MACHINES ARE TAKING OVER – ARE WE READY?

Law and Artificial Intelligence

Artificial intelligence ("AI") has consequences for practical legal matters like liability, procedure and similar, and for philosophical and ethical questions: is it always suitable to use AI, how to deal with consequences for human rights? This article presents practical examples from Estonia, which is beginning to include AI in legislation, and discuss what questions should be asked when creating and implementing AI law. Some legislation can quite easily be adapted but sometimes a new way of thinking may be needed. This is not primarily a legal question, but lawyers need to contribute in order to highlight challenges and suggest solutions.

Katrin Nyman **METCALF**
BA, LLM, PhD (Uppsala University);
Adjunct Professor of Communications Law,
Tallinn University of Technology.

Tanel **KERIKMÄE**
BA (Tartu), LLM, LL.Lic (Helsinki University),
PhD (Tallinn University);
Professor of European Legal Policy and Law & Technology,
Tallinn University of Technology.

"Information Technology is a science at the service of man, it must not infringe on human identity, the private life of the individual, human rights, individual or collective public freedoms."[1]

1 *Loi n° 2009-09 portant protection des données à caractère personnel en République du Bénin*, Art 2: "*L'informatique étant une science au service de l'homme, elle ne doit pas porter atteinte à l'identité humaine, à la vie privée de l'individu, aux droits de l'homme, aux libertés publiques, individuelles ou collectives.*" (Author's translation to English)

I. Introduction

1 Most of us have seen films with robots taking over the world or at least dominating in social relations.[2] It is easy to have these images in mind when thinking about whether there should be legal rules to govern the activities of any form of machines, including robots that are programmed to be capable of carrying out a complex series of actions automatically. While some machines are quite straightforward and carry out the commands they were given, others, including those that deploy machine learning, may act beyond the scope of their original commands. This is a popular view taken of artificial intelligence ("AI"). The authors would like to draw attention to how, despite a large amount of research and writing on AI, the issue of a globally recognised definition of the research object remains a work in progress. In an interdisciplinary context, involving different branches of social sciences (*eg*, law) as well as information technology, it is especially difficult to agree on a common definition. Instead, we find various discipline-based perceptions of what exactly it is that is analysed. In some contexts the term "machine learning" is preferred, as more exact, but the legal debate tends to use AI – albeit without a clear definition.

2 The European Union ("EU") Commission's communication on AI states: "Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals."[3] The EU High Level Working Group on AI has further developed this definition.[4] In a 2020 White Paper of the Commission[5] it is stated that a key issue in the creation of a specific regulatory framework on AI is to determine the

2 Examples include movies and television series such as *I, Robot* (2004), *Ex Machina* (2014), *Almost Human* (2013–2014), *Black Mirror* (2011–), *Westworld* (2016–) and others.

3 European Commission, *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 on Artificial Intelligence for Europe* (Brussels, 25.4.2018 COM(2018) 237 final) at p 1.

4 "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions." See <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence> (accessed 1 July 2020).

5 European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust* (Brussels, 19.2.2020 COM(2020) 65 final).

scope of its application and a clear definition. The mentioned definition is to be seen as a starting point. In the White Paper, it is also stated that: "Simply put, AI is a collection of technologies that combine data, algorithms and computing power."[6] The White Paper stresses that in any new legal instrument to be developed, the definition of AI will need to be sufficiently flexible to accommodate technical progress while being precise enough to provide the necessary legal certainty. The EU "Ethics Guidelines for Trustworthy AI"[7] focuses on ethical requirements of AI systems, while not defining the object itself clearly. A recent attempt in a different forum to create global standards on AI technologies is the United Nations Educational, Scientific and Cultural Organization/International Research Centre on Artificial Intelligence draft text of a recommendation on the ethics of AI. Also in this context, the question of a definition is still debated.[8]

3 This article focuses on different aspects of machine learning, mainly those that fall under the imperfectly defined term of AI. The rapid increase in applications and deployments of machine learning makes the topic of regulating such activities appear both attractive and urgent. However, it is perhaps less exciting to learn that "thinking machines" exist in various contexts already for some time and fit quite well into existing legal rules. We have autopilots in airplanes, driverless trains, and many kinds of industrial robots. Incremental change with small steps toward more automation (like for cars for example) is more common than giant leaps from completely "human-made" decisions to full automation. In cases of gradual change, legal regulation normally manages to keep more or less in step with the technical changes through regular updates of rules or new interpretations of them. However, even if it is possible to de-dramatise the question, it is nevertheless true that the pace of technological change is getting faster and faster, and the aspects of our daily lives where automation, including AI, plays a role are getting ever more diverse. There are constantly new questions regarding how the law should deal with this new reality.[9]

---

6 European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust* (Brussels, 19.2.2020 COM(2020) 65 final) at p 2.

7 European Commission, High-Level Expert Group on Artificial Intelligence (Independent), *Ethics Guidelines for Trustworthy AI* (8 April 2019).

8 One of the authors, Tanel Kerikmäe, is invited as a national consultant for Estonia in this work and has raised (in July 2020) the point that the text is using different terms such as "AI", "AI systems", "algorithms", "AI technologies" that are not sufficiently explained or even consistently used throughout the text. See International Research Centre on Artificial Intelligence, "Consultation 2020" <https://ircai.org/consultation2020/> (accessed 1 July 2020).

9 Katharine K Duvivier, "E-Legislating" (2013) 92(9) *Oregon Law Review* 48; Pawan Dutt & Tanel Kerikmäe, "Concepts and Problems Associated with eDemocracy" in

(cont'd on the next page)

4 In this article, the question of the legal approach to the use of AI is divided into two main parts: the specific questions about liability, protection of people in their roles as consumers, patients, travellers and so on; and the fundamental, ethical questions about whether AI should be allowed to do everything that it is technically capable of doing. These different aspects are clearly linked. The second, fundamental, question is primarily one of policy rather than of law. Lawyers can and should nevertheless make an important contribution to the debate by pointing out if and how fundamental legal values such as protection of rule of law and human rights may be affected by AI. Furthermore, if policy decisions are adopted that set limits to what AI can or should do, there will be a need for appropriate legal instruments to properly implement the chosen direction. Lawyers will interpret and implement these, making sure that the restrictions are necessary and proportional. Still, the authors would like to highlight that the basic and very important decision on *whether* AI should be limited is not a question of applying law. It is also not a question of which law provides the answers as to how and why it should be done. Instead, it is a philosophical and ethical question.

