Essays

Machine Rules. Of Drones, Robots, and the Info-Capitalist Society

Guido Noto La Diega*

Abstract

Italy has been one of the first countries in the world to enact ad hoc regulations on drones. Therefore, the Italian approach may constitute a model for many regulations to come; nonetheless, the legal literature seems to overlook the phenomenon. In this article, I place the discourse on drones in the context of some more general considerations on the main legal issues related to the deployment of machines, including robots, in our everyday life. Indeed, most considerations apply equally to robots and drones, moving from the unrefined, albeit practical, observation that the latter are robots equipped with wings. An analysis of the intellectual property, data protection, privacy, and liability issues is carried out bearing in mind the complexity arising from the increasing implementation of cloud computing and artificial intelligence technologies. The article claims that autonomous machines will outclass human beings in all their tasks, but the horror vacui ought to be avoided: a new unforeseeable society will come. Therein, human beings – granted that a distinction between them and machines will still make sense – will not have to work in order to be able to live.

> *Wiederum aber steigt aus der Zerstörung neuer schöpferischer Geist empor; der Mangel an Holz und die Notdurft des täglichen Lebens drängten auf die hin, drängten auf die Auffindung oder die Erfindung von Ersatzstoffen für das Holz hin, drängten zur Nutzung der Steinkohle als Heizmaterial, drängten zur Erfindung des Kokesverfahrens bei der Eisenbereitung. Daß dieses aber die ganze Großartige Entwicklung des Kapitalismus im 19. Jahrhundert erst möglich gemacht hat, steht für jeden Kundigen außer Zweifel.*
>
> W. Sombart, *Krieg und Kapitalismus* (Barsinghausen: Unikum-Verlag, 2013), 207.

* Lecturer in Law (tenured), Northumbria University; President of Ital-IoT. This article would have not been possible without the valuable collaboration with the fellows of the Nexa Center for Internet & Society within the 'The Law of Service Robots' project, generously supported by Telecom Italia Mobile (TIM). I am grateful to Ms Susanna Crispino (Second University of Naples) for the excellent work of preparatory research. The responsibility for this article and the errors therein are, however, solely mine.

I. Introduction

It has been a while since the Count de Jonval, assertedly moving from Gottfried Wilhelm von Leibniz's and Giovanni Alfonso Borelli's theories,[1] said that

> *'la machine creuse qu'il faudroit imaginer pour soûtenir le corps de l'homme, & le mettre en équilibre avec l'air, seroit si démesurément grande & embarassante, que le gouvernement & l'usage en ont paru à d'habile gens des choses totalment despérées, & aussi interdites à l'homme aussi que le mouvement perpétuel.*'[2]

Not only men have flown,[3] but today they can make use of drones, so that they can fly and explore the world while sitting on a sofa.

Italy has been one of the first countries in the world to enact ad hoc regulations[4] on remotely piloted aircraft systems (RPAS).[5] Therefore, the

[1] In a scholium, N.-A. Pluche, *Le spectacle de la nature, ou Entretiens sur le particularités de l'histoire naturelle* (Amsterdam, I, 1, 1741), 291, attributes the idea to Giovanni Alfonso Borelli and to the famous thinker of Leipzig. In the English edition Id, *Nature Delineated* (London, 1740), 177, there is no mention to Borelli, but Leibniz himself clarified, in 1686, that he owed much to the Neapolitan scientist, who had anticipated him in this field. See, in particular, G.A. Borelli, *De vi percussionis* (Bologna, 1667), 279, proposition 116, on '*il metodo della estimazion delle forze pe' quadrati delle velocità*' (cf F. Colangelo, *Storia dei filosofi e dei matematici napolitani, e delle loro dottrine* (Napoli, III, 1834), 291). One could agree with P. Napoli-Signorelli, *Vicende della coltura nelle due Sicilie. Dalla venuta delle Colonie straniere sino a' nostri giorni* (Napoli, V, 1811), 339, whereby the original work '*De motu animalium*' positions Borelli above the philosofers of his time: he belongs to the most excellent circle of Kepler, Galileo, Leibniz, and Newton.

[2] N.-A. Pluche, *Le spectacle* n 1 above, 291-292.

[3] The analogy is justified also from a historical point of view. In order to build the first airplane, the Wright brothers tested their ideas by using remotely piloted gliders (see for instance R. Freedman, *The Wright Brothers: How They Invented the Airplane* (New York: Holiday House, 1991), 31).

[4] Ente Nazionale per l'Aviazione Civile (ENAC), Regolamento 'Mezzi aerei a pilotaggio remoto', 2nd ed, 16 July 2015 as amended on 21 December 2015 (hereinafter also '*regolamento* ENAC' or '*regolamento*'). The first edition had been adopted by ENAC, *Consiglio di Amministrazione, delibera* no 42 of 16 December 2013. A courtesy English translation is available at https://www.enac.gov.it/repository/ContentManagement/information/N1220929004/Regulation_RPAS_Issue_2_Rev%201_eng_0203.pdf (last visited 6 December 2016). See also the lettera no 136156/CRT of 29 December 2015, available at https://www.enac.gov.it/repository/ContentManagement/information/N353070060/136156_CRT-Chiarimenti.pdf (last visited 6 December 2016); the draft guidelines on '*qualificazione del personale di volo* APR' (delibera 22 May 2014 no 1 and the '*Nota esplicativa ai fini della presentazione della dichiarazione o autorizzazione*' of 26 May 2014).

[5] Drones are also known as unmanned aerial vehicles (UAV), remotely piloted aerial vehicles (RPAV), remotely piloted aircrafts (RPA) and unmanned aircraft system (UAS). ENAC, the Italian regulator of civil aviation, calls them *'mezzi aerei a pilotaggio remoto'*, translated, rather approximately, as RPAVs. The single aircraft is referred to as RPA. However, UASs (endorsed by ISO, see ISO/TC 20/SC16) and UAVs are to be considered as the genus, RPAVs

Italian approach may constitute a model for many regulations to come; nonetheless, the legal literature seems to overlook the phenomenon.[6]

In this article, I attempt to place the discourse on drones in the context of more general considerations of the main legal issues related to the deployment of machines, including robots, in our everyday life.

Most considerations apply equally to robots and drones, moving from the unrefined, albeit practical, observation that the latter are robots equipped with wings.[7] The study of data protection, privacy, and liability will be carried out,[8] bearing in mind the complexity arising from the increasing use of cloud computing (cloud robotics), machine learning, and other artificial intelligence (AI) technologies.[9]

Machines are indeed an ordinary topic in the news.[10] Unfortunately,

and RPASs as the species, and drones as the customary term in common language.

[6] In Italy, before the adoption of the ENAC regulations, a notable exception was constituted by U. La Torre, 'La navigazione degli UAV: un'occasione di riflessione sull'art. 965 c.nav. in tema di danni a terzi sulla superficie' *Rivista del diritto della navigazione,* I, 553 (2012); B. Franchi, 'Aeromobili senza pilota (UAV): inquadramento giuridico e profile di responsabilità (prima parte)' *Responsabilità civile e previdenza,* 732 (2010); Id, 'Aeromobili senza pilota (UAV): inquadramento giuridico e profili di responsabilità (seconda parte)' *Responsabilità civile e previdenza,* 1213 (2010); Id, 'Gli aeromobili a pilotaggio remoto: profili normativi e assicurativi' *Responsabilità civile e previdenza*, VI, 1770 (2014). In the matter of robots, one can find a slightly clearer field thanks to U. Pagallo (see, eg, Id, 'Robots in the Cloud with Privacy: A New Threat to Data Protection?' 29 *Computer Law & Security Review,* 501 (2013)). Cf also C. Artusio and M.A. Senor eds, 'The Law of Service Robots. Ricognizione dell'assetto normativo rilevante nell'ambito della robotica di servizio: stato dell'arte e prime raccomandazioni di policy in una prospettiva multidisciplinare' 4 December 2015, available at http://nexa.polito.it/nexacenterfiles/robots-2015.pdf (last visited 6 December 2016); A. Santosuosso et al, 'Robot e diritto: una prima ricognizione' *Nuova giurisprudenza civile commentata,* II, 494 (2012).

[7] I will point out below that most mistakenly think that drones constitute a higher danger for privacy, if compared to robots. Moreover, the provisions of the *codice della navigazione* (regio decreto 30 March 1942 no 327, navigation code) apply to drones and not to robots. In general, since the drone is a species of the genus *robot*, all the provisions relevant for the latter apply to the former, but not necessarily the other way around.

[8] Some legal issues will be overlooked, especially those emerging from the perspective of rights of robots and legal personality (issues that are becoming critical due to the developments of AI). Cf C. Sarzana di S. Ippolito, 'I riflessi giuridici delle nuove tecnologie informatiche' *Diritto dell'informazione e dell'informatica*, III, 505 (1994); P. McNally and S. Inayatullah, 'The Rights of Robots: Technology, Culture and Law in the 21st Century' 20(2) *Futures*, 119 (1988); H. Putnam, *Mente, linguaggio e realtà* (Milano: Adelphi, 1987), 426; S. Gozzano, 'I cinque sensi dei robot. Percezioni artificiali: l'informatica non imita solo l'intelligenza ma anche le capacità sensoriali' *Sapere*, IV, 9 (1990).

[9] In G. Noto La Diega, 'The Internet of Citizens. A Lawyer's View on Some Technological Developments in the United Kingdom and India' *Indian Journal of Law & Technology* (forthcoming), I suggest using *Thing* instead of *smart device*, *smart home*, etc, for at least two reasons that apply also to the phrase *artificial intelligence*. Firstly, most new products are designed with *smart* capabilities; thus if everything is smart, nothing is. Secondly, *smartness* and *intelligence* are human attributes and one does not want to commit the epistemological crime named *anthropocentricism*.

[10] It would be impossible to give account of the most recent news on drones, but by

there is also some sad news. For instance, in the wars carried out by the US against Pakistan and Yemen, in the failed attempt to kill forty-one targeted individuals, drones have killed one thousand one hundred forty-seven innocent people.[11]

Now, the law is characterised by an increasingly central role played by facts, in the sense that there is 'an extreme virulence of facts, which have the vigour to affect the law and shape it.'[12] Therefore, the factual importance of machines is already in itself sufficient to justify some legal considerations on the topic. This is a task that cannot be delayed any longer, since the *regolamento* of the *Ente Nazionale per l'Aviazione Civile* (ENAC) has come into force.[13] Machines stand amongst us and are here to stay.

The focus of this article will be on intellectual property, data protection, privacy, and liability, but it is clear that there are numerous legal issues emerging from the deployment of robots and drones, which shall be the subject of future research from a comparative perspective.[14]

II. Scope of the Study and Methodological Caveats

Before going into detailed legal analysis, one ought to define the scope of the investigation and to justify a methodology that appears heterodox from a traditional *civil law* approach.

Since drones are a species of the genus *robot*, one ought to define the

analysing the press, one notes a trend: drones are increasingly coupled with other protagonists of the Internet of Things. See, for instance, the research of the Aerial Robotics Lab (Imperial College London, http://www3.imperial.ac.uk/aerialrobotics, last visited 6 December 2016) that has led to the creation of a hexacopter, which 3D-prints while flying. R. Moro Visconti, 'Valutazione dei Big data e impatto su innovazione e digital branding' *Il diritto industriale*, I, 46, 47 (2016) considers robotics and avionic systems as the first species of the Internet of Things.

[11] Cf Reprieve, 'You Never Die Twice. Multiple Kills in the US Drone Program' 25 November 2014, available at http://www.reprieve.org/wp-content/uploads/2014_11_24_PUB-You-Never-Die-Twice-Multiple-Kills-in-the-US-Drone-Program-1.pdf (last visited 6 December 2016). Less tragically, it is not rare to hear of falling drones, as one may want to ask the world cup skier Marcel Hirscher.

[12] P. Grossi, 'Sulla odierna fattualità del diritto' *Giustizia civile*, I, 13 (2014).

[13] Even though legal scholars have generally overlooked robotics, one should mention the monographic contributions of R. Calo, A.M. Froomkin and I. Kerr eds, *Robot Law* (Cheltenham: Edward Elgar, 2016) and U. Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* (Dordrecth-Heidleberg-New York-London: Springer, 2013), as well as C. Holder et al, 'Robotics and Law: Key legal and Regulatory Implications of the Robotics Age (Part I of II)' 32 *Computer Law & Security Review*, 383 (2016).

