Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics

*Robert van den Hoven van Genderen**

Robots have been a part of the popular imagination since antiquity. And yet the idea of a robot — a being that exists somehow in the twilight between machine and person — continues to fascinate.[1]

Privacy, data protection and physical integrity will be structurally influenced by the pervasive integration of Artificial Intelligence (AI) and robotics. Can we find ways to control this development or do we just have to live with the disintegration of privacy as we know it? Will the new rules by the GDPR on data protection suffice to protect our personal data or are these processes in the AI era impossible to regulate? How vulnerable is AI concerning the processing of our personal data? Do we still care about our privacy, if we increasingly share our personal information with other parties? What should our itinerary for the future be when attempting to create an acceptable solution? In this article these questions are discussed but the answers lie in actions for the future.

I. Some Introductory Thoughts about AI and Personal Information

Are we giving up privacy for security? This unsavoury choice — that should not be a choice at all — was recently proposed by the prime minister of the UK, Theresa May, who, coincidentally, suffered the loss of a considerable amount of public votes after announcing her plans to adapt fundamental human rights to protect security. Certainly, privacy is one of the first bulwarks to be sacrificed, next to 'habeas corpus' in the battle against terrorism. But also an important question is if the population is seriously concerned by this development, even if more intrusive Artificial Intelligence (AI) technologies are used.

Do citizens still value privacy and integrity while simultaneously participating in an increasingly transparent society where they apparently unhesitatingly, share their personal information with people they (hardly) know or give access to their personal data to any commercial company or social network which appears to offer advantages for their personal life? How will this tendency develop in the coming era of pervasive technologies such as AI and robot technology used by governments, industry and personal households? Personal robots will know everything about you, the most intimate parts of your life, your family, finances and physical history. Moreover, they will be connected to the Internet. It is of great importance to recognise this development and stimulate research on the impact of design of AI on both social relationships and the functioning of legal systems to protect our fundamental values.[2]

How valuable will Article 8 of the European Convention of Human Rights (ECHR) and the fundamental rights in the Charter of Fundamental Rights of the European Union (European Charter) prove to be in protecting human privacy? What about personal data protection rules?

Is the General Data Protection Regulation, which will be the standard for the protection of our personal data in Europe, sufficiently equipped to protect our data in our personal bubble, against the techno-

* Dr Robert van den Hoven van Genderen is director of the Center for Law & internet (CLI) Vrije Universiteit Amsterdam, visiting fellow at Peking university and Tohoku University Japan and partner of Switchlegal Lawyers, Amsterdam. For correspondence: <rob.vandenhovenvangenderen@switchlegal.nl>.

1 Ryan Calo, 'Robots as Legal Metaphor' (2016) 30(1) Harvard Journal of Law & Technology.

2 As is the core of these provided by Lawrence Lessig, Which code is necessary to regulate the architecture (in this case cyberspace) and provide for the protection of our freedoms? Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999); Lawrence Lessig, *Code and other laws of cyberspace* (Basic Books 1999).

logical developments in processing by AI and the use of this technology by authorities, industry, our fellow citizens and more criminally intended parties? The Committee on Civil Liberties, Justice and Home Affairs thinks so:

> A. Whereas the technological advancements in the area of robotics will bring positive effects for the Union economy and also for the daily life of individuals, but might also imply risks which need to be addressed; whereas the development of all new technological and production paradigms, within or outside of the framework of Horizon 2020, must respect ethical principles and have due regard to the fundamental rights enshrined in the Charter of Fundamental Rights (CFR);
>
> B. Whereas a number of third countries have adopted guidelines and legislation on robotics and some Member States have launched specific reflections in this area; whereas a regulatory framework that governs at Union level the development and the use of robotics and artificial intelligence and builds on existing rules such as the Union's General Data Protection Regulation could prevent a fragmentation of rules in the single market and further safeguard the protection of the fundamental rights of all EU citizens to human dignity, privacy and family life, the protection of personal data and intellectual property, freedom of expression and information, equality and non-discrimination, solidarity, and citizens' rights and justice, as well as security and safety, while being subject to the principle of proportionality;[3]

1. Privacy and Data Protection

Defining privacy in a technologically developing world is one of the most intractable problems in privacy studies.[4] Perhaps even more difficult is the weighing of the value of privacy against that of public interest in a broad sense.[5] Do we hamper the economic development of AI if we want to control the processing of personal data and want to protect our personal life? And what do we want to control? From a socio-philosophical perspective, privacy can also be defined as a 'control-right' to which I concur:

> A privacy right is an access control right over oneself and right to information about oneself. Privacy rights also include a use or control feature—that is, privacy rights allow me exclusive use and control over personal information and specific bodies or locations.[6]

The fundamental right to privacy, in the sense of non-interference by government, is protected by international and national law. In their essence, the elements of privacy are based upon the non-interference principle of Article 8 of the ECHR: 'Everyone has the right to respect for his privacy and family life, his home and his correspondence.'

Although the protection of privacy, family life and communications is secured by Article 7 of the European Charter,[7] the European Union specifies, in Article 8, the protection and control of personal data. By specifying protection and control over personal data, the Charter stresses the importance of data protection. De Hert and Gutwirth explain the differentiation between privacy and data protection as:

> For us privacy is an example of a 'tool of opacity' (stopping power, setting normative limits to power), while data protection and criminal procedure can be mainly -not exclusively- seen as 'tools of transparency' (regulating and channelling necessary/reasonable/legitimate power).[8]

A substantial aspect of the willing or unwilling intrusion of privacy these days consists of processing of personal data of individuals. Individuals have a strong urge to be in control of their personal information under a variety of circumstances. Opacity will make it difficult to effectuate this control. There is such an abundance of data, which is used in both social and commercial networks, that control by the da-

---

3 European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on Legal Affairs with recommendations to the Commission on Civil Law Rules on Robotics' (23 November 2016) 2015/2103(INL).

4 As described by the author: Robert van den Hoven van Genderen, *Privacy Limitation Clauses: Trojan Horses under the Disguise of Democracy* (Kluwer 2016) 12, also citing Reidenberg 1992.

