BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 12, NUMBER 2 (2019)
ISSN 2029-0454

Cit.: *Baltic Journal of Law & Politics* 12:2 (2019): 47–77
https://content.sciendo.com/view/journals/bjlp/bjlp-overview.xml
DOI: 10.2478/bjlp-2019-0011

RETHINKING THE IMPLICATIONS OF TRANSFORMATIVE ECONOMIC INNOVATIONS: MAPPING CHALLENGES OF PRIVATE LAW

Julija Kiršienė

Professor; Dr.
Vytautas Magnus University, Faculty of Law (Lithuania)

Contact information
Address: Jonavos str. 66, Kaunas, LT-44191, Lithuania
Phone: +370 37 203775
E-mail address: julija.kirsiene@vdu.lt

Christopher Kelley

Associate Professor; Dr.
University of Arkansas, School of Law (United States)

Contact information
Address: Fayetteville, AR 72701, United States
Phone: +479 575 3230
E-mail address: ckelley@uark.edu

Deividas Kiršys

Ph.D. Student
Mykolas Romeris University, School of Law (Lithuania)

Contact information
Address: Ateities st. 20, LT-08303 Vilnius, Lithuania
Phone: +370 5 271 4578
E-mail address: deividas@kirsys.lt

Juras Žymančius

LL.M. in Law
Vytautas Magnus University, Faculty of Law (Lithuania)

Contact information
Address: Jonavos str. 66, Kaunas, LT-44191, Lithuania
Phone: + 370 37 203775
E-mail address: juraszymancius@gmail.com

Received: April 30, 2019; reviews: 2; accepted: December 20, 2019.

ABSTRACT

This article participates in mapping existing legal implications stemming from contemporary innovation. The article relies on a case analysis of artificial intelligence, drones and blockchain, to reflect a majority of the underlying legal issues to which many emerging innovations might contribute, and it attempts to map them into different categories of challenges – liability, privacy, and property. It concludes by pinpointing three main reasons behind the identified legal implications: the growing "consciousness" and autonomy of emerging technologies, the growing availability of transformative innovations to the broad public and the development of participatory models in economy and other social spheres, including law, and the tendency for transformative innovations to function in regulatory uncertainty. As a means to cope with challenges generated by technological progress, the article leans towards a process-focused approach that promotes embedding values in the early stages of technological development.

KEYWORDS

Transformative innovation, artificial intelligence, blockchain, drones, private law, privacy, liability, property

NOTE

This research is funded by the European Social Fund according to the activity "Improvement of researchers" qualification by implementing world-class R&D projects of Measure No. 09.3.3-LMT-K-712.

INTRODUCTION

The world is shifting from the age of digital electronics, which can be described as the third industrial revolution, to the fourth industrial revolution, which is characterized by a fusion of technologies.[1] Klaus Schwab believes that it is changing not only how we live but also who we are and that it is evolving on a scale and at a pace that was never before witnessed in the history of humankind.[2]

Because technology tends to develop faster that legal regulation, it is easy to forget that innovations are meant to aid human progress in various dimensions, not only mere economic growth. Therefore, a human-centred approach to legal regulation of technological development is required. The present paper aims to identify early warning signs of change in the economic environment and to provide a research basis for legal regulation issues stemming from this change.

The paper relies on a case analysis of three emerging innovations that are very different in terms of application, economic and social impact, pace of evolving, yet are also interconnected and indeed share homogeneity of challenges for private law: artificial intelligence, drones, and blockchain.[3] Each case analysis will distinguish the main legal implications that the innovation under consideration raises. Then, the identified implications will be generalized and assigned to different areas of law, outlining the main concerns towards which policy makers should be shifting their attention when drafting regulation. The paper will conclude by offering a value-based approach to legal regulation.

The scope of this work is civilian contexts and excludes any scenarios related to war. Therefore, some examples of issues that are out-of-scope include the ethics of using transformative innovations in war, politics and practices of smart weapons, increased ability of warfare without harm to the human resources of the party that started the war. Any analysis of existing doctrine, legislation and institutional guidelines is limited to the European Union and the United States of America.

This article consists of three main segments. The first part takes a short glimpse at the implications inherent in artificial intelligence, drones, and blockchain. The second part expands the implications case-by-case. Finally, the last part

[1] Chris Holder, et al., "Robotics and Law: Key Legal and Regulatory Implications of the Robotics Age (Part I of II)," *Computer Law & Security Review* Vol. 32, No. 3 (June 2016): 383 // https://doi.org/10.1016/j.clsr.2016.03.001.
[2] Klaus Schwab, *The Fourth Industrial Revolution*, 1st U.S. edition (New York: Crown Business, 2017), 1.
[3] Although there are many other technological innovations that have emerged over the recent years, we feel that the examples of artificial intelligence, drones and blockchain technologies are able to reflect many of the underlying implications that transformative innovations have brought about to private law and that conducting similar case analysis of other emerging innovations such as robots, the internet of things, sharing economy and so on, would most likely indicate the same or at least strongly related trends.

attempts to generalize and map the emerging challenges of transformative innovations and suggests guidelines for regulatory responses considering the layer of values.

1. IMPLICATIONS OF TRANSFORMATIVE INNOVATIONS IN ECONOMY

Although it is argued that "society and technology develop in tandem,"[4] it is also obvious that technologies such as internet, artificial intelligence, robots, blockchain, autonomous cars, drones, gene editing and the like, which are blurring the lines between human and technological capabilities[5], can change the world profoundly and irrevocably.

Transformative innovations are not just tools,[6] objects of the material world or neutral mediators used to realize human potential, goals, relationships or identity.[7] They influence all layers of society's life – economic, political, and social. On one hand, innovation can be expected to expand opportunities for people, help us live more fulfilling, healthier lives, as well as solve many global challenges. On the other hand, the voices of concern on complex issues of fundamental rights, ethics, equality of opportunities, access to resources, a greater sense of wellbeing in global context as well as existential risks are increasing in volume.[8] This moment in history is often addressed as "critical", "revolutionary", "chaotic", because technocratic transformation seems inevitable and out of human control.[9]

At the heart of transformative innovations is artificial intelligence (AI). In an open letter, which was already signed by more than 8000 scholars, leaders and experts, the Future of Life institute acknowledged that AI has already overstepped the threshold of being merely a laboratory research to an economically valuable technology. With the consensus that AI is progressing steadily, the letter argues that the impact on society is likely to increase prompting greater investments in research of the field. The letter calls for expanded research to reap the benefits of

[4] World Economic Forum, "Values, Ethics and Innovation: Rethinking Technological Development in the Fourth Industrial Revolution" // https://www.weforum.org/whitepapers/values-ethics-and-innovation-rethinking-technological-development-in-the-fourth-industrial-revolution/.
[5] David C. Vladeck, "Machines without principals: liability rules and artificial intelligence," *Washington Law Review* Vol. 89, No. 1 (2014): 2.
[6] *Ibid*.: 120.
[7] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015); Rathenau Instituut, "Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence and virtual and augmented reality" // https://www.rathenau.nl/en/digital-society/human-rights-robot-age.
[8] Future of Life Institute, "An Open Letter: Research priorities for robust and beneficial artificial intelligence" // https://futureoflife.org/ai-open-letter/.
[9] Alexander Bard and Jan Söderqvist, *Syntheism: Creating God in the Internet Age* (Stockholm: Stockholm text, 2014); World Economic Forum, *supra* note 4.

AI while avoiding potential pitfalls.[10] McKinsey global institute predicts that AI could potentially deliver additional global economic activity of around $13 trillion by 2030, which would amount to about 16 percent higher cumulative GDP compared with today.[11] From autonomous vehicles to self-learning personal assistants, the application scenarios are overwhelmingly vast, but so are the possible ethical, societal, and legal implications. AI gives rise to questions about how to ensure safety and security of interconnected autonomous devices, about who is responsible for damages caused by an autonomous device, about how laws and institutions should be redesigned to deal with this technology, and about which values autonomous systems should serve.[12]

Another great example of highly influential innovations is the drone. The military counterparts of drones have been used for almost a century,[13] whereas smaller, consumer drones have only emerged recently as their components became cost-effective to mass-produce. Consulting group PricewaterhouseCoopers LLP estimates that drone powered solutions will replace 127 billion dollars' worth of global business and labour in by the year 2020.[14] New ways to apply drones to our everyday lives seem to appear daily. In the commercial sector drones are already used to take "jaw dropping" pictures from above by photographers and journalists,[15] to create 3D maps for construction,[16] to spray crops and monitor livestock in agriculture,[17] and to deliver goods to stranded locations.[18] Consumers are using drones for racing,[19] and capturing travel videos or simply as toys for

