Press, Teell, España, 2017, page 1.

calculations, solve problems and make decisions. An algorithm is not an accurate calculation, but the method followed when making a calculation[7].

The most salient characteristics of artificial intelligence (and the ones inviting us to reflect the most) are its autonomy and self-learning capability. This means AI will make decisions without outside intervention or control, and that it will also learn from such interactions to modify predictions in the future. The report under study highlights the following characteristics of emerging technologies: complexity, opacity, openness, autonomy, predictability, data-drivenness, and vulnerability[8].

We should also talk about the Opinion of the European Economic and Social Committee "Artificial intelligence – The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society."[9] Even though they acknowledge the lack of uniformity in the definition of AI, it evidences that the central aim of AI research and development is, however, to automate intelligent behaviour, such as reasoning, the gathering of information, planning, learning, communicating, manipulating, detecting and even creating, dreaming and perceiving[10].

III.- Artificial intelligence and civil liability: a match with an uncertain game score.

As commonly known, there are different civil liability systems depending on the different legal systems. Although several instruments have been created to harmonize them[11], truth is we deal with considerable discrepancies between countries.

The European continent does not escape this reality. Some legal systems are "classic" in the sense that they either arise from a list of protected interests (Germany,) or else classify civil offences, where the commission later gives room for liability (English case.) Indeed, these systems are not entirely closed since, one way or another, a valve is necessary (such as the § 823 (2) German BGB or the *tort of negligence*) to make it possible to palliate such an excessive rigidness. Nonetheless, this flexibility is only marginal and has little to do with systems like the Spanish or French ones, which begin with the existence of a general fault-based liability clause, and leave the

---

[7] Harari, Yuval Noah, Homo Deus Breve Historia del Mañana, Ed. Debate, 2015, Buenos Aires, page 100.

[8] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019, page 5.

[9] Opinion of the European Economic and Social Committee "Artificial intelligence – The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society", available Dec 6th, 2019 at http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.C_.2017.288.01.0001.01.SPA&toc=OJ:C:2017:288:TOC .

[10] It is also affirmed that AI is a catch-all term for a large number of sub(fields) such as: cognitive computing (algorithms that reason and understand at a higher (more human) level), machine learning (algorithms that can teach themselves tasks), augmented intelligence (cooperation between human and machine) and AI robotics (AI imbedded in robots). Additionally, there is a distinction between 2.2 AI is broadly divided into narrow AI and general AI. Narrow AI is capable of carrying out specific tasks. General AI is capable of carrying out any mental task that can be carried out by a human being. Moreover, the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence (AI) explains that AI refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).

[11] The American Law Institute, Restatement of The Law Third Torts: Liability for Physical and Emotional Harm, Vol. 1, USA, 2010; European Principles on Tort Law, European Groupon Tort Law, available Dec 6th, 2019 on http://www.egtl.org/ and; Regulation (EC) N° 864/2007 of the European Parliament and of the Counsil of 11 july 2007 on the Law applicable to non-contractual obligations (Rome II).

task of creating regulations and the criterion needed to point out which cases lead to liability to jurisprudence and doctrine[12].

Across the European Union, although with some common dispositions,[13], there is no uniformity in terms of the normative applicable to cases with damages caused by artificial intelligence. Mainly, several of these regulations will be affected by breakthroughs in robotics, cyber physical systems and AI[14]. This evidences the indisputable need to analyse this phenomenon and also explains the reason behind the creation of the Expert Group on Liability and New Technologies, whose interesting report will be discussed next[15].

IV.- Giving AI systems a status of electronic legal persons.

Making an autonomous system an electronic legal person is not a mere illusion of science fiction. Some legal systems have already taken this road. For example, Saudi Arabia awarded legal persona citizenship to a humanoid robot named Sophia[16]. Still, this proposal has received different contradictory opinions, even across the European Union.

The Report with recommendations to the Commission on Civil Law Rules on Robotics hopes to analyse the possibility of creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots can be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently[17].

Quite on the contrary, the report with recommendations to the Commission on Civil Law Rules on Robotics opposes to any form of legal status for robots or AI (systems), as this entails an unacceptable risk of moral hazard. Liability law is based on a preventive, behaviour-correcting function, which may disappear as soon as the maker no longer bears the liability risk since this is transferred to the robot (or the AI system). There is also the risk of inappropriate use and abuse of this kind of legal status. The comparison with the limited liability of companies is misplaced, because in that case a natural person is always ultimately responsible[18].

The report under study follows this last stance. It highlights that any "harm caused by even fully autonomous technologies is generally reducible to risks attributable to natural persons or

---

[12] Casals, Miquel Martín, "Una primera aproximación a los "Principios de Derecho europeo de la responsabilidad civil", InDret, Barcelona, 2/2005, available Dec 6th, 2019 on http://www.indret.com/pdf/284_es.pdf.