5 Gregory Walters, 'Privacy and Security: An Ethical Analysis' (2001) Computers and Society, 9, in reference to Arendt (1949) 69-71.

6 Adam Moore, 'Defining Privacy' (2008) 39(3) Journal of Social Philosophy 411, 414.

7 Charter of Fundamental Rights of the European Union (2010/C 83/02).

8 Serge Gutwirth and Paul De Hert, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2007).

ta-subject of the processing of his/her own data is almost impossible. The processing of personal data by AI systems can hardly contribute to increasing the transparency if the legal system lags behind.

If AI is used as an instrument we can try to regulate its use. If the autonomy of AI entities increases it will be much harder to maintain transparency concerning their processing of personal data by regulations directed to human authorities and humanly directed rights.

Concerning the protection of privacy and personal data the Committee on Civil Liberties, Justice and Home Affairs is giving high-level indications for future regulations by stressing the responsibility of the developers and designers of AI applications by the following:

> (6.) Reiterates that the right to the protection of private life and the right to the protection of personal data as enshrined in Article 7 and 8 CFR and Article 16 TFEU apply to all areas of robotics and artificial intelligence and that the Union legal framework for data protection must be fully complied with; underlines the responsibility of designers of robotics and artificial intelligence to develop products in such a way that they are safe, secure and fit for purpose and follow procedures for data processing compliant with existing legislation, confidentiality, anonymity, fair treatment and due process;[9]

Furthermore, the Committee stresses the fact that the rapid development of AI and robotics is to be controlled by legislation that will ensure the principles of privacy by design, also or certainly concerning cyber-physical systems, being integration of human bodies (and minds!) with AI appliances:

> (7.) Calls on the Commission to ensure that any Union legislation on robotics and artificial intelligence will include measures and rules which take into account the rapid technological evolution in this field, including in the development of cyber-physical systems, to ensure that Union legislation does not lag behind the curve of technological development and deployment; stresses the need for such legislation to be compliant with rules on privacy and data protection, i.e. concerning information obligations, the right to obtain an explanation of a decision based on automated processing, the requirement to follow the principles of privacy by design and by default, the principles of proportionality, necessity, data minimization, purpose limitation, as well as transparent control mechanisms for data subjects and data protection authorities, and appropriate remedies in compliance with current legislation; calls for the review of rules, principles and criteria regarding the use of cameras and sensors in robots, artificial intelligence in accordance with the Union legal framework for data protection;
>
> (8.) Calls for a uniform, horizontal approach to robotics and artificial intelligence in the Union regulatory framework which is technology-neutral and applies to the various sectors in which robotics could be employed, such as transport, health, industrial manufacturing, telecoms, law enforcement and many others; emphasizes that, where appropriate, the existing legal framework should be updated and complemented to ensure an equal level of data protection, privacy and security;
>
> (9.) Highlights the importance of preventing mass-surveillance through robotics and artificial intelligence technologies;
>
> (10.) Calls on the Commission and the Member States to promote strong and transparent cooperation between the public and private sectors and academia that would reinforce knowledge sharing, and to promote education and training for designers on ethical implications, safety and respect of fundamental rights as well as for consumers on the use of robotics and artificial intelligence, with particular focus on safety and data privacy.[10]

This advice focusses on preventing the risks on data privacy by new technologies and stimulating knowledge. The problem is that for a large part we do not know which developments will take place in the applications of AI and robotics. Requiring a technological neutral regulatory framework will not be possible because the technological development will be varying in such a broad spectrum that specification of these different applications, certainly concerning the differences in autonomy, will be unavoidable.

The warning for the use of AI technology in surveillance systems is a realistic fear that is based on the (less) technologically advanced surveillance of the past and present. The use of advanced technolo-

9 Committee on Civil Liberties, Justice and Home Affairs (n 3).

10 ibid.

gy by authorities has been a point of concern with regard to the protection of the privacy of European citizens and will be increased by intrusive technologies.

2. Intrusive Instruments in a (Less) Intelligent Perspective

Several court decisions have issued warnings about the use of new intrusive technology by police authorities. Crossing the border of ascertained protection of privacy by new technology was considered justifiable for the acceptable use of intrusive instruments:

> The court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.[11]

The *Malone v UK* case, before the European Court on Human Rights (ECtHR), determined that no right guaranteed by the European Convention should be interfered with unless a citizen knows the basis for the interference through an ascertainable national law.[12] In *Kruslin v France*,[13] concerning the use of surveillance techniques, it was stated by the European Court that: 'It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated'

And in the case *S and Marper v the United Kingdom*:[14] 'The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned [...].'

Concerning the interception of communications, the ECtHR stated that this represents a 'serious interference' with private life; therefore, the law must be particularly precise.[15] With regard to interferences with private life in the 'prevention of crime' context, it appears that the European Court is demanding increasingly rigorous legal provisions as made clear in the case *Valenzuela v Spain*.[16]

Also, the Article 29 Working Party (A29 WP) has issued an Opinion on the use of new (AI) technology concerning the introduction of the General Data Protection Regulation (GDPR) where it states that it will be easier for authorities and industry to make use of new intrusive technology. The A29 WP Opinion on technology-enabling, data processing at work can now be implemented at a fraction of the costs of several years ago whilst the capacity for the processing of personal data by these technologies has increased exponentially; new forms of processing, such as those concerning personal data on the use of online services and/or location data from a smart device, are much less visible to employees than other more traditional types, such as overt CCTV cameras. This raises questions about the extent to which employees are aware of such technology since employers might unlawfully implement the same without prior notice to the employees; and the boundaries between home and work have become increasingly blurred. For example, when employees work remotely (eg from home) or travelling for business, monitoring of activities outside physical working environment can take place and potentially include monitoring of the individual in a private context.[17]

The question emerges if it would be possible, considering that the amount of information about ourselves is increasing dramatically, that this data can be protected; and if the concept of informational sovereignty - in so far as it ever existed - will develop in to an empty casket.