[14] For instance, on 21 June 2016, the US Federal Aviation Administration (FAA) adopted the first operational rules for routine commercial use of small unmanned aircraft systems. The Advisory Circular 21 June 2016 no 107-2 'Small Unmanned Aircraft Systems (sUAS)' is available at http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_107-2.pdf (last visited 6 December 2016). It would be interesting to compare the ENAC regulations with those of the US FAA, as well as with those in the UK.

latter.[15] Following the International Organization for Standardization (ISO) definition, a robot is an 'actuated mechanism programmable in two or more axes with a degree of autonomy, moving within its environment, to perform intended tasks'.[16] A robot includes the control system and interface of the control system. ISO classifies robots into industrial robot and service robot; the former will not be the object of this article.

There are several robotic taxonomies. For instance, some argue that the main characteristics of a robot are interactivity, autonomy, and adaptability.[17] To be precise, interactivity is not an intrinsic characteristic of all robots, but only of the collaborative ones,[18] while adaptability applies to intelligent robots.[19] It would seem, consequently, that the core concept, the one ontologically attached to all the robots, is *autonomy*; that is, the 'ability to perform intended tasks based on current state and sensing, without human intervention.'[20] What is happening with machine learning, predictive analytics, etc, is a switch of paradigm. In a bizarre return to the original meaning of the word, *autonomy* is not only the capability of acting without human intervention; it means the power to dictate laws to oneself, with clear consequences for the human beings interacting with the machine. Even though not every robot and drone is genuinely autonomous, notwithstanding some Artificial Intelligence (AI) fiascoes,[21] one cannot deny the spread of AI algorithms made possible by the processing capability of cloud robotics.

[15] According to P. Comanducci, 'Le tre leggi della robotica e l'insegnamento della filosofia del diritto' *Materiali per una storia della cultura giuridica*, I, 193 (2006), the laws have been first conceived by I. Asimov, *Runaround* (New York: Street and Smith Publications, 1942). U. Pagallo, 'Ermeneuti, visionari, circospetti: La "quarta via" alla robotica tra diritto e letteratura', in M.P. Mittica ed, *Diritto e narrazioni. Temi di diritto, letteratura e altre arti* (Milano: Ledizioni, 2011), 159, considered it as a '*primo, suggestivo elemento di raccordo tra diritto, letteratura e robotica*.'

[16] ISO 8373:2012(en) Robots and robotic devices — Vocabulary, para 2.6. Cf UN World Robotics, *Statistics, Market Analysis, Forecasts, Case Studies and Profitability of Robot Investment* (Geneva: UN Economic Commission for Europe e International Federation of Robotics, 2005), 21.

[17] C. Allen et al, 'Prolegomena to Any Future Artificial Moral Agent' 12 *Journal of Experimental and Theoretical Artificial Intelligence*, 251 (2000).

[18] Collaborative robots are those designed for direct interaction with a human (ISO 8373: 2012, n 16 above, para 2.26).

[19] An 'intelligent robot' is, indeed, 'capable of performing tasks by sensing its environment and/or interacting with external sources and adapting its behaviour.' (ISO 8373:2012, n 16 above, para 2.28). ISO makes the examples of an industrial robot with vision sensor to pick and place an object; a mobile robot with collision avoidance; and a legged robot walking over uneven terrain.

[20] ISO 8373:2012, n 16 above, para 2.2.

[21] B. Fung, 'Why Microsoft's racist Twitter bot should make us fear human nature, not A.I.' 24 March 2016 available at https://www.washingtonpost.com/news/the-switch/wp/2016 /03/24/why-microsofts-racist-twitter-bot-should-make-us-fear-human-nature-not-a-i/ (last visited 6 December 2016). As to self-driving cars, see https://static.googleusercontent.com/medi a/www.google.com/it//selfdrivingcar/files/reports/report-0216.pdf (last visited 6 December

The bridge between robots and drones is the category of *mobile robots*. These machines are 'able to travel under (their) own control'[22] and can well encompass aerial mobility.

Drones are no longer limited to remotely piloted and radio-controlled aerial systems used for military purposes.[23] Alongside the military drones, popularised during the Gulf War,[24] one has 'all sorts and sizes of radio controlled, remotely piloted, semi-autonomous or fully autonomous aircraft, including hobbyist, radio controlled airplanes.'[25] Sometimes they serve the public interest, as in the *green* use in the *Terra dei Fuochi*[26] or the cargo-drones that transport medicines to Africa.[27] Nonetheless, one should not be

2016).

[22] ISO 8373:2012, n16 above, para 2.13.

[23] Even though, when thinking military machines, drones come to mind first, robots are also significantly used for military purposes. For instance, on 7 July 2016 the Dallas Police Department used a bomb-disposal robot to kill one of the shooters involved in the killing of five law enforcement officers.

[24] ENAC has no jurisdiction over military drones. Art 15 of decreto ministeriale 16 January 2013 ('*Struttura del Segretariato generale, delle Direzioni generali e degli Uffici centrali del Ministero della difesa, in attuazione dell'articolo 113, comma 4 del decreto del Presidente della Repubblica 15 Marzo 2010 no 90, recante il testo unico delle disposizioni regolamentari in materia di ordinamento militare*'), reads that the *Direzione degli armamenti aeronautici* (ARMAEREO) is responsible for authorising the navigation of military aircrafts. Before the regolamento ENAC, nearly all the Italian provisions on drones dealt with the phenomenon from a military perspective. One need only think to Art 1 para 1 of the decreto del Presidente del Consiglio dei Ministri 30 November 2012 no 253 ('*Regolamento recante individuazione delle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale*'), whereby the study, research, design, development, production, and integration of *velivoli a pilotaggio remoto* (remotely-piloted aerial means) both for surveillance (UAV MALE) and for attack (UCAV) are considered as activities which are of strategic relevance for the defence and national security system (therefore, business operating in the field of military drones are bound to Art 1, decreto legge 15 March 2012 no 21 converted by legge 11 May 2012 no 56; cf Art 1 para 1 letter b) no 3 of the decreto del Presidente del Consiglio dei Ministri 6 June 2014 no 108). The Italian legislature has *discovered* drones with the legge 14 July 2004 no 178 '*Disposizioni in materia di aeromobili a pilotaggio remoto delle Forze armate*', repealed by Art 2268 para 1 no 1027 of decreto legislativo 15 March 2010 no 66 (*Codice dell'ordinamento militare*). The said *codice* has introduced the *ad hoc* provisions of the *codice dell'ordinamento militare*, which will be touched on below.

[25] T.T. Takahashi, 'Drones and Privacy' *Columbia Science & Technology Law Review,* 83 (2012), who refers to J. Ukman, 'Privacy Group Seeks to Lift Veil on Domestic Drones' *Washington Post*, 13 January 2012.

[26] As pointed out in G. Noto La Diega, 'Il cloud computing. Alla ricerca del diritto perduto nel web 3.0' *Europa e diritto privato*, II, 577, 631 (2014), the decentralised legislatures (Regioni) show to be more sensitive to new technologies, in comparison to the central one. It is the case of Art 8 para 2 of the legge regionale Campania 9 December 2013 no 20 ('*Misure straordinarie per la prevenzione e la lotta al fenomeno dell'abbandono e dei roghi di rifiuti*'), which promotes agreements with the defence corps aimed to develop programs of environmental monitoring; these agreements have to provide the use of innovative technologies, included RPAs.

[27] On 'The Flying Donkey Challenge' project, see http://www.flyingdonkey.org/ (last visited 6 December 2016).

naïve, since the military use is still the main use, as suggested, *inter alia*, by the fact that the first commercial drone has been approved by the US Federal Aviation Administration (FAA) fairly recently and its first flight was in June 2014.[28]

The same applies to robots, which are mainly used for military and industrial purposes[29] and are thus ignored by most scholars. However, today's drones and 'robot(s) leave the factory floor and battlefield and enter the public and private sphere in meaningful numbers',[30] and the phenomenon will affect society even more than computers.[31] Therefore, a thorough analysis of machine rules is long overdue.

In Italy, Art 743 of the *codice della navigazione*,[32] as amended by the decreto legislativo 15 March 2006 no 151,[33] included in the concept of *aeromobile* (aircraft):

> 'Aircraft shall mean any machine designed for the transportation by air of persons or property. Remotely piloted aerial vehicles are also considered aircraft, as defined by special laws, ENAC regulations and, for the military, by decrees of the Ministry of Defence. The distinctions of the aircraft, according to their technical specifications and use shall be established by ENAC with its regulations and, in any case, by special

[28] The Puma AE drone of AeroVironment Inc monitors BP Exploration Inc's oil pipelines in Alaska as from 8 June 2014 (see the licence of 19 July 2013).

[29] Cf the decreto ministeriale 7 May 2014 (*Ministero della Difesa*) on the '*Approvazione del nuovo elenco dei materiali d'armamento da comprendere nelle categorie previste dall'articolo 2, comma 2, della legge 9 luglio 1990 no 185, in attuazione della direttiva 2014/18/UE.*' It regards also robots and the relevant component, provided that they have at least one of the following characteristics: 1. Built for military purposes. 2. Equipped with idraulic junctions resistant to perforations cause by balistic framents and designed for fluids having an inflamation point superior to eight hundred thirty-nine K (five hundred sixty-six°C); or 3. Designed for or apt to function in an environment with electromagnetic pulses (Annex, category 17, letter e).

[30] R. Calo, 'Robots and Privacy', in P. Lin et al eds, *Robot Ethics: The Ethical and Social Implications of Robotics* (Cambridge: MIT Press, 2011), 187 (but one of the online versions available at ssrn.com/abstract=1599189, last visited 6 December 2016). In the footnotes of this article, the page number of the cited work will be the one of the online version.

[31] B. Gates, 'A Robot in Every Home' *Scientific American,* 58 (2006), describes robotics as the first technological revolution after computers; indeed 'we may be on the verge of a new era, when the PC will get up off the desktop and allow us to see, hear, touch and manipulate objects in places where we are not physically present.'

[32] Regio decreto 30 March 1942 no 327. It has been amended several times, most recently by decreto legge 12 September 2014 no 133, converted with amendments by legge 11 November 2014 no 164, which has introduced Art 733 bis. See also decreto del Presidente della Repubblica 15 February 1952 no 328 '*Approvazione del Regolamento per l'esecuzione del Codice della navigazione*' (maritime navigation regulation), last amended by decreto legislativo 12 May 2015 no 71, which has amended Art 271, para 2, no 2.

[33] '*Disposizioni correttive ed integrative al decreto legislativo 9 maggio 2005 n. 96, recante la revisione della parte aeronautica del codice della navigazione*'.

legislation in this field.'[34]

The regolamento ENAC includes, therefore, implementation of this provision and denotes a scope that is narrower than what is indicated by Art 743. It concerns two species of RPASs: remotely piloted aerial vehicles and model aircrafts. The former are RPASs 'operated or intended to be operated for specialised operations or for experimental, scientific or research activities' (Art 1 para 3 regolamento ENAC) and fall within the scope of the codice della navigazione. The latter are not regarded as aircraft for the purposes of the provisions of the *codice della navigazione* and can be used for recreational and sporting activities only. Nevertheless, the regolamento ENAC sets out specific provisions and limitations applicable to the use of the model aircraft to ensure the safety of persons and property on the ground and of other airspace users. Moreover, pursuant to the EU regulation no 216/2008,[35] RPASs of operating take-off mass not exceeding one hundred fifty kilograms and those designed or modified for research, experimental, or scientific purposes fall under the competence of ENAC.[36]

A notable provision is Art 5 (Glossary and acronyms), which looks very peculiar to civil law scholars.[37] It is useful to report on the distinction between RPAS and autonomous systems. A RPAS is

> 'a system consisting of an aerial vehicle (remotely piloted aircraft)

[34] According to the traditional approach of legal scholars, the concept of aircrafts under criminal law does not cover RPASs. Consequently, Art 428 of the codice penale (criminal code) does not apply. Under Art 428 it is punished with the imprisonment from five to twelve years whomever causes the wreck or submersion of a ship or other saling means, or the fall of an aerial vehicle, which do not belong to the person who caused the said events. Cf E. Battaglini and B. Bruno, 'Incolumità pubblica (delitti contro la)' *Novissimo Digesto italiano* (Torino: Utet, 1962), VIII, 552 and C. Erra, 'Disastro ferroviario, marittimo, aviatorio' *Enciclopedia del diritto* (Milano: Giuffrè, 1963), XIII, 4. However, in favour of a broad interpretation see C. Medina, 'Aeromobile' *Novissimo Digesto italiano* (Torino: Utet, 1980), appendix I, 119. The translation of the provision is provided by ENAC in the courtesy version referred to above.