[10] Future of Life Institute, *supra* note 8; Stuart Russell, Daniel Dewey, and Max Tegmark, "Research Priorities for Robust and Beneficial Artificial Intelligence," *Ai Magazine* Vol. 36, No. 4 (2015).
[11] Michael Chui, et al., "Sizing the Potential Value of AI and Advanced Analytics," *McKinsey and Company* (April, 2018) // https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-applications-and-value-of-deep-learning.
[12] European Commission, European Group on Ethics in Science and New Technologies, "Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems," B-1049, Brussels (2018) // http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf.
[13] Katharine Hall Kindervater, "The Emergence of Lethal Surveillance: Watching and Killing in the History of Drone Technology," *Security Dialogue* Vol. 47, No. 3 (2016) // https://doi.org/10.1177/0967010615616011.
[14] Patrick Cairns, "World Drone Market Seen Nearing $127bn in 2020, PwC Says," *Moneyweb* (May 9, 2016) // https://www.moneyweb.co.za/news/tech/world-drone-market-seen-nearing-127bn-2020-pwc-says; "Clarity from above. PwC global report on the commercial applications of drone technology," *PricewaterhouseCoopers* (May 2016) // https://www.pwc.pl/pl/pdf/clarity-from-above-pwc.pdf.
[15] Will Coldwell, "High Times: Why Drone Photography Offers a Different View of Travel," *The Guardian* (June 17, 2016) // http://www.theguardian.com/travel/2016/jun/17/why-drone-photography-offers-a-different-view-of-travel.
[16] "DroneDeploy is a company that builds cloud-based software for drone mapping, making it possible to create aerial maps and 3D models with a single click. DroneDeploy's software automates drone flight and makes it easy to capture aerial data with a mobile app"; more at: Amit Chowdhry, "The Story Behind DroneDeploy And How It Built The Largest Drone Mapping Repository," *Forbes* (July 16, 2017) // https://www.forbes.com/sites/amitchowdhry/2017/10/16/dronedeploy/.
[17] Caspar van Vark, "How Drones Can Detect Crop Problems Early to Keep Farmers on Track," *The Guardian* (December 26, 2015) // http://www.theguardian.com/global-development/2015/dec/26/drones-farming-crop-problems-uavs.
[18] Sara Salinas, "Biggest Delivery Breakthrough since Amazon Prime," *CNBC* (May 22, 2018) // https://www.cnbc.com/2018/05/22/biggest-delivery-breakthrough-since-amazon-prime.html.
[19] Ian Frazier, "The Trippy, High-Speed World of Drone Racing," *The New Yorker* (January 29, 2018) //

children. Governments are known to use drones for military purposes, search and rescue operations or crime prevention. As drone technology is further developed, they may be used as modes of transportation,[20] antennas to extend cellular networks[21] or as super weapons.[22] However, together with potential benefits also come implications. Photo-capable flying robots may have negative effects on multiple dimensions of individual privacy, high congestion in the low altitude airspace may lead to problems with airspace ownership, extending drone autonomy with high-tech sensors and advanced artificial intelligence software may lead to security and liability issues.

The third ground-breaking technology analysed in this paper is blockchain. The popularity and applicability of distributed ledger technologies, broadly referred to as blockchains, has risen significantly in the past few years.[23] Even though at present the most famous way to use this technology is for decentralized cryptocurrencies, such as Bitcoin or Ethereum, it has various other applications that have the potential to redesign digital business altogether. For example, it can be used for smart contracts, real-estate title transfers, protection of intellectual property, supply chain auditing, identity management, governance (elections, poll taking, electronic government), direct interaction between parties in sharing economy, crowdfunding and venture capital funds, and stock trading.[24] However, blockchain technology also comes with a set of legal issues. Since blockchain-based transactions are difficult to trace, it can cause liability governance issues. The immutability of distributed ledger technologies poses dangers to privacy, data protection and consumer protection. Other key implications include the legal enforceability of smart contracts, and the legal status of Decentralized Autonomous Organizations (DAOs) as entities. [25]

Transformative innovations may lead our lives to "chaos", if we fail to find adequate measures to frame them.[26] One of these measures is legal regulation.

---

https://www.newyorker.com/magazine/2018/02/05/the-trippy-high-speed-world-of-drone-racing.
[20] Jane Wakefield, "Dubai Tests Drone Taxi Service," *BBC News* (September 26, 2017) // https://www.bbc.com/news/technology-41399406.
[21] Ludovico Ferranti, et al., "Drone Cellular Networks: Enhancing the Quality Of Experience of Video Streaming Applications," *Ad Hoc Networks* 78 (2018) // https://doi.org/10.1016/j.adhoc.2018.05.003.
[22] Alexis C. Madrigal, "Drone Swarms Are Going to Be Terrifying and Hard to Stop," *The Atlantic* (March 7, 2018) // https://www.theatlantic.com/technology/archive/2018/03/drone-swarms-are-going-to-be-terrifying/555005/.
[23] "Size of the blockchain technology market worldwide from 2018 to 2023 (in billion U.S. dollars)" *Statista* // https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/.
[24] The Law Society, "Blockchain: The legal implications of distributed systems" (August 1, 2017) // https://www.lawsociety.org.uk/support-services/research-trends/horizon-scanning/blockchain/.
[25] Philip Boucher, et al., *How Blockchain Technology Could Change Our Lives: In-Depth Analysis* (2017), 22 // http://bookshop.europa.eu/uri?target=EUB:NOTICE:QA0217043:EN:HTML; The Law Society, *supra* note 24.
[26] Rathenau Instituut, *supra* note 7; Patrick Lin, Keith Abney, and George A. Bekey, eds., *Robot Ethics: The Ethical and Social Implications of Robotics* (Cambridge, Mass: MIT Press, 2012), 183.

2. IMPLICATIONS OF TRANSFORMATIVE ECONOMIC INNOVATIONS: CASE ANALYSIS

2.1. CASE ANALYSIS: ARTIFICIAL INTELLIGENCE[27]

Transformative innovations are increasingly based on artificial intelligence (AI) technology, with human-like skills such as learning, speech recognition, automated reasoning, sensing, interaction, problem solving or creativity[28]. One of the first technologies to put legal regulation to the test is autonomous vehicles. In many aspects autonomous vehicles are better at performing precarious activities that are currently performed by man (such as driving), because machines never fall asleep, they never drive drunk, get distracted by a text message or conversation, they never drink coffee or eat, they do not get angry or drowsy. Bearing in mind these human deficiencies, it would be no surprise if the massive introduction of autonomous vehicles considerably lessened the rate of accidents.[29] In a world where driverless cars or drones will have the capacity to „sense-think-act„ at their own will and plan[30], the legal system will, first of all, have to address the liability issues[31] of autonomously[32] thinking machines.

In this regard, a distinction between deterministic and cognitive devices is important. Both deterministic and cognitive devices perform their tasks through algorithms;[33] however, the difference between the two types is that the first do not have the ability to learn and are predictable, whereas the latter have learning capabilities which make their behaviour stochastic (random).[34] AI technology uses cognitive algorithms which are not merely programmed to perform specific tasks, but also to learn and further develop themselves in interaction with their environment. Given the complexity of the design, construction and programming of

[27] Artificial intelligence is defined as "a discipline concerned with the building of computer programs, that perform tasks requiring intelligence when done by human", for example, Andrew Butterfield and Gerard Ekembe Ngondi, eds., *A Dictionary of Computer Science*, 7th edition (Oxford University Press, 2016), 26.
[28] United Nations Educational, Scientific and Cultural Organization, "Robotics Ethics": 4 // http://www.unesco.org/new/en/social-and-human-sciences/themes/comest/robotics-ethics/.
[29] David C. Vladeck, *supra* note 5: 126.
[30] *Ibid*.: 122.
[31] Lawrence B. Solum, "Legal personhood for artificial intelligences," *NCL Review* Vol. 70: 1231; *Civil Law Rules on Robotics: European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))*, European Union: European Parliament, 2017.
[32] Autonomy is defined as "the capacity to operate in the real-world environment without any form of external control, once the machine is activated and at least in some areas of operation, for extended periods of time" (George A. Bekey, "Current trends in robotics: technology and ethics"; in: *Robot ethics: the ethical and social implications of robotics* (Cambridge: The MIT Press, 2012); Patrick Lin, Keith Abney, and George A. Bekey, *supra* note 26, 18; *Civil Law Rules on Robotics*, *supra* note 31.
[33] An algorithm is defined as "a prescribed set of well-defined rules or instructions for the solution of a problem, such as the performance of a calculation, in a finite number of steps" (Andrew Butterfield and Gerard Ekembe Ngondi, *supra* note 27, 16).
[34] United Nations Educational, Scientific and Cultural Organization, *supra* note 28: 4, 7.

AI devices, a central legal issue will be the possibility to track the reasons of all past actions (and omissions).[35] This is ethically and legally crucial because "a robot's decision paths must be re-constructible for the purposes of litigation and dispute resolution."[36]

Notions of clarity, traceability and transparency that are usually associated with traditional views of mathematics and technology will only work well with deterministic algorithms, whereas cognitive algorithms will be far from clear and might be difficult to trace. This would lead to epistemically opaque[37] machines the decisions of which would not only be unpredictable, but also hard to trace. Moreover, cognitive technologies also have the ability to learn from past human experiences and calibrate their algorithms themselves. It means they will also learn from materials that are indeed full of typical human moral imperfections, such as partiality, selfishness, emotional bias or prejudice, weakness of will and so on. Hence, there is obvious tension between the 'traceability' requirement (considering the problem of epistemic opacity) and the development of robots with a high level of autonomy in decision-making and advanced learning capabilities. On the other hand, this legal limitation is unlikely to have a significant impact on the further development of cognitive devices, since their ability to outperform humans in various tasks will most likely outweigh their detriments.