3. Privacy, Data Protection and Intrusive Technology

It seems to be that the statement Daniel Solove uttered 11 years ago - 'Privacy seems to be about everything, and therefore it appears to be nothing' - is proving to be a rational way of thinking about privacy.[18] This concept can become true if the means to maintain the law on privacy and data protection by au-

11 See eg, *S and Marper v the United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), para 112.

12 *Malone v UK* App no 8691/79 (ECtHR, 2 August 1984); *Leander v Sweden* App no 9248/81 (ECtHR, 26 March 1987).

13 *Kruslin v France* App no 11801/85 (ECtHR, 24 April 1990).

14 *S and Marper v the United Kingdom* (n 11) paras 99, 103.

15 *Kopp v Switzerland* App no 23224/94 (ECtHR, 25 March 1998).

16 *Valenzuela Contreras v Spain* App no 58/1997/842/1048 (ECtHR, 30 July 1998).

17 Article 29 Working Party, 'Opinion 2/2017 on data processing at work' (8 June 2017) WP 249 <http://ec.europa.eu/newsroom/document.cfm?doc_id=45631> accessed 5 September 2017.

18 Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154(3) University of Pennsylvania Law Review 477, 479.

thorities is not available and at the same time, it is impossible for data subjects to control what is happening with their personal data. Although privacy protection concerns the defence of our personal bubble and data protection concerns the protection of personal data during processing, these two concepts seem to come near to each other regarding AI applications. The uncontrolled use of AI to process data will invade the most intimate parts of our personal life. The integral use of our data by society as a whole will undeniably become part of the new social and economic system. Data is the new currency for which, knowingly or unknowingly, we trade our most sensitive information.

WhatsApp is not 'free'. Facebook uses all personal data, even if it has to pay a €110 million fine to the European Commission.[19] Governmental authorities such as the police and security agencies will use the technology available to select and profile individuals as well as specific groups of people, to prevent terrorism or simply curtail any anti-social behaviour. This is not science fiction anymore. Robot drones of the size and in the shape of a mosquito can follow whoever they are targeted upon with camera eyes, even equipped with a sucking needle to retrieve a drop of blood to analyse the subject's DNA or inject poison if the individual is an enemy of the state.[20] Furthermore, mass surveillance by governmental security agencies, data mining by use of intelligent big data analysing algorithms, the use of intelligent sensor-equipped devices, will undoubtedly be applied in the very near future to protect public and national security, easily stepping over the fact that mass government surveillance could be a greater threat to democratic society than the security it would like to protect by these measures. By creeping surveillance techniques, the use of AI for reasons of protecting society in the name of national and public security, the basis of democracy itself could easily be destroyed. The umbrella of the ECHR and the European Charter should be protecting the citizen against unfettered use of AI technologies in surveillance activities. The ill-used comparison of trading privacy for security will certainly not stand the test of using AI techniques to create a more intrusive control system of citizens by governments.

Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention.[21]

There is a clear evolution of the fear of Louis Brandeis in 1928 that:

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard.[22]

And his well known, prophesising citation related to time works brings into existence new conditions and purposes. Be it that the technology will not only be available to governments but also to the commercial industry as well as the 'criminal industry':

> Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[23]

This can also be considered in an artificial intelligent daylight where the need for clear rules of use in a transparent manner is recognised:

19 European Commission, 'Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover' (Press release, 18 May 2017) <http://europa.eu/rapid/press-release_IP-17-1369_en.htm> accessed 5 September 2017.
'Commissioner Margrethe Vestager, in charge of competition policy, said: "Today's decision sends a clear signal to companies that they must comply with all aspects of EU merger rules, including the obligation to provide correct information. And it imposes a proportionate and deterrent fine on Facebook. The Commission must be able to take decisions about mergers' effects on competition in full knowledge of accurate facts."'

20 'US Develops Robot Mosquito Spy Drones' (*HNN*, 23 July 2015) <http://alexanderhiggins.com/us-develops-robot-mosquito-spy-drones/> accessed 5 September 2017.

21 *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2017), paras 68-70.

22 *Louis Brandeis in Olmstead v United States*, 277 US 438 (1928), 277 US 475.

23 ibid 277 US 473.

> It is essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures[24]

Although, as in the *Zakharov* case, it was recognised that the possible use of surveillance instruments must be clear to citizens, invasion of privacy is going beyond tapping by police and secret services. Even when rules are clear, the use of intelligent invasive technologies will make it harder to control a just execution of the legal possibilities of governmental authorities.

II. Internet of Intelligent Things and People

Not just in surveillance appliances, but more dramatically, in everyday life, we can conclude that the physical, intelligence and digital converge in the Internet of Things. More and more connected devices will peep, creep, fly or walk into our lives. The emerging technology in information processing will produce incredible amounts of specified personal data that will be used by all governmental, social and economic actors in our society. To give an example, the owner of a semi-autonomous car, such as a Tesla, agrees with the producer to transfer personal information considering all aspects of the driving experience. This information, of course, will be only reserved for the improvement of the technology and safety of the driving. But the information is going beyond driving since it also includes the access to contacts, browsing history, navigation history and radio listening history.[25] The question may be posed if this is really necessary for the purpose.

This certainly is not the last step in the use of personal data for further developments of increasingly autonomous vehicles and other devices. Integration of humans with machines is considered a 'real life' possibility. The personified autonomous intelligence is evolving. Elon Musk, CEO of Tesla, recently launched Neuralink, a company that is researching methods to upload and download thoughts. He stated in Dubai that there is a need for humans to become cyborgs if we are to survive the rise of artificial intelligence. As Musk himself predicts: 'Over time I think we will probably see a closer merger of biological intelligence and digital intelligence'.[26]

Ultimately, Neuralink wants to change how we interact with devices by linking our brains to the machines we interact with most often: cars, mobile devices and smart items in our smart home.[27] That development of machine-human integration can already be noticed all around us. We can accentuate the positive aspects of using artificial limbs with our own nerve system, walking for people with a spinal cord lesion by means of exoskeletons and other appliances. Diabetics will be controlled by insulin sensors and pumps in the body, possibly connected to human specialists via the Internet. But what is the effect on our privacy? Who can use this data, how is this sensitive data protected? And do we mind? Will developments in robotics, artificial intelligence and computing in general increase our consciousness of the threat to privacy? Are we aware of the different ways in which our privacy is being eroded and how this erosion could increase in the future? Privacy has not, and will not, disappear all at once; rather, it dynamically adapts; or, in a negative sense, becomes degraded slowly over time. As Solove puts it: 'Privacy is rarely lost in one fell swoop. It is usually eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone.'[28]

---

24 *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015), para 229.