5 This article deals with the practical, the fundamental and the policy-oriented questions regarding whether, why and how AI should be limited by law. What does current law say about how AI fits into our societies? Are there reasons not to let machines do everything they can do? If so, what are these reasons and what are they based on? How can limitations be made and implemented – if they can be effectively made at all? In order to give a fuller picture of the topic, some examples of the "everyday" rule-making for AI will be mentioned, and in this context, examples from Estonia will be used to make the topic practical rather than just theoretical. Estonia is among the world leaders in e-governance and thus has studied the use of technology in society for several decades. Estonian e-governance does not rely primarily on AI, but in a system of governance which utilises information and communications technology ("ICT"), it may be a logical next step to increase the amount of automated decision-making. Some practical legal changes in Estonia, which are in many instances similar in other countries, will be considered before the authors proceed to the more fundamental discussion about the role of AI in society.

Regulating eTechnologies in the European Union (Tanel Kerikmäe ed) (Heidelberg: Springer, 2014) at pp 286–287.

II. Mapping the need for change

A. Basic areas and questions of law

6 To accommodate the expanding use of AI, in legislative activities different steps are necessary.[10] These include:

(a) analysing the legal system in order to identify and if required remove such norms that do not fit with the use of AI (or other technology) and thus *per se* prevent use of technology and hinder innovation;

(b) based on the above-mentioned analysis, ensuring that the law in force adequately reflects the use of AI and that the use of AI is defined with sufficient clarity as far as responsibility is concerned; and

(c) drafting new laws or other rules and – if necessary – restricting the development and use of AI.

7 The multitude and variety of ways in which technology can be used means that there are very many different areas of law that should be evaluated. This includes acts regulating legal procedures (administrative or criminal), sector-specific laws for different areas (transport, health care, different industries, *etc*), consumer protection law, criminal law, contract law, and so on. Technology should not be the main determining factor for what kind of regulation is needed and suitable. As for the first point above, on removing hindering norms, it is evidently necessary to evaluate what the reason is for the norms, and whether there is still a need for these norms. If not, they may have to be amended, or entirely new norms with a similar aim may need to be passed. Technological advances should not be prevented, but if the norms provide important legal protection, this protection should nevertheless remain. One example could be the need for notarised signatures in certain contexts, to underline the importance of a transaction and to guarantee that not only has the right person signed a document, but that he or she has also understood it. Perhaps in such a case, an automated decision is not suitable even if this blocks innovation towards using only digital signatures or even, in the future, no "man-made" signatures at all. In other cases, the requirement of a specific form or something similar that hinders a digital or automatic process may just be there because of tradition and does not serve any specific

10 These steps were proposed to the Estonian government in a major study commissioned from Tallinn University of Technology by the Government in 2019, to which the authors made major contributions. See Tanel Kerikmäe *et al*, *1st Report on Legal Framework and Analysis Related to Autonomous Intelligent Technologies* (Riigikantselei/Estonian Government Office, 2019).

purpose, in which case the provision can be abolished. Here, the example can be rules on forms of documents like different coloured paper or the use of certain colours of ink.

8 In general, the required careful overview and analysis of many different areas of law should lead to the conclusion that there is no need for too much specialised legislation or regulation for "digital" matters or AI.[11] The most important factor should be what certain rules are made for, and what the situation being regulated is: the rules should be as technology-neutral as possible. Technology should be seen primarily as a tool. This tool may mean that some special rules are needed, but it should not change the fundamental principles of the legal system.

9 Many of the special questions caused by new technologies are of a horizontal nature – meaning that they should not be regulated for specific sectors or issues but fit better in legislation that applies across many different areas. Legislation on digital identities that can be used for different legal transactions is one example. Another general question highlighted by the advancement of AI includes determining whether there is an unavoidable need to require the direct participation of a natural person to perform transactions. This is a question not only for data processors but also data owners. Such requirements for personal involvement may be found in various special laws where it says that something has to be signed or otherwise handled in some manner that presupposes that a person does it. In order to facilitate the implementation of AI, it is wise to abandon both direct and indirect requirements for human participation, at least for activities that are both practically and ethically feasible without direct human intervention.[12] However, the recent case law in Europe and in the US demonstrates that there is a growing resistance against trusting AI-based risk-assessment tools that have been used by governments and judicial systems.[13] If this is

11 Katrin Nyman Metcalf, "How to Build E-governance in a Digital Society: The Case of Estonia" (2019) 58 *Revista Catalana de Dret Públic* 1.

12 Tanel Kerikmäe *et al*, *1st Report on Legal Framework and Analysis Related to Autonomous Intelligent Technologies* (Riigikantselei/Estonian Government Office, 2019).

13 For example, in 2020, the non-profit Pretrial Justice Institute (US) stated after years of supporting an algorithmic risk assessment tool (Public Safety Assessment), that there are serious concerns about racial bias and the model should not be used in criminal justice (mainly overestimated risk of recidivism by black defendants). See the Pretrial Justice Institute website <https://www.pretrial.org>. In Europe, in a landmark judgment, SyRi (System Risk Indication, used by the Dutch government for anti-corruption purposes) was adopted on 5 February 2020 by the District Court of the Hague which ruled that the right to privacy prevailed over the legality of the AI-based tool.

the case, limitations of AI solutions may be needed – or at least more time to introduce them.

B. Avoiding specialised legislation

10 As with most new technologies, there tends to be a lot of enthusiasm – not always fully realistic – when something is very new. After a while, this gives way to a need to deal with more mundane matters. There is a risk involved with making new and specific legislation for technology. Perhaps the most obvious risk is that such legislation becomes obsolete, as technology develops rapidly. Many authors quote the amusing but nevertheless true example of how in England the law foresaw that a man should walk ahead with a red flag to warn people each time a motor vehicle travelled on the road![14] If we had made technology-specific legislation for call-up modems or floppy discs, these laws would no doubt appear equally quaint today. As already mentioned, law should be as technology neutral as possible, focusing on the reasons why there is a need for the law in the first place (what is it protecting, what are the risks to combat, what are the questions of liability, *etc*?) rather than on the technologies involved.

11 However, the risk of obsolescence is only one of the disadvantages with specific digital or AI legislation. Such laws furthermore risk creating a parallel system in which there are different rules for the same thing, depending on what technologies are used. As an example, we can mention the idea of data protection rules only applying to electronic data, in which case something would be more or less protected depending on whether it is on paper or in another form, which makes no legal sense. Another example is the idea of one application system for public grants if the application is made online and another for offline applications, with different rules for the same substantive process. Put like this, it is quite easy to see why it would not be a good idea to have such specialised – "digital only" – laws, but it is nevertheless not uncommon in many countries that legislation is made for "digital transactions", thus losing sight of the fact that the digital mode is just a means of performing a transaction and not the determining factor that should affect its substantive validity.