[35] Art 2 para 2 *regolamento* ENAC refers to 'Regulation (EC) no 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC'. See namely Art 4 para 4 and letter i) of Annex II.

[36] Equally, the regolamento ENAC does not apply to a) State RPASs (Arts 744, 746 and 748 of the *codice della navigazione*); b) RPASs operating within indoor space (but to fly over gatherings of persons during parades, sports events, or different forms of entertainment or any areas where there is an unusual concentration of people, is prohibited); c) Balloons used for scientific observations or tethered balloons.

[37] The *codice dell'ordinamento militare* includes a notable exception, where it introduces an *ad hoc* section to definitions. For present purposes, one need only refer to Art 246 of the ordinamento, where it provides that a RPA is an aerial means piloted by a crew that operates from a remote command and control station, thus excluding completely autonomous systems also from military avionics.

> without persons on board, not used for recreation and sports, and the related components necessary for the command and control (remote ground pilot station) by a remote pilot.'

In turn, an autonomous system is a RPAS that does not allow the pilot intervention in the management of the flight on a real time basis. It falls outside the scope of the *regolamento*.

It is rather self-explanatory that the main risks, especially in terms of liability, come from the latter. Therefore, it is a commendable decision to leave this use unregulated, while progress in terms of the security of autonomous systems is not yet advanced enough. However, risks are present also in the current system, particularly when it comes to Beyond Visual Line Of Sight (BVLOS)[38] and Extended Visual Line Of Sight (EVLOS)[39] operations.

Notwithstanding the above definition, I claim that one should not draw a clear line between robots, drones, and human beings. Thanks to artificial enhancement techniques, human beings are becoming more and more similar to machines. At the same time, machines are becoming increasingly more similar to human beings, both in their aspect and in their sensing and actuating capabilities. Therefore, one should view the considered phenomena as a continuum of machine to human being.[40]

The last caveats are of a methodological nature. First, whereas common law scholars are relatively used to studying unconventional legal documents, the tradition of civil law (especially the one guarded by the *civilisti*)[41] frowns

[38] BVLOS are 'operations at a distance that do not allow the remote pilot to continuously remain in direct visual contact with the RPA, that do not allow him to manage the flight, to maintain separation and avoid collisions.' (Art 5 para 1 regolamento ENAC).

[39] EVLOS are operations at a distance exceeding the limits of the Visual Line of Sight (VLOS) operations, which comply with the VLOS conditions via alternative means. In principle, the safest operations should be the VLOS ones: 'operations at distances, both horizontal and vertical, in which the remote pilot maintains continuous visual contact with the aerial vehicle, without the aid of tools to enhance the view, so to be able to directly control it with the aim to conduct the flight and to meet separation and collision avoidance responsibilities.' (Art 5, para 1, regolamento ENAC). Distances by which operations can be considered VLOS are subject to the capability of the pilot to be aware of the actual RPA conditions in terms of position, altitude, and speed as well as of obstacles and other aircraft. The remote pilot has the final responsibility to define the VLOS conditions that might be affected by weather conditions, sunlight, and the presence of obstructions.

[40] This assertion is far from being widely accepted. Just to name an example, the Court of Justice has stated that 'when citizens move, they do so as human beings, not as robots. They fall in love, marry and have families.' (Case C-34/09 *Ruiz Zambrano* v *Office National de l'Emploi (ONEm)*, [2011] ECR I-1177) This may be true now, but it is likely to become incorrect in a near future.

[41] Although there are many notable exceptions, the Italian academy has traditionally focused on the *Costituzione*, the *leggi*, and kindred primary legislation. Many scholars tend even to diminish the role of case law. To be precise, I still think that *leggi*, *codici*, and judgements are the patricians of the law-poietic society, but one ought to look at the microhistory *à la* Braudel, being aware of the actual, albeit rarely formalised, influence that the

upon studies focused on secondary legislation and soft law. In the age of global law and legal hysteresis,[42] the scholar has to abandon the cathedral[43] and walk the unbeaten path of guidelines, *circolari*, codes of conduct, terms of service, and even press releases, hardware designs, and algorithms.[44]

The proliferation of legal sources and legal *inflation* have been described as the reasons for the defeat of both Antigone and Creon.[45] I do not know if the regolamento ENAC and the galaxy of robot *law* is the last expression of these phenomena. However, I do know that heterodox norms are affecting people's lives and their violation is punished, even in informal and privately enforced ways;[46] therefore, they ought not to be overlooked.

As a conclusive methodological (and *ideological*) caveat, one should point out that, when it comes to binomial-technology law, legal scholars tend either to declare that we are facing a revolution (a *disruptive innovation*)[47] and traditional principles will not apply, or to affirm that the technology is

plebeians had on history.

[42] See G. Noto La Diega, 'In Light of the Ends. Copyright Hysteresis and Private Copy Exception after the British Academy of Songwriters, Composers and Authors (BASCA) and Others v Secretary of State for Business, Innovation and Skills Case' *Studi giuridici europei 2014*, 39, (2016).

[43] Cf G. Calabresi and A.D. Melamed, 'Property Rules, Liability Rules, and Inalienability: One View of the Cathedral' 85(6) *Harvard Law Review,* 1089, 1090, fn 2 (1972), who recognise, with mirable humility and foresight, that their approach is only one of Monet's paintings of the Cathedral at Rouen: 'to understand the Cathedral one must see all of them' (the reference is to G.H. Hamilton, *Claude Monet's Paintings of Rouen Cathedral* (London: Oxford University Press, 1960), 4-5, 19-20, 27).

[44] With ubiquitous computing, the law is increasingly implemented in technological ways, which suggests, *inter alia*, to adopt a multisciplinary methodology. The most common example is the *privacy by design* approach followed by the general data protection regulation (GDPR). In G. Noto La Diega, 'Uber Law and Awareness by Design. An Empirical Study on Online Platforms and Dehumanised Negotiations', *Revue européenne de droit de la consummation*, II, 383, (2016), I suggest an *awareness by design* mobile application.

[45] It is the opinion expressed by L. Ferrajoli, 'Antigone e Creonte, entrambi sconfitti dalla crisi della legalità' *Giustizia civile*, I, 27 (2014). As is common knowledge, Antigone represents justice and Creon represents certainty. Cf T. Ascarelli, 'Antigone e Porzia' *Rivista Internazionale di Filosofia del Diritto*, 756 (1955) translated by C. Crea in this *Journal*, II, 167 (2015).

[46] Rating agencies grades are the most obvious, albeit not the only, example of this trend. One could also think of the policies of the main social networks: to be excluded by the platform (for instance due to the *real name policy*) may soon be perceived as an *aquae et igni interdictio*. See Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *Anordnung* of 24 July 2015 and Verwaltungsgericht Hamburg, *Beschluss* of 3 March 2016, 15 E 4482/15, available at http://justiz.hamburg.de/contentblob/5359282/data/15e4482-15.pdf (last visited 6 December 2016). More generally, the role of online platforms in oligopolistic markets – with a focus on consumers and not only on competitors – should be the subject of future research.

[47] For a critique to Clayton M. Christensen's idea of disruptive innovation (first sketched in his *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Boston: Harvard Business School Press, 1997)), see A.A. King and B. Baatartogtokh, 'How Useful Is the Theory of Disruptive Innovation?' *MIT Sloan Management Review* (2015), available at http://sloanreview.mit.edu/article/how-useful-is-the-theory-of-disruptive-innovation/ (last visited 6 December 2016).

not actually new, but is just '*die erzwungene Vernichtung einer Masse von Produktivkräften*';[48] that is, the problems may be old, but old barrels are suitable for new wine. It is the perennial conflict between *apocalyptic* and *integrated*.[49] This article stands for a middle way and advocates a problem-based multidisciplinary approach, whereby one should assess whether the technology at issue is new and how and whether the existing (if any) legal framework can accommodate the emerging problems. Whilst the psychological and social consequences of the increasing deployment of robots and drones might justify, to some extent, a nihilistic approach,[50] the same does not apply to law. The dynamic combined action of interpretation of the existing legal framework, soft law tools (especially co-regulatory ones) and *enforcement by design* can provide the solution. Beware of whoever relies entirely on the law or, alternatively, on technology: neither will suffice with autonomous robots and drones becoming commonplace.

III. Machine-Related Inventions and Machine-Generated Works

Intellectual property is a critical aspect that must be addressed when it comes to contemporary machines. To make two general remarks: first, proprietary models can hinder interoperability, which is vital to the interaction between (and sometimes the functioning itself of) most machines in an Internet of Things era. Moreover, many machines can be carried by the user in several jurisdictions, and intellectual property, given the principle of territoriality, can constitute an obstacle in the access to the service provided by the machine, especially as long as geo-blocking is not tackled properly.[51]

Research commissioned by the World Intellectual Property Organization[52]

[48] Building on the idea of 'enforced destruction of a mass of productive forces' expressed by K. Marx and F. Engels, *Manifest der Kommunistischen Partei* (London: Bildungs-Gesellschaft für Arbeiter, 1848) I, read at https://www.marxists.org/deutsch/archiv/marx-engels/1848/manifest/1-bourprol.htm (last visited 6 December 2016), J.A. Schumpeter, *Capitalism, Socialism and Democracy* (London: Routledge, 1994, 1942), 82-83, developed the theory of the *schopferische Zerstörung*, the creative destruction.

[49] Cf U. Eco, *Apocalittici e integrati. Comunicazioni di massa e teorie della cultura di massa* (Milano: Bompiani, 1964). A balanced position has been recently expressed by L. Floridi, 'Should we be afraid of AI?' *Aeon* (2016), available at https://aeon.co/essays/true-ai-is-both-logically-possible-and-utterly-implausible (last visited 6 December 2016).

[50] I am studying the right to solitude in a context of ubiquituous computing, but an already studied, albeit still interesting, phenomenon is the so-called uncanny valley. Cf M. Mori, 'Bukimi No Tani – The Uncanny Valley' *Energy*, IV, 33 (1970).

[51] On 25 May 2016, the European Commission has adopted the Proposal for a regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (COM(2016) 289 final).

[52] C.A. Keisner, J. Raffo, and S. Wunsch-Vincent, 'Breakthrough Technologies – Robotics,

has shown that the countries with the highest number of patent filings are Japan, China, Republic of Korea and the US. Businesses in the car and electronics sectors file the most, but medical technologies and the Internet are growing in importance. Copyright protection is relevant too,[53] mainly in its role in protecting computer programmes and netlists.

In this paragraph, I will touch on intellectual property through the prisms of machine-related inventions and machine-generated works.[54]

In Italy, as in most European countries, computer programmes per se are copyrightable, but they cannot be patented. Indeed, under Art 2 of the legge 22 April 1941 no 633 (*'Protezione del diritto d'autore e altri diritti connessi'*, hereinafter also 'copyright act'), computer programmes are protected as literary works under the Berne Convention for the Protection of Literary and Artistic Works, ratified and implemented by the legge 20 June 1978 no 399, regardless of how they are expressed, provided that they are original, being the outcome of the author's intellectual creation. In turn, the *codice della proprietà industriale* (decreto legislativo 10 February 2005 no 30), which regards mainly inventions, designs, and trade marks, clarifies that computer programmes are not inventions and, therefore, cannot be patented (Art 45, para 2, letter b). Lastly, when it comes to registered designs, Art 31 specifies that the concept of product whose design can be registered encompasses its components, but it openly excludes the software components.

Nonetheless, the patentability exclusion regards only computer programmes *per se* (as such, '*in quanto tali*', under Art 14 para 3 of the *codice della proprietà industriale*). This phrase refers to the constantly growing world of the computer-implemented (or computer-related) inventions which – we claim – would be better named *machine-related*, because their scope is broader than the one identified with traditional computers. (For instance software implemented in a wearable device can easily qualify as a machine-related invention). A machine-related invention involves the use of a computer, computer network or other programmable apparatus (that is, also robots and drones), where one or more features are realised wholly or partly by means of a computer programme.

Since nearly all machines are equipped with computer programmes, the growth of the former will result in the spread of machine-related inventions. Indeed, these kind of inventions are a critical topic in patent law, since a too-

Innovation and Intellectual Property', Economic Research Working Paper No 30 (2015).

53 Cf M. de Cock Buning, 'Is the EU Exposed on the Copyright of Robot Creations?' *The Robotics Law Journal*, 8 (2015).

54 There are several other intellectual property issues when it comes to machines. For instance, nowadays, sporting events are recorded by smart cameras and drones, equipped with slow motion features, high-definition videos, etc. In this context, the original contribution of the director is of a quality that renders it difficult to deny copyright protection. Cf S. Longhini and F. Catanzaro, 'Tra il dire e il fare c'è di mezzo … il piratare' *Diritto d'autore*, I, 72 (2014).

relaxed approach in granting patents for these kind of inventions may risk allowing a double protection for computer programmes: copyright and patents. A much too broad monopoly would be legitimised, with a subsequent increased propertisation of intangibles.