Where human involvement in decision-making of AI is obvious, there is no need to re-examine legal regulation.[38] The companies that currently manufacture devices with AI are already subject to a well-developed doctrine of product liability.[39] So, all harms potentially caused by AI technologies are treated the same way as with any other technological product (e.g. toys, cars or weapons). As a matter of fact, most accidents occur due to inevitable errors in design, programming and production of such machines. Because of this, possible failures are usually categorized into design defects, manufacturing defects, information defects and failures to instruct.[40]

---

[35] David C. Vladeck, *supra* note 5: 141–43; United Nations Educational, Scientific and Cultural Organization, *supra* note 28: 6-7.
[36] Laurel Riek and Don Howard, "A code of ethics for the human-robot interaction profession," *Proceedings of We Robot* (2014): 6.
[37] Epistemically opaque machines are said to represent a black box, the internal functioning of which cannot be fully elucidated, whose decisions are unpredictable and untraceable (Julian Newman, "Epistemic Opacity, Confirmation Holism and Technical Debt: Computer Simulation in the Light of Empirical Software Engineering"; in: Fabio Gadducci and Mirko Tavosanis, eds., *History and Philosophy of Computing, Vol. 487* (Springer International Publishing, 2016) // https://doi.org/10.1007/978-3-319-47286-7_18.
[38] David C. Vladeck, *supra* note 5: 120.
[39] Peter M. Asaro, "A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics": 169; in: *Robot ethics: The ethical and social implications of robotics* (Cambridge: The MIT Press, 2012).
[40] David C. Vladeck, *supra* note 5: 127–141; *Civil Law Rules on Robotics*, *supra* note 31.

However, researchers argue that the already existent product liability legal framework is likely to become inadequate as commercially available AI machines become more sophisticated and autonomous, eventually blurring the lines between responsibilities of manufacturers and responsibilities of users.[41] For example, if a manufacturer offered different versions of AI algorithms, and a buyer knowingly chose one of them, is the buyer to blame for the harmful consequences of the algorithm's decisions? In this regard, it would be difficult to hold the manufacturer responsible for any creative, even if dangerous, uses of their products. Cars and weapons are also very dangerous consumer products, but users still tend to be liable for most of the harms they have caused, because the use of those potentially dangerous products place an additional burden of responsibility on the user.[42] Hence, the increasing autonomy of smart devices poses an additional question: who exactly should bear ethical and/or legal responsibility for the behaviour of cognitive (with learning abilities) machines. Currently, there typically seems to be a 'shared' or 'distributed' responsibility between robot designers, engineers, programmers, manufacturers, investors, sellers and users, because none of these agents can be indicated as the ultimate source of action.[43] Scholars argue that this solution tends to dilute the notion of responsibility altogether: if everybody has a part in the total responsibility, no one is fully responsible.[44] On the other hand, most European jurisdictions already have rules providing that damage caused by the concurrent actions of several tortfeasors as a consequence generally result in collective liability. A tortfeasor can also be liable individually for the whole damage through the concept of "joint and several" liability or solidary liability. This concept prevents actors that have contributed to the damage from avoiding liability and complex accidents from fractioning, in this sense, offering better protection for the victim.[45]

Further analysing AI liability, another important question is related to standard of care. Normally, the professional standard of care is higher when a certain activity is dangerous. Danger is often measured by the probability of occurrence and the gravity of harm, which, in other words, means that the greater the danger, the higher degree of care. Danger is also usually the source of strict liability regulatory regime in many legal systems or at least more strict liability based for example on the reversal of the normally set burden of proof. On the other hand, should we, in terms of product liability rules, apply a lower standard of care

[41] Peter M. Asaro, *supra* note 39:174; *Civil Law Rules on Robotics*, *supra* note 31.
[42] Peter M. Asaro, *supra* note 39: 170–74.
[43] United Nations Educational, Scientific and Cultural Organization, *supra* note 28: 4.42.
[44] *Ibid*: 4.
[45] Bénédict Winiger, Håkan Andersson, and Österreichische Akademie der Wissenschaften, eds., "Essential Cases on Natural Causation": 344-352; in: Digest of European Tort Law, Vol. 1 (Springer International Publishing, 2007).

for autonomously thinking machines just because we expect them to be so technologically advanced that they should fail much less than humans?[46] If we move towards this approach, modern devices would be expected to be much more effective in discovering danger before it manifests than humans. In an unexpected event, for example, a child darting in front of a moving vehicle, a tree limb unexpectedly crashing down on the road ahead, or other traffic participants breaking traffic laws and creating pre-accidental driving situations, cognitive machines would be expected to react at speeds humans cannot match.[47]

In this context, one more issue discussed by scholars is: why should we apply a strict liability regime in AI cases if cognitive devices are likely to be less dangerous than the products they replace? Strict liability rules are an exemption to the fault-based liability regime. They are based on risk theory, i.e. the notion that the activity or device being used is dangerous. Some scholars argue that applying this theory on cognitive devices might be problematic because they are likely to be far less hazardous or risky than the products they replace.[48] However, others argue that there are strong policy reasons to establish an insurance based[49] strict liability regime for cases related to intelligent devices. One reason is the already discussed traceability and opacity problem. The injured person should not bear the loss when causal failure is hardly explicable.[50] Also, as "complexity of such products rises geometrically, the cost of litigating products liability cases would increase exponentially,"[51] strict liability regime would then spare enormous transaction costs, that is, if parties decided to litigate. The second logic suggests that, according to insurance-based theory, the manufacturers are in a better economic position to absorb the costs of loss through pricing decisions, spreading the burden of loss. These arguments conform to the notions of compensatory justice and apportionment of risk in society.[52] Also, a predictable liability regime like this would spur innovation much better than an "uncertain fault-based liability system."[53]

Eventually, in spite of how sophisticated and autonomous in decision making an AI machine is, even if it is capable of independent initiative and plans, some scholars suggest that it is still an instrument of other entities and has no attributed legal personhood.[54] Therefore, the conceptual legal question that autonomously thinking machines pose is whether it is fair to think of them as a tool. The question

[46] David C. Vladeck, *supra* note 5: 131–41.
[47] *Ibid.:* 131–41.
[48] *Ibid.*: 146.
[49] Some legal liabilities cannot be met by insurance (Lawrence B. Solum, *supra* note 31: 1245).
[50] *Civil Law Rules on Robotics*, *supra* note 31.
[51] David C. Vladeck, *supra* note 5: 147.
[52] *Ibid.*: 146–48.
[53] *Ibid.*: 147.
[54] *Civil Law Rules on Robotics*, *supra* note 31; David C. Vladeck, *supra* note 5: 121.

of limited personhood attributed to artificial intelligence is currently broadly discussed in research[55] at least on a theoretical level.[56] The idea of an AI machines as an agent would perfectly match the above discussed insurance based strict liability regime.[57]

The analysis shows that there should be a correlation between AI level of autonomy and applied liability regime. In case of deterministic AI devices with no or only basic level of autonomy, the applied liability regime is strict, based on well-known product liability doctrine. In case of cognitive AI devices with high level of autonomy, the applied liability regime is strict too, but the novel regulation of limited personhood based on insurance should be considered. The correlation between AI level of autonomy and possible liability regime is presented in Figure 1.

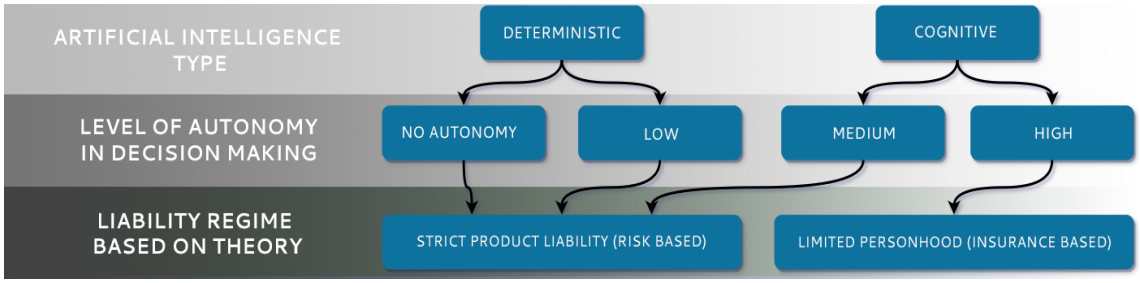

Figure 1: Correlation between level of AI autonomy and liability regime

2.2. CASE ANALYSIS: DRONES

The emergence and surprising popularity of drones have not only triggered major investment by companies but also discussions among academics and public authorities regarding legal implications. Drones may have negative effects on public safety, individual privacy, property rights which eventually may lead to socio-economic problems.

One of the major concerns is public safety, which is a basic human right that provides protection from physical, social, or emotional harm. There have been reports of drones colliding with other aircraft[58] and numerous reports of near misses.[59] Some drones have crashed into people causing minor injuries.[60] Lethal

[55] *Ibid*.: 129; Peter M. Asaro, *supra* note 39: 169; Lawrence B. Solum, *supra* note 31.
[56] *Ibid*: 1231.
[57] David C. Vladeck, *supra* note 5.
[58] Jonathan Vanian, "Drone Smashes Into Army Helicopter," *Fortune* (December 14, 2017) // http://fortune.com/2017/12/14/drone-army-helicopter-smash; "Drone Collides with Commercial Aeroplane," *BBC News* (October 16, 2017) // https://www.bbc.co.uk/news/technology-41635518; "'Drone' Hits BA Plane near Heathrow," *BBC News* (April 17, 2016) // https://www.bbc.co.uk/news/uk-36067591.
[59] According to Australian Transport Safety bureau (ATSB) there have been 242 recorded drone related incidents in Australia between 2012 and 2017 most of which nearly collided with other aircraft

injury is obviously possible having in mind larger commercial drones; however, it has not yet happened in civilian contexts.

