1.

The power of algorithms stands in the possibility of replacing the relationship with the communication and it's used to spy and gather a lot of data that it's then processed by a big power of computer and algorithms. The difference between the relationship and the connection is that the first is related to the unpredictability and the originality of the conversation of the two (or more) parts while the second supposes that the human being is deprived of its original part and it's treated like calculable thing.

Clearly the data generated by a connection work better if used in a diagram or in an algorithm, but it leads to a depersonalization if they don't ever meet the dialogical relationship, without which it is impossible to calculate or anticipate the agreement or disagreement of one part. And the best part is that these data about an internet user are based on the tracks he leaves on the net, from which he can't take the distances.

So, it is important for the common good and the law to keep the dialogical relationship, where everyone can really manifest itself and the differences between each other. In particular the common good is nourished by the quality of the communication and not the quality of information: algorithms will care about the latter and show completely no interest about the first, only working on the pattern of the connections.

Connections are depersonalized, relationships are interpersonal.

2.

The Meaning is the risk of applying our freedom in the communication with other beings, ruled by the concept of equality and legal rules.

During the data processing there is no free space that allows any consideration about the future: the concept of future is based on the data we have in the present and ALL is confined into the algorithm schemes that deletes completely the anticipability, the wonder and the risk behind the communication of the relationship.

Game, dialogue and law share the concept of searching a meaning that in particular aims to create a uniform agreement about the individuals.

Indirect communication allows you to say a concept to another being, leaving to him the risk of interpreting or misinterpreting it: it leaves way more space to interpretations because the concept expressed in the message is not clear as it should be but lets the recipient draw conclusions.

The direct communication will tend to depersonalize the human being, that will not be authentic or original: it is the scheme followed by the algorithms; therefore, the human being will only follow the flow projected with the algorithms.

If in human beings everything would be resolved in the execution of the results of the algorithms, the responsibility of some decisions and the non-anticipability for games, dialogues and laws would be lost.

Clearly algorithm have not any aim: therefore, they miss that part that instead belongs to the human beings of making choices based on the ego. An example are the trials where more beings interact before the judge makes a choice (guilty or not) basing on the interpretation of the concepts.

3.

Big data creates its model behind the 4V that are velocity, veracity, variety and volume. Big data brings 3 problems:

- Technical and analytical barriers found while collecting the data:
- Cases that reveal the ethical problems of the big data;
- The complexity of the data and the possibility of losing their contexts.

4 secondary rules in the GDPR:

- Mechanism of delegation of power;
- Mechanism of legal coordination;
- Procedures for data protections;
- Procedures for judicial remedies;

The aim of the secondary rules of change is to allow the creation, modification, and suppression of the primary rules.

The law can be treated as a technique that starts from an assumption and continues with a consequence; and that's the distinction of legal order from other orders.

Now, if the law is a technique that regulates another technique, and if that other technique is the process of technological innovation, we may consider the law to be a meta-technology.

4.

Individuals must know why their data are being processed and in particular, with "informationelle selbst-bestimmung ", it is decided when the data can be collected and transmitted. In short, the aim of the GDPR is to strengthen both individual's rights and the powers of the European authorities, while reinforcing the obligations and responsibilities of data controllers.

Some primary rules are:

- Article 17 on the right to erasure, or the right to be forgotten
- Article 20 on data portability
- Articles 21 and 22 on individual self-determination and automated decision-making
- Article 33 on notifications of personal data breaches to the supervisory authority

Sometimes it can be difficult to estimate what the real power or meaning of the data is, at the moment of the collection: so, the definition of strict guidelines about the individual consent could represent a big obstacle to the data collection itself.

Pseudonymization comes in help to make the collection and the use of bigdata compatible with the GDPR rules, so the fields that would identify an individual are replaced with pseudonyms. It would be impossible to reach the original individual without additional information that are kept separately. Another solution has to do with the exemption of data processing for statistical purposes.

Plus, primary rules cooperate with secondary rules, for example considering the processing of data for statistical purposes: the member states have to define the limits, the content and the modalities that this statistical calculation must respect to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality

Now we understand how primary rules interplay with secondary rules:

- The rules of recognition are the meta-rules by which all other rules of the system are identified and understood as valid
- The rules of adjudication prescribe a remedy for all cases in which a rule has been violated
- The rules of change allow for creating, modifying, or suppressing the primary rules of the system.

Clearly the secondary rules can strengthen each other.