The protection of computer programmes has always been a much debated topic: whether to protect them, how to protect them, using copyright, patents, both? The European Patent Convention excludes the patentability of computer programmes claimed *as such* (Art 52(2)(c) and (3)).[55] Patents are not granted merely for programme listings, which are protected by copyright. If a technical problem is solved in a novel and non-obvious manner, a machine-related patent can be granted.[56]

Computer program/computer program product is one of the trickiest categories. The European Patent Office (EPO), indeed, stresses the (unclear) difference between this category and computer programmes as a list of instructions: the subject matter is patentable

> 'if the computer program resulting from implementation of the corresponding method is capable of bringing about, when running on a computer or loaded into a computer, a "further technical effect" going beyond the "normal" physical interactions between the computer program and the computer hardware on which it is run.'[57]

[55] In an attempt to address whether case-law concerning excluded matter is settled, and derive uniformity of application of European patent law, the President of the EPO referred four questions on the patentability of computer programs to the Enlarged Board of Appeal in October 2008 (G3/08, opinion on 12 May 2010, available at http://www.epo.org/law-practice /case-law-appeals/pdf/g080003ex1.pdf (last visited 6 December 2016)). However, the Board concluded that the referral was inadmissible because the decisions referred to were not considered to be *divergent*, and declined to answer the questions beyond determining their admissibility. This led to the Court of Appeal reaffirming its view that practice was not yet settled in *HTC Europe Co Ltd* v *Apple Inc* (Rev 1) [2013] EWCA Civ 451 (3 May 2013) at 44.

[56] The machine-related inventions do not receive a stricter assessment in comparison to other inventions. Indeed, in EPO Board of Appeal, T 1606/06 (*DNS determination of telephone number/HEWLETT-PACKARD)* of 17 July 2007, EP:BA:2007:T160606.20070717, the appellant argued that, since the patent concerned a CII, the triviality test should have been stricter. According to the Board, there is no basis for doing so and '(t)he only "special" treatment for computer-implemented inventions relates to aspects or features of a non-technical nature; in fact this treatment is only special in the sense that the presence of non-technical features is a problem which does not arise in many fields.'

[57] European Patent Office, 'Patents for software? European law and practice' (2013), available at documents.epo.org/projects/babylon/eponet.nsf/0/a0be115260b5ff71c125746d 004c51a5/$FILE/patents_for_software_en.pdf (last visited 6 December 2016). For a landmark case of the Board of Appeal see T 1227/05 (Circuit simulation I/Infineon Technologies) of 13 December 2006, EP:BA:2006:T122705.20061213, available at https//www.epo.org/law-practice /case-law-appeals/pdf/t051227ep1.pdf (last visited 6 December 2016), whereby 'technical and inventive Specific technical applications of computer-implemented simulation methods, even if involving mathematical formulae, are to be regarded as "inventions" in the sense of Article

Mischievous commentators may argue that machine-related inventions are a surreptitious way to obtain a double binary for software protection. This may become true with the rise of machines, especially in the context of the Internet of Things. Indeed, with the gradual substitution of old machines with connected devices, we will face an unprecedented growth of machine-related inventions; therefore, asserting that computer programmes are not patentable in Europe may sound hypocritical. I predict that in the future most computer programmes will be embedded in machines, with the consequential patentability of most computer programmes under the label of machine-related inventions.

The second IP-related aspect I will briefly touch on regards machine-generated works (more commonly known as computer-generated works).

Machines can already create copyrightable works without any human intervention or with little human input.[58] Let us think, for example, of the weather images created by a machine directly in communication with a satellite. With machines becoming more and more autonomous, machine-generated works will increase, leading scholars to rethink the traditional solutions for the relevant authorship, usually revolving around the developer of the software and the user operating the machine. In Italy, whilst it is believed that machine-generated works are protected as long as they are distinct from the computer programme that generated them,[59] the legislature has not taken a position on their authorship,[60] whereas in other countries

52(1) of the European Patent Convention. Circuit simulations possess the required technical character because they form an essential part of the circuit fabrication process.' The most recent EPO case regarding computer programmes is T 1722/11 of 18 December 2015 on an Apple Inc's application for a 'Method and system for message delivery management in broadcast networks.' It is available at https://www.epo.org/law-practice/case-law-appeals/pdf/t111722eu1.pdf (last visited 6 December 2016). As Fox LJ stated in *Merrill Lynch's Application* [1989] RPC 561, 569, 'it cannot be permissible to patent an item excluded by section 1(2) [of the Copyright, Designs, and Patents Act 1988] under the guise of an article which contains that item – that is to say, in the case of a computer program, the patenting of a conventional computer containing that program. Something further is necessary.'

[58] I am taking into consideration only *pure* machine-generated works. There are already umpteen websites and apps offering tools to edit (sometimes radically) the photos uploaded by the user. I will not cover this kind of works, but let us just say that usually authorship and ownership will be vested on the user, but the latter is required to grant a very broad licence to the service provider. For instance, under s 3 of the Snapchat's Terms of Service (effective as of 29 March 2016, available at https://www.snapchat.com/l/en-gb/terms (last visited 6 December 2016)), the user must grant Snapchat 'a worldwide, royalty-free, sublicensable, and transferable licence to host, store, use, display, reproduce, modify, adapt, edit, publish, and distribute that content.' It is arguable that such a broad licence is not very different from a proper transfer of ownership.

[59] And, of course, as long as the other copyright requirements occur, for instance originality. Cf B.M. Gutierrez, *La tutela del diritto di autore* (Milano: Giuffrè, 2008), 43. Cf, in general, V. Ercolani, 'Computer-generated works' *Diritto d'autore*, 604 (1998).

[60] One could be mislead by Art 7 para 2 of the copyright law. Indeed, it provides that the author of the elaborations is the *elaboratore*, which in Italian means both computer and

there are *ad hoc* provisions on the subject. For instance, in the UK, a computer-generated work is defined as one generated in circumstances when there is no human author of the work (s 178 of the Copyright, Designs, and Patents Act 1988) and under s 9(3) of the Act, which concerns literary, dramatic, musical or artistic works that have been computer-generated, the author is the person who made the necessary arrangements to create the work, such as the program author.[61]

The regime in the UK seems to exclude that the author can be the machine itself, which could be unfair when proper superintelligence becomes a reality. Given that there is no *ad hoc* provision in Italy and given that the Italian copyright act does not limit the concept of *author* to humans,[62] one could argue that the Italian regime is more suitable for an AI scenario,[63] since it allows machines to be authors and hence owners of the works they produce.[64]

IV. Inner Eye. Privacy, Data Protection, and Security

It is hard and probably useless to propose a unitary discourse on robots and drones when it comes to privacy and data protection. Therefore, I will take a concentric circles approach by analysing the genus and then assessing whether the same rules apply to the species.

As the first Asimov law of robotics reads, 'a robot may not harm a human being, or, through inaction, allow a human being to come to harm.' Even though the reference was originally to physical arms, nowadays one of the

person who does the elaboration. The impression of an authorship attributed to the machine is soon dispelled by the first para of the same article, which clarifies the scope of the provision: collective works. See Consiglio di Stato 21 January 1993 no 77, *Giustizia civile*, I, 1125 (1993).

[61] Cf *Nova Productions Ltd* v *Mazooma Games Ltd & Ors* (CA) [2007] EWCA Civ 219.

[62] Under Art 8 para 1 of the copyright act, the author is the entity (not necessarily the human being) who is indicated to be the author according to custom or, who is mentioned to be the author in the acting, execution, performance, or broadcasting of the work. Thus it is important to read the contracts or the terms of service to undertand who is the author.

[63] An *ad hoc* regime or a revision of the current general regime would be needed to accommodate the specific characteristics of the works generated by machines. For instance, machines do not die, therefore the usual duration system (seventy years after the death of the author) would be unsuitable. One could either provide *ad hoc* mechanisms (eg the British system, with the machine-generated works falling into the public domain after fifty years from the date they had been made), or the rise of machines could constitute a good opportunity to review the current system by, for instance, limiting the duration of copyright to the author's lifetime.

[64] Given the current development of AI, it is still valid the theory of P. Samuelson, 'Allocating Ownership Rights in Computer-Generated Works' 47 *University of Pittsburgh Law Review*, 1185 (1985), whereby it is more convenient to consider the user as the original owner of the work (even though one should assess on a case-by-case basis the individual contribution of the user).

main risks of the deployment of robots and drones is the threats to citizens' privacy.[65]

It ought to be said that the relationship between robots and privacy is amphibious. Not only can robots jeopardise privacy, but they can also protect it. The existence of the latter is somehow usually ignored.[66] There are several commercial offers for security robots,[67] such as Knightscope K5, allegedly an autonomous[68] 'force multiplier, data gatherer and smart eyes and ears on the ground helping protect your customers, your property and your employees 24/7.'[69] Making use of cloud computing,[70] it patrols geo-fenced areas randomly or based on a particular patrolling algorithm and is defined as a 'marked law enforcement vehicle'.[71] It is noteworthy that Knightscope's motto is 'hardware + software + humans' and it is explained by observing that

> '(h)umans are best at decision-making and situational analysis, while our technologies excel at monotonous, computationally heavy and sometimes dangerous work'.[72]

This approach is likely to be overcome soon, when the company deploys the new version equipped with object recognition tools and machine learning algorithms.[73] Finally, under K2's privacy policy, the personal and non-personal data collected by the robots may be shared for law enforcement purposes 'if we are compelled to by a court order'.[74] Elsewhere, however, the

[65] According to ComRes, 'Big Brother Watch – Online Privacy', 31 March 2015 available at http://www.comres.co.uk/wp-content/uploads/2015/03/Big-Brother-Watch_UK-Tables_9-March-2015.pdf (last visited 6 December 2016), seventy-eight per cent of the one thousand respondents are very concerned or at least fairly concerned about privacy online. The axiological statute of privacy in Italy may well be inferred by the Dichiarazione dei diritti in Internet (the charter of rights in the Internet) of 14 July 2015, whereby Art 8 of the Charter of Fundamental Rights of the EU (Protection of personal data) '*costituisce il riferimento necessario per una specificazione dei principi riguardanti il funzionamento di Internet, anche in una prospettiva globale*' (preamble). See also Arts 5-11 of the *Dichiarazione*.

[66] Along the same lines, see R. Calo, n 30 above, 3, whereby 'vulnerable populations such as victims of domestic violence may one day use robots to prevent access to their person or home and police against abuse.'

[67] See, eg, http://robotsecuritysystems.com/ and http://www.irobot.com/For-Defense-and-Security.aspx#PublicSafety (last visited 6 December 2016).

[68] *Autonomous* at least in the double sense of non-remotely-controlled and capable of charging itself.

[69] http://knightscope.com/ (last visited 6 December 2016).

[70] It comes with a browser-based web application, with no downloading of black box software required.

[71] n 69 above.

[72] Ibid.

[73] B. Schiller, 'Meet the Scary Little Security Robot That's Patrolling Silicon Valley', 13 August 2015, available at http://www.fastcoexist.com/3049708/meet-the-scary-little-security-robot-thats-patrolling-silicon-valley (last visited 6 December 2016).

[74] Section 5 of the Knightscope Privacy Policy, last modified on 13 August 2015, available

company admits that they may also proactively report the user and release its information 'without receiving any request to third parties where we believe that it is proper to do so for legal reasons'[75] (at least they will not do so for illegal reasons). It is debatable that all the sections of the policy and of the terms of service are enforceable, for example when the former reads '(i)f you have submitted information to our Site you will be unable to edit that information'.[76] Moreover, K5 shares data with third party individuals and organizations, including contractors, web hosts, 'and others'[77] and gives them the right to 'collect, access, use, and *disseminate* your information'.[78] Therefore, it would be preferable to have the company bind third parties to confidentiality agreements, especially given that the user is forced to agree 'not to hold (the company) liable for the actions of any of these third parties'[79] and that the third parties will not ask for the user's consent when processing its data.[80]

On the other hand, the potential for privacy-threatening uses are considerable. Robots can interact with human beings ('human-robot interaction, or HRI), with other robots, and with the environment overall;[81] they are equipped with sensors to perceive reality and can process and store big data, especially due to the developments of cloud robotics.[82] The main categories of robots are military, industrial, and service: each of them can be used to monitor people, acquire their data, and make decisions from the data.