12 A further risk with specialised legislation is the temptation to "tick the box" and regard the matter as closed once a specialised law has been passed. This may create a situation in which no sufficiently thorough overview is made of all areas of law to determine if there are any issues that may hinder the use of modern technology. Such analytical work

14 Locomotive Act 1865 (c 83) (UK). See <https://archive.org/stream/statutesunitedk30britgoog#page/n246/mode/2up> (accessed 1 July 2020).

may appear less exciting than drafting a high-tech law, but it is essential. The temptation must be avoided to think that everything and anything that is affected by AI and other technologies can be written into one or even a few laws. The legal system is a complex and living phenomenon, and different branches of law use distinct terminology and are based on distinct traditions. AI has the potential to transform society and needs to be adequately reflected across all of society.

13 For technology to have the beneficial effect that it could and should have, it must be understood and properly used. For example, in judicial proceedings, the problem may well be that judges do not understand what is in the "black box" of the algorithm and may then not use legally-allowed AI support correctly. Administrative officials may in the same way steer away from AI because they do not understand it. If the kind of thorough overview and analysis that this article calls for takes place, a beneficial by-product is that the risk of avoidance of AI due to lack of knowledge should also be reduced.

III. Machines are learning – The law is adapting

A. Procedural legislation

14 Estonia is in many ways seen as a world leader in e-governance. To some extent, this is due to the fact that the country was an early innovator with several e-governance solutions (for example, the Government started conducting cabinet meetings in a paperless fashion in the year 2000), but this assessment also rests upon the fact that e-services are frequently used by different categories of people in Estonia. It is perhaps indicative of the emotional attachment to technological developments demonstrated by many Estonians that there is a domestic, mythological word used for machine learning or AI applications. These are labelled in government studies and statements with the word "*kratt*", which refers to a magical creature in old Estonian mythology, a treasure-bearer.

15 Estonians like to point out how advanced we are with e-governance as well as other forms of technology use. Many attractive technological inventions originate from Estonia, like Skype or Transferwise, and the small country has a disproportionate number of start-ups, primarily in the technology sector. However, as Estonian leaders – from the President on – have continually stressed for the past decade, no one remains at the forefront of technological development and use unless they constantly innovate. Today, the fact that citizens and government officials use ICT tools does not mean that a society or its governance can be regarded as cutting-edge – this is commonplace. However, it would be new and exciting if public administration tasks were to be performed solely by

technology: if machines were to be in charge! To express this in a less romantic and more realistic manner, the latest innovations in public as well as private services rely on the use of AI and this is what the legislation now tries to adapt to. In March 2018, the Government Office and the Ministry of Economic Affairs and Communications set up a cross-sectoral expert group for analysing and preparing for the introduction of AI in Estonia, including the development of a test environment.[15] The authors of this article were both experts appointed to this research group and the following conclusions are in part inspired by the outcomes of the discussions of the reports to the Government Office.

16 The following are a few examples to demonstrate an overview of what AI-relevant procedural legislation can mean. In February 2018, changes were made to the Estonian Administrative Procedure Act to take into account the specificity of administrative procedures in electronic form. The aim was to ensure that there is effective protection of the rights of the person involved in the proceedings, given the requirements and challenges of electronic communication. One reason for the change was to pave the way for the use of AI, such that no direct intervention of humans is needed. However, several elements of the administrative procedure are still formulated so that they presuppose direct human action, although there would appear not to be any fundamental obstacles to the automation of the respective processes.[16] Examples where unnecessary human intervention is still presupposed include the requirements for drafting protocols,[17] means of access to documents and files[18] and the regulation of formal requirements for administrative acts.[19]

17 There are also many places in which Estonian legislation explicitly recognises that administrative acts can be undertaken without human intervention. This is possible thanks to the fact that data in the Estonian public administration is digital by default. There is an elaborate system of interoperable databases. These features technically support automatic data handling. The formulation differs in different Acts, but is generally similar to this phrase, taken from the Commercial Pledges

15 See Republic of Estonia, Government Office, "Eesti saab tehisintellekti strateegia" (27 March 2018) <https://www.riigikantselei.ee/et/uudised/eesti-saab-tehisintellekti-strateegia> (accessed 1 July 2020).

16 Tanel Kerikmäe *et al*, *1st Report on Legal Framework and Analysis Related to Autonomous Intelligent Technologies* (Riigikantselei/Estonian Government Office, 2019).

17 Administrative Procedure Act (2001) (Estonia) Arts 18(2) and 18(3), in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/527032019002/consolide> (accessed 1 July 2020).

18 of the Administrative Procedure Act (2001) (Estonia) Art 37(3).

19 Administrative Procedure Act (2001) (Estonia) Chapter 4, Division 2.

Act:[20] "If a digitally signed application can be submitted directly to the commercial pledge register's online information system, the application and the time of receipt thereof will be registered in the journal of the register automatically." Such mentions can be found in the Land Register Act,[21] the Law of Ship Flags and Ship Registers Act,[22] the Taxation Act, the Environmental Charges Act, and the Commercial Code. They share the similarity of recognising automatic administrative acts and documents. The specific regulation quoted could serve as a model for general regulation of administrative procedures to make it possible to make decisions automatically, via AI.

18 Creating automated solutions for court proceedings requires a deeper analysis but given that one such pilot project – making an automated regulation in the order for payment procedure – has been in place since 31 May 2014,[23] the extension of the use of similar solutions should not be excluded. The Estonian "AI powered judge" as presented in the media[24] was claimed to be supposed to analyse legal documents and other relevant information and come to a decision. In reality, the algorithm created for a pilot project was meant to deal only with small uncontested claims, for example, parking tickets or child benefit cases with claims of up to €6,400. This is an example of how the exciting image of AI overtook real events and created media interest in what turned out in fact not to be such a revolutionary change.

19 In another example, it is questionable whether the written warning procedure provided for in the Code of Misdemeanour Procedure (in the ordinary sense of the so-called "speed camera fine" procedure) requires that a notice of penalty be drawn up by an official and signed, which means that the machine cannot "send out" its own decision by itself.[25] It

20 See Arts 16(41) and 16(42) of the Commercial Pledges Act (1996) (Estonia), in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/519062017010/consolide> (accessed 1 July 2020).

21 See Arts 39(3) and 39(4) of the Land Register Act (1993) (Estonia), in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/512122019012/consolide> (accessed 1 July 2020).

22 See Law of Ship Flags and Ship Registers Act (1998) (Estonia), in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/512122019011/consolide> (accessed 1 July 2020).

23 Code of Civil Procedure (2005) (Estonia) Art 4892(2), in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/512122019004/consolide> (accessed 1 July 2020).