According to the European Aviation Safety Agency (EASA), the two main risks threatening this basic right are air risks (collision with a manned aircraft or other drones) and ground risks (collision with persons or critical infrastructure).[61] Harmful incidents can arise in a variety of different scenarios. Harm may be caused deliberately, for example, if the drone drops its payload to damage people or property or it may be sent on a "kamikaze" mission. Deliberate behaviour might be motivated by simply seeking thrill, revenge, aiding criminal or terrorist acts. Drones may also be hijacked through signal jamming, falsification of data-feed, interference with the control-feed, interference with software used by the drone pilot, or physical threat to the pilot.[62]

Dangers to public safety can also derive from poor reliability of internal components of the drone. As drone technology becomes cheaper, more drones may be used by unexperienced pilots and less safety-related features may be included in the drone.[63] Since component reliability is inseparably tied to the cost of the drone, one might argue that imposing major security thresholds by design might put unreasonably high burdens on the manufacturers and might interfere with further advancement of the technology. Harm may also occur because of failure of the user. Piloting a drone from the ground may involve long periods of boredom, interruptions and lapses in concentration[64] which may cause the drone to accidently crash into obstacles. Most contemporary consumer and commercial drones have sense and avoid capabilities that may reduce the risk of harm; however, bearing in mind quite frequent drone incidents, we can assume sense and avoid technology needs to be further developed to be reliable. Failure of the user may be avoided

(Australian Transport Safety Bureau, "A safety analysis of remotely piloted aircraft systems" (August 9, 2017) // https://www.atsb.gov.au/publications/2017/ar-2017-016/).

[60] Vanessa Ogle, "Drone Strike! Our Photographer Injured by TGI Friday's Mistletoe Copter," *Brooklyn Daily* (July 4, 2018) // https://www.brooklyndaily.com/stories/2014/50/bn-drone-disaster-at-tgifridays-2014-12-12-bk_2014_50.html; "Athlete Injured after Drone Crash," *BBC News* (April 7, 2014) // https://www.bbc.co.uk/news/technology-26921504; "Drone Crashes into Virginia Bull Run Crowd," Washington Post // https://www.washingtonpost.com/local/drone-crashes-into-virginia-bull-run-crowd/2013/08/26/424e0b9e-0e00-11e3-85b6-d27422650fd5_story.html; Kate Pickles, "Toddler, 18 Months, Left Blind in One Eye by Drone Propeller," *Mail Online* (November 27, 2015) // http://www.dailymail.co.uk/health/article-3336366/Horrific-picture-shows-toddler-left-blind-one-eye-drone-propeller-sliced-eyeball-half.html.

[61] European Aviation Safety Agency, "Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories" (2018) // https://www.easa.europa.eu/sites/default/files/dfu/Introduction%20of%20a%20regulatory%20framework%20for%20the%20operation%20of%20unmanned%20aircraft.pdf.

[62] Roger Clarke and Lyria Bennett Moses, "The Regulation of Civilian Drones' Impacts on Public Safety," *Computer Law & Security Review* Vol. 30, No. 3 (June 1, 2014) // https://doi.org/10.1016/j.clsr.2014.03.007.

[63] *Ibid.*

[64] *Ibid.*

entirely if fully autonomous control of the drone is developed. However, increasing levels of autonomy might cause other safety issues.[65]

Another major concern is privacy. Most drones carry on-board video cameras that are able to capture images of superior quality, some are equipped with sensors that can help avoid obstacles, others have the ability to autonomously follow a person around, the higher-end drones even have advanced facial recognition capabilities. With such extensive technological surveillance capabilities, relative invisibility and silent flight of drones, it is no surprise that individuals might feel like they are being constantly under surveillance.[66] There are different dimensions of privacy that might be infringed by drone use. In the light of emerging technologies Rachel Finn and David Wright identify seven dimensions of privacy and argue that drones raise issues for at least four: "privacy of behavior and action, privacy of data and image, privacy of location and space and privacy of association."[67] Drone impacts on behavioral privacy may alter the way individuals behave in society. As more and more drones with surveillance capabilities are taking to the skies, everyone can expect to be constantly watched, regardless of whether they behave suspiciously or not. Overt surveillance, which is commonly exercised by CCTV cameras, discourages individuals from bad behavior, whereas covert surveillance, which may be exercised by using drones, may cause individuals to fear that they are under observation at any time. This, in turn, may result in a form of self-discipline called the "chilling effect" and may cause "the stultification of freedoms of expression and of innovation."[68] Drones can be used collect large volumes of image data which, as data storage becomes cheaper, can be stored indefinitely. In the near future, Big Data software and artificial-intelligence technologies could be used to aggregate large volumes of stored data and to create behavioral patterns of individuals. This could enable large corporations that can afford to buy such data to abuse their dominant position in the market by foreseeing the behavior of customers and rival companies. Because most of this data will be gathered covertly, even more troubling is the fact that the identity of drone operators may be hard to

[65] A study of accident data of a military drone called "Global Hawk" found that higher levels of drone autonomy lead to more errors in mission planning (Kevin W. Williams, *A summary of unmanned aircraft accident/incident data: Human factors implications*, No. DOT/FAA/AM-04/24, Federal Aviation Administration (Oklahoma City, OK: Civil Aeromedical Inst, 2004).

[66] Rachel L. Finn and David Wright, "Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications," *Computer Law & Security Review* Vol. 28, No. 2 (April 1, 2012) // https://doi.org/10.1016/j.clsr.2012.01.005.

[67] Seven types of privacy identified in the research are: 1) privacy of the person, 2) privacy of behavior and action, 3) privacy of communication, 4) privacy of data and image, 5) privacy of thought and feelings, 6) privacy of location and space and 7) privacy of association (Rachel L. Finn, David Wright, and Michael Friedewald, "Seven Types of Privacy"; in: Serge Gutwirth, et al., eds., *European Data Protection: Coming of Age* (Springer International Publishing, 2013) // https://doi.org/10.1007/978-94-007-5170-5_1).

[68] Roger Clarke, "The Regulation of Civilian Drones' Impacts on Behavioural Privacy," *Computer Law & Security Review* Vol. 30, No. 3 (June 1, 2014) // https://doi.org/10.1016/j.clsr.2014.03.005.

determine, which leads to a limited possibility for individuals to exercise data protection principles contained in the General Data Protection Regulation (GDPR), such as transparency, consent and right of access.[69] Privacy of location and space can also be infringed upon by using drones to transmit images of people's activities within homes, enclosed backyards, they may be used to track the movement of private vehicles.[70] Whereas privacy of association may be undermined by using drones to gather and analyze information about groups and organizations of individuals. Combining drone-gathered information with facial-recognition software would allow for the identification of people's affiliation with certain groups or organizations, could be used to predict meeting locations and schedules.[71]

Property is another basic human right directly infringed upon by drone use. Drones usually operate in the lower altitude airspace – an area just above the surface of the earth. This area is quite ambiguous since it is governed both by aviation law and property law. Aviation law regulates lower altitude airspace from "above", whereas property law regulates it from "below". Aviation law is grounded on the fundamental right of safety, while property law is a fundamental right by and of itself. The most sensitive part of lower altitude airspace, where drones use can be most intrusive, is in the closest reaches of the earth which are governed by property law. The classic scenario of intrusion is drone flights over private land and other real property, and a rather simple question to ask is: has the drone operator violated the property rights of the property owner? The answer would be: possibly, but proving a violation would be quite difficult since boundaries of lower airspace property belonging to a real estate owner are not as clearly defined as land plot boundaries. In other words, neither the real estate owner, nor the drone operator know precisely at what altitude the drone may fly to avoid intrusion. Until now property disputes in the low altitude airspace have been resolved on an *ad hoc* basis, which means that in every case the court would have to determine that the intrusion was "so immediate and direct as to subtract from the owner's full enjoyment of the property and to limit his exploitation of it."[72] This might have been a sound system when lower altitude airspace was practically empty, but it will gradually become too arduous to employ as our skies become congested with drones and more disputes emerge.[73] Evidently, a new system to govern property relations in the lower altitude airspace is required. To date, there are already technological solutions to the property dilemma of lower altitude airspace and

[69] Rachel L. Finn, David Wright, and Michael Friedewald, *supra* note 67.
[70] *Ibid.*
[71] *Ibid.*
[72] *United States v. Causby*, 328 U.S. 256 (1946) // https://supreme.justia.com/cases/federal/us/328/256/.
[73] Troy A. Rule, "Airspace in an Age of Drones," *Boston University Law Review* Vol. 95 (2015).

drones, one of which is the Geo-fencing technology.[74] However, it will not work for protection of property rights until a clear regulatory framework for lower altitude airspace is established.

European Commission has accurately observed in its opinion that the drone market can rapidly develop once an enabling policy framework is adopted.[75] For example, as the opinion suggests:

> The number of Japanese RPAS operators was multiplied by 18 to about 14,000 between 1993 to 2005, with a spectacular increase after the entry into force of regulations on agricultural use. In France an initial regulation has led to an increase of the number of approved operators from 86 in December 2012 to more than 400 in February 2014. Similar market growth and related job creation has been seen in Sweden and the UK.