Robots can see and hear better than human beings and can go where human beings cannot, with resistance and memory capabilities that are increasingly superior to human capabilities.[83] In principle, drones can

at http://knightscope.com/terms-conditions/ (last visited 6 December 2016). The scope of the section is not clear, since the following sentence reads '(a)dditionally, you agree that we may disclose your information if we reasonably believe that you have violated US laws or the terms of any of our agreements with you or if we believe that a third party is at risk of bodily harm.'

[75] Ibid, section 9.

[76] Ibid, section 6. Cf Art 7 para 3 letter a) of the *codice della privacy* (decreto legislativo 30 June 2003 no 196), whereby data subjects have the right to have their data up-to-date, to rectify them, and complete them. All the Member States have a similar provision on the right to amend one's personal data.

[77] Ibid, section 8.

[78] Ibid, section 8, italics added.

[79] Ibid, section 8.

[80] Ibid, section 8.

[81] Cf T. Fong et al, 'A Survey of Socially Interactive Robots' 42 *Robotics and Autonomous Systems*, 143-166 (2003).

[82] Cf P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (London: Penguin, 2009) and T. Denning et al, 'A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons' *11th International Conference on Ubiquitous Computing* (New York: ACM Press, 2010).

[83] According to B.J. Fogg, *Persuasive Technologies: Using Computers to Change What We Think and Do* (Burlington: Morgan Kaufmann Publishers Inc, 2003), 8, '(c)omputers don't get tired, discouraged, or frustrated. They don't need to eat or sleep. They can work around the

constitute an even more dangerous threat to privacy and data protection because in principle they can move more than robots. However, this is not always the case, not only because the distinction between robots and drones is blurred (for example, the Shigeo Hirose Ninja can climb, thanks to a suction cup system), but also and most importantly because robots are likely to become familiar components of our everyday life. Consequently, even in the event robots were not anthropomorphic, one would feel free to behave and talk in front of them as if they were family.

A society of machines and surveillance might easily recall Orwell's *1984*. It is, however, possible to suggest some similarity with Kafka's *The Trial*.[84] It is arguable that the problem of contemporary life is the lack of knowledge as to whether information will be used against us. Incidentally, this may be confirmed by the incredible fortune of the Google Spain ruling[85] on the so-called *right to be forgotten*.

Nonetheless, I have the feeling that our scenario is rather Orwellian. In fact, we are not capable of assessing the degree of control to which we are subject throughout our lives, thanks to the combined use of new technologies and bad laws.[86] I suggest everyone use Lightbeam, a Firefox add-on that enables users to see who is tracking them. The consequent shock may worsen once users realise that the tool is limited to the tracking that is carried out via cookies.

Surveillance capabilities and the possibility of accessing private spaces make drones and robots an unprecedented threat to privacy. Indeed,

> 'the home robot in particular presents a novel opportunity for government, private litigants, and hackers to access information about the interior of a living space'.[87]

clock in active efforts to persuade, or watch and wait for the right moment to intervene.'

[84] D. Solove, 'The Digital Person: Technology and Privacy in the Digital Age' 36 *GWU Law School Public Law Research Paper no 121* (2004).

[85] Case C-131/12 *Google Spain SL and Google Inc.* v *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (European Court of Justice Grand Chambre 13 May 2014). Cf A. Mantelero, 'The Protection of the Right to Be Forgotten: Lessons and Perspectives from Open Data' *Contratto e Impresa / Europa,* II, 734 (2015); Id, 'Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso Google: ricordare e dimenticare nella digital economy', in G.Resta and V. Zeno-Zencovich eds, *Il diritto all'oblio su Internet dopo la sentenza Google Spain* (Roma: Roma-Tre Press, 2015), 125; A. Viglianisi Ferraro, 'La sentenza Google Spain ed il diritto all'oblio nello spazio giuridico europeo' *Contratto e impresa/Europa*, 159 (2015).

[86] The increasing importance of cloud robotics enables me to refer to G. Noto La Diega, 'Cloud computing e protezione dei dati nel web 3.0' available at http://giustiziacivile.com/soggetti-e-nuove-tecnologie/approfondimenti/cloud-computing-e-protezione-dei-dati-nel-web-30 (last visited 6 December 2016), where I stress, *inter alia*, the problem that there is no technical means of ensuring that no one is accessing our data on the cloud.

[87] R. Calo, n 30 above, 2. Even before robots and drones, it was possible to gather personal

A hacker who accesses our computer can steal data, but a hacker who accesses a robot can map the house, record the habits of the inhabitants, and be remotely controlled so as to steal physical properties without the risk of being caught. It is not a coincidence that law enforcement agencies are increasingly making use of robots.[88]

Robots, and especially service robots, are becoming commonplace, thanks to increasing competition and a decrease in prices. Houses are being invaded by computers with legs (and sometimes wings) – machines usually connected to the Internet and capable of collaborating with other machines – due to cloud technologies. Public authorities, competitors, hackers, as well as the parties to a trial, can have access to the big data gathered by these machines, especially if they transmit information to or through the cloud. The relevant data are big in quantity and (potentially) personal in quality. Robots are increasingly equipped with sophisticated infrared cameras, Global Positioning System (GPS), accelerometers, sonars, electronic noses,[89] etc.

The issues are not different from those we are observing in the context of the Internet of Things. One need only consider the possibility of remotely activating the microphone in a car without the driver knowing it.[90] Similarly, one can intercept the audio-visual flows processed by robots and remotely control their moves, as well as orientate the sensors and the cameras. Moreover, every robot can be (and increasingly is) a component of a network of connected devices, which provides a formidable chance to third parties willing to recombine the information produced by the devices in order to exploit it for commercial purposes.[91]

One of the reasons why privacy is critical in every robotic scenario is that the internal memory of the machines is limited, whereas they need a fair

information – for instance, via webcams. However, nowadays there are more tools to gather and analyse information, thus changing the quantity and quality of the data themselves.

[88] See N. Sharkey, '2084: Big Robot is Watching You. Report on the Future of Robots for policing, surveillance and security' (2008), available at https://www.scribd.com/doc/139971746/Noel-Sharkey-2084-Big-robot-is-watching-you-Future-Robot-Policing-Report-Final (last visited 6 December 2016).

[89] Cf, eg, N. Schactman, 'Drones See, Smell Evil from Above', available at https://www.wired.com/2003/03/drones-see-smell-evil-from-above/ (last visited 6 December 2016) and J. B. Chang and V. Subramanian, 'Electronic Noses Sniff Success' *IEEE Spectrum* (2008), available at http://spectrum.ieee.org/biomedical/devices/electronic-noses-sniff-success/ (last visited 6 December 2016).

[90] This fact is cited by J. Zittrain, *The Future of the Internet: And How to Stop It* (New Haven-London: Yale University Press, 2008), 110.

[91] One need only think of the problem of cross-device tracking through advertisements that cannot be heard by human beings, but which enable the identification of the devices which are part of the relevant network. It is not coincidental that the Federal Trade Commission (FTC) has organised a workshop on the topic. See C. Calabrese et al, 'Comments for November 2015 Workshop on Cross-Device Tracking' (2015), available at https://cdt.org/files/2015/11/10.16.15-CDT-Cross-Device-Comments.pdf (last visited 6 December 2016).

amount of processing and storing resources, especially with the diffusion of artificial intelligence technologies. Therefore, traditionally, 'lacking the onboard capability to process all of the data, the robot periodically uploads it the manufacturer for analysis and retrieval'.[92] This leads to the issue of cloud robotics.

Cloud robotics enables, *inter alia*, potentially infinite storing and processing capabilities. Therefore, there is not necessarily the need to send over the information to the manufacturer (which usually retains this possibility), since the information is sent to the cloud provider (which is usually a third party). Cybersecurity in the cloud is becoming sound, especially thanks to the latest developments of homomorphic encryption; consequently, one can rely on the currently deployed clouds. As a recommendation to lawyers drafting cloud robotics contracts, it is critical to address encryption, redundancy, and geo-location of servers through *ad hoc* contractual sections.

Cloud servers are often outside Europe, which can cause problems in terms of jurisdiction, applicable law, and, recently, legality of the transnational transfer of personal data. The legal basis for the transfer of European personal data to the United States had always been the so-called Safe Harbour agreement, which was nearly automatically integrated in most of the contracts with big transnational corporations. Mostly as a consequence of Snowden revelations and kindred scandals, the Court of Justice has declared this international agreement void,[93] which has created a situation of utter uncertainty. In order to fully overcome the uncertainty, one should wait for the full effectiveness of the EU-US Privacy Shield.[94]

[92] R. Calo, n 30 above, 8.

[93] Case C-362/14 *Maximilian Schrems* v *Data Protection Commissioner* (European Court of Justice Grand Chamber 6 October 2015) available at www.eurlex.europa.eu. According to A. Mantelero, 'The "medieval" sovereignty on personal data. Considerations on the nature and scope of the EU regulatory model', available at http://bileta2016.co.uk/wp-content/uploads/2016/03/Mantelero-Alessandro.pdf (last visited 6 December 2016), only in appearance would the Schrems case reaffirm the strength of the European protection of personal data, 'but actually unveils the frail nature of this regulatory wall: the ECJ judgment has pointed out the inadequacy and the limits of the different remedies available to legitimate trans-border data flows and, therefore, the frailness of the apparent EU supremacy in protecting personal data.' Cf G. Resta, 'La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE' *Il diritto dell'informazione e dell'informatica*, 697-718 (2015).

[94] On 2 February 2016, the EU and the US agreed on a new framework for transatlantic data flows: the EU-US Privacy Shield. The College of Commissioners has mandated Vice-President Ansip and Commissioner Jourová to prepare a draft adequacy decision, which should be adopted by the College after obtaining the advice of the Article 29 Working Party and after consulting a committee composed of representatives of the Member States. In the meantime, the US side will make the necessary preparations to put in place the new framework, monitoring mechanisms, and new Ombudsman. The draft adequacy decision (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf (last visited 6 December 2016)) and the text of the Privacy Shield (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf (last visited 6 December 2016)) were presented on 29

Service robots, however, are not merely home robots. Robots are increasingly used in commercial contexts, such as the robotic shopping assistants first used in Japan and now becoming commonplace in Europe and America. Like a human shopping assistant, this robot identifies the potential client and drives him or her towards the product. However, unlike the human, the robot can record all of the information produced during the (attempted) transaction, crunch big data, and identify a customer who is returning (for example through the use of face-recognition technologies).[95] The resulting data can be exploited 'in both loss prevention and marketing research'.[96]

Shifting to the applicable law, one should move from Directive 2006/42 (machinery directive),[97] implemented in Italy through decreto legislativo 27 January 2010 no 17 (*decreto macchine*).

Art 18 of the machinery directive provides a regime that juxtaposes with the general data protection rules.[98] The directive calls on the Member States to ensure that the people involved in its application do not disclose confidential information, such as trade, professional, and commercial secrets.[99] However, there is awareness of the central role of the balance of opposed interests; therefore, the disclosure of confidential information is allowed when the health and security of people require it.

February 2016. On 13 April 2016, Article 29 Working Party adopted its 'Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision', thus pointing out that further clarification of the adequacy decision is in order. According to Commissioner Jurova, the 'European Commission is set to present a new draft of its data-exchange pact with the US, the Privacy Shield, in early July.' (N. Nielsen, 'EU to adopt new US data rules in July', available at https://euobserver.com/justice/133941 (last visited 6 December 2016)).

[95] On face recognition and machines see, for instance, Article 29 Working Party, opinion 27 April 2012 no 3 on the development of biometric technologies. On 5 May 2016, the District Court of Northern California rejected Facebook's motion seeking dismissal of a complaint filed under the Illinois Biometric Information Privacy Act. Some users of the social networking platform complained that the collection and storage of biometric data derived from their faces in photographs, for the purposes of *tag suggestions*, were illegal. The decision is available at https://cdn.arstechnica.net/wp-content/uploads/2016/05/Biometric-Ruling.pdf (last visited 6 December 2016).

[96] R. Calo, n 30 above, 4.

[97] The wording of the machinery directive is broad enough to encompass the vast majority of robots and drones. Some applications, however, may be excluded. See, for instance, machinery that is also a medical device, hence subject to the Medical Devices Directive 93/42/EC.

[98] On 4 May 2016, the GDPR was published on the Official Journal. See Regulation (EU) 2016/679 of the 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. It must be transposed by 25 May 2018, but it does not need acts of implementation.

[99] The listed types of information do not have a clear classification. In some countries they may fall under *intellectual property*, and in other systems under *data protection and privacy*. In Italy, I argue that they would be closer to the intellectual property realm.