The freedom left to every member state could impact on the ones which work in different states, because some can be more restrictive about big data and others can be more permissive. This problem of fragmentation can be tackled with a standardization of some rules thanks to the meta-rules that we've discussed.

On the one hand, the use of secondary rules may represent a mechanism of legal flexibility that allows us to address the interaction between regulatory systems wisely. On the other, specific types of secondary rules can improve the future proofing of the law, assuring that it does not curtail technological innovation or require over-frequent revision to address such progress.

5.

The overall idea of this set of rules is not to replace today's personal data protection with a sort of US-like privacy group regime, but rather to complement it with a new collective right to lodge complaints.

Since the data subject can be targeted and her privacy infringed due to her membership in a given (racial, ethnic, genetic, etc) data group, it makes sense to grant such a group, a procedural right to a judicial remedy against the data controllers, processors or supervisory authorities.

Data controllers will have more responsibility in those processes that can represent a risk for the rights and freedom of the people. Data protection should be pre-emptive, assuring that the security policy works even before that any bit of information is collected.

It is still difficult to say if the net of secondary rules will be sufficient to tackle the Big Data trends: it remains an open challenge. This margin of uncertainty is not, in itself, inherently a fault. It may represent a wise mechanism of legal flexibility as to the great and fast evolution of technology

6.

The classic response by existing tort laws in Europe in such cases of alternative causation is that, while decisive proofs are missing the blame is of no one, or the alternative is that the blame goes to all the litigant part. The law in Europe is already fault-based and there is a compensation for the victim. The Tortfeasor is intended as a behavior that is distant from the expected and acceptable one.

Whether or not a legal system distinguishes between objective or subjective wrongdoing 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 can be defined in advance, and could allow or prohibit some conduct.

Emerging technology cannot apply easily this fault-based liability rules due to the lack of proper models of functioning of these machines that have learnt without a proper human control. 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.

7.

In the Legge Fallimentare is introduced the concept of electronic hearings also as a way to safeguard the adversarial.

The Italian Telematic Administrative Process (P.A.T.) undoubtedly constitutes the most advanced Italian justice automation system. The system, valid for all trials before the administrative courts is obligatory from 2017. The system has been defined as a set of technical rules, that have been approved before making it obligatory.

PAT is more advanced with respect to PCT. The modules are completely telematic and not on paper and are signed by the defenders of all the parties who provide the related deposits by PEC. The system is so automated that very frequently some stationery communications are made at night or on holidays.

The algorithmic justice to date, appears to be far removed from the Italian process. With this brief contribution, attention was focused on the evolution of I.A. and on the progress of the telematic process. It has been shown that the same expression telematic process alludes, to date, to a growing (sometimes mandatory) use of the IT tool for the execution of procedural requirements, for the formation of measures and for the related communication. Strengthen the IT tool also with the aid of I.A. could be an essential tool to remove these obstacles, ensuring greater usability of justice, a reduction in the duration of proceedings and the adoption of more efficient organizational forms for the PA.

8.

The technology involved in such processes should be able to log, so to register all the information and the operation that have been done, taking in account the costs for it, the technical feasibility, and the availability of other methods for obtaining such information. Logging must be done in accordance with otherwise applicable law, in particular data protection law and the rules concerning the protection of trade secrets.

If it happens a mistake or a damage that the safety rules could have been avoided, then it should be proven the causation, the fault and should be admitted the presence of a defect.

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.

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.

9.

Justice cannot be defined once for all but have to be shaped during the path, basing on the concepts of equality and identity/alterity. Blended intelligence (artificial + human intelligence) is a given fact today.

Technique is based on a convergent reason: every technical problem has a technical solution and technique cannot develop a critical reflection on itself.

The phenomenon is based on appearance and so some sides of it can be perceived, other sides are hidden: hermeneutics can show all the hidden sides of a word or a text thanks to the interpretation of it, used as investigation tool. Plus: binary language is closed: all is reduced to information that can be represented by 0s and 1s. Symbolic language is open to a lot of interpretations instead.

Human beings can experience the world because they have a language that is not an object that we step on while living the reality, it’s an original equipment. Experience of truth is a dialogical experience.

The algorithms should have the aim of reducing/avoiding mistakes, lies, corruptibility. A society that denies limits has no time for justice.

10.

Is transparency a right or a privilege? It pushes everything inward to information and it is intolerant with:

- negativity, opposition, conflict, dissent;
- secrecy
- foreignness

Man is not even fully transparent to himself: decisions can also be taken by intuition. We must be intelligible to artificial intelligence: AI is not plastic, HI is, so it’s adaptable.