Sadly, lack of proper regulation (and enforcement) remains one of the two major limitations for the rapid adoption of drones, the second limitation being short battery life.[76]

It would be hard to argue that state actors are lacking effort to regulate drone use. Discussions about drones in the European Union (EU) started as early as 2002 and full integration of drones into civil airspace is predicted to be finished by 2028.[77] The European Commission published a strategy in 2014 by which it committed to take regulatory action dealing with all relevant issues, including the insertion of safety, security, privacy and data protection requirements within existing EU rules in these areas.[78] By now, the European Aviation Safety Agency has already published draft rules that deal primarily with the safety of drone use.[79] The United States (US) has also started drone regulation initiatives in 2012 with the FAA Modernization and Reform Act[80] primarily focused on safe integration of drones in the national airspace. At the international level the International Civil Aviation Organisation (ICAO) has published two key publications: the ICAO RPAS Guidance Manual and ICAO Circular 328 on Unmanned Aircraft Systems which provide basic guidance material of basic procedures for operating remote controlled drones. ICAO

[74] The main idea behind Geo-fencing is to pre-program locations where drone use is prohibited into the software of the drone, thereby drawing virtual boundaries that the drone could not cross by default.
[75] European Commission, "Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner," Communication, Brussels (2014) // https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0207.
[76] Bharat Rao, Ashwin Goutham Gopi, and Romana Maione, "The Societal Impact of Commercial Drones," *Technology in Society* Vol. 45 (May 2016) // https://doi.org/10.1016/j.techsoc.2016.02.009.
[77] Ben Hayes, Chris Jones, and Eric Töpfer, *EURODRONES Inc.* (Transnational Institute and Statewatch, 2014) // https://www.statewatch.org/news/2014/feb/sw-tni-eurodrones-inc-feb-2014.pdf.
[78] European Commission, *supra* note 75.
[79] European Aviation Safety Agency, *supra* note 61.
[80] John L. Mica, "Text - H.R.658 - 112th Congress (2011-2012): FAA Modernization and Reform Act of 2012" (February 14, 2012) // https://www.congress.gov/bill/112th-congress/house-bill/658/text.

expects that there will be "global readiness" for the widespread use of drones by 2028.[81]

While legislative solutions to drone related legal implications still seem to be in the discussion phase, the drone industry is encouraged to regulate itself. For example, since 2015 the EU has started funding the development of a web portal which facilitates public access to relevant regulations, requirements and procedures.[82] It successfully publishes up-to-date information about national regulatory profiles of EU member states, provides comprehensible handbooks and case studies that convey the most important legal implications and the best ways to avoid them.[83]

Nevertheless, although first steps in the right direction have already been taken, they are very small steps considering the current growth rate of the drone industry. Current legislation may address the arising issues of drone use to some extent but it could only probably be a temporary solution. It would be naïve to expect the whole drone industry to regulate itself bearing in mind the considerable extent of new issues drones use is creating to safety, privacy or property. It is safe to say that current developments in drone legislation still seems to be lagging behind the economic and technological developments of the industry.

2.3. CASE ANALYSIS: BLOCKCHAINS

Blockchain technology is not revolutionary or ground-breaking by itself and is more like an integral or updated part of a distributed peer-to-peer system.[84] It serves as a tool to solve a core problem of software systems, which have struggled to achieve and maintain the integrity of a purely distributed peer-to-peer system that consists of an unknown reliability and trustworthiness.[85] This has been particularly hard to achieve because in order for a distributed peer-to-peer network to work without a centralized authority, it must have consensus upon every message transmitted. Before blockchain, a scattered group of random individuals did not have a way to confirm that a particular event had occurred if it had not been verified by a central authority.

---

[81] Ben Hayes, Chris Jones, and Eric Töpfer, *supra* note 77.
[82] *COS-RPAS-2014-2-03: Facilitating Access to Regulation for Light Remotely Piloted Aircraft Systems (RPAS)*, EASME: European Commission //https://ec.europa.eu/easme/en/cos-rpas-2014-2-03-facilitating-access-regulation-light-remotely-piloted-aircraft-systems-rpas.
[83] "Drone Rules" // http://dronerules.eu/en/#modal-disclaimer.
[84] P2P is a network where computer systems are connected to each other via the internet and files can be shared directly between systems on the network without the need of a central server (Quang Hieu Vu, Mihai Lupu, and Beng Chin Ooi, "Architecture of Peer-to-Peer Systems"; in: *Peer-to-Peer Computing* (Springer, 2010)).
[85] Nicolas Kube, *Daniel Drescher: Blockchain Basics: A Non-Technical Introduction in 25 Steps* (Springer International Publishing, 2018), 31.

Technically speaking, blockchain is simply a data structure where each block is linked to another block. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work,[86] forming a record that cannot be changed without redoing the proof-of-work.[87] It basically suggests that data stored in blockchain is immutable, because in order to access data of the oldest block, one must go through all of them from the newest one, until the first block is reached. Performing this task in order to change any data contained in the blocks becomes almost impossible, because all stored data is encrypted using cryptography techniques and each time a new node is added, it has to download the entire ledger and synchronize with the network. Software developers have already realized the potential of blockchain technology and have started to use it to create digital currencies, self-executing smart contracts, as well as cryptographic tokens that can represent property or ownership interest in emerging services. It is also being used to create censorship-resistant communications and file sharing systems, decentralized domain name management systems (DNS) and fraud-resistant digital voting platforms.[88] Due to vast applicability, various types of blockchains constantly arise: payment processing and currency, supply chain management, asset protection, identification, personal record systems and passwords.[89]

There are two central features of blockchain technology that make it exclusive: the system can be completely decentralized and the data contained in blocks can become immutable. These features also prove to represent the greatest challenge in terms of data protection under the General Data Protection Regulation (GDPR). The fundamental idea of GDPR is to provide data subjects with the ability to control their personal data, allowing them to freely access and erase any unwanted records. Exercising these rights relies entirely on central authorities who are controllers of data. Public blockchain technology, on the other hand, may store data in its databases perpetually, which means that once data is stored into a distributed ledger system, it cannot be deleted. From a data security point of view, it could be seen as an advantage due to the inability to change data after it was stored and prevent double spending.[90] Yet, a huge disadvantage could be seen from the privacy perspective. European data privacy laws seek to give data

[86] This mechanism specifies as compulsory for computers on the network to solve computationally-intensive mathematical puzzles.
[87] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" // http://bitcoin.org/bitcoin.pdf.
[88] Aaron Wright and Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (2015): 8 // Available at SSRN 2580664.
[89] I.e. Shocard, Onename, Everledger.
[90] Double spending problem is a risk that digital currency can be spent twice. This is possible because a digital token consists of a digital file that can be duplicated or falsified (Meni Rosenfeld, "Analysis of Hashrate-Based Double Spending," *ArXiv Preprint ArXiv:1402.2009* (2014)).

subjects better control over their personal data, whereas public blockchain technology, restricting future access to the data stored in a ledger, achieves the complete opposite of the European vision. Moreover, public blockchains have no central authority that can be held accountable for inadequate use or storage of personal data, which also contradicts data privacy laws of the European Union. Analysing GDPR articles regarding data controllers,[91] every node could be considered a data controller as they can freely join a public blockchain and seek objectives of their own. However, nodes themselves only have an uninvolved scenario: they cannot change anything in a block, neither can they see clear information of other nodes.[92] On the other hand, only public blockchain technology contradicts the principles of data protection of the EU, whereas private blockchains are still based on the idea of central oversight and can have central operators that would be held accountable under the GDPR.

In light of the innovative technology of public blockchain, it seems that GDPR may have become outdated the second it came into force. GDPR is built around data controllers and their ability to oversee and manage how personal data is processed, while public blockchain takes a completely opposite approach to that of the GDPR – it relies upon a decentralized governance model, which prevents any interference through central controllers. With vast amounts of various personal information stored publicly and indefinitely, problematic situations are sure to arise. For example, it is likely that an individual at some point in time may want to withdraw his consent or to delete his personal information stored on a public blockchain.[93] Also, there may be situations where the purpose of processing data ceases to exit (if processing cannot be based on another legal ground).[94] The economic cost of erasing must be considered too, since changing or deleting data in a chain requires significant resources. Consequently, blockchain technology may have become a victim of its own innovation regarding GDPR.

Currently, neither the European Union nor the United States has legislation or clear guidelines towards data protection regarding blockchain. Lack of legislation creates not only legal uncertainties, but also a privacy risk regarding personal data. The present situation is similar to the emergence of the internet – it took

[91] Regulation 679/16 defines controller as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
[92] Michèle Finck, "Blockchains and Data Protection in the European Union," *Eur. Data Prot. L. Rev.* Vol. 4 (2018): 30.
[93] Satoshi Nakamoto, *supra* note 87: 26.
[94] Paul Voigt and Axel Von dem Bussche, *The EU General Data Protection Regulation (GDPR): Practical Guide*, 1st ed. (Springer International Publishing, 2017), 157.

approximately two decades for people and regulators to understand that putting a vast amount of personal data (in most cases, without any particular reason) for everybody to see, without a mechanism to properly control/regulate, can induce serious negative effects on our daily lives, as Cambridge Analytica has shown. Even though the United States recognizes a signature secured through blockchain technology as an electronic signature and even the validity of blockchain records and their admissibility in courts as evidence without the need for authentication, questions about data privacy remain open across the world. Such questions are: can people who use public blockchain (for example, Bitcoin) exercise rights granted by GDPR? If so, who should be held liable for breaches of these rights (or who is the data controller of such platform)? Moreover, if they fail to comply with GDPR, fines for data controllers are calculated on the basis of the total worldwide annual turnover of the preceding financial year, but given the model public blockchains are based on, with thousands of individual nodes, it seems that the current calculation method would not work. In spite of all these already prominent issues, the European Data Protection Board, which is an independent European body that contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the data protection authorities of the union, remains silent.