24 See Eric Niiler, "Can AI Be a Fair Judge in Court? Estonia Thinks So" *Wired* (25 March 2019) <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/> (accessed 1 July 2020).

25 Code of Misdemeanour Procedure (2002) (Estonia) Art 542(4), in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/515012020005/consolide> (accessed 1 July 2020).

is not easy to see what additional protection of rights is afforded by this formality being made by a person rather than a machine – given that the person in any event relies on the machine-made determination of the event.[26] In general, procedural law can adopt AI with less complications than substantive law, as it is not in the same way based on the "law of the excluded middle" according to digital or Boolean logic (named after George Boole) – the basic logic that is seen as the theoretical foundation of the digital age and helps to explain the basic idea behind AI decision-making.[27]

B. Responsibility for AI

20 As a general principle, the State should be responsible for damage caused if AI is used to perform a public task, in the same way as if the damage had been caused by a person acting on behalf of the State. The fact that the public worker is a machine does not mean that the State can absolve itself from its liability. It has chosen this way to perform a task and must accept the liability that results. We can see this as the State "employing" a machine as its agent to carry out certain duties. The sphere of responsibility of the State is not altered by this. In some special sectoral laws, this principle is also fixed. This relates, for example, to cases mentioned above of "automatic" processes, where human intervention is not necessary.[28] In the private sector, the way in which intent is shown and the question of whether AI can show intent is likely to become more and more relevant, as there are more and more automated processes without direct human intervention.

21 There is, however, a difference between human workers and AI. Humans are (still) expected to be able to take decisions, weigh facts, act in unexpected situations and so on. In the public sector, workers should ensure that what they do on behalf of the State is that which is most suitable in the particular circumstance. The requirements for different competencies for various posts in the public sector show how this is taken into consideration in a practical way. AI is as of today not expected

26 Tanel Kerikmäe *et al*, *1st Report on Legal Framework and Analysis Related to Autonomous Intelligent Technologies* (Riigikantselei/Estonian Government Office, 2019).

27 Bahman Zohuri & Masoud J Moghaddam, *Business Resilience System (BRS): Driven Through Boolean, Fuzzy Logics and Cloud Computation* (Springer, 2017) ch 6 at pp 183–198 explains Boolean logic, see especially p 184.

28 Land Register Act (1993) (Estonia) Art 795, in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/512122019012/consolide> (accessed 1 July 2020); Law of Ship Flag and Ship Registers Act (1998) (Estonia) Art 1005, in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/512122019011/consolide> (accessed 1 July 2020).

to "help" the State to do the right thing in this way. Its role is more limited and specific. Damage caused by authorities in a public law relationship as a result of AI "action" including cases where the damage was caused by an error in the algorithm, software or data underlying the operation of the AI qualifies as an unlawful activity of a public authority in the sense of state liability legislation.[29] Responsibility is normally based on fault but the Estonian legal system as well as many others recognises situations of increased responsibility, so-called risk liability (liability for innocence). Many jurisdictions contain the notion of "major source of danger",[30] which may be related to nuclear power plants, motor vehicles or specific equipment and tools. This principle has been used for cases of errors in algorithms (and similar cases), analogising the application of the principle of risk liability arising from AI as something similar to a major source of danger. Even if there may be contexts where problems with the AI may entail major risks, it is questionable if a general principle that AI is equal to a "major source of danger" can remain if AI is to be used more widely.

22 When AI performs public tasks, it should be ensured that the recipient of the administrative act unambiguously understands when a decision is made by AI. This is required not just by many national laws but also in Europe by the EU General Data Protection Regulation[31] ("GDPR"). From the perspective of the recipient of a decision, the legal force of the decision and the possibility of challenging it should be no different, whether the decision is made by an AI or a human being. It is another matter to decide which decisions are to be made by AI, what the permissible error rate would be and how to deal with it. This is one of the situations where human decision-makers have to accept that they have to *decide* this – there is no common logic for when it should be the case and when not. It is suggested that at least initially the use of AI should be assessed and decided on a case-by-case basis. As a general principle, it should be ensured that, in the event of administrative decisions being challenged, a complaint is reviewed by a person, *ie*, decisions taken by AI are not reviewed by AI. Whether this principle can be retained is interesting, as it sets up a limitation for AI. Should we presume that humans should stay in charge and is that what we should promote by law?

29 State Liability Act (2001) (Estonia) Art 7(1), in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/507062016001/consolide> (accessed 1 July 2020).

30 In the common law, an analogue would be the rule in *Rylands v Fletcher* (1868) LR 3 HL 330.

31 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) [2016] OJ L 119/1 (General Data Protection Regulation) (hereinafter "GDPR").

At the same time, it is not necessary to make all fundamental changes immediately, as the legal adjustments should continue as technological development continues.

23 One important challenge related to AI is that there are many stages in creating and "teaching" the machine that all, in their different ways, contribute to its activity. This includes the creator, the manufacturer (which can involve multiple entities) and the user of the AI. It would often be the case that different persons share the risk in a situation where the AI causes damage or breaches the party's obligations.[32] This is different from cases of human workers, where it is possible to determine who was involved. In general, Estonian law today provides for a mechanism that allows for strict liability of users of complex technology that uses or is based on AI.[33] However, concrete assessment of damages arising from equipment may be unsuitable in a situation in which the user of the technology is found solely responsible but does not have the financial means to compensate the damage suffered. Using the concept of increased responsibility, which can normally be avoided only in cases of *force majeure*, the so-called rule of risk liability ("liability even if innocent") places a lot of pressure on the owner and user of the technology. The question that has to be resolved is the legal borderline between "more than usually dangerous" and "just complicated AI". In 2019, the expert group led by the authors[34] first suggested that the State identify and register the emerging categories of AI-use cases but the private sector representatives claimed that this would be an additional burden that disturbs innovation. In the alternative, the idea of setting up a public insurance fund was proposed (as a predecessor of the market-based insurance system to be provided by private companies who would need to first learn the value of the market and ascertain the possible damages and problems that may occur in this new field). That idea was not well received by the public sector, based on the concern that there was a risk that private insurance companies would not be interested to "take over" the new market, and this would thereby create an unexpected financial

32 Tanel Kerikmäe *et al*, *1st Report on Legal Framework and Analysis Related to Autonomous Intelligent Technologies* (Riigikantselei/Estonian Government Office, 2019).

33 Article 1056 (liability for damage caused by major source of danger) and Art 1061 (liability of producer) of the Law of Obligations Act (2001) (Estonia), in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/515012020004/consolide> (accessed 1 July 2020).