So, we train algorithms to analyse a man’s physical profiles (traits, facial recognition) and inner profile (if the man does X then often Y occurs) but we cannot say why: it is just based on statistics and numbers.

Plus, we are destroying the possibility of growth to differences since there is an abolition of negativity that pushes everyone towards the sameness. Transparency is inherently positive because it has a stabilizing effect. Systems of transparency abolishes all the negativity to accelerate itself while suffering and passion are avoided as figures of negativity.

11.

We want to bring together mechanical laws that are unequivocable and human laws that are interpretable: hybrid laws. Pandemic found the solution for the inner need for relationships in social networks, making the society fully technical. It requires no effort, bringing banality and teaching the people how disengage when it is needed indeed: so, there is no dialogue and growth of the individuals. Plus, as said before, this society is going to delete and destroy negativity and imperfection: the lives of the people are no more authentical but exposed and influenced by standard of the society of the web.

People are not intended as faces but as data; it is a danger. And the dialogue does not exist anymore since it is done by words and silence, and the silence is not considered.

12.

Robotics is the area of AI concerned with the use of robots: machines that ‘‘sense, think, and act”. This field is interdisciplinary par excellence, involving not only artificial intelligence and computer science, but also cybernetics, physics, mathematics, mechanics, electronics, neuroscience, biology, and humanities.

Three laws of Asimov:

- A robot may not harm a human being, or, through inaction, allow a human being to come to harm
- A robot must obey the orders given to it by human beings, except where such orders would conflict with First Law

- A robot must protect its own existence, as long as such protection does not conflict with the First or Second Law
- Zeroth law: A robot may not injure humanity, or, through inaction, allow humanity to come to harm

The First Law of Robotics should be integrated by a meta-law, which determines that a robot may not act unless its actions are subject to the Laws of Robotics.

Quests: should we exempt the robots from their liabilities? Can we correct them so they don't commit those crimes anymore?

13.

Neural nets are computer model inspired by the structure of biological neural systems. A neuron receives signal from other neurons. Synapse is plastic in the sense that strength of their connection to the neuron can increase or decrease. The artificial neural network can be defined as a processing system consisting of a series of simple and highly interconnected processing elements

The neural network is organized in more layers that are:

- Input layer that receives the information from outside;
- Hidden layer that processes the information received;
- Output layer that shows the results of the calculation (what it has learnt) to the external world.

The network exploits a particular algorithm that is based on back propagation in which the actual result is compared to the desired output and the difference between the two results is used to weigh the connection between the different layers starting from the output layers.

With machine genetic learning we're experiencing a new kind of learning based on obscured starting data and obscured learning mechanism.

In civil law area neural projects for dealing conflicts are developed both to reach a composition and to advise the choice between contrasting hypotheses. Significant is ECHO and We should also mention the MAIRILOG project which uses neural networks to draw logical rules from Cases.

14.

Taddeo has tried to bring together the traditional just war theory (JWT) and the revolutionary information ethics (IE) to create a new framework for understanding cyberwarfare, named 'just information warfare' (JIW): it is an attempt to merge the principles for adjudicating warfare found in JWT with the 'ontocentric' ethics of IE. It becomes obvious how applying JWT to a warfare that is not in the traditional space, but in the cyberspace, appears to be difficult and confusing. JIT seems to solve most of the problems that were left behind in JWT: all but discrimination. This is probably the most important one because it makes a difference between the civilians and the soldiers. This difference is impossible to be kept up into the cyberspace.

Taddeo believes that cyber war fare can be justified so long as it is only intended to return the info sphere to its status quo ante, but this requires that we know what the status quo ante is.

Mediation theory is a descriptive and normative theory of human-technology-world relations, of how technologies mediate the relationships humans have to the world: «When a computer unexpectedly and abruptly ceases to work properly, a user may become explicitly conscious of the computer's identity as a technology, and of her or his situation as a user, all of the sudden, When the computer functions as expected, we lose sight of it, working not at it or on it, but with it and through it»

A malfunction does not tend to lead us to new insights and learning opportunities, as instead we become irritated, angry, fixated, unable to focus on anything or anyone other than the malfunction, for which reason, as Rosenberger puts it, 'the experience can be jarring".

15.

Cyber technologies – through forming embodiment, hermeneutic, and background relations with users – belong to the same domain as biotechnologies, the domain of everyday life. It is for this reason that the weaponization and militarisation of cyberspace is the weaponization and militarisation of everyday life. A further parallel between biological and cyber weapons is thus that of paranoia. Releasing toxins into the atmosphere can not only result in 'uncertain area coverage and effects' due to 'environmental and meteorological conditions' but fear and anxiety about being able to safely go outside.