It is not a *lex specialis* which applies instead of the general regime (it does not *derogat generali*). It adds to it. Indeed, Art 14 of *decreto macchine* is clear where it reads that the application of the code of privacy and of decreto legislativo 10 February 2005 no 30 (*codice della proprietà industriale*) is not affected. The domestic provision reproduces verbatim the European one, but the privacy is not balanced only with the health and security of people. The balance encompasses also the security of pets, goods, and the environment as a whole.

The Italian legislature might have been braver by introducing stronger privacy protections. However, the existing regime can be interpreted in a more privacy-friendly way. The manufacturer can determine that the machine does not threaten security and health before putting it on to the market. These data must be part of the technical attachment (Art 3, para 3, *decreto macchine*). The annex I of the directive clarifies the essential security requirements. The manufacturer must assess the limitations of the machine, including the foreseen usage and reasonably foreseeable incorrect usage.

Now, my suggestion is that the limitations to be assessed have to encompass privacy and data protection. The measures to be enacted in order to avoid an incorrect usage of the machine have to include the so-called privacy by design and privacy by default approaches that have become binding, due to the general data protection regulation (GDPR).[100] Without being naive, it is clear that these measures can only minimise, rather than eliminate the risks. However, the annex I is ready to face this scenario. If the measures *by design* do not eliminate all the risks, the manufacturer has to adequately inform the customer.

As to the mentioned technical attachment, it must include the documents related to risk assessment and give account of the essential requirements of security and health, as well as of the protection measures embedded, in order to avoid risks where possible and clarify the remaining risks. As a policy recommendation, the data protection impact assessment (DPIA)[101] needs to

[100] Under Art 25 para 1 GDPR, '(t)aking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

[101] Under Art 35 para 1 GDPR, '(w)here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a

become a compulsory tool for manufacturers of machines, be they robots, drones or the devices of the Internet of Things. Now, Art 15 of the *decreto macchine* provides fines for placing on to the market products inconsistent with annex I or products without the required technical attachment. Even though privacy and data protection can be interpreted as already included in the concept of security, I recommend that the legislature expressly state it and impose the DPIA (whilst the privacy by design and by default measures have become compulsory, thanks to the GDPR).

Shifting to drones, a communication of the European Commission on civil RPASs[102] is one of the main relevant documents.[103] The European strategy stresses the need for a public debate on societal concerns, that is, namely, data protection, privacy, liability, insurance, and security.[104] At a closer look, its para 3.4, entitled 'Protecting the citizens' fundamental rights,' is a sort of handbook on privacy in a drone context. The Commission recognises that some civil RPAS applications can jeopardise privacy; therefore, the operators of RPASs must respect the European privacy regimes.[105] The communication goes on to point out that the processing of data must always be carried out for a legitimate purpose. The creation itself of a market for RPASs is held dependent on the assessment of the appropriate measures to protect the fundamental rights, such as data protection and privacy. There is more. The Commission underlines that there shall be a constant monitoring of data protection.

Even if the *Garante per la Protezione dei Dati Personali* (*Garante*) does

set of similar processing operations that present similar high risks.'

[102] Communication from the Commission to the European Parliament and the Council on 'A new era for aviation – Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner', COM/2014/207, para 3.

[103] Cf also the communication of 13 February 2008 on 'Examining the creation of a European Border Surveillance System (EUROSUR)', COM/2008/68 final, whereby many activities, such as the monitoring of frontiers by using UAV 'may involve the processing of personal data. Thus the principles of personal data protection law applicable in the European Union are to be observed, meaning that personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The processing of personal data within the context of EUROSUR must therefore be based on appropriate legislative measures, which define the nature of the processing and lay down appropriate safeguards.' (Para 5).

[104] Com. 2014/207 final, para 3.

[105] The reference was to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, now repealed by the GDPR and to the Council Framework Decision 2008/977/JHA, now repealed by Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. The directive must be transposed by 6 June 2018.

not seem to have taken clear steps in the matter of machines, things are moving. One should mention two recent facts.

On the one hand, it ought to be mentioned that in April 2016, twenty-eight data protection authorities launched the 'Privacy Sweep 2016'. It is an international survey coordinated by the Global Privacy Enforcement Network and it aims to assess the relation between the Internet of Things and privacy. Its results will be of great relevance also in the robotics sector.

On the other hand, the *Garante* has recently ruled[106] in favour of the use of smart closed-circuit televisions (CCTVs) for access control and surveillance. It is noteworthy that the *Garante* authorises the processing on the ground that the requesting company was following an ISO standard. It is recognised that, even though standards are not legally binding provisions, they concern areas of critical public interest, which are technologically very complex. Therefore, public bodies endorse them increasingly and there is a long-standing practice to refer to standards in contracts. Consequently, one cannot deny that 'actually, one recognises in these technical specifications a statute which is considerably higher than the one they should have, given their adoption procedures'. The *Garante* concludes that such security standards have become, nationally and internationally, an inescapable reference point in high-tech markets.

The European Commission committed itself to launch consultations in order to assess how RPAS applications can be consistent with data protection. I am not aware of any such consultation, at least not one that has involved civil society. However, the Commission has sought some institutions' advice. It is worth mentioning the European Data Protection Supervisor (EDPS)'s opinion.[107] EDPS stresses that 'only those RPAS that will have integrated data protection and privacy in their design will be well regarded by society at large'.[108] According to the EDPS, most of RPAS applications process personal data, due to the broad scope of application and technologies in use.[109] Things get trickier when it comes to the full adoption of technologies, such as machine learning, that are leading to the creation of autonomous machines.

Some observations, then, would need an update. For instance, according to the EDPS, the European data protection regime is applicable 'as long as the processing takes place in the context of the activities of an establishment of

[106] *Garante per la Protezione dei Dati Personali* (Garante or GPDP) 17 March 2016 no 127 on '*Verifica preliminare. Sistemi di videosorveglianza dotati di software "intelligent video"*'.

[107] EDPS, Opinion on the Communication from the Commission to the European Parliament and the Council on 'A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner', 26 November 2014.

[108] Ibid, para 10.

[109] EDPS refers to the example of a camera with video processing software; it could be capable of high power zoom, facial recognition, behaviour profiling, movement detection, and number plate recognition.

the controller in the EU or with equipment or means located in the EU'.[110] As stated by the Court of Justice in *Weltimmo,*[111] the absence of a physical establishment and even of any equipment in the territory of the European Union is immaterial, insofar as there is evidence that the service is targeted at a Member State (for example, if a website is translated into a certain language).

The RPAS are usually compared to airplanes and CCTVs. According to the EDPS, however, drones constitute an even higher threat to privacy. Even though an airplane can be equipped with sensors and technologies far more refined than those of drones, the latter fly closer to the human being, and thus able to catch more personal data. The main difference between drones and CCTVs is the former's mobility, which 'offers more and also increasingly different uses.' Mobility and stealth make drones a perfect surveillance tool.

As stated by the European Court of Human Rights in *Von Hannover* v *Germany*,[112] the fact that certain activities are carried out in public does not exclude, in principle, any expectation of privacy. In fact, there is 'a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life'.[113] For instance, a citizen would have the right not to be targeted by zooming cameras and directional microphones, regardless of the public or private nature of the setting.

For what concerns private activities, for example for hobby purposes, the EDPS espouses a restrictive interpretation of the personal and domestic use exception (Art 3, para 2, second hyphen of directive 95/46/EC).[114] This is in line with the subsequent ruling in *František Ryneš* v *Úřad pro ochranu osobních údajů*,[115] where the Court of Justice found that the European privacy regime applies to the recording carried out by a private surveillance camera installed in a house and directed to a public path. On this point, the EDPS refers to *Lindqvist*[116] and infers that the processing of personal data carried out by private subjects does not fall within the said exception,[117]

[110] EDPS, n 107 above, para 31.

[111] Case C-230/ *Weltimmo s.r.o.* v *Nemzeti Adatvédelmi és Információszabadság Hatóság* (European Court of Justice Third Chamber 1 October 2015), available at www.eurlex.europa.eu.

[112] Eur. Court H.R., *Von Hannover* v *Germany,* Judgement of 24 June 2004, Reports of Judgments and Decisions 2004-VI, on Princess Caroline of Munich and her attempts to prevent the publication of pictures of her private life on tabloids.

[113] Ibid, para 97.

[114] The reference was Directive 95/46/EC. The relevant provision of the GDPR is Art 2 para 2 letter c, which repeats verbatim the wording of the directive.

[115] Case C-212/13 *František Ryneš* v *Úřad pro ochranu osobních údajů* (European Court of Justice Fourth Chamber 11 December 2014), available at www.eurlex.europa.eu.

[116] Case C-101/01 Criminal proceedings against Bodil Lindqvist, [2003] ECR I-12971.

[117] According to Article 29 Working Party, when assessing the household exception, one needs to take into consideration '- if the personal data is disseminated to an indefinite number of persons, rather than to a limited community of friends, family members or acquaintances, -

when it is aimed

> 'at sharing or even publishing the resulting video/sound captures/images or any data allowing the direct or indirect identification of an individual on the Internet and, consequently, to an indefinite number of people (for instance, via a social network)'.[118]

Moreover, as to the commercial and administrative use of drones, *Google Spain*[119] justifies an extraterritorial application of the GDPR. It follows that even the manufacturers of RPASs that are established outside the European Union need to embody data protection by design and by default measures, as well as to adopt a DPIA.

Finally, a couple of recommendations. The European Commission has no jurisdiction on RPASs under one hundred and fifty kilograms. Yet, the manufacturers of small RPASs need to be aware that the privacy and data protection regimes still apply. Moreover, it is important to raise customers' awareness; therefore, I suggest carefully drafting privacy notices to be included with the packaging of drones.

More recently, the Article 29 Working Party[120] has issued its opinion 'on Privacy and Data Protection Issues relating to the Utilisation of Drones'.[121]

The Article 29 Working Party calls on policy makers and regulators so that the deployment of civil drones is accompanied by several measures. Let us only mention the need to make the authorisation to fly dependent on declarations of the assessment of the impact on data protection, as well as the invitation to draft DPIAs by liaising with stakeholders.

if the personal data is about individuals who have no personal or household relationship with the person posting it, - if the scale and frequency of the processing of personal data suggest professional or full-time activity, - if there is evidence of a number of individuals acting together in a collective and organised manner,- if there is a potential adverse impact on individuals, including intrusion into their privacy.' See Annex 2, Proposals for Amendments regarding exemption for personal or household activities, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf (last visited 6 December 2016).

[118] EDPS, n 107 above, para 35.

[119] Case C-131/12 *Google Spain* n 85 above, particularly when it states that the exception must be interpreted 'as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State' (para 60).

[120] The Article 29 Working Party is about to be substituted by the European Data Protection Board (see Art 68 GDPR).

[121] Article 29 Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, 16 June 2015, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf (last visited 6 December 2016).

Manufacturers and operators, then, shall embody privacy by design and by default; adopt codes of conduct assisted by *ad hoc* remedies (in a *sui generis* co-regulation model);[122] and render the drone identifiable (for example through wireless signals or bright colours).[123]

Law enforcement agencies, finally, shall respect the principles of necessity, proportionality, and minimisation; inform the data subjects 'as far as possible';[124] ensure that the continuous surveillance is covered by a warrant; as to the automated execution of decisions, ensure that a human operator controls the data processed by the drone.

The Italian *lex specialis* is the regolamento ENAC. Its Art 34 is rather different from the wording of the above analysed provision of the machinery directive, inasmuch as it provides the following. First, when the RPAS operations involve (or can involve) the processing of personal data, this risk ought to be mentioned in the documents produced when applying for an authorisation. Second, the processing of personal data ought to be consistent with the code of privacy, especially with regard to adopting techniques that render the data subject identifiable only when necessary under Art 3 of the said code. The data processing, third, ought to follow the measures enacted by the *Garante*. It should also be noted that, in case of operations carried out on behalf of third parties, the regolamento mandates the parties to include provisions relevant to data protection (Art 7 para 3).

Art 34 does not go beyond the mere reference to the general data protection regime. However, it is commendable that the *Garante* suggests what I have wished above with regard to the machinery directive, that is, the need for the documents accompanying the authorisation to cover privacy issues. The sensitiveness towards the trend of data minimisation is noteworthy.[125] Lastly, the reference to the decisions of the *Garante* can be a dynamic and flexible tool, as the procedures of the authorities are simpler than those of the legislature.[126] One should wish that the reference was

[122] The code of conduct is usually an example of self-regulation. However, in this context, it is accompanied by proper remedies, thus giving rise to a public-private collaboration which can be described as co-regulation.