34 Tanel Kerikmäe *et al*, *1st Report on Legal Framework and Analysis Related to Autonomous Intelligent Technologies* (Riigikantselei/Estonian Government Office, 2019).

burden for the Government.[35] Therefore, as the law currently stands, the burden of responsibility (in cases which do not relate to producer liability) stays with the user.

24 In this context, we see how AI is still regarded as "special" in some respects. It is known from other sectors that one way to deal with increased risk is through voluntary (or mandatory if the State so decides) liability insurance. The idea is that those who benefit from using technology have the obligation to share the burden of risks.

25 The complex relationships between different parties behind the creation of AI may explain why special liability rules are discussed. However, compared with other sectors where there has traditionally been such division of responsibility between users, manufacturers and possibly also others, it is important to note that AI is such a wide concept, with so many potential uses, that it cannot be said that it, as such, poses major risks. Differentiation between different uses of AI will be necessary. There may be particularly sensitive areas of use but also others where no special dangers follow from the work done through the use of AI. Risk-sharing is, in the current legal understanding, guided by the idea that those who benefit primarily from AI should be responsible for the errors and risks, even if the system is unpredictable. Liability should be assessed by case law and judicial discretion in each particular case. A parallel can be drawn with a motor vehicle, the classification of which as a "major source of danger" depends on many factors including technical standards and the context. Consideration may also be given to setting up a special position similar to that of the liability of the keeper of an animal.[36] The European Commission admits in its recent Report that "the characteristics of emerging digital technologies like AI, the IoT and robotics challenge aspects of Union and national liability frameworks and could reduce their effectiveness".[37]

26 Another area of law that deals with responsibility and is in need of careful consideration in any country introducing more AI in different sectors is consumer protection and product liability legislation. In many instances, there is no need for new or even amended legislation,

35 Tanel Kerikmäe *et al*, *1st Report on Legal Framework and Analysis Related to Autonomous Intelligent Technologies* (Riigikantselei/Estonian Government Office, 2019).

36 Tanel Kerikmäe *et al*, *1st Report on Legal Framework and Analysis Related to Autonomous Intelligent Technologies* (Riigikantselei/Estonian Government Office, 2019).

37 European Commission, *Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics* (Brussels, 19.2.2020 COM(2020) 64 final).

but attention needs to be given to questions of interpretation and establishment of who should be responsible when AI consists of many components that act as a unit. The questions may be very complex in practice but the theory behind would not be much different from what is already well known for less complex machines and devices. As far as defective products are concerned, there is legislation, including EU law,[38] with the general principle that the producer is liable for damage caused by a defect in his product. A product which is not safe must not be placed on the market or put into service. EU rules on producer responsibility and product safety provide for increased responsibility of the manufacturer (strict liability). The producer can be released from liability if he can prove that the defect in the product could not be detected at the time of placing the product on the market according to the level of scientific and technical knowledge at that time, the so-called development risk exception.[39] This exception has been seen to have the positive effect of keeping liability insurance costs relatively stable. At the same time, the Directive allows the producer to be held liable even if the latter proves that the level of scientific and technical knowledge at the time of release of the product did not allow for the detection of the defect, leading in practice to a kind of absolute liability for the producer.[40] Five Member States have made use of the option to derogate from the development risk exception, two of which apply this principle to all sectors, two of which exclude liability on this basis for pharmaceutical products and the last excluding products derived from the human body. The idea of the exception is to achieve a balance between consumer expectations about safety of products and fostering innovation, as the derogation from the exception increases the liability of the producer. In practice, with or without the derogation, at least for pharmaceutical products, case law has shown that proving causality, including that the person using the product has followed all instructions, may still prevent the producer from being held liable, so there have not been any remarkable differences in the actual liability of producers between countries with the derogation and others without.[41] The difference may be more relevant for producers of new and untested products, who have to assess the scope and extent of

38 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 (hereinafter "Directive 85/374/EEC").

39 Directive 85/374/EEC Art 7e.

40 Directive 85/374/EEC Art 15(1b).

41 Commission Staff Working Document (Brussels, 7.5.2018, SWD(2018) 157 final): *Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products*, and accompanying the document: *Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive 85/374/EEC*.

their risks from making such products publicly available. The exception clause and its derogation have been discussed in the context of AI where it is recognised that technological developments may make it difficult to interpret and ascertain the scope and application of the clause.[42]

C. Special AI legislation

27 As shown, in many cases the legal framework in which AI operates exists and can remain the same or with few changes, but there are also new issues that need to be considered. The EU in its White Paper on AI[43] calls on EU Member States to build "ecosystems of trust". These should be based on the key principles that the EU has enumerated on responsible and trustworthy AI and should be strengthened by using systems of impact assessment on AI. Fundamental rights as well as consumer rights need to be protected. The Council of Europe has elaborated on principles of AI and human rights.[44] Such measures aim to mitigate apparent conflicts and contradictions.

28 One element of AI that may create complexities is the fact that its operation is based on something which by definition is not transparent. The more complex the AI, the more complex the algorithms behind it are likely to be. This may appear to suggest that it would be a good idea to supplement certain procedural rules related to the use of AI with an obligation to publish the algorithm and basic data necessary for understanding how a specific decision was made. This would enable identifying possibly inappropriate biases resulting from the algorithm or data. It is not only theoretically but also practically possible that an algorithm will be biased and discriminate against certain individuals or groups, and it must be possible to understand when this has happened. Whether such a rule would be practically feasible, given the complexity of the technology, is unclear. As for so many things, what we see today may not match what technology can do tomorrow. There is not even a uniform and clear understanding of what is to be understood as an

42 Commission Staff Working Document (Brussels, 7.5.2018, SWD(2018) 157 final): *Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation* of *the laws, regulations and administrative provisions of the Member States concerning liability for defective products*, and accompanying the document: *Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive 85/374/EEC*.

43 European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust* (Brussels, 19.2.2020 COM(2020) 65 final).

44 "Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights" (Council of Europe, Commissioner for Human Rights) <https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights> (accessed 1 July 2020).

algorithm (especially in legal terms). However, this should not mean that there should be no attempts to institute transparency requirements to get at what the algorithm does. One recent example is the Ethical Charter[45] that emphasises that AI in judicial systems must be assessed by the principle "under user control", precluding a prescriptive approach and ensuring that users are informed actors and in control of their choices. We may not yet know enough about how AI can work, but that is no reason not to try to ensure the best possible legal framework.