Entering infected places (by cyber of biological weapons) would require us a defence that will reduce our freedom and will make us continuously afraid about our protection.

16.

We can see the pros of the legal automatization in the ontologies, that are the branches that have the aim to model concepts normally treated by lawyers through the formalization of norms, rights and duties such that the machine should be able to differentiate the relevant information of a particular problems through the use of taxonomies and the set of rules of the domain of that problem. Implementation of ontologies could be very difficult to be perfectioned since the information of a legal problem could rarely be compressed. But the studies about this branch will not be abandoned so easily. Instead the methodology of work is switched from top-down, to bottom-up.

The idea of embedding privacy safeguards into information systems and other technologies is nothing new. It has been defined as privacy by design. requirements such as informed consent can be implemented in system design. Furthermore, robots could be designed in a privacy friendly way, so that the amount of data to be collected and processed is reduced to a minimum and in compliance with the finality principle

Ann Cavoukian thinks that the data protection safeguard should be seen as proactive rather than reactive, making privacy preventive and not remedial.

17.

A debate has been kept about the role that ISPs should have to ensure the protection of individual rights: some say that they should safeguard online security, while others ask the public authorities to enforce their security through the use of filtering systems: these ones represent one end of the spectrum in which the opinions of the debate fall in; on the other end we find constitutional limits that explain why some filtering systems cannot be applied.

Therefore, on the one hand, "such an injunction [requiring the installation of the contested filtering system] would result in a serious infringement of the freedom of the hosting service provider to conduct its business since it would require that hosting service provider to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions which requires that measures to ensure the respect of intellectual property rights should not be unnecessarily complicated or costly".

18.

In the case of the law regulating technological innovation, i.e. the law conceived as a "meta-technology", the focus is on the different normative purposes that the law can have, including that which scholars often dub as the "technological neutrality" of the law; we should differentiate between:

(a) technological indifference, i.e. legal regulations which apply in identical ways, whatever the technology, such as the right to authorize communication of a work to the public in the field of copyright law;
(b) implementation neutrality, so that regulations are by definition specific to that technology and yet, they do not favour one or more of its possible implementations
(c) potential neutrality of the law that sets up a particular attribute of a technology, although lawmakers can draft the legal requirement so that even non-compliant implementations can be modified to become compliant

We propose four steps of analysis. First, a meta-regulatory approach to the field of legal automation should allow us to determine whether, and to what extent, lawmakers shall not (or cannot) delegate decisions to automated systems. Second, focus should be on the impact of technology on the formalisms of the law, and how the latter competes with further regulatory systems. Third, we have to pay attention to the principles and values which are at stake with the delegation of decisions to automated systems, namely the institutional dimension of the law with matters of interpretation and deliberation. Fourth, the distinction between automatic and non-automatic decisions of the law, and their legitimacy, may entail a class of legal problems, i.e. the hard cases of the law, where disagreement can revolve around semantics, or legal reasoning, or the role and logic of the principles in the system.

19.

If a product fails to contain a logging option and the operator is for this reason exposed to liability, the operator should be able to pass the loss resulting from not being able to disclose the logged data to the victim, to the producer. 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. 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. This solution is better because it helps the victim to prove the elements of liability in settings that involve technology.

As to the burden of proofs, as a general rule the victim should continue to be required to prove what caused her harm: whoever demands compensation from another should in general prove all necessary requirements for such a claim. 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 analyzed in retrospect, even from the victim's point of view

20.

Existing tort laws in Europe differ substantially in their approach to holding someone (the principal) liable for the conduct of another (the auxiliary). Some holds the principal liable without further acknowledgements just because the auxiliary acted for the principal benefits. Others hold the principal only in some circumstances, like when it is known that the auxiliary is dangerous. Some jurisdictions use both with a neutral definition of strict liability, as liability without fault of the liable person, regard vicarious liability as a mere variant of this strict liability.

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. Clearly at least in those jurisdictions which consider vicarious liability a variant of fault liability, holding the principal for the wrongdoing of another could be difficult since there should be a reflection of the behaviour of the non human helper in the behaviour of the human one.

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.

In the 19th century, legislators introduced strict liability, replacing the notion of responsibility for misconduct with liability. 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. Strict liability for the operation of computers, software or the like is so far widely unknown in Europe. 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.