[123] Given that the invisibility of drones is one of the reasons of their appeal, marketing considerations may lead to not enforcing this provision.

[124] Article 29 Working Party, n 121 above, para 5.4.

[125] Cf, eg, Article 29 Working Party, *Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire*, 16 December 2013, para 3, whereby a 'need for policy guidelines has been identified in order to address the practical difficulties regarding the enforcement of some data protection rules regarding the use of data processing equipment onboard RPAS, for example fair processing, information notice, data minimization and compliance with data subjects' access rights'.

[126] The Garante has not taken a position yet. However, there are many documents which are indirectly relevant to machines and privacy (see, in text, the reference to smart CCTV and the survey on the Internet of Things). On robots as internet bots see GPDP, opinion 4 July 2013, doc. web no 2574977 on *'Linee guida redatte dall'Agenzia per l'Italia Digitale ai sensi*

extended also to EDPS and the Article 29 Working Party (and in the future to the European Data Protection Board).

To conclude, there are three takeaways. First, machines can both help protect us from privacy threats, yet also constitute a threat themselves. Second, even though there seems to be more concern about drones, robots can be even more dangerous, because they are present in the most private spaces and they become a familiar component of the everyday landscape in a household. Third, existing legislation and regulations – *in primis* the code of privacy and the regolamento ENAC – are applicable even in the event of threats to privacy posed by robots and drones. However, on the one hand, the Italian legislature needs to amend the code of privacy to react to the GDPR, particularly regarding the DPIA, data protection by design and by default, and certifications.[127] On the other hand, the Italian and European data protection authorities need to take machines seriously and hopefully the results of the survey on the Internet of Things will constitute a good step towards this direction.

V. Torts, Contracts, and Special Regimes of Liability

In late June 2016, Tesla announced that a man died while driving in autopilot mode because the sensors of the vehicle, which help to steer the car by identifying obstructions, had failed to recognise 'the white side of the tractor trailer against a brightly lit sky'.[128] The US *National Highway Traffic Safety Administration has just opened* a preliminary evaluation into the performance of the autopilot, so it is too soon to reach any conclusions, but the first fatal crash of a (quasi)[129] driverless car has reminded us all of the importance of the topic of liability.

dell'art. 58, comma 2, del D. Lgs. 7 marzo 2005, n. 82 (CAD)', especially para 5.5.2.3. Robots and bots, however, shall not be confused.

[127] Art 42 of the GDPR encourages the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with the regulation of processing operations by controllers and processors.

[128] The Tesla Team, 'A tragic loss', 31 June 2016, available at https://www.teslamotors.com /blog/tragic-loss (last visited 6 December 2016).

[129] The Tesla model S's autopilot requires the driver to leave the hands on the steer, in order to allow them to contradict the machine's decisions. In a case like this, Tesla could argue that the driver should have distinguished the white side of the tractor from the bright sky. Probably, the conclusion will be different with proper driverless cars. Since the tests are showing that mortality and accidents are by far less frequent with driverless cars, in comparison with human-driven cars, I believe that regulators should allow the deployment of this kind of machines, but they should clarify that manufacturers of cars are liable for driverless cars even in the case the driver (or their family) was not able to prove the manufacturers' or the developer's fault. Indeed, the manufacturer is the (economically and contractually) strongest actor in the supply chain and the one who can have a more direct control on the embedded software (for security reasons, driverless cars will likely be 'closed' systems), therefore a

From an Italian civil law perspective, the main general liability regimes that apply to machines are breach of contract (*responsabilità contrattuale*), torts (*responsabilità extracontrattuale*), and product liability. When it comes to drones, one should also take into account the special provisions of the regolamento ENAC and of the codice della navigazione.

The *responsabilità contrattuale* is an objective liability, insofar as it does not require the proof of negligence or fault of the defendant. It derives from the *inadempimento,* the violation of an obligation (be it contractual or not) and it is accompanied by a large array of remedies, such as damages and specific performance. Machine contracts (that is, contracts created when buying a robot or a drone) may contain disclaimers of any liability, but such sections may not be enforceable, especially in business-to-consumer transactions.[130] Moreover, there are specific provisions, such as Art 1494 para 2 of the codice civile, regarding the seller's liability for damages deriving from the defects of the sold good.[131] A good use case is provided by the Unibox service provided by Octo Telematics Italia srl to the clients of the insurance company Unipol Assicurazioni spa. The company provides a *black box* equipped with several sensors that drivers install in their car in order to allow the insurance company to monitor their driving habits, while the driver can benefit from discounts on the insurance fee. As one can read in the *Condizioni Generali del Contratto di abbonamento ai servizi* (terms of service),[132] the contract is a *comodato* – that is, a complimentary leasing.[133]

presumptive strict liability regime should operate.

[130] The *codice del consumo* (decreto legislativo 6 September 2005 no 206) provides a higher level of protection to consumers; this results, for instance, in special remedies and in the restriction of the freedom of contract on the side of businesses. The codice del consumo has been amended several times, lastly by decreto legislativo 6 August 2015 no 130, which has transposed Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR).

[131] Under Art 1490 of the codice civile, the seller shall guarantee that the sold good has no defects that render the good unsuitable for the designated use or that decrease its value substantially. However, the seller has two defences: either he proves that the buyer knew the defects, or he proves that the defects could easily be recognised. In the latter scenario, the buyer can rebut the evidence by showing that the seller has declared that the good had no defects (Art 1491). On the nature of this liability, see Corte di Cassazione 11 February 2014 no 3021, in R. Mazzoni, *Risarcimento del danno per inadempimento contrattuale* (Sant'Arcangelo di Romagna: Maggioli, 2014), 276.

[132] *Condizioni Generali del Contratto di abbonamento ai servizi Octo Telematics Italia srl*, edition of 1 July 2011, available at http://www.unipol.unipolsai.it/utile-e-facile/preventivatori/autoveicoli/Documents/05_Condizioni-Octotelematics_9533_PA002%20OCTO%20TELEM.pdf (last visited 6 December 2016).

[133] Under Art 1803 of the *codice civile,* the *comodato* is an essentially complimentary contract whereby a party delivers a movable or immovable good to another party, so that the latter can use it for a limited time and specified purpose, with the duty to return the same thing they had received.

One of the relevant provisions of the codice civile reads that if the defects of the good damage the *comodatario* (the user), the *comodante* (the provider) shall compensate the loss, provided that the latter knew the defects and did not warn the former (Art 1812).

It is harder for a claimant to be successful in a *responsabilità extracontrattuale* claim, since there are less favourable rules, especially on the burden of proof, causality link, and subjective element (for example, the *dolo* and *colpa grave* required by Art 2043 of the codice civile). The more complex regime is due to the fact that the damage occurs in a moment when there is not a qualified relationship between the claimant and the defendant. Furthermore, there are a number of specific provisions that can apply, depending on the characteristics of the specific dispute. For instance, Art 2050 of the civil code creates a form of objective liability for those who carry out dangerous activities (*responsabilità per esercizio di attività pericolose*). Another provision that is potentially applicable is Art 2049 of the civil code, which deals with the liability of the owner and of the commissioner for the damages caused by the tort of the person under the former's responsibility. Lastly, Art 2052 of the civil code regards the damages caused by things held in custody.

Machines *per se* do not lead one to rethink these general liability regimes. Autonomy is the real question. The use of artificial intelligence is leading to the manufacturing of machines that can make autonomous decisions, learn from experience, and act in a way that was not foreseeable at the time of production. Currently, machines have no legal personality; therefore they cannot be subject to rights, enter into contracts, be bound by obligations, be condemned to pay damages, be arrested, etc. Nevertheless, for reasons I will explain in the conclusions, it is just a matter of time until we will have to recognise legal personality of machines.

Nonetheless, let us deal with the current status of autonomy and the lack of personality. Even though the machine itself cannot be found liable, if no obligations bind the damaged person or the person behind the machine, it becomes harder and harder to spot a causality link when one faces autonomous decisions. Moreover, who is the person behind the machine? The manufacturer of the hardware? The developer of the software? What if the damage derives from the interoperability with third-party software and machines?

A generalised system of compulsory insurance, along the lines of the *responsabilità civile auto* (mandatory car insurance), as well as a public debate on simpler and fairer contracts, should be the answers. In the meantime, the product liability regime[134] may provide temporary and imperfect answers.

[134] The decreto del Presidente della Repubblica 24 May 1988 no 224 implemented Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and

This regime is imperfect mainly because it is limited to just some items of losses and only if they are the consequence of a defect. Moreover, it is not entirely clear what happens if the defect is to the software and not to the hardware component. Elsewhere,[135] I have argued that the devices of the Internet of Things (and most robots and drones are subsumable under said category) are an inextricable mixture of hardware, software, and service. Consequently, I argue that even defects to software can give rise to product liability claims. As a policy recommendation, updates to the defective products directive and to the codice del consumo are much needed. However, the rules are still most suitable for when one deals with damages caused by machines because it is a strict liability regime.[136] The burden to prove damages does not fall on the person actually responsible for the defect but falls presumptively on the manufacturer. However, these rules are still the most suitable when one deals with damages caused by machines, since it is a strict liability and does not impose on the damaged person the burden to find the single person actually responsible for the defect, thanks to a presumptive system revolving around the manufacturer.

It is unclear whether the machinery directive and the decreto macchine apply to drones. They both leave out of their scope, *inter alia*, the means of transport by air. It is not certain whether all drones can be considered means of transport, but one should take these regimes into account because they undoubtedly apply to robots.

From a liability perspective, the manufacturer (*fabbricante*) is at the centre. It is defined as the legal or natural person who designs and/or builds a machine: he is responsible for conforming to the decreto macchine (Art 2 para 2 letter i). This regime comes with a notable array of remedies. For

administrative provisions of the Member States concerning liability for defective products (product liability directive). The current regime is provided by art 114 ff of the *codice del consumo,* which is completed by the health and safety regime provided by art 102 ff of the same codice.

[135] G. Noto La Diega and I. Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' *Queen Mary School of Law Legal Studies Research Paper no 219/2016*, available at http://ssrn.com/abstract=2725913 (last visited 6 December 2016), now in *European Journal of Law & Technology*, 2016, II.

[136] As clarified by Corte di Cassazione 28 July 2015 no 15851, *Danno e responsabilità*, I, 41 (2016), it is a presumptive regime, whereby one assumes the manufacturer's fault, but it can still prove the inexistence of the defect (it is a *colpa presunta* regime, not a *responsabilità oggettiva* one). The Italian ruling is inconsistent with Joined cases C-503/13 and C-504/13 *Boston Scientific Medizintechnik GmbH* v *AOK Sachsen-Anhalt – Die Gesundheitskasse and Betriebskrankenkasse RWE* (European Court of Justice Fourth Chamber 5 March 2015), available at www.eurlex.europa.eu, whereby Art 6(1) of the product liability directive must be interpreted as meaning that, where it is found that products belonging to the same group or forming part of the same production series have a potential defect, such a product may be classified as defective without there being any need to establish that that product has such a defect.

instance, unless the offence is criminal, the manufacturer or its agent (*mandatario*), which places the machine on the market without meeting the provided requirements of conformity, is fined with a sum up to twenty-four thousand euros.

Shifting to the special regimes that are applicable to drones, the *regolamento* ENAC is relevant also with respect to liability, since it regulates the conditions of the flight and the role and responsibility of pilots, as well as the mandatory insurance[137] (which it is not clear why should be limited to this kind of machine).

In order to fly a drone, one needs the ENAC's authorisation or a declaration of conformity.[138] The main content of these documents is safeguards for security and safety, for the same reasons it is compulsory to have a flight manual. It is noteworthy that the RPAS has to be identified through a placard with information about the system and the operator. Since the identification is fundamental in order to be able to allocate responsibilities, this mechanism appeared rather inadequate. Therefore, the new version of the *regolamento* provides that, as of 1 July 2016, RPASs must be equipped with an electronic identity device, which enables the real-time transmission and recording of the data on the drone and on the owner/operator, alongside the basic flight data.

The main person responsible appears to be the remote pilot.[139] The remote pilot is defined as the person charged by the operator as responsible for the conduct of the flight, who commands the RPAS by manipulating the remote ground pilot station. This applies particularly to visual line of sight (VLOS) operations, where the remote pilot keeps continuous visual contact with the aerial vehicle, without the aid of tools to enhance the view, thus being able to control it directly with the aim to conduct the flight and to meet separation and collision avoidance responsibilities. The remote pilot has the final responsibility to define the VLOS conditions, which might be affected by the weather condition, the sunlight, or the presence of obstacles. It is their responsibility to ensure the continued compliance with the conditions for the experimental activity, which is an essential prerequisite for the critical operations. More generally, pursuant to *codice della navigazione*, 'the pilot is responsible for the safe management of the flight' (Art 20).