29 AI comes in many forms, with many functions. Much of it may have to do with machinery, which most people do not have any specific insight about. It is thus quite natural that something that we can all imagine and envisage like so-called self-driving, or autonomous, vehicles attracts specific attention even when the actual use of AI may be limited. In Estonia, early changes to the Traffic Act[46] (from 2017) provided definitions of self-driving delivery robots, self-driving delivery robot users and the controlling of a self-driving delivery robot, as well as the requirements for the self-driving delivery robot and its use in traffic (including, for example, the speed limit of 6km/h). In particular, it is necessary to consider the extent to which all the requirements and restrictions provided for by law are appropriate as technology progresses, and whether it is necessary and proportionate to replace the currently clearly identifiable identification number, the user's phone number and the user's name requirement on the delivery robot by an automated registry solution.[47]

30 The financial sector is expected to be one of the largest economic sectors where the use of AI is present and increasing in the future. This is another sector that concerns broad sectors of society in some way – even if we are not all traders, many have some form of financial exposure. It needs to be analysed whether legislation[48] providing for the regulation of algorithmic trading is sufficient to mitigate the risks associated with this phenomenon, but also whether there is a need for additional requirements for how, for example, credit institutions and insurance companies use

45 European Commission for the Efficiency of Justice ("CEPEJ"), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment* (adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018)).

46 Traffic Act (2010) (Estonia), in English at <https://www.riigiteataja.ee/en/eli/516022016004/consolide> (accessed 1 July 2020).

47 Article 1511(4) of the Traffic Act (2010) (Estonia), in English at <https://www.riigiteataja.ee/en/eli/516022016004/consolide> (accessed 1 July 2020).

48 In Estonia, the Securities Market Act (Art 8215), in English at <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523122019001/consolide> (accessed 1 July 2020).

AI in pricing and to provide services to customers. Here, workable transparency requirements would also be very useful, if at all possible.

31 AI can be found in all kinds of sectors, including in private law situations. The use of algorithms in contracts raises the question whether today's contract law regulation is sufficient considering technological developments, and whether algorithms can be dealt with in the context of standard terms. We have the possibility of algorithmic contracts where the algorithm is used to conclude a contract. Alternatively, algorithmic contracts may be such where the terms are defined by algorithms (*eg*, price calculation). As is well known, a standard term is a contract term that has been previously developed for use in standard contracts, or which has not been negotiated separately by the parties for any other reason, and which is presented by the party using the standard term (the term user) to the other party who is therefore unable to influence the substance of the term. Many common consumer contracts are of this kind but also contracts between enterprises. The definition of referenced standard terms is sufficiently abstract to include an algorithmic contract. In principle, an algorithmic contract (or a standard term in it) may be harmful to the consumer, in which case it should be void under the relevant law on obligations. Fulfilling a contract without knowing the algorithm is probably not possible. At the same time, given how common standard contract terms are and how useful AI could be to deal with such bulk issues, we are likely to see much more of this. Perhaps it is also best treated today as something where one can leave the decision of exactly how to handle things for the future and take a case-by-case approach for now.

32 Data protection rules also need to be evaluated to see if the use of AI falls within what is permitted. The GDPR regulates the processing of personal data in both the public and private sectors and ensures the technologically neutral protection of natural persons in the processing of personal data. According to the GDPR, protection should not depend on the methods used – what matters is the basis on which personal data can be used, *ie*, when the processing of personal data is lawful and legitimate.[49] The consent of the data subject is almost always the legal basis for data processing in the private sector, while the public sector often relies on other legal bases. This is the case even if the processing of personal data takes place with the assistance of AI.[50]

49 For this purpose, the GDPR provides six legal bases (Arts 6(1)(a)–6(1)(f)). These can include AI or "manual" actions.

50 See also European Commission, *A European Strategy for Data* (Brussels, 19.2.2020 COM(2020) 66 final).

33 The GDPR provides[51] that personal data shall be collected for specified, explicit and legitimate purposes and should not be further processed in a manner that is incompatible with those purposes (purpose limitation). This is one aspect of data protection that may cause problems for the introduction of the "once-only principle" – something which AI could help make efficient. How to solve this is frequently discussed in Europe where the "once-only" principle is seen as very attractive, but the question of what limits data protection poses is not easy to answer. As machine learning – the background to AI – depends to a large extent on the availability of lots of data, there must be vigilance against a temptation to gather lots of data just because it might be useful for the AI. This would not be in accordance with the GDPR. AI as well as humans may process personal data only for purposes that are originally defined. Processing of personal data that is contrary to the purpose of the original legitimate processing is prohibited –not because of the use of AI, but because it violates the purpose limitation. It would be the same if a person did the same thing. If the once-only principle or other forms of new data use are to be introduced, the emphasis should be on how to define the purpose for which data is collected and can be used. If the definition is purpose oriented, there is no need to collect and process a lot more data, but it is still possible to use the data more efficiently, even across authorities and from different databases. The use of AI is not decisive in this respect. However, some processing is only practically possible thanks to AI. Profiling is such a phenomenon, which is much less effective without AI (even if not impossible). The GDPR contains provisions addressing the risks of profiling and automated decision-making. Profile analysis and individual decision-making based on automated processing (whether or not it involves profiling) must not unduly affect the rights of individuals. There are specific transparency and fairness requirements; there is also greater responsibility and a need for specific legal bases for processing as well as additional, specific safeguards.

34 As an example of the practice of automatic decision-making, we return to the imposition of speed-based penalties via speed cameras. Data controllers can make profile analyses and automated decisions if they follow all the principles and have a legal basis for processing. The imposition of fines using the method described above is lawful in Estonia and under the GDPR, since the processing of the said personal data is derived from the Traffic Act with appended relevant regulations. There will be more specific situations in the future that need specific regulation. The general principles that processing is lawful if it has a specific legal basis, and that its purpose has to be defined and any processing linked to this, are derived from the GDPR (Art 6) and here it is neither appropriate

51 GDPR Art 5(1)(b).

nor necessary to create additional regulation for AI. In the private sector it is possible to rely on provisions regarding the explicit consent of the individual.

IV. Legal personality

A. Relevance of the concept and topic in the possible regulation of the field

35 A Massachusetts Institute of Technology professor, in his bestseller *Life 3.0*,[52] tells the tale of the creation of Prometheus, a super AI agent. The more powerful and capable Prometheus became, the greater the concern the team members had about "imprisoning" it. It was consequently kept under custody without the possibility of accessing the Internet. The fear of robots becoming more intelligent than humans, being non-submissive and going out of control is the nightmare *par excellence* for many who are trying to predict the future. A question which straddles the division between the more practical and the more fundamental/philosophical issues is whether AI should have legal personality. Legal personality means that a natural or legal person can have the rights and obligations that he or she can claim through the courts and other bodies in his own name. Artificial agents would then "enter law's ontology, to take place alongside humans and corporations".[53] Particularly in the case of legal persons, legal personality is created and not a natural feature – the law sets certain criteria on the basis of which subjective rights are given. Rather, individuals are automatically granted these rights except in certain statutory situations where it has been withdrawn from them. If we compare AI with the idea of the legal personality of non-physical persons (companies, *etc*) it appears less dramatic to accord such legal personality to inanimate beings.