21.

All the member states have introduced the product liability, that still is not harmonized with defective products. The PLD is based on the principle that the producer 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. The PLD was defined under the basis of technological neutrality, but it has been defined considering the traditional products. 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, taking into account all relevant circumstances.

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

At the same time, the producer's control may be limited and nonexclusive if the product's operation requires data provided by third parties or collected from the environment, and depends on self-learning processes and personalizing 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.

Development risk defense: which allows the producer to avoid liability if the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered. This is related to another limitation of liability. The defense may become much more important practically with regard to sophisticated AI-based products.

22.

In jurisdictions where the prescription period is comparatively short, 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.

The application of liability frameworks in practice is also affected by challenges in the field of procedural law

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. 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.

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 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

23.

Today's legal robotics are relevant in the realm of law that belongs to the private law field, namely contractual and extra-contractual obligations.

An English or US lawyer will define as torts (obligations between private persons imposed by the Government), to compensate the damaged done by wrongdoing, facts that fall in three different kinds of liability:

- liability for harm caused by intentional torts: liability for an intentional tort is established when a person has voluntarily performed the wrongful action.
- negligence-related tortuous: liability based on lack of due care when the reasonable' person fails to guard against foreseeable' harm
- liability and liability without fault (strict liability): Strict liability is established without fault as in the paradigmatic case of liability for defective products, which may be due to a lack of information about certain features of the artefact (that's why it is possible to find extremely detailed labels on the products informing about the risk of using the products in a wrong way).

But there are different reasons for which a robot should not only defined as an enhanced toaster, but as a possible new way to raise problems: just imagine that a robot can learn from the surrounding environment, that means that it will develop behaviours that can be unpredictable to its owner and also to its human designer. On the other hand, it is likely that autonomous robots will create new forms of legal agency, that is, the relationship by which a party grants authority for another to act on her behalf so as to deal with a third party: Accordingly, the legal responsibility for the actions of a robot falls on the individual who grants the robot permission to act on their behalf.

Putting aside the ethical aspects concerning new possible reasons for charging humans, the parallelism between robots and slaves casts light on two further fields of the foreseeable future of legal robotics: First, we have to examine how the law can cope with both the enforcement of rights and obligations created by robots and the question of liability for damages caused by them. Secondly, we need to widen our perspective so as to take into account the very possibility that robots will soon represent a new source of personal responsibility for others' behaviour.

24.

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, in which it is applied the res ipsa loquitur, of lowering the standard of the proofs for certain cases. Yet another method of aiding the claimant to prove the cause of harm is by focusing on whoever is in control of key evidence but fails to produce it. If there are multiple possible causes and it remains unclear what exactly triggered the harm 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

As is already commonly used 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.

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. In these cases, could be justified trying to think again about the use of the traditional approaches to prove liability.

Adopting any rule concerning the distribution of the burden of proving fault requires explaining fault in the first place.

Ex. 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;
- facts that allow the court to establish that breach of the duty of care was intentional or negligent breach of a duty of care on the part of the producer with regard to the product

25.

The introduction of strict liability should offer victims easier access to compensation, without excluding, of course, a parallel fault liability claims if its requirements are fulfilled. 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

In the case of emerging technologies, we don't talk about keeper, user or owner, though. It is preferred to talk about an "operator" which is the person that is in control of the risk connected with the operation of the technology itself. Control is a variable concept: 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; a backend operator could 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.

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.

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. 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 defense should not apply. Only recently, the EU has confirmed 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.

For the use of more traditional technologies, it is already recognized that their operators have to discharge a range of duties of care. 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.

26.

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 and with emergent technologies these duties are often magnified even more.

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: Under many national jurisdictions, a general product monitoring duty on the part of producers has already been developed for the purposes of tort law.

One option proposed for addressing the risks of emerging digital technology is the potential expansion of the notion of vicarious liability to functionally equivalent situations where use is made of autonomous technology instead of using a human auxiliary.

27.

Digitalization brings fundamental changes to our environments, some of which have an impact on liability law. This affects, in particular:

- Complexity: Modern-day hardware can be a composite of multiple parts whose interaction requires a high degree of technical sophistication; it may be increasingly difficult to find out where a problem has its source and what ultimately caused an accident.
- 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.
- 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. 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

- 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.
- Predictability: 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.

which may be only gradual in nature, but whose dimension and combined effect results in disruption.

28.

Modern emerging technologies are always more dependent from data: these data can be given by an external environment given as input; but considering that 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 cyber security breaches.