[137] Under Art 32 of the *regolamento* ENAC, '(n)o RPAS shall be operated unless it has in place a third party insurance, adequate for the operations and not less than the minimum insurance coverage of the table in Art. 7 of Regulation (CE) 785/2004 is in place for the operations.'

[138] The dichotomy is between critical and non-critical operations. The former must be preceeded by an authorisation, and the latter by a declaration.

[139] However, see Art 28 of the *regolamento*, whereby 'The operator, the manufacturer, the design organization, the pilot shall keep and make available to ENAC documents issued in order to demonstrate compliance with this Regulation, upon to their respective responsibilities.'

The operator plays an important role in terms of prevention and security (Art 33). He shall put in place appropriate measures to protect the RPAS from unlawful acts during operations, including the prevention of unlawful interference with the radio link. Moreover, the operator shall establish procedures to prevent unauthorized access to the area of operations, with particular attention to the remote ground pilot station, and to the storage location of the RPAS.

RPAS operations can be carried out on behalf of third parties. In this event, a contract between the RPAS operator and the client shall allocate the responsibilities for such specific operations.

Some remedies accompany the *regolamento*. For instance, ENAC can suspend authorisations and certifications if the *regolamento* is violated. Moreover, if one undertakes specialised operations without authorisation for critical operations or declaration of conformity, they shall be subject to the remedies provided by Arts 1174, 1216, 1228, and 1231 of the *codice della navigazione*.

The second title of the third book of the codice is dedicated to the liability for damages to third parties both for what are known as *surface* and *impact* damages. Under Art 965, the *esercente*[140] is liable for the damages caused by the aerial system to people and goods on the Earth's surface, even in the case of *force majeure*. However, the *esercente* can still prove that the damage was the consequence of the harmed person's fault. Moreover, the harmed person will not be entitled to damages if he could have avoided the injury or the loss by being diligent (Art 966). A cap to damages is provided, depending on the weight of the system (Art 967, but see Art 971 for the exclusion of the limitation) and it is excluded an overlap between this special tort[141] liability and the contractual one. Indeed, Art 965 ff are not applicable when there is a contract binding the *esercente* and the harmed person (Art 972).

A second scenario is the impact damage (*danno da urto*) due to slipstream effects or a similar cause (Art 974). Unlike surface damages, in the event of *force majeure* or unforeseeable circumstances, no damages will be granted. It is irrelevant whether there has been a material collision between the aerial systems or between the aerial system and the moving ship.

Lastly, Art 978 regards surface damages occurring from in-flight impact.

[140] The *esercente* is the person entitled to operate the aerial system. Under Art 874 of the *codice della navigazione*, the one who operates the aerial system has to declare it to ENAC, as well as record it in the *Registro Aeronautico Italiano* and on the *Certificato di Immatricolazione*.

[141] For instance, the right to damages lapses after one year from the day of the loss or injury (Art 973 of the *codice della navigazione*). On the contrary, the general term of *prescrizione* for torts is five years, which is reduced to two years in case of vehicle traffic (Art 2947 of the *codice civile*). The *prescrizione* for the second scenario (impact damage) is two years (Art 487 of the *codice della navigazione*).

For instance, what happens if two drones collide and, therefore, plummet to the ground, injuring a passerby? The *esercenti* are jointly and severally liable (*responsabilità solidale*). Therefore, the passerby is entitled to claim damages from each of them for the entire sum. The *esercenti*, then, will split the amount in proportion to the severity of fault and of the relevant consequences. If the accident occurred due to *force majeure* or if it is not possible to ascertain the fault or the severity of the respective faults (or of the consequences), the damages will be shared equally.

The compliance with the regolamento and with the technical standards provide a good defence in liability claims, but it may not help when strict liability regimes apply.

VI. 'If This Is a Machine.' Conclusions

No contemporary discourse on machines can end without some words on autonomous systems and the future of the info-capitalist[142] society. Recently,[143] the polarisation of the debate between *Singularitarians*[144] and *AItheists*[145] has been underlined. The former are sure that true superintelligence is around the corner and it will disrupt everything we know, thus leading to an apocalyptic scenario where human labour will become useless and human beings will become the machines' slaves. In turn, the latter argue that even imagining an intelligent machine is preposterous and, in any case, no real disruption will come, since we will able to keep machines under our control. The author of the Singularitarians/AItheists classification proposes a more nuanced approach, but ultimately he affirms that real AI is utterly implausible and invites intellectuals to focus on more important issues.

It is probably true that both positions are incorrect and I have dealt with the current legal issues because I cannot see proper superintelligence[146] happening in the next few years.[147] However, I am quite sure that AI will

[142] I use *info-capitalism* to focus on a major aspect of the so-called biocapitalism; that is, the mass exploitation of personal data, big data, and, more generally, information.

[143] L. Floridi, n 49 above.

[144] For those who are not familiar with this kind of literature, the reference is to K. Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York: Viking, 2006). An eminent intellectual belonging to this class is Stephen Hawking, who said that 'the development of full artificial intelligence could spell the end of the human race.' (R. Cellan-Jones, 'Stephen Hawking warns artificial intelligence could end mankind' (2014), available at http://www.bbc.co.uk/news/technology-(last visited 6 December 2016)).

[145] See, eg, J.R. Searle, 'What Your Computer Can't Know' *The New York Review of Books* (2014).

[146] On a caveat against the anthropocentrism underlying expressions such as artificial intelligence, smart city, etc, please see G. Noto La Diega, n 9 above, fn 1.

[147] Cf, eg, W.E. Halal, 'Artificial Intelligence Is Almost Here' *On The Horizon – The*

happen, for at least four reasons.

First, machines have been constantly, sometimes exponentially, increasing – far faster than human beings. Let us think what a computer could do fifty years ago and what a human being could do. If we think of the development of the latter, it is mainly due to the use of machines.

Second, big transnational corporations are massively investing in AI technologies[148] and governments[149] are increasingly interested in this realm. One may suppose that this is related to the potential of AI in terms of predictive analytics, profiling, and surveillance.

Third, it is wrong to assume there is a *before* and an *after* of AI: AI is already happening[150] and it is doing so incrementally. This is due mainly to the fact that we are growing over-dependent on machines. Consider our addiction to smartphones.[151] The British check their smartphones fifty times a day, adding up to more than two hours of staring at the screen.[152] Moreover, if one has a smartphone, one is quite likely to be constantly connected to Facebook.[153] As pointed out by a survey of four thousand respondents in thirty countries, the

> 'most fascinating aspect of the adoption of the smartphone is the extent to which it has become not just our primary access to digital sources, but an ever more comprehensive and capable remote control to life'.[154]

Strategic Planning Resource for Education Professionals, II, 37 (2003) and the more realistic R. Kumar et al, 'Prediction of Metabolism of Drugs Using Artificial Intelligence: How far Have We Reached?', *Current Drug Metabolism*, II, 129 (2016).

[148] See, eg, the alarming H. Hodson, 'Revealed: Google AI Has Access to Huge Haul of NHS Patient Data' *New Scientist* (2016), available at https://www.newscientist.com/article/2086454-revealed-google-ai-has-access-to-huge-haul-of-nhs-patient-data/ (last visited 6 December 2016).

[149] For instance, on 3 May 2016, the White House announced a workshop series and an interagency working group on artificial intelligence. In particular, it is established a new National Science and Technology Council (NSTC) Subcommittee on Machine Learning and Artificial Intelligence; the first meeting will be in June 2016.

[150] Let us just think to Google's Deepmind AlphaGo, which (who?) defeated the world's best player of the boardgame Go.

[151] For a complementary aspect see E.H. Kwon et al, 'Excessive Dependence on Mobile Social Apps: A Rational Addiction Perspective' (2016), available at http://ssrn.com/abstract=2713567 (last visited 6 December 2016).

[152] See T. Tamblyn, 'Brits Check Their Phones 50 Times a Day' *The Huffington Post* (2015), available at http://www.huffingtonpost.co.uk/2015/05/07/brits-check-their-phones-50-times-a-day-on-average_n_7233188.html (last visited 6 December 2016).

[153] International Data Corporation (IDC), 'Always Connected to Facebook' (2013) available at https://www.idc.com/prodserv/custom_solutions/download/case_studies/PLAN-BB_Always_Connected_for_Facebook.pdf (last visited 6 December 2016).

[154] Deloitte, 'Mobile Consumer 2015: The UK Cut Game of Phones' (2015), available at http://www.deloitte.co.uk/mobileuk2015/assets/pdf/Deloitte-Mobile-Consumer-2015.pdf

In fact, the current dependence (and sometimes addiction) to machines is part of a clearly upward trend, due to the critical role played by the smartphone in the Internet of Things.

Intertwined with the third reason is a fourth, which refers to Kahnemann's theories on System 1 and System 2 of the brain.[155] The Nobel Prize in Economics winner describes two ways the brain forms thoughts. System 1, which we use for tasks such as speaking our mother tongue is fast, automatic, frequent, emotional, stereotypic, and subconscious. When I speak Italian, I do not have to put considerable effort in building propositions and I can do other things at the same time. In turn, we use System 2 for complicated tasks, such as doing maths problems; this system is slow, effortful, infrequent, logical, calculating, and conscious. Its laziness is the fourth reason why proper superintelligence will be a reality. It is common experience that we started using calculators to save time and now most of us are incapable of doing maths, because we have delegated that chore to machines. Therefore, on the one hand we keep on delegating to machines tasks pertaining to System 2 (and consequently we demand that these machines are as accurate and *intelligent* as possible). On the other hand, the boundaries between System 1 and System 2 are shifting. One may assume, for instance, that reading in one's mother tongue is clearly subsumable under System 1. Maybe surprisingy, it has been shown[156] that only twenty per cent of the Italian population has mastered the minimal reading, writing, and calculating skills required to navigate contemporary society.

When machines become truly intelligent, the legal discourse will have to change radically. We will not only be required to discuss which rights we have in terms of intellectual property, privacy, liability, etc. Indeed, we will have to recognise the legal personality of machines, and, accordingly, accept that they are entitled to rights and obligations. This will happen for several reasons. To name one: we are becoming machines ourselves. Even leaving aside artificial enhancement developments, it is already happening that if one is deaf, he can get an artificial ear; if one loses a limb, he can get a prosthetic one, or cells and tissues can be 3D printed; if one cannot see, biometric eyes will soon be found in shopping centres. Any traditionally human function will soon be potentially substituted by chips. It is hard to draw a clear line between a *being* who was born as a machine but now it is fully autonomous and a *being* who was born *human* but whose functions are entirely carried out by chips and other artificial substitutes. Since distinguishing between human beings and machines, human and artificial, legislators and regulators will no longer be able to discriminate on biological

(last visited 6 December 2016).

[155] D. Kahnemann, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

[156] T. De Mauro, 'Analfabeti d'Italia' 734 *Internazionale* (2008).

grounds. Therefore, real AI may have machines' rights and machines' obligations as the main consequence.

If one must use Floridi's dichotomy, I can be considered a Singularitarian in a moderate sense. I do believe that we will have true superintelligence,[157] but, at the same time, this will not lead to the apocalypse. I believe that machines will outclass us in all our tasks, but the *horror vacui* ought to be avoided: an unforeseeable society will come and we will not have to work in order to be able to live (at least, not work in the traditional sense of the word).[158] For most academics' happiness, *usefulness* will not be the benchmark of social value and mass unemployment will be a treat, as opposed to a threat.[159] In the post-biocapitalist society, freed from the fight on the control of the means of production, human beings – granted that such a category will exist as separate from machines – will have the time to regain control of themselves and construct the foundation of a new society,[160] which shall be more just for everyone, no matter how many chips and transistors they have in their body.

[157] A caveat always stands. Following the mostly still valid A.M. Turing, 'Computing Machinery and Intelligence' 59 *Mind*, 433 (1950), to pose the question, 'can machines think?' is absurd.

[158] Just a few years ago, who could have imagined that people could have earned a living by allowing others to watch them play videogames? See, for instance, the incredible growth of Amazon's Twitch.tv, with more than one million five hundred thousand broadcasters and one-hundred million visitors per month.

[159] Cf M. Ford, *The Rise of the Robots – Technology and the Threat of Mass Unemployment* (London: Oneworld Publications, 2015).

[160] I share the optimism of N. Srnicek and A. Williams, *Inventing the Future: Postcapitalism and a World without Work* (London-New York: Verso, 2015).