25 'Your vehicle collects and stores certain telematics data regarding its performance and condition, including the following: vehicle identification number, speed and distance information, battery use management information, battery charging history, battery deterioration information, electrical system functions, software version information, infotainment system data, safety-related data (including information regarding the vehicle's SRS systems, brakes, security, e-brake), and other data to assist in identifying and analszing the performance of the vehicle (collectively, 'Telematics Log Data'). We collect and process this Telematics Log Data.' - 'Tesla privacy statement' (Rev 14 June 2013) <http://www.tesla.com/sites/default/files/pdfs/tmi_privacy_statement_external_6-14-2013_v2.pdf> accessed 9 September 2017.

26 Mahita Gajanan, 'Elon Musk Says Humans Need to Merge With Machines to Remain Relevant' (*Fortune*, 13 February 2017) <http://fortune.com/2017/02/13/elon-musk-human-artificial-intelligence/> accessed 12 September 2017.

27 Liat Clark, 'Elon Musk reveals more about his plan to merge man and machine with Neuralink' (*Wired,* 21 April 2017) <<http://www.wired.co.uk/article/elon-musk-neuralink>> accessed 7 June 2017.

28 Daniel J Solove, *Nothing to Hide: The False Trade off Between Privacy and Security* (Yale University Press 2011).

The question is if we will notice how much is gone; or are we already so much integrated with the mechanisms of our information technology that the next step will go unnoticed. Will the smart home still be our private home?[29]

III. Robots and Artificial Intelligence

1. Artificial Intelligence

This last mentioned concept of machine-human integration is a development that is taking a step beyond AI and robotics technology. What is considered artificial intelligence to start with? Its definitions seem to already be outdated, considering the integration between man and machine. Also, the integration between robotics and AI results in widely varying descriptions of the phenomena. The European Economic and Social Committee (EESC) recently recognised this in its Opinion (reported by Catelijne Muller) on 'The Consequences of Artificial Intelligence on the (Digital) Single Market, Production, Consumption, Employment and Society':

> There is no single accepted and rigid definition of AI. AI is a catch-all term for a large number of sub(fields) such as: cognitive computing (algorithms that reason and understand at a higher (more human) level), machine learning (algorithms that can teach themselves tasks), augmented intelligence (cooperation between human and machine) and AI robotics (AI imbedded in robots). The central aim of AI research and development is, however, to automate intelligent behaviour such as reasoning, the gathering of information, planning, learning, communicating, manipulating, detecting and even creating, dreaming and perceiving.[30]

Moreover, the report specifies narrow and general AI, stepping out of the commonly agreed concept of AI:

> AI is broadly divided into narrow AI and general AI. Narrow AI is capable of carrying out specific tasks. General AI is capable of carrying out any mental task that can be carried out by a human being.[31]

The narrow definition is not very well explained but it addresses specific application areas such as playing strategic games, language translation, self-driving vehicles and image recognition.[32]

Generally, AI is considered the imitation of human behaviour by machines. Originally, the term was conceived in the so-called 'Dartmouth Conference,' convened on invitation by John McCarthy in 1956.[33] The proposal considered: 'An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans and improve themselves.'[34]

This means that there are elements of human-like behaviour and a possibility of (deep) learning to improve the functioning of the programme, or entity, or combination. A possible means to determine the level of AI is the so-called 'Turing Test' developed by Allen Turing in 1950, developed from his first experiment, the Turing machine in 1936. This test could more or less prove that a computer/machine cannot be distinguished from the reaction, intelligence, behaviour and answers of a human being.[35]

In the US presidential paper 'Preparing for the Future of Artificial Intelligence', reference is made to the following taxonomy: (1) systems that think like humans (eg cognitive architectures and neural networks); (2) systems that act like humans (eg pass the Turing Test via natural language processing, knowl-

29 See also, Giles Birchley et al, *Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies* (December 2017) BMC Medical Ethics <https://link.springer.com/article/10.1186/s12910-017-0183-z> accessed 9 September 2017.

30 Catelijne Muller, European Economic and Social Committee, Artificial intelligence, 'Opinion Section for the Single Market, Production and Consumption Artificial Intelligence – The Consequences of Artificial Intelligence on the (Digital) Single Market, Production, Consumption, Employment and Society' (Own-initiative opinion, 31 May 2017) 7 (EESC Opinion).

31 ibid.

32 'Narrow AI is not a single technical approach, but rather a set of discrete problems whose solutions rely on a tool kit of AI methods along with some problem-specific algorithms. The diversity of Narrow AI problems and solutions, and the apparent need to develop specific methods for each Narrow AI application, has made it infeasible to "generalize" a single Narrow AI solution to produce intelligent behavior of general applicability.' Executive Office of the President National Science and Technology Council, 'Preparing for the Future of Artificial Intelligence' (12 October 2016) 7.

33 John McCarthy et al, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence: August 31, 1955' (2006) 27(4) AI Magazine 12.

34 ibid.

35 Alan M Turing, 'Computing Machinery and Intelligence' (1950) 59(236) Mind 433. The Turing Test is an experiment by Alan Turing in 1936, further elaborated in the mentioned article to determine if a machine can perform with humanlike intelligence.

edge representation, automated reasoning and learning); (3) systems that think rationally (eg logic solvers, inference and optimisation); and (4) systems that act rationally (eg intelligent software agents and embodied robots that achieve goals via perception, planning, reasoning, learning, communicating, decision-making and acting).[36]

2. Robots

Robots are considered a different concept from AI; but increasingly, AI and robots will be less separate. A robot is nothing else than an AI system, albeit different in form and function, and will be continuously developing.