[13] Product Liability Law under Directive 85/374/EC; 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) (art. 82); Liability for infringing competition law (Directive 2014/104/EU 19); Directive 2009/103/EC, Insurance against Civil Liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability; Regulation (EC) N° 864/2007 of the European Parliament and of the Counsil of July 11th 2007 on the Law applicable to non-contractual obligations (Rome II).

[14] See report by the European Parliament's STOA from June 2016, available Dec 5th, 2019 on http://www.europarl.europa.eu/RegData/etudes/STUD/2016/563501/EPRS_STU(2016)563501(ANN)_EN.pdf.

[15] Given the extension of the report, we will only analyze matters we believe to be the most relevant.

[16] Hanson Robotics, avilable Dec 5th, 2019 on http://www. hansonrobotics.com/robot/sophia/ y http://sophiabot.c

[17] Report with recommendations to the Commission on Civil Law Rules on Robotics, Committee on Legal Affairs (27/01/17), page 18, available Dec 6th, 2019 on http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html.

[18] Opinion of the European Economic and Social Committee "Artificial intelligence – The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society", page 10, available Dec 6th, 2019 on http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.C_.2017.288.01.0001.01.SPA&toc=OJ:C:2017:288:TOC
..

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"[19]. It also adds that any sort of legal personality for emerging digital technologies may raise a number of ethical issues and that, 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.

Accordingly, we agree with the report's opinion since regulations on risky activities or things (existing in some countries[20]) or those applicable to defective products or consumers are enough –*for now*- to apply to damages caused by AI. We should emphasize on the "so far" trait, since technological discoveries, the way they irrupt in societies, and, mainly the way in which they affect people's lives might invite us to re-evaluate this idea in the future and think otherwise. Fortunately, the law is not rigid.

V.- Directive on defective products.

The first issue that was debated surrounding the mentioned Directive was whether its enforcement was appropriate – or not. Art. 2 establishes that "product" means all movables, and therefore, AI systems do not meet this requirement. For example, those lent through via the cloud were apparently excluded. However, the different documents discussing this consider the directive can be indeed applicable to AI systems.

The report with recommendations to the Commission on Civil Law Rules on Robotics from 27/01/2017 estimates that even if such directive were to be applied, it "would not be sufficient to cover the damage caused by the new generation of robots, insofar as they can be equipped with adaptive and learning abilities entailing a certain degree of unpredictability in their behaviour, since those robots would autonomously learn from their own variable experience and interact with their environment in a unique and unforeseeable manner"[21].

Likewise, the report by the Expert Group on Liability and New Technologies affirms that 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[22].

A while ago, we presented the following considerations – still current today – regarding the studied Directive. In the first place, in terms of the defence foreseen in Art. 7[23], we highlight that any breakthroughs in AI are continuous. This means knowledge in a determined field might present considerable growth in a short period of time, making the system quickly obsolete. But what is truly relevant for these systems is that they are permanently connected to the Internet, and must receive updates daily[24]. This is why this defence could not be applied to these cases.

---

[19] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019, page 102 .

[20] See ap. VI.

[21] Report with recommendations to the Commission on Civil Law Rules on Robotics, Committee on Legal Affairs (27/01/17), page 7, available Dec 6th, 2019 on http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html.

[22] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019, pages 42/43.

[23] The producer shall not be liable as a result of this Directive if he proves: (e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered.

[24] Digital technology products are open to software extensions, updates and patches after they have been put into circulation. Any change to the software of the system may affect the behaviour of the entire system or of individual components or may extend its functionality. Software can be patched, updated or revised, by the producer of the system

This exact reasoning is admitted in the studied report, which stresses that the producer is still in control of updates to, or upgrades on, the technology. It also points out that the development risk defence should not apply. It explains that when the defect comes 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. Also, this task will obviously imply economic compensation.

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[25].

On a different note, we should also understand that the Directive places the burden of proof on the victim's head, meaning that, given the peculiarities presented by these new technologies[26], it might prove to be extremely difficult for them, except when the system keeps a record of any operation (a.k.a., the "black box") and when this cannot be manipulated. In connection to this, the report correctly the idea that if it can be proved 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.

It further explains that the features of emerging digital technologies, such as opacity, openness, autonomy and limited predictability, 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. Last, it claims producers' strict liability for defective products should be supplemented with fault-based liability for failure to discharge monitoring duties[27].

As it can be appreciated, it proposes that the burden of proof (existence and extension) remains on the victim's head, but lightening up the one on the defective product. In this sense, it

---

or of individual system components or by third parties, in a way that can affect the safety of these technologies. Updates would usually close safety holes through patches, but new codes also add or remove features in ways that change the risk profile of these technologies ("Liability for emerging digital technologies", Commission Staff Working Document , European Commission, accompanying the document "Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial intelligence for Europe" COM(2018) 237 final, 25/04/18).