36 In different contexts, it has been discussed whether new, specific legal entities should be created. For example, in space law, the term "humanity" has been given certain rights. At the same time, it has not been resolved how "humanity" could claim its rights, because it cannot act as a whole. If there was a representative for humanity, it would be likely to be an existing or new international organisation, and there is no system to ensure that this would represent the whole of humanity. In such a situation, it can be stated that the name of "humanity" and the

52 Max Tegmark, *Life 3.0, Being Human in the Age of Artificial Intelligence* (New York: Knopf, 1st Ed, 2017).

53 Samir Chopra & Laurence F A White, *Legal Theory for Autonomous Artificial Agents* (University of Michigan Press, 2014) at p 153.

protection of its interests remain the overriding objective of law and the rule of law rather than an actual legal entity.

37 Another topical discussion of granting legal personality is in relation to animals. Laws may protect animals, but they cannot themselves stand before the court or other bodies to defend their rights. At the same time, there have been recent cases in several countries where greater rights have been granted to an animal than to an object that is protected. Animal protection and rights movements have started to vigorously argue that animals should have their own legal personalities. Most lawyers are not in favour of this, as an animal cannot protect its rights.[54] In addition, it is difficult to equate the behaviour of animals with human behaviour: if animals had similar legal personality as humans,[55] they would legally (but not necessarily practically) be able to bring legal claims against each other.

38 Legal personality has been used as a political instrument to protect certain objects. For example, it was decided in 2014 in New Zealand to grant legal personality to the river Whanganui, which had been demanded by natives – aborigines – as it, in their worldview, has the same rights as humans. However, it should be mentioned that the use of such legal personality can only have a symbolic meaning, as it is difficult to imagine that the river could be heard in court. It is not easy to incorporate the worldview of another culture into an entirely different legal tradition and system, and here too – as with humanity – it is rather a political symbol and a statement about the strengthening of aboriginal rights as a national group rather than a "real" legal personality.

B. The legal personality of AI

39 A similar symbolic value as that of the New Zealand river can be given to the subject of AI. This would emphasise the importance of AI and the fact that it plays a greater role in society than merely as an object. If we think of physical intelligence (robots) in physical form, we can even imagine that they can appear in court – as opposed to "humanity", animals or rivers. However, what added value does legal personality have and what kind of problem would it solve?

40 Creating legal personality – making someone a legal subject – declaratively/symbolically without that person actually being able to use

54 See, *eg*, Jan Zibner, "Legal Personhood: Animals, Artificial Intelligence and the Unborn [Review]" (2018) 12(1) *Masaryk University Journal of Law and Technology* 81.

55 See for detailed discussion *Legal Personhood: Animals, Artificial Intelligence and the Unborn* (A J Kurki Visa & Tomasz Pietrzykowski eds) (Heidelberg: Springer, 2017).

it does not add value to the legal system. The greater the role AI plays, the more "independent" it should be. However, legislation and social order must remain human-centred, in which AI supports and helps people and does not act arbitrarily. Legal personality in itself does not create clarity. If AI is independent, it must also be able to regulate relationships between different AI, but for this it seems to be too diverse. If AI is at least as wise as a human being, one can nevertheless pose the question: why treat it differently? In this context, it is worth pointing out that AI has intelligence, but does not have awareness (consciousness), which is part of being a human being and one of the reasons for subjectivity. What we do in our discussions on giving AI legal personality may be to unnecessarily project human properties on AI. Although different "levels" of legal personality or subjectivity already exist because legal entities do not have human rights, for example, AI is too diverse to be able to decide in general which rights would suit it.

41 A scenario where AI would have legal personality would only create apparent legal certainty and would not solve the problem of whether and how liability can be claimed as long as the AI is so diverse that we cannot classify it in any coherent manner. The foregoing is to be considered as a statement of the situation at this time, because the rapid development of technology makes it impossible to exclude the possibility of granting legal personality to AI completely. The issue of legal personality is related to the topic of personification of machines and how it may change social relations. Here the determinator is the consciousness that brings legal rights and duties to an AI agent. Can the robot be enslaved, tortured, punished, humiliated? These questions are becoming more relevant with the revolution of companion robots and AI-driven sex robots ("sexbots")[56] – even if these types of technologies do not have (yet?) soul or consciousness and are not able to feel emotions, be born or die, the acts of the owner or customer may change their attitudes and behavioural patterns that may further affect the values of society in general. There are clear signs that the market for sexbots is growing fast. It is assumed that sexbots may bring a shift to the values of society in general. There are significant ethical and legal dilemmas that reflect the hesitations and temptations in regulating the emerging market. The main concerns are related to the question of whether the human–sexbot interaction can be identified with social relationships and intercourse between humans. The level of identification can become an important margin of appreciation for lawmakers beside other considerations such

56 David Levy, "The Ethics of Robot Prostitutes" in *Robot Ethics: The Ethical and Social Implications of Robotics* (Patrick Lin ed) (Cambridge, Massachusetts: MIT Press, 2012).

as benchmarks for safety and privacy. Questions to be discussed involve sociology, medicine, technology studies and psychology.

V. Should we limit AI?

42 Technology as such is neither good nor bad – it is the use of it that can be positive or negative. The question we need to ask is whether law and regulation can support positive impacts while preventing negative effects, without stifling innovation. On the one hand, it looks like it is still too early to make fundamental decisions about AI, as we still see fairly limited versions of this technology in any major role. On the other hand, regulating things after they are already well established in an unregulated fashion is notoriously difficult. Determining whether technology or regulation should come first is a classic chicken-or-egg problem.[57] For specific legislation on concrete matters, from traffic or ships to administrative procedure or product liability, many states follow a step-by-step method, recognising where it is necessary to eliminate express requirements of human intervention. This appears a suitable approach to take, which meets the practical needs of adapting legislation without making changes just for change's sake or overly complicating the law, making it technology-dependent rather than technology neutral.[58]

43 Inevitably, as technology becomes an increasing part of our daily lives, more ethical issues will arise. It becomes more and more evident that whether technology should be limited is not only a question of what it actually can do in practice. Naturally those who develop new technology focus on this: what can it do in practice, how can it be improved to do more and more in an ever better way. This is why it is important to involve different stakeholders in the debate about what role AI should be given in our societies. Perhaps not everything than can be done should necessarily be done. Reasons to limit technological advancement may be that it would present unforeseeable risks to humans or the environment or that it would dehumanise society. The role of law is to consider these "soft" aspects in addition to the more practical ones of liability, standards and so forth.