The first references to robots were mainly given to the anthropomorphic appearance, the human-like robot. Originally, the term 'robot' was introduced in a play by the Czech writer Karel Čapek who was inspired by his brother Joseph. The play was named: RUR, or Rossum's Universal Robots. The word 'robot' comes from an Old Church Slavonic word '*Robota*' for 'slavery,' 'forced labour' or 'monotonous work.' Robotics as a collective name - loosely translated - refers to automate labour-intensive processes and the replacement in an action of the human component by a robot. This automation has been around since the industrial revolution and became a widely used technique in production. Usually, the robot is instructed by human programmers and performs a number of tasks that used to be carried out by an individual.

Robots, however, can be distinguished into different categories that range from the simple industrial robot to the more intelligent, specialised robots such as surgical robots and intelligent vehicles until the fully autonomous intelligent robots that are capable to function without and beyond human control. These robots will be fully AI-integrated entities, probably sentient and capable of using all kinds of data available to this entity. The most important trait is the qualification of being an autonomous entity:

> Autonomy refers to the ability of a system to operate and adapt to changing circumstances with reduced or without human control. For example, an autonomous car could drive itself to its destination; autonomy is a much broader concept that includes scenarios such as automated financial trading and automated content curation systems. Autonomy also includes systems that can diagnose and repair faults in their own operation, such as identifying and fixing security vulnerabilities.[37]

This autonomously functioning robot will act and decide on an independent basis and will, in the end, probably perform acts with legal effect and will have a kind of legal personhood. This autonomously qualified robot is the subject of many science fiction books and films, mostly with a negative connotation such as: they will take over the world; and will destroy the human parasite that is detrimental to earth; and the machine evolution. Even modern scientists and industrialists as Steve Hawking, Elon Musk and Bill Gates have proclaimed that: 'The development of full artificial intelligence could spell the end of the human race.'[38]

On the other hand, Elon Musk, in Davos and Dubai, recently prophesised a positive development in the form of human-robotic integration.[39]

Bostrom and Yukowski note that the transition from object to legal personhood forces other legal persons to treat the AI as an end and not as a means to an end.[40] The moral and ethical question will be if we want robots to take decisions that we do not have control over.[41]

The optimal approach to protect humans at the current time is to ensure that autonomous robots are designed to comply with all laws in any jurisdiction in which they operate. The robotic law in the EU and

---

36 Executive Office of the President (n 32).

37 ibid 8.

38 A more positive view would be that the autonomous intelligent robot is not interested in power, considering this as a malfunction of the human mind, and will take part in improving science, industry, environmental and social structures.

39 'Over time I think we will probably see a closer merger of biological intelligence and digital intelligence,' Musk told an audience at the World Government Summit in Dubai, where he also launched Tesla in the United Arab Emirates (UAE). 'It's mostly about the bandwidth, the speed of the connection between your brain and the digital version of yourself, particularly output.' Arjun Kharpal, 'Elon Musk: Humans must merge with machines or become irrelevant in AI age' (*CNBC*, 13 February 2017) <https://www.cnbc.com/2017/02/13/elon-musk-humans-merge-machines-cyborg-artificial-intelligence-robots.html> accessed 9 September 2017.

40 Nick Bostrom and Eliezer Yudkowsky, 'The Ethics of Artificial Intelligence' in Keith Frankish and William Ramsey (eds), *The Cambridge Handbook of Artificial Intelligence* (Cambridge University Press 2014) 321.

41 Roman Yampolskiy, 'Artificial Intelligence Safety Engineering: Why Machine Ethics is a Wrong Approach' in Vincent Mueller (ed), *Philosophy and Theory of Artificial Intelligence* (Springer 2013) 390.

member states should also be very specific concerning actions prohibited to robots such as intentionally disclosing private information without explicit authorisation from the natural person whom the information concerns.

Explicit language is necessary to prevent the development of ambiguities concerning permitted behaviours that may result in confusion for the artificial intelligent entities.

Despite safeguards, it may be possible to deceive a robot so that it engages in acts that

could be harmful to humans, such as privacy intrusions, without understanding that it is violating the law.[42]

But still, it will be difficult or even impossible to control the processing of personal data of natural persons by autonomous or even less independent robots. A solution to this could be found in the development of algorithms that exclude the further processing of personal data of natural persons beyond the defined functions of the robot. But with self-learning autonomous robots the control over these processes will be difficult.

IV. Privacy, AI and the General Data Protection Regulation

The ECHR and Charter are the (European) basis for the principles concerning the protection of privacy, personal life and personal data. The specific protection of personal data in the EU will be covered by the GDPR. It is considered of great importance in the GDPR that the ways and means of data processing are transparent to the data subject. This will be a complicating aspect when using AI. One could expect that this development would have some attention in the new regulation. Surprisingly, there is no vision on the use of AI and robotics in the GDPR. These concepts are nowhere to be found in the text or recitals.

It could be argued that this General Data Protection *Regulation* is not the proper instrument to reflect on future developments and that such a Regulation should be technologically neutral in its terms and generally applicable. In the former Council text, this principle was described in Recital 13, and in the definitive text, in Recital 15: 'In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.'

However, if that was to be the case, references to the 'internet' should be absent; but these are definitely present.

Certainly, the definitions of 'processing' and 'personal data' will apply to the processing of personal data by AI entities and systems as well. Also, the scope and material application in the sense of Article 2(1) GDPR will apply to the processing of personal data by AI entities and systems:

> Processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

But can the robot be considered a filing system? And will the contents of Recital 4 always be applicable:

> The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

How proportionate would be the use and control of personal robots by governments or even insurance companies to improve society? How can a natural person give his explicit permission to process information by AI; or is this a "household" processing? Will the 'processor' or 'controller' be responsible if there is no possibility to check the processing and if it is not clear what the autonomous robot is doing with personal information, be it within the purpose of its function? Should we exclude AI systems from the applicability of this Regulation?

Still, there are valuable principles within the GDPR that can be of importance to the protection of personal data and privacy in a broader sense and could be related to AI. In Recital 78 it is stated that:

> The requirements of the protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation [...].

42 Chris Holder et al, 'Robotics and Law: Key Legal and Regulatory Implications of the Robotics Age (Part I of II)' (2016) 32(3) Computer Law and Security Review 397.

This could easily apply to the use and also the developing, designing, selecting and using applications, services and products that are based on the processing of data by AI applications. The state of the art protection, however, could be insufficient if we make use of 'self/deep-learning AI entities'. Also, requirements with regard to transparency would be very difficult to maintain.