[25] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019, page 42. In line with these ideas, the 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 has been recently approved, and the EU 2019/770 Directive 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.

[26] See ap. II.

[27] See ap. VI.

follows the so-called "Theory of dynamic burden of proof"[28], which arises from victims' difficulties in proving a medical mala praxis, and argues that a specific fact can be proved by whoever is in better position to do so. I.e., it proposes a proactive attitude on behalf of all the parties involved in the process.

To conclude this section, we suggest these alterations to the burden of proof should be stipulated by law in detail so that the jurisprudence cannot entail uneven solutions in the future.

VI.- Operator's strict liability.

Some legal systems include the regulation of the theory of created risk in their regulatory bodies. This claims that if a party introduces a risk into society (might be a dangerous thing or activity) and this leads to damage, a case of strict liability will apply.

For example, the Argentinian legal system supports this theory (originated in a French case[29]), regulated in articles 1757 and 1758 of the Civil and Commercial Code. This is why it feels the most appropriate to apply to damages caused by artificial intelligence[30]. The former establishes that when damage is caused by a risk or vice, or in the case of activities that are risky or dangerous in their nature, we will work with strict liability. The following article states the owner and holder will be deemed responsible. The holder is defined as the one executing for him or herself or for third parties, the use, direction and control of the thing, or else the one profiting from it (i.e. benefiting.) In the case of a risky or dangerous activity, the one conducting it or profiting from it is the one to be held accountable.

The report in question establishes that strict liability is an appropriate response to the risks posed by emerging digital technologies if, for example, they are operated in non-private environments[31] (such us autonomous cars, aircraftand or some drones) may typically cause significant harm (the significance being determined by the interplay of the potential frequency and the severity of possible harm.)

Concerning the liable person, the 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. I.e., it creates a new category: the one with the "operator", which must meet two requirements: controlling the risk and benefitting from it. As to this last portion, we must think of benefit in a wide sense, not just economically. As to its control, the report guarantees some

---

[28]Peyrano, Jorge and Chiappini, Julio, "Lineamientos de las cargas probatorias dinámicas", Ed. 107; Peyrano, Jorge "Doctrina de las cargas probatorias dinámicas", L.L. 1991-B- 1034 and López Mesa, Marcelo, "La doctrina de las cargas probatorias dinámincas", January 1998, Tomo Zeus Nro. 76, page 1, Zeus Editora S.R.L., Id SAIJ: DASA990043 available Dec 6th, 2019 on http://www.saij.gob.ar/doctrinaprint/dasa990043-lopez_mesa-doctrina_las_cargas_probatorias.htm.

[29] A*rrêt Franck* de la Corte de Casación, Sáenz, Luis, Código Civil y Comercial de la Nación Comentado, Dir. Herrera, Marisa, Picasso, Sebastián y Caramelo, Gustavo, T. IV, Ed. Infojus, Buenos Aires, page 491, available Dec 6th, 2019 on http://www.saij.gob.ar/docs-f/codigo-comentado/CCyC_Nacion_Comentado_Tomo_IV.pdf and Galdós, Jorge Mario, Código Civil y Comercial de la Nación Comentado, Dir. Ricardo Luis Lorenzetti, Rubinzal-Culzoni, Buenos Aires, 2014, T. VIII, page 594.

[30] Due to its autonomy and selflearning capabilities, AI is a dangerous thing with high/strong harmful potential. This makes AI a tool which is very difficult for human beings to control. Also, the theory of created risk makes it possible to include the "holder" figure, i.e., the person who has to maintain and update the software.

[31] Mentions to "operated in non-private environments" seems to exclude the application of strict liability in private environments. Given that strict liability –in this case- is risk-based, we believe the context (private or else) does not alter the application of this regime.

(non-exhaustive) aspects to define it: the one 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.

We are right to highlight the more sophisticated and more autonomous a system is, 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.

There is a distinction between diverse operators. Let us analyse them with an example. In the case of an autonomous vehicle (AV), the person deciding when, how and where to use it is the "frontend operator"; i.e. the person who primarily decides on and benefits from the use of the relevant technology.

The producer of the AV or another service provider is likewise controlling the AV on a continuous basis[32] is the "backend operator". Basically, the person continuously defining the features of the relevant technology and providing essential and ongoing backend support. Needless to say, this person, obviously receives an economic compensation for this task.

On the other hand, in case there is more than one subject qualified as operator, the report shows it chooses to award the liability to the one who has more control over the risks of 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. Anyway, it is shows 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[33].