44 The legal system is intentionally slow moving and has a conservative, stabilising effect. Laws should provide stability and

57 Katrin Nyman Metcalf, "E-governance in Law and By Law" in *Regulating eTechnologies in the European Union* (Tanel Kerikmäe ed) (Heidelberg: Springer, 2014) at p 37.

58 Ulrich Kamecke & Torsten Körber, "Technological Neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood" (2008) 29(5) *European Competition Law Review* 330.

predictability – two notions that are essential for the rule of law. This may be a problem in a fast-moving high-tech world, and it may appear as if the best way to achieve this would be to limit AI in areas where we are uncertain about what effect it actually may have. If the uncertainty is only about details or very practical issues, the argument that such an approach hinders innovation would be important. However, maybe we should be less afraid of sometimes stepping on the brakes if the uncertainty is about the fundamental nature of our society.

45 Having raised the possibility that technology should sometimes perhaps be limited, it should be emphasised that it can play a very positive role not just for various practical things but also to protect rights. Too often, the legal discussion about the interrelationship between law and technology focuses on the potential or incapability of the legal system to mitigate risks connected with technology. We should not forget to look at how technology can support the legal system. To mention an Estonian example, any access by authorities to personal data leaves a "footprint" which the individual can easily see. This automatic footprint means that persons can obtain a good overview of how their data is used. All data held on Estonian residents is kept in one place (<eesti.ee>) which is accessible with the digital identity that all Estonians have. Any access by an authority that has the right to use personal data is listed on the personal pages.[59] The data use is controlled within authorities and by the data protection inspectorate as well, in addition to the individual. Transparency is provided and a culture of serious and well-considered data use supported by technology is fostered. Another globally known example is the concept of "privacy by design", whereby data protection standards are automatically implemented in the design of systems.[60]

46 To turn back to the possible risks and the need to take decisions on limiting AI, we should be aware that as AI develops, there will be more and more ways of using it in situations where ethical questions can arise. We have to imagine situations we cannot even imagine yet! When machines start "deciding" by themselves and not just carry out the exact commands of humans it is important to think of possible consequences before the machines are "let loose" in this way. It is essential to see if protection of rights can be built into the systems, as mentioned above, in which case there is clearly an incentive to allow the use of AI. For such situations where in the process of carrying out a task there is a need to weigh things against one another it is difficult to imagine that AI will for

59 An overview is available even without logging in at <https://www.eesti.ee/en/>.

60 Addi Rull Ermo Täks & Alexander Norta, "Towards Software-Agent Enhanced Privacy Protection" in *Regulating eTechnologies in the European Union* (Tanel Kerikmäe ed) (Heidelberg: Springer, 2014) at pp 73–94.

some time be able to adequately do this. Such situations may be the last ones in which the different nature of humans will be needed, with our ability to decide in atypical situations, to take things into consideration that are not clearly delineated and so on. What exactly those situations are is not something that can be generalised, but it requires a case-by-case analysis. A related but separate question relates to the "ethical cover" when robots are used in warfare, for example.[61]

47 However, apart from such tough considerations, there can also be far easier considerations on whether to limit AI based on policy choices and not on the nature of technology. If AI or other technology can help to eliminate dangerous, dirty or humiliating jobs, most of us would agree that this is excellent. However, it can also eliminate various jobs that are not dangerous, dirty or humiliating but perhaps only somewhat repetitive and not in need of very high-level considerations. This includes things like selling train tickets or answering simple customer service enquiries. Machines may do these things better than humans in that they can do it faster and with fewer mistakes. Of course, also, the machine will not mind working 24 hours and under stress. But at the same time, there will always be people who need work that is of a routine nature, in a concrete setting: not everyone will ever become an app developer or create start-ups. Provided the decisions on the extent of automation to allow are taken in a deliberative, transparent manner, what is wrong about just deciding to preserve certain jobs for humans? The discussion on the possible limits of automation needs to be as inclusive as possible and form part of educational, academic, professional and political debate.

VI. Concluding remarks

48 Some people can hardly wait for robots to play a greater role in society, as they see technology as the best way to solve most problems. For others, technology brings with it unknown but probably increasing risks for privacy, dignity and it may even end up dehumanising society. When AI can achieve a degree of autonomy and "make its own decisions", this can be seen either to threaten the world as we know it, or to facilitate our lives in an unprecedented way. Technology moves so rapidly that it is risky to make any predictions, but the authors still dare to suggest that for now, the legal system does not need substantive changes to its fundamental principles. For the foreseeable future, AI is likely to remain a tool for humans in the sense that it will fulfil human-appointed tasks and express, directly or indirectly, the will of the human being (even

61 Mike Ryder, "Killer Robots Already Exist, and They've Been Here a Very Long Time" *The Conversation* (27 March 2019).

if the AI seemingly has a lot of "freedom"). The theoretically possible "super-agent" (super AI) capable of acting independently from the human being with its own "will" is further along in the future. If and when such a creature may appear, it is questionable whether a human-created legal environment could have any power over it in any case, any more than our laws can affect the movements of a natural phenomenon like the coronavirus.

49 If there are reasons to not let AI do anything that it can do, such decisions of limitations are policy questions rather than purely legal ones. At the same time, lawyers have a role to play, to indicate what rule of law, respect for human rights and so on, requires. To some extent, the philosophical issues have been concretised into specific norms in the form of human rights provisions, data protection rules (most notably the GDPR) and so on. It is not necessary to go to the philosophical level of what rights are and why they exist, every time that a concrete situation is considered. This can be done through the filter of the concrete norms in treaties or legislation. This layer forms a more specific element of the big questions. Finally, the top of this pyramid of issues to consider is made up of laws dealing with specific matters, where use of technology – AI specifically – may affect concrete provisions, entail a need to change procedures or requirements and so on. Here we may find anything from procedural codes to traffic legislation, consumer protection law or the regulations on the functioning of the data traffic between registers and databases. What happens in this sector is dependent on the decisions made on the principled and fundamental questions of how we want to integrate AI into our societies.

50 The pyramid of what to consider thus consists of a base of philosophy, general principles, considerations on what society should look like, what should determine the relationship between humans and machines and so on. There are many disciplines involved and these range from philosophy, ethics, religion, law, political science to medicine, engineering and security studies. The next level is where principles have been given a concrete form through international conventions, national and EU law and so on. Here we move into more legal territory but still with important elements of philosophy, political science, international relations and so on. The superstructure is that of actual laws, which require a mapping more than a profound analysis.