V. Physical and Informational Integrity; Use of Sensitive Data

All of the above makes it very difficult to have a credible enforcement of regulations and sanctions as increasingly semi-intelligent products flood our society. Three cases of use of personal data without permission by still semi-intelligent products can be demonstrated to clarify some of the future problems. These examples concern the connection of the 'intelligent' product to the internet and third parties, without knowledge or consent of the user.

The first case concerns the doll "Cayla" that can have 'smart' communication with its child user.

The German Federal Network Agency (*Bundesnetzagentur*) told parents to destroy a doll – 'Cayla' - made by Genesis Toys because its smart technology could be used to reveal personal data by connecting to the Internet via Bluetooth. The doll responded to children's queries by using a concealed internal microphone and this mechanism apparently violated German privacy law. The controversy over Cayla highlighted the privacy perils of a world where toys can be connected to the Internet, and where a child may confide private secrets to a 'doll' that records what the child says. Even if a toy company has no intention of violating privacy, the Internet connection could serve as a tempting target for hackers or ambitious marketers.[43]

The second case is possibly even more sensitive. It concerns the case of two women against the Standard Innovation Corp. This company used the personal information of the user of the 'We-Vibe Rave' vibrator, accessible via Bluetooth and Wi-Fi over the Internet. Obviously, that information was meant to improve the product and improve service to the user, but the Court of Illinois ruled that using this intimate information without permission was unlawful and convicted the company to pay $3.75 million to plaintiffs.[44]

These cases are examples of the current evolution of semi-intelligent devices. In the future, an increasing amount of 'wearables' will be connected to communities and manufactures.

Another example of the illegal use of sensitive information concerned the investigation by the Dutch Privacy Authority into the Nike 'intelligent' running shoes. Data about the physical activities were connected to the user's smartphone or watch appliance. These appliances were not only communicating with the owner of the shoes but also with the manufacturer. Sensitive information was processed and stored by Nike. This was against privacy regulations.

The processing of health data entails risks, including the risk of discrimination based on an individual's presumed or actual health condition. This is, therefore, a processing of special personal data (data concerning the data subject's health) as referred to in section 16 of the Wbp.

Nike was obliged to inform (future) users in The Netherlands about the data processing via the app by means of two different privacy policies, a specific privacy policy for the app and a general privacy and cookie policy.[45]

Nevertheless, can we be bothered to enact serious and effective legal data protection rules if everyone is already giving personal information to the Internet by using their smartphone? It is now a technical possibility to give every device its own IP address and connect it to the Internet, if so desired. This is manifest in the concept of the Internet of Things, whereby, typically, ordinary objects are connected to the internet in order to be imbued with smart properties. This is already taking place. For example, smart thermostats such as 'Toon' gather energy measurements and other smart household objects. The future holds even more extensively invading options. Consider, for example, an advanced version of an AI – a personal assistant software, such as Apple's Siri,

43 Feliz Solomon, 'Germany is Telling Parents to Destroy Dolls that Might be Spying on Their Children' (*Fortune,* 20 February 2017) <http://fortune.com/2017/02/20/germany-cayla-doll-privacy-surveillance/> accessed 7 September 2017

44 *NP v Standard Innovation (US), Corp, d/b/a WE-VIBE* [2016] The United States District Court for the Northern District of Illinois Eastern Division Case No 1:16-cv-8655.

45 College Bescherming Persoonsgegevens, *Selection from DPA Investigation Nike+ Running App* (Public version, 2 November 2015) <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_dpa_investigation_nike_running_app.pdf > accessed 7 September 2017.

Microsoft's Cortana, or Amazon's Alexa, that could help you manage your home. These commonly used applications will be combined with your movements, daily activities, physical data and can profile your whereabouts, physical conditions, needs and interests.

1. Social Interacting, AI and Privacy

In light of the concept of personal informational sovereignty, the control of one's personal information will be increasingly difficult and the isolated autonomous view of controlling information is changing to a system of social privacy and social interaction in a spectrum of either sharing, or not sharing information with others. Besides that concept, there is the question of unconscious, tacit information sharing. Will this be a matter of privacy becoming the morphing, dynamic construct in social relations within society? Are natural persons the only actors in this field, or can AI play a role to find a new 'privacy equilibrium', if it ever will be an equilibrium? Will we hold on to an outdated idea at the complete other side of the spectrum: the choice for splendid isolation as informational hermit in a sea of continuous information exchange. It seems that nowadays people will easily give up privacy for convenience and will not take expensive or even small actions to preserve their privacy, according to Susan Athey of Stanford University.[46]

The youngest millennial generation is already of the opinion that social progress, in general, owes a debt to privacy as it allows one the ability to freely realise and express oneself and not be bound to whatever social norms are currently in place. It upholds a way of living that most millennials want and appreciate. Millennials conceive privacy as something social, rather than individual. A small personal research gave me the impression that this group has no problem trading privacy away for other perceived social or personal gains, services or products.[47]

Alongside the above-mentioned group, people can decide for themselves what they want to trade and where they set their boundaries. But will they do that? Are they conscious of the fact that they have the choice to be 'master of their own personal universe'? Or is that just a theoretical possibility in the AI society?

Another aspect of the ultimate AI surveillance society - that exists due to the use of all kinds of sensors and controlling devices - may be that people will tend to behave differently, such as with a form of self-censorship or chilling effect, when they know that they are being watched or when their behaviour is registered.

In any case, privacy conception in the future seems to be constructed around the weighing process of using personal information to reach certain targets and to have an acceptable position in a more or less controlled society.