We do not share this proposal for we consider, in this case, both should respond in solidarity. First, because in terms of civil liability, the spotlight is usually set on fixing the unjustified damaged caused to the victim. Second, because if facing a case like the one we are analysing, the reasoning behind liability is the risk introduced into society. Consequently, all the creators of risk respond in solidarity when there is a victim and then, the one who has spent more than due, should have a recourse claim against the other. Aside from this, asking the victim to determine which operator has greater control before they sue in Court is highly cumbersome.

To eliminate any uncertainty, the report proposes the legislator regulated which operator is liable, and under which circumstances (including questions linked to mandatory insurance)[34]. In line with what we have been saying, we estimate the legislation cannot establish closed concepts when facing a technology that is incessantly growing. Or else, it will imply the risk of excluding some cases that may arise in the future. The regulation must be broadly comprehensive, leaving the judge the key role of analysing each particular case separately.

Finally, it claims 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[35].

---

[32] 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.

[33] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019, page 39/42.

[34] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019, page 42.

[35] Idem.

VII.- The burden of proof, vicarious liability, logging by design and duties of care.

Despite the fact that the short extension of this work does not enable us to probe into all the topics within the report; before we conclude, we wish to at least mention some other relevant aspects, which will without a doubt deserve later further studying.

On the one hand, the report (as previously mentioned[36]) recommends applying regulations of vicarious liability of a principal for such auxiliaries (or in some systems known as liability for the actions of others) to cases in which harm is caused by autonomous technology used in a way functionally equivalent to the employment of human auxiliaries. 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[37].

It should be noted that the application of these rules comes as an analogy, since considering an autonomous system a "person" could imply a clear contradiction to what was mentioned in the ap. IV.

On the other hand, another point from the report that should come under the spotlight is the burden of proof. Although it expresses that (as a general rule) the victim should continue to be required to prove what caused her harm, it establishes several cases in which it alleviated this burden. One of them is the one commented in ap. V in the case of the directive of defective products. Another one is the presumption seen in the "Logging by design" case we comment on here.

Aside from these, it also proposes that 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 and (f) the kind and degree of harm potentially and actually caused"[38].

It also believes that 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[39].

The report also includes the case pertaining to "Logging by design," which consists in a duty on producers to equip technology with means of recording information[40] about the operation of the technology. This applies to cases in which such information is typically essential for

---

[36] Danesi, Cecilia Celeste, "Civil liability in the Artificial Intelligence era", La justicia uruguaya, Law Review, N° 156, Dec. 2019, page. 156/7.

[37] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019, page 45/6.

[38] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019, page 49.

[39] Idem, page 52.

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

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.

This consideration pretends to contribute to the burden proof on the victim's heads, mainly in these cases where safety measures are too high, where access to the system deems almost impossible (and is also protected by rules of intellectual property) and where the way it works evidences strong lack of awareness. By establishing this duty on the producer, breach or failure to give the victim reasonable access to information should trigger a rebuttable presumption that the condition of liability to be proven by the missing information is fulfilled.

In the case 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.

Last, the report dedicates some paragraphs to fault liability and duties of care. It states that 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[41]. This works precisely as a parameter to judge the liability of operators.

As to the producers[42], they should have to: (a) design, describe and market products in a way effectively enabling operators to comply with the duties outlined in the previous paragraph (we should add "Logging by design" as mentioned above, especially, duty of information for consumers;) and (b) adequately monitor the product after putting it into circulation.

VIII.- Conclusion.

Based on what was exposed and considered throughout this work, we believe that strict liability is the most appropriate to face any damages caused by artificial intelligence. The "operator" category created in the report - although somehow already contemplated in the guardian figure - seems fit to face the peculiarities autonomous systems present. Still, we estimate all those exercising some kind of power of risk control on AI should be solidary liable (no matter the recourse claim against them.) It is not like this operator will only pose greater interference, since proof of this might be too difficult for the victim.

As to the Directive of Defective Products, it is vital to make some adjustments to update it to fit these autonomous technologies. This means including autonomous systems in the notion of product (vgr. software), to alleviate the victim from the burden of proof connected with the defective product in some cases, and to suppress the defence from section e) of article 7.

Overall, we celebrate the creation of the valuable "Liability for artificial intelligence and other emerging digital technologies" report written by the Expert Group on Liability and New Technologies. It covers in great detail the diverse issues presenting a controversy as to artificial intelligence.

---

[41] "Liability for artificial intelligence and other emerging digital technologies", report from the Expert Group on Liability and New Technologies, European Union, November 2019, page 44/5.

[42] This regardless of whether they incidentally also act as operators (in terms highlighted in ap. VI) or in the case of the directive on defective products (ap. V.)

This phenomenon of unique characteristics is here to stay, and will for sure make many of our daily activities better. As professionals of the law, we must update and adapt ourselves to these new technologies and offer answers arising from this new social reality.

"*When the winds of change are blowing, some build walls and others build windmills*"

Chinese proverb.