Another noteworthy implication that emerges through blockchain is the existence of Decentralized Autonomous Organizations (DAOs). A DAO is an organization that functions through rules encoded as computer programs called "smart contracts."[95] Instead of a traditional organization structure managed by a set of humans interacting in person and controlling property via the legal system, in DAOs management and control are automated according to protocols specified in code and enforced on the blockchain. In other words, DAOs are based on self-governing software that lives on the internet and exists autonomously (humans are not involved) with the benefits, but without the inflexibility of formal corporate structures (instead of concentrating decision-making at the executive level, shareholders of DAOs can participate in decision-making by decentralized voting). By removing centralized management, DAOs could eliminate the errors and corruption introduced by humans and bring new forms of democratic collective action, transforming top-down governance approaches that are criticized for their inflexibility, opacity, slowness and democratic deficit.[96] A well-known example,

[95] Usman W. Chohan, "The Decentralized Autonomous Organization and Governance Issues" (2017): 1 // Available at SSRN 3082055.
[96] Philip Boucher, et al., *supra* note 25, 21–22.

intended for venture capital funding, was THE DAO, which launched with $150 million in crowdfunding in June 2016, and was immediately hacked and drained.[97]

Just as regular legal entities, DAOs could engage in commerce, therefore not only legal problems with damages and/or losses can occur (who should be responsible if the organization is operated autonomously), but also traditional notions of legal personality could be challenged. As opposed to traditional corporations or organizations, DAOs are neither owned, nor controlled by any single corporate or governmental agency, nor any individual person. Yet they can interact with the public in a way that might give rise to specific rights and obligations. Decentralized organizations can thus have a significant effect on third parties, and might even be at the source of certain torts or wrongdoings.[98] There are opinions that the aforementioned problems could be mitigated by adopting the nearest person principle with the given example of autonomous vehicle (manufacturer of an autonomous vehicle would be held liable should any sort of damages occur)[99] but only if creators of DAOs are known. However, if DAOs are created by other DAOs or anonymous persons, this principle would not suffice. Either way, creating functionally working DAOs is no easy task. Directly embedding legal rules into codes of DAOs should be well thought through before launching such organisations to avoid legal uncertainty, possible disputes, or ineffective management. Traditional "dumb" contracts may still need to be signed in order for the involved parties to recognize from the beginning how a particular DAO will operate. Therefore, close cooperation between business people, lawyers, and programmers will be inevitable.

IN LIEU OF CONCLUSIONS: MAPPING PRIVATE LAW CHALLENGES

Analysis of cases shows that transformative innovations create a non-exhaustive list of interdependent challenges which are summarized in Figure 2. From the case analysis we can distinguish at least three fields of law that will suffer the strongest impact: privacy, liability and property.

Although the mapped challenges are based on the case analysis of only three innovations examined in this article, most of them would be applicable to other technologies as well. It is likely that the vast majority of emerging innovations will have at least some properties inherent to artificial intelligence, drones, or

[97] Samuel Falkon, "The Story of the DAO — Its History and Consequences," *Medium* (August 12, 2018) // https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.
[98] Satoshi Nakamoto, *supra* note 87: 26.
[99] Steve Tendon and Max Ganado, "Legal Personality for Blockchains, DAOs and Smart Contracts," *GANADO Advocates* (June 4, 2018): 4 // https://ganadoadvocates.com/resources/publications/legal-personality-for-blockchains-daos-and-smart-contracts/.

blockchains; therefore, their analysis seemingly addresses a lot of the legal implications that other technologies might entail.[100]

For example, artificial intelligence might drastically improve every smart device that we use in our day to day lives, enabling robotic vacuum cleaners, personal assistants, smart thermostats, driverless cars, personal drones and many others to learn and function on their own; it might be used to process, classify and interpret huge amounts of information; and when combined with medical software and equipment it might monitor, diagnose and even cure patients. Drones can be paired with a variety of onboard components such as data receivers/transmitters, video cameras, thermal sensors, facial recognition software, and they can be tools for collecting large amounts of information as well as function in groups or swarms that learn and think collectively. The decentralized, immutable and secure nature of blockchain technology enables it to converge with other technologies because it has the potential of making every centralized process fully autonomous – it can be used to protect self-driving cars or to secure the internet of the future.

[100] Some implications mentioned in the case analysis have not been mapped in Figure No. 2 because they were only relevant to the particular technology in discussion, for example, safety of drone operations or enforceability of blockchain-based smart contracts.

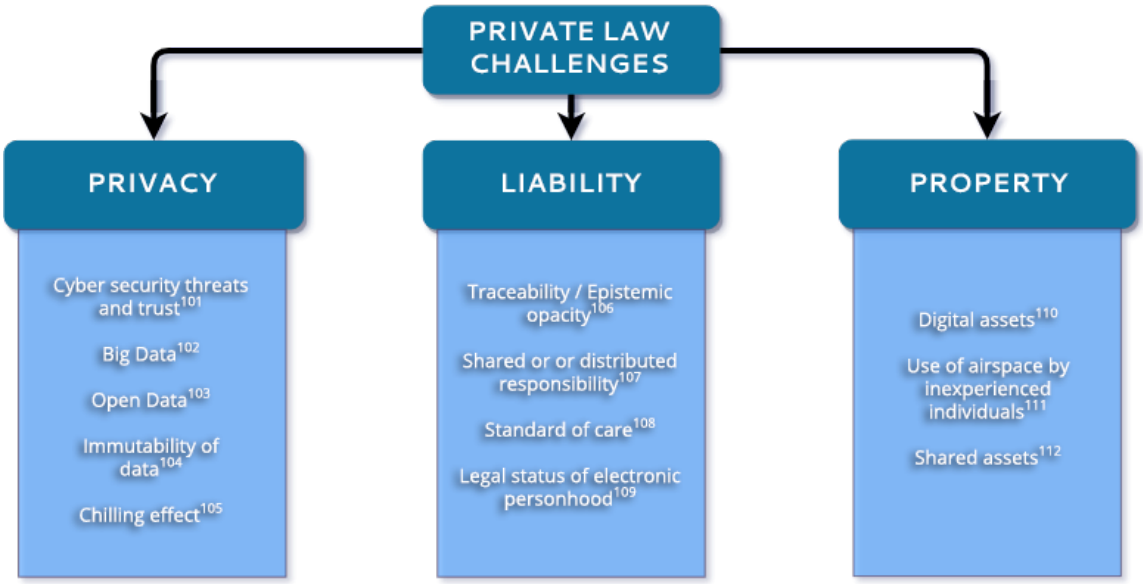

Figure 2: A non-exhaustive list of private law challenges generated by transformative innovations.

[101] Cybersecurity threats include hacking, identity theft, surveillance, cybercrimes, spam, behaviour targeting, internet jurisdiction and the like. Some of the cyber trust enhancing measures are privacy and data protection, cryptography, identity management, encryption and the like. More about challenges of cybersecurity and trust in section 2.2 (example of drones) of this article.

[102] According to World Economic Forum, in a few years, more than a trillion sensors will be connected to the internet, including most home appliances or cars. Big data is "huge amounts of data gathered from different sources, aggregated and analysed through algorithms". It could be used especially involving AI technologies for automated assessments and decision-making processes. Together with the potential for Big Data (personal and environmental) of becoming essential for data-driven innovations, it also poses risks especially in terms of unlawful discrimination and bias (Ana Gomes, "REPORT on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law-Enforcement," *European Parliament* // http://www.europarl.europa.eu/doceo/document/A-8-2017-0044_EN.html).

[103] The idea behind Open Data conception is that some data should be freely available to everyone to use for global public good, without restrictions from copyright, patents and other licensing. It is related to the participatory model phenomenon, discussed in section 2.3 of this article (example of blockchains) and includes such open access measures like internet affordability, net neutrality, cloud computing and the like.

[104] For example, public blockchains have the feature of immutability: once data is stored into distributed ledger system, it cannot be deleted. See section 2.3 (example of blockchains) of this article.

[105] Covert surveillance, which may be exercised by using transformative innovations, may cause individuals to fear that they are under observation at any time, resulting in a form of self-discipline called the "chilling effect" and accordingly stultification of freedoms of expression. See section 2.2 (example of drones) of this article.

[106] The decisions of epistemically opaque machines are not only unpredictable, but also hard to trace, because they can learn from past human experiences and calibrate their algorithms themselves. See section 2.1 (example of artificial intelligence) of this article.

[107] With the increasing autonomy of smart devices, the question is who will bear legal responsibility for their behaviour. Currently, there typically seems to be a 'shared' or 'distributed' responsibility between designers, engineers, programmers, manufacturers, investors, sellers and users, because none of these agents can be indicated as the ultimate source of action, but this solution tends to dilute the notion of responsibility altogether. See section 2.1 (example of artificial intelligence) of this article.

[108] In many aspects autonomous vehicles are expected to be better at performing precarious activities that are currently performed by man (for example, driving), because machines never fall asleep, they never drive drunk, get distracted by a text message or conversation, they never drink coffee or eat, they do not get angry or drowsy. It poses the question of standard of care in liability regulation. See section 2.1 (example of artificial intelligence) of this article.

[109] See section 2.1 (example of artificial intelligence) of this article.

As transformative technologies become more and more embedded in our daily routine, we begin to notice that they are not just neutral objects or tools, but mediators,[113] which indeed shape, interpret, transform, and make meaning of human lives.[114] The potential of transformative innovations, however, comes along with a set of tensions and risks, which can ultimately work against the wellbeing of humankind.

The case analysis has shown some of the reasons behind these emerging legal implications. Anticipating that every smart device will eventually be able to exhibit at least some degree of autonomy because of advancements in artificial intelligence technology, one of the most evident reasons is the growing level of "consciousness" and autonomy of emerging technologies. Some of the identified challenges that reflect this reason could be epistemic opacity in AI decision making, the vague legal status of electronic personhood, the ability to aggregate significant amounts of data in ways that reveals private behaviour of individuals, and property legislation that is no longer up to date to regulate the use of digital assets.