The question is who will be controlling this: government, industry, the people or the AI system?

a. The Threats for Privacy in the AI Society

i. General Problems

In the EESC report on AI, it is noted that there are some downsides to AI integration in society:

> As with every disruptive technology, AI also entails risks and complex policy challenges in areas such as safety and monitoring, socio-economic aspects, ethics and privacy, reliability, etc.[48]

It is striking that the EESC uses the word 'disruptive' for this technological revolution of society. It therefore also describes these threats going beyond the limits of privacy. Still, the threats are connected to privacy, in the sense that they also concern ethical questions about the impact of autonomous (self-teaching) AI on personal integrity, autonomy, dignity, independence, equality, safety and freedom of choice. The question is how one will ensure that fundamental norms, values and human rights remain respected and safeguarded. Also, the transparency mentioned above, the ability to understand, monitor and certify the operation, actions and decisions of AI systems, retrospectively as well, will become a problem. The comprehensibility, monitoring ability and accountability of the decision-making process of an AI system is crucial in this regard.

Currently, many AI systems are very difficult for users to understand. This is also increasingly true for

46 Susan Athey, Cristian Catalini and Catherine Tucker, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk' (Stanford University, 13 February 2017) <https://people.stanford.edu/athey/sites/default/files/digital_privacy_paradox_02_13_17.pdf> accessed 7 September 2017.

47 Opinion of several of my students in the course 'Robot-Law and Privacy' (2017).

48 EESC Opinion (n 30) 5.

those who develop the systems. In particular, neural networks are often 'black boxes,' in which the (decision-making) processes taking place can no longer be understood and for which there are no explanatory mechanisms.[49]

Concerning the specific privacy issues, the opinion is rather high level: not giving a specific roadmap how to solve the problems concerning privacy.

Privacy of AI systems is considered an issue of concern. Reference only has to be made to the many (consumer) products with already built-in AI: household appliances, children's toys, cars, health trackers and smartphones. It is noted that these products transmit (often personal) data to the cloud-based platforms of their manufacturers. Whether or not privacy is sufficiently guaranteed is an issue of concern, particularly given that trade in data is now booming; meaning that the generated data does not remain with the producer, but is sold to third parties.

> AI is also able to influence people's choices in many areas (from commercial decisions to elections and referendums) by analysing large quantities of (often) personal data. Children are a particularly vulnerable group. The EESC is concerned about AI applications that explicitly aim to influence the behaviour and desires of children.[50]

This last observation was also applicable in the case of the above mentioned doll Cayla that told the children to visit Disneyland and other fun parks.

The EESC Opinion on the GDPR applicability just mentions the fact that in the light of the development of AI, it should be properly monitored whether people's right to informed consent and freedom of choice when submitting data - as well as their right to access, amend and verify data - are reasonably assured in practice. As already mentioned, this will be a hard case to crack.

The fact is that there will be an increasing amount of smart robots and AI applications that will have an arsenal of sensors, cameras and data processing devices. These applications will not just be separate entities but will consist of integrated systems connected to internet and an innumerable amount of other users.

What is more, these applications can also be integrated in human bodies, intelligent medical appliances or nano-robots that coordinate our physical processes.

ii. Other Threats to Privacy; Hacking of AI and robots

There can be all kinds of data breaches, eg misuse of personal data by different parties: producer, owner, developer or hacker. This can produce problems. Consider the use of personal information of several AI applications as autonomous cars, household devices, medical appliances or recreational appliances, such as Fitbit and the above mentioned running shoes app.

With all these appliances we must not underestimate the actions of a more dangerous group of potential users - the malignant hackers.

Hackers can create access to personal information. If one considers the actual situation, then one may conclude that new sensors, new algorithms, developments in AI and more sharing of information will increase our threat surface area drastically. There is almost no such thing as 'useless' data. Even seemingly innocuous information can be used to glean personal information from us, if not on its own, then in combination with other data. For example, the gyroscopic sensor information on one's phone can be intercepted and used to decipher a PIN code. This happens by capturing the sensor input using an infected website or application, and then using the sensor data as input through a neural network trained to recognise numbers. Using this technique, it is possible to accurately recreate 4-digit PIN codes with up to 99% precision.

The hacking of webcams is becoming more popular among hackers. This can be illustrated by the fact that hackers are already on a level where they can disable the webcam light that is often next to your webcam. Guides that describe how to hijack a laptop webcam are already available on the Internet.[51]

All of these new data can be used to build a better picture of who you are and what you do. Additionally, from a security perspective, what used to be virtual attacks are now becoming physical realities. It is not just one's email account that can be hacked to send spam messages to confused family and friends; now also physical devices in your home can poten-

49 ibid 7.

50 ibid.

51 'Are Hackers Using Your Webcam to Watch You?' (*Norton*, nd) <https://us.norton.com/internetsecurity-malware-webcam-hacking.html> accessed 14 September 2017.

tially be hacked. A hacker may not only 'steal' data from these physical devices, but also manipulate the physical devices; for example, unlocking a smart lock. Thus, as technology progresses, so do the amount of data, the amount of things one has to protect and secure increases.

One not only has to protect one's information but also one's physical security. Imagine that physical and medical appliances could be hacked, and that a person would receive this message: 'pay a certain amount or we will disturb or stop your pacemaker, artificial heart or kidney'.

Even more drastic action could take place: killing people; taking over autonomous cars to kill the user or use the car as a weapon for terrorist attacks; disturb flight control systems by using personal passwords or identifying data of other people, etc.

An example of an intrusion with severe consequences is the hacking of a surgical robot. One can imagine what consequences this could have.

Bonaci describes the possibilities of hacking when robots use standard networks. According to the author, security is no concern for developers of the surgical robot. He explains this with two reasons: (1) it is not known how easy it could be to hack a surgical robot; and (2) the implications of a hack directed against such robots are not known.[52]

The author divides the hacks into three groups: intention modification, intention manipulation and hijacking attacks. Firstly, intention modification is attacks in which the hacker modifies the information that the operator sends to a robot. Such hacks are not easy to detect by observing unusual actions of the robot.

Secondly, a manipulation attack is just the opposite of an intention modification attack, although now the feedback of the robot is modified. This means that the operator could get false feedback from the robot which will cause the operator to take the wrong decision. This is a result of the operator thinking that the information is valid. Such attacks are extremely hard to detect, because the operator does not realise that something is wrong.

Finally, during hijacking attacks the hacker with malicious intentions is taking over the entire robot, meaning that nobody except the hacker can control the robot. This implicates that a hacker is blocking all communication between the robot and a possible operator or operating system.

A more positive connotation can be made for the medical area, albeit that the privacy issue is not handled well. In a very recent report on AI by the UK parliamentary committee, Cotton-Barratt identified the 'large benefits,' as well as the challenges, that arise when AI is applied in healthcare:

> If it can automate the processes and increase consistency in judgments and reduce the workload for doctors, it could improve health outcomes. To the extent that there are challenges, essentially it means there is less privacy from the same amount of shared data, in that people can get more information out of a limited amount of data.[53]

2. Lost, Compromised or Destroyed Personal Data

Another risk for privacy and the rights and position of natural persons in an AI-oriented society, will be the loss, compromising or destruction of personal data by external or internal disturbances during the processing or storage of this data. Due to the immense increase of data processing by AI, the chance of loss or damaging of personal data will increase too. As a result of the absence of transparency or diminished transparency, this could go unnoticed by the processor as well as by the data subject. Lost, compromised or destroyed data could have a devastating effect on the data subject; for instance for persons who are dependent on certain medical appliances, for persons in autonomous cars, for persons depending on smart devices or depending on social robots, for those depending on simpler but important actions such as the payment of salaries, the functions of alarm systems, etc.

3. Intelligent Robots Are Vulnerable

Robots that have embedded AI are going to be a part of society, causing additional privacy concerns in ad-

52 Tamara Bonaci et al, 'To Make a Robot Secure: Experimental Analysis of Cyber Security Attacks on Teleoperated Surgical Robotics' (2015) arXiv:1504.04339v2 [cs.RO], in preparation to the ACM Transaction on Cyber-Physical Systems <https://arxiv.org/abs/1504.04339> accessed 7 September 2017.

53 'Robotics and artificial intelligence: Ethical and legal issues' (*UK Parliament website*, 5 October 2016) <https://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/14506.htm#_idTextAnchor019> accessed 7 September 2017.

dition to the privacy concerns related to already available technology on the market. When people bring autonomous robots into their homes, the privacy risks also grow. Robots and other AI appliances process enormous amounts of data and share the data to be able to function according to their tasks. However, the concept of self-learning that will be embedded in the algorithm will make it difficult, maybe even impossible, to control what will happen with this personal data. If deemed necessary, AI appliances will share the data with third parties. Governments, industry and third parties will find themselves in a sharing loop without knowledge thereof by the data subject.

Robots and intelligent appliances with audio-visual sensors - certainly when connected to the Internet - could be a threat to privacy. All these devices could be used or hacked and malicious use of the data could occur for blackmailing or more serious crimes. Ransomware is already creating problems for industry and utilities organisations. Therefore, the security of robots and AI needs to vastly improve in order to make future robots better protected against hacking and other security threats.

Firstly, the security of a robot must be an important part of its design. Therefore the security and privacy measures have to be built-in by design. Secondly, robots must use types of communication that are encrypted by algorithms based on cryptography. Further, with the introduction of autonomous robots, people have to accept the fact that they presumably will have less or a different kind of privacy than they used to.

VI. Conclusion

AI and autonomous robots will be part of our future society. Integration of AI and the human body will also occur. Our physical and informational integrity will be invaded, with or without our knowledge or consent. We already share a substantial part of our personal data with third parties and appear not really concerned. On top of that, government and industry are forcing us to share even more personal information to regulate or protect the social system or to lower risks and costs of services and products.

The GDPR describes the protection of personal data during processing in outdated terminology concerning AI. Due to the non-technological orientation and the hinge on conventional directions of thinking, the GDPR will not be sufficient to protect personal data in the age of AI.

Informational rights for the data subject and transparency of the process cannot be applied to the integrated AI, certainly not if this is integrated into the physical functions of the human being. There is a big risk of chilling effects for the development of AI and robotics if the GDPR has to be enforced on all AI applications.

In a Science and Technology Committee of a UK Parliament report, the need for unhindered but controlled applications of AI technology is stressed:

> It is important to ensure that AI technology is operating as intended and that unwanted, or unpredictable, behaviours are not produced, either by accident or maliciously. Methods are therefore required to verify that the system is functioning correctly. According to the Association for the Advancement of Artificial Intelligence: it is critical that one should be able to prove, test, measure and validate the reliability, performance, safety and ethical compliance—both logically and statistically/probabilistically—of such robotics and artificial intelligence systems before they are deployed.[54]

Can we control these developments in AI and robotics and handle our own informational privacy accordingly? Will it be possible to create legal instruments to do so if the positive legal framework is insufficient? If AI entities will obtain a certain degree of (sui generis) legal personhood, can we then still ensure that privacy and the protection of personal data will be handled according to legal requirements?[55]

---

54 Interesting is the concluding recommendation: '73. We recommend that a standing Commission on Artificial Intelligence be established, based at the Alan Turing Institute, to examine the social, ethical and legal implications of recent and potential developments in AI. It should focus on establishing principles to govern the development and application of AI techniques, as well as advising the Government of any regulation required on limits to its progression. It will need to be closely coordinated with the work of the Council of Data Ethics which the Government is currently setting up following the recommendation made in our Big Data Dilemma report.'
74. Membership of the Commission should be broad and include those with expertise in law, social science and philosophy, as well as computer scientists, natural scientists, mathematicians and engineers. Members drawn from industry, NGOs and the public, should also be included and a programme of wide ranging public dialogue instituted.' 'Robotics and artificial intelligence' (n 52).

55 See also, Mireille Hildebrandt and Laura Tillmans, 'Data Protection by Design and Technology Neutral Law' (2013) 28 Computer Law and Security Review 509, 512.

And if so, will there also be a requirement for the protection of 'personal' data of this new legal person, certainly when they develop into sentient entities.[56]

The regulatory gaps will continue to grow wider unless laws keep up pace with advances in technology. Law enforcement will not be able to police and regulate future technology accordingly. There will not be an intermission where we can calmly decide measures against each and every issue. Patchwork will not hold. Technology continues to develop and we have to think about the consequences that come into existence. We have to create a system of securing AI and autonomous robots before super intelligence will create it for us in a way where we do not act as participants but as subjects. How we act now may decide which future we will be confronted with.

56 ibid. As this also reflected a discussion concerning artificial legal persons as data protection for companies.