Another reason could be the growing availability of transformative innovations to the broad public and the development of participatory models in economy and other social spheres, including law. Social networks (Facebook, Twitter, Instagram), sharing economy (Uber, Airbnb, Task Rabbit) and cryptocurrencies (Bitcoin, Ethereum) are just a few examples of this phenomenon. In terms of the analysed technologies, the mapped challenges that reflect this tendency are airspace ownership and regulation of air traffic in lower airspace congested with unlicensed users, the immutability of data in public blockchain fair distribution of value in co-created ownership (sharing economy), and distributing machine responsibility among stakeholders.

A further reason is the tendency for transformative innovations to function in regulatory uncertainty. In the system of legal rules, there is a very common

[110] As a matter of fact, property legislation is outdated for regulating digital assets, because property laws were mostly created for tangible assets, so such causes ownership, inheritance, transfer of digital assets, as well as of cryptocurrencies, consumer protection, e-commerce to be regulated inadequately.
[111] Massive drone use has caused a previously empty area of airspace (in the closest reaches of the earth) to congest with thousands of small devices piloted by inexperienced individuals. See section 2.2 (example of drones) of this article.
[112] Shared assets are referred to as a part of a so-called shared or collaborative economy, which refers to business models where activities are facilitated by collaborative platforms that create an open marketplace for the temporary usage of goods or services often provided by private individuals, enabling people to offer services, promote new employment opportunities, flexible working arrangements and new sources of income, encouraging more asset-sharing and more efficient use of resources (European Commission, "A European Agenda for the Collaborative Economy," Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions (June 2, 2016) // https://www.eesc.europa.eu/resources/docs/com2016-356-final.pdf).
[113] Mireille Hildebrandt, *supra* note 7, 174.
[114] Katinka Waelbers and Tsjalling Swierstra, "The Family of the Future: How Technologies Can Lead to Moral Change"; in: Jeroen van den Hoven, et al., eds., *Responsible Innovation 1* (Springer International Publishing, 2014) // https://doi.org/10.1007/978-94-017-8956-1_12.

division of legal categories into certain binary systems, for example: public vs. private, business vs. personal, labour vs. professional, manufacturer vs. consumer, commercial property vs. personal property, and so on. However, in the context of transformative innovations these regulatory schemes often do not correspond to reality, as quasi-professional, quasi-commercial, quasi-public legal relationships emerge, whose regulation is in the so-called "grey zone."[115] Some argue that most current legal instruments are too slow and ineffective for regulating transformative innovations. According to prof. Milleire Hildebrant modern law grew up in a culture of print and remains firmly wedded to the medium of text. So, legal concepts and instruments which were developed in print culture may be ineffective in internet age.[116] Therefore, we argue that traditional hierarchical regulatory models ought to be replaced by decentralized, soft, inclusive governance tools as well as foresight instruments.

There could be at least two approaches for how to cope with challenges generated by technological progress. The first is to wait while technology is still developing and try to understand issues stemming from the process. According to this approach, lawmakers should delay regulation in order to stimulate the emergence of new transformative technologies and focus on products (outcomes) as a core value rather than the process of innovation. This is a dominating regulatory response to innovation in the United States. The other approach is more precautionary, focusing on possibilities to understand the true ends of emerging technologies, to prepare for complex, but fundamental societal impacts, appreciating and shaping the moral role of technologies toward a human-centred framework. This kind of approach is prevailing in the European Union.[117]

Choosing the right approach can be quite challenging. If we focus on the process rather than the outcomes, it is difficult to ascertain the full impact of transformative innovations while they are still emerging, whereas if we focus on the outcomes, technologies will probably have matured so much that they will already be embedded in social and economic layers of society, and the impacts may be difficult to change (Collingridge dilemma).[118]

A Call for Value-Based Legal Regulation

In a future where all devices will be interconnected, intelligent, able to learn from past experiences, where every technology will be able to monitor, interpret

[115] Vanessa Katz, "Regulating the Sharing Economy," *Berkeley Tech. Law Journal* Vol. 30 (2015): 1092.
[116] Mireille Hildebrandt, *supra* note 7, 140–218.
[117] World Economic Forum, *supra* note 4: 5; European Parliament calls for "a gradualist, pragmatic and cautious approach" with regard to future initiatives on robotics and AI (*Civil Law Rules on Robotics*, *supra* note 31).
[118] *Ibid*: 5.

and predict human behaviour, the values that we embed in their design during the early stages of their development become crucial to ensure a good life for human beings. Waiting until technology is fully developed and only then trying to understand their social, economic, and political impact would be too difficult, if not impossible.

Value-based legal regulation should comport the principles and values enshrined in Article 2 of the Treaty on European Union and in the Charter of Fundamental Rights, i.e. the principles of beneficence, non-maleficence, autonomy and justice, human safety, health and security; freedom, privacy, integrity and dignity; self-determination and non-discrimination, equality, justice and equity, informed consent, private and family life, personal data protection,[119] as well as on other underlying principles and values of the Union law, such as "non-stigmatization, transparency, autonomy, individual responsibility and social responsibility"[120].

BIBLIOGRAPHY

1. Asaro, Peter M. "A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics": 169-186. In: *Robot ethics: the ethical and social implications of robotics.* Cambridge: The MIT Press, 2012.
2. "Athlete Injured after Drone Crash." *BBC News* (April 7, 2014) // https://www.bbc.co.uk/news/technology-26921504.
3. Australian Transport Safety Bureau. "A safety analysis of remotely piloted aircraft systems" (August 9, 2017) // https://www.atsb.gov.au/publications/2017/ar-2017-016/.
4. Bard, Alexander, and Jan Söderqvist. *Syntheism: Creating God in the Internet Age.* Stockholm: Stockholm text, 2014.
5. Bekey, George A. "Current trends in robotics: technology and ethics": 17–34. In: *Robot ethics: the ethical and social implications of robotics.* Cambridge: The MIT Press, 2012.
6. Boucher, Philip, et al. *How Blockchain Technology Could Change Our Lives: In-Depth Analysis*. 2017 // http://bookshop.europa.eu/uri?target=EUB:NOTICE:QA0217043:EN:HTML.
7. Butterfield, Andrew, and Gerard Ekembe Ngondi, eds. *A Dictionary of Computer Science*. 7th edition. Oxford University Press, 2016.

[119] *Civil Law Rules on Robotics*, *supra* note 31.
[120] *Ibid.*

8. Cairns, Patrick. "World Drone Market Seen Nearing $127bn in 2020, PwC Says." *Moneyweb* (May 9, 2016) // https://www.moneyweb.co.za/news/tech/world-drone-market-seen-nearing-127bn-2020-pwc-says/.
9. Chohan, Usman W. "The Decentralized Autonomous Organization and Governance Issues" (2017) // Available at SSRN 3082055.
10. Chowdhry, Amit. "The Story Behind Drone Deploy And How It Built The Largest Drone Mapping Repository." *Forbes* (July 16, 2017) // https://www.forbes.com/sites/amitchowdhry/2017/10/16/dronedeploy/.
11. Chui, Michael, et al. "Sizing the Potential Value of AI and Advanced Analytics." *McKinsey and Company* (April 2018) // https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-applications-and-value-of-deep-learning.
12. *Civil Law Rules on Robotics: European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))*. European Union: European Parliament, 2017.
13. Clarke, Roger, and Lyria Bennett Moses. "The Regulation of Civilian Drones' Impacts on Public Safety." *Computer Law & Security Review* Vol. 30, No. 3 (June 1, 2014): 263–85 // https://doi.org/10.1016/j.clsr.2014.03.007.
14. Clarke, Roger. "The Regulation of Civilian Drones' Impacts on Behavioural Privacy." *Computer Law & Security Review* Vol. 30, No. 3 (June 1, 2014): 286–305 // https://doi.org/10.1016/j.clsr.2014.03.005.
15. Coldwell, Will. "High Times: Why Drone Photography Offers a Different View of Travel." *The Guardian* (June 17, 2016) // http://www.theguardian.com/travel/2016/jun/17/why-drone-photography-offers-a-different-view-of-travel.
16. *COS-RPAS-2014-2-03: Facilitating Access to Regulation for Light Remotely Piloted Aircraft Systems (RPAS)*. EASME: European Commission // https://ec.europa.eu/easme/en/cos-rpas-2014-2-03-facilitating-access-regulation-light-remotely-piloted-aircraft-systems-rpas.
17. "Drone Collides with Commercial Aeroplane." *BBC News* (October 16, 2017) // https://www.bbc.co.uk/news/technology-41635518.
18. "Drone Crashes into Virginia Bull Run Crowd." *Washington Post* // https://www.washingtonpost.com/local/drone-crashes-into-virginia-bull-run-crowd/2013/08/26/424e0b9e-0e00-11e3-85b6-d27422650fd5_story.html.

19. "'Drone' Hits BA Plane near Heathrow." *BBC News* (April 17, 2016) // https://www.bbc.co.uk/news/uk-36067591.
20. "Drone Rules" // http://dronerules.eu/en/#modal-disclaimer.
21. European Aviation Safety Agency. "Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories" (2018) // https://www.easa.europa.eu/sites/default/files/dfu/Introduction%20of%20a%20regulatory%20framework%20for%20the%20operation%20of%20unmanned%20aircraft.pdf.
22. European Commission. "A European Agenda for the Collaborative Economy." Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions (June 2, 2016) // https://www.eesc.europa.eu/resources/docs/com2016-356-final.pdf.
23. European Commission, European Group on Ethics in Science and New Technologies. "Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems." B-1049, Brussels (2018) // http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf.
24. European Commission. "Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner." Communication, Brussels (2014) // https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0207.
25. Falkon, Samuel. "The Story of the DAO — Its History and Consequences." *Medium* (August 12, 2018) // https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.
26. Ferranti, Ludovico, et al. "Drone Cellular Networks: Enhancing the Quality Of Experience of Video Streaming Applications." *Ad Hoc Networks* 78 (2018): 1–12 // https://doi.org/10.1016/j.adhoc.2018.05.003.
27. Finck, Michèle. "Blockchains and Data Protection in the European Union." *Eur. Data Prot. L. Rev.* Vol. 4 (2018): 17–35.
28. Finn, Rachel L., and David Wright. "Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications." *Computer Law & Security Review* Vol. 28, No. 2 (April 1, 2012): 184–94 // https://doi.org/10.1016/j.clsr.2012.01.005.

29. Finn, Rachel L., David Wright, and Michael Friedewald. "Seven Types of Privacy": 3–32. In: Serge Gutwirth, et al., eds. *European Data Protection: Coming of Age*. Springer International Publishing, 2013 // https://doi.org/10.1007/978-94-007-5170-5_1.
30. Frazier, Ian. "The Trippy, High-Speed World of Drone Racing." *The New Yorker* (January 29, 2018) // https://www.newyorker.com/magazine/2018/02/05/the-trippy-high-speed-world-of-drone-racing.
31. Future of Life Institute. "An Open Letter: Research priorities for robust and beneficial artificial intelligence" // https://futureoflife.org/ai-open-letter/.
32. Gomes, Ana. "REPORT on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non-Discrimination, Security and Law-Enforcement." *European Parliament* // http://www.europarl.europa.eu/doceo/document/A-8-2017-0044_EN.html.
33. Hall Kindervater, Katharine. "The Emergence of Lethal Surveillance: Watching and Killing in the History of Drone Technology." *Security Dialogue* Vol. 47, No. 3 (2016): 223–38 // https://doi.org/10.1177/0967010615616011.
34. Hayes, Ben, Chris Jones, and Eric Töpfer. *EURODRONES Inc.* Transnational Institute and Statewatch, 2014 // https://www.statewatch.org/news/2014/feb/sw-tni-eurodrones-inc-feb-2014.pdf.
35. Hildebrandt, Mireille. *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology.* Edward Elgar Publishing, 2015.
36. Holder, Chris, et al. "Robotics and Law: Key Legal and Regulatory Implications of the Robotics Age (Part I of II)." *Computer Law & Security Review* Vol. 32, No. 3 (June 2016): 383–402 // https://doi.org/10.1016/j.clsr.2016.03.001.
37. Katz, Vanessa. "Regulating the Sharing Economy." *Berkeley Tech. Law Journal* Vol. 30 (2015): 1067–1126.
38. Kube, Nicolas. *Daniel Drescher: Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Springer International Publishing, 2018.
39. Lin, Patrick, Keith Abney, and George A. Bekey, eds. *Robot Ethics: The Ethical and Social Implications of Robotics*. Cambridge, Mass: MIT Press, 2012.
40. Mica, John L. "Text - H.R.658 - 112th Congress (2011-2012): FAA Modernization and Reform Act of 2012" (February 14, 2012) // https://www.congress.gov/bill/112th-congress/house-bill/658/text.

41. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System" // http://bitcoin.org/bitcoin.pdf.
42. Newman, Julian. "Epistemic Opacity, Confirmation Holism and Technical Debt: Computer Simulation in the Light of Empirical Software Engineering": 256–272. In: Fabio Gadducci and Mirko Tavosanis, eds. *History and Philosophy of Computing*. *Vol. 487.* Springer International Publishing, 2016 // https://doi.org/10.1007/978-3-319-47286-7_18.
43. Ogle, Vanessa. "Drone Strike! Our Photographer Injured by TGI Friday's Mistletoe Copter." *Brooklyn Daily* // https://www.brooklyndaily.com/stories/2014/50/bn-drone-disaster-at-tgifridays-2014-12-12-bk_2014_50.html.
44. Pickles, Kate. "Toddler, 18 Months, Left Blind in One Eye by Drone Propeller." *Mail Online* (November 27, 2015) // http://www.dailymail.co.uk/health/article-3336366/Horrific-picture-shows-toddler-left-blind-one-eye-drone-propeller-sliced-eyeball-half.html.
45. PricewaterhouseCoopers. "Clarity from above. PwC global report on the commercial applications of drone technology" (May 2016) // https://www.pwc.pl/pl/pdf/clarity-from-above-pwc.pdf.
46. Rao, Bharat, Ashwin Goutham Gopi, and Romana Maione. "The Societal Impact of Commercial Drones." *Technology in Society* Vol. 45 (May 2016): 83–90 // https://doi.org/10.1016/j.techsoc.2016.02.009.
47. Rathenau Instituut. "Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence and virtual and augmented reality" // https://www.rathenau.nl/en/digital-society/human-rights-robot-age.
48. Riek, Laurel, and Don Howard. "A code of ethics for the human-robot interaction profession." *Proceedings of We Robot* (2014): 1–10.
49. Rosenfeld, Meni. "Analysis of Hashrate-Based Double Spending." *ArXiv Preprint ArXiv:1402.2009* (2014): 1–13.
50. Rule, Troy A. "Airspace in an Age of Drones." *Boston University Law Review* Vol. 95 (2015): 155–208.
51. Russell, Stuart, Daniel Dewey, and Max Tegmark. "Research Priorities for Robust and Beneficial Artificial Intelligence." *Ai Magazine* Vol. 36, No. 4 (2015): 105–114.
52. Salinas, Sara. "Biggest Delivery Breakthrough since Amazon Prime." *CNBC* (May 22, 2018) // https://www.cnbc.com/2018/05/22/biggest-delivery-breakthrough-since-amazon-prime.html.

53. Schwab, Klaus. *The Fourth Industrial Revolution*. 1st U.S. edition. New York: Crown Business, 2017.
54. "Size of the blockchain technology market worldwide from 2018 to 2023 (in billion U.S. dollars)." *Statista* // https://www.statista.com/statistics/647231/worldwide-blockchain-technology-market-size/.
55. Solum, Lawrence B. "Legal personhood for artificial intelligences." *NCL Review* Vol. 70: 1231–1288.
56. Madrigal, Alexis C. "Drone Swarms Are Going to Be Terrifying and Hard to Stop." *The Atlantic* (March 7, 2018) // https://www.theatlantic.com/technology/archive/2018/03/drone-swarms-are-going-to-be-terrifying/555005/.
57. Tendon, Steve, and Max Ganado. "Legal Personality for Blockchains, DAOs and Smart Contracts." *GANADO Advocates* (June 4, 2018) // https://ganadoadvocates.com/resources/publications/legal-personality-for-blockchains-daos-and-smart-contracts/.
58. The Law Society. "Blockchain: The legal implications of distributed systems" (August 1, 2017) // https://www.lawsociety.org.uk/support-services/research-trends/horizon-scanning/blockchain/.
59. United Nations Educational, Scientific and Cultural Organization. "Robotics Ethics" // http://www.unesco.org/new/en/social-and-human-sciences/themes/comest/robotics-ethics/.
60. *United States v. Causby*. 328 U.S. 256 (1946) // https://supreme.justia.com/cases/federal/us/328/256/.
61. Vanian, Jonathan. "Drone Smashes Into Army Helicopter." *Fortune* (December 14, 2017) // http://fortune.com/2017/12/14/drone-army-helicopter-smash/.
62. Vark, Caspar van. "How Drones Can Detect Crop Problems Early to Keep Farmers on Track." *The Guardian* (December 26, 2015) // http://www.theguardian.com/global-development/2015/dec/26/drones-farming-crop-problems-uavs.
63. Vladeck, David C. "Machines without principals: liability rules and artificial intelligence." *Washington Law Review* Vol. 89, No. 1 (2014): 117–150.
64. Voigt, Paul, and Axel Von dem Bussche. *The EU General Data Protection Regulation (GDPR): A Practical Guide.* 1st edition. Springer International Publishing, 2017.

65. Vu, Quang Hieu, Mihai Lupu, and Beng Chin Ooi. "Architecture of Peer-to-Peer Systems": 11–37. In: *Peer-to-Peer Computing*. Springer International Publishing, 2010
66. Waelbers, Katinka, and Tsjalling Swierstra. "The Family of the Future: How Technologies Can Lead to Moral Change": 219–236. In: Jeroen van den Hoven, et al., eds. *Responsible Innovation 1.* Springer International Publishing, 2014 // https://doi.org/10.1007/978-94-017-8956-1_12.
67. Wakefield, Jane. "Dubai Tests Drone Taxi Service." *BBC News* (September 26, 2017) // https://www.bbc.com/news/technology-41399406.
68. Williams, Kevin W. *A summary of unmanned aircraft accident/incident data: Human factors implications.* No. DOT/FAA/AM-04/24, Federal Aviation Administration. Oklahoma City, OK: Civil Aeromedical Inst, 2004.
69. Winiger, Bénédict, Håkan Andersson, and Österreichische Akademie der Wissenschaften, eds. *Digest of European Tort Law Vol. 1.: Essential Cases on Natural Causation.* Springer International Publishing, 2007.
70. World Economic Forum. "Values, Ethics and Innovation: Rethinking Technological Development in the Fourth Industrial Revolution" // https://www.weforum.org/whitepapers/values-ethics-and-innovation-rethinking-technological-development-in-the-fourth-industrial-revolution/.
71. Wright, Aaron, and Primavera De Filippi. "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (2015) // Available at SSRN 2580664.