LEGAL TECHNOLOGIES AND CYBER SECURITY IN THE SINGULARITY AGE

Dr. Paulius ASTROMSKIS[1]
Vytautas Magnus University

SUMMARY

This paper explores what regulation framework should be used to regulate the cyber security in the context of singularity age and emerging legal technologies thereof. Singularity and post-humanism scenarios may be seen as a matter-of-science fiction, but the ongoing technological revolution is already fundamentally altering every human transaction and institutions in the unprecedented ways. While one narrative touts the benefits of the greatest technological developments and bright future of cyber dependent opportunities, other warns the cyber dangers. In the search of the ways to reconcile regulation and technology, the need to turn to the fundamental roots of the regulation framework per se is obvious.

Therefore, the aim of this paper is to develop the conceptual cyber-security regulation framework in the context of singularity age and emerging legal technologies thereof. In order to achieve it, this paper uncovers the status quo of cyber security problem, by highlighting recent cyber incidents and the vulnerabilities of human error. It also develops a conceptual cyber security regulation framework, based on the fundamentals of transaction cost theory. This framework is evaluated in the context of emerging legal technologies.

KEYWORDS

Regulation, cyber security, singularity, legal technologies, transaction cost theory

IN LIEU OF INTRODUCTION: THE CONTEXT OF SINGULARITY AGE

Singularity defines "the destiny of the human-machine civilization"[2]. It starts with the moment in time and velocity (power) of computation, when artificial intelligence becomes equal to a human intelligence, and transcends towards the post-humanistic era.

The Singularity and its law of accelerating returns[3] essentially is an economic theory and a powerful driver of transforming, as Kurzweil states, "*every institution and aspect of human life, from*

[1] Vytautas Magnus University, S.Daukanto str. 28, Kaunas (Lithuania), Phone: +370 601 04524, fax: +370 37 201 107, e-mail: paulius@astromskis.lt
[2] R. Kurzweil, *The Singularity is near. When Humans transcend biology*, (NY Penguin Group, 2005)
[3] Id, Law of accelerating returns describes the acceleration of the pace of and the exponential growth of the products of an evolutionary process. These products include, in particular, information-bearing technologies such as computation,

sexuality to spirituality"[4]. Therefore, it also may be viewed through the lens of the new institutional economics. Moreover, singularity is also a transcendence phenomenon, since it allows us to transcend the limitations of human intelligence and biological bodies, thus empowering us to gain power over our fates:

> *Our mortality will be in our own hands. We will be able to live as long as we want (a subtly different statement from saying we will live forever). We will fully understand human thinking and will vastly extend and expand its reach. By the end of this century, the nonbiological portion of our intelligence will be trillions of trillions of times more powerful than unaided human intelligence*[5]

Kurzweil predicts that in 2029 artificial intelligence will pass a valid Turing test and therefore achieve human levels of intelligence. He sets the date 2045 for the singularity.[6] Two years before Softbank CEO Masayoshi Son prediction that the dawn of super-intelligent machines will happen by 2047[7]. Of course, there is no unanimous agreement if such scenario may be predicted on the ground of simple equation with computational power, as Kurzweil and Son did. According to Russell[8], even with a computer of virtually unlimited capacity, we still would not know how to achieve the brain's level of intelligence.

Although singularity and post-humanism scenarios may be seen as a matter-of-science fiction, it is beyond any reasonable doubt that the currently ongoing fourth industrial revolution is already fundamentally altering every human transaction and institutions in the unprecedented ways. In its scale, scope, and complexity, the transformations are unlike anything humankind has experienced before[9]. Thus although we are still in the early stage of the intellectual technologies development and, in fact, there is a probability that artificial intelligence will never transcend the human one, the ongoing technological evolution trends exponentially towards the predicted singularity scenario.

Of course, the law and institutions are at the centre of these unprecedented technological transformations. The Industrie 4.0 Working Group clearly and convincingly established that "*existing legislation will also need to be adapted to take account of new innovations*" [10], therefore requiring develop the regulatory framework in a way that facilitates innovation. Hence, besides the laws on robots, there have been developed alternatives of laws by robots and laws in robots[11]. Accordingly, in the search of the ways to reconcile regulation and technology, the need to turn to the fundamental roots of the regulation framework *per se* is obvious. Which of the regulation alternatives would be

---

and their acceleration extends substantially beyond the predictions made by what has become known as Moore's Law. The Singularity is the inexorable result of the law of accelerating returns.

[4] See footnote 2.

[5] Id.

[6] D. Galeon, C. Reedy, *Kuzweil Claims That the Singularity Will Happen by 2045*, (Futurism) https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045/ , accessed 2017-05-02.

[7] D. Galeon, *Softbank CEO: The Singularity Will Happen by 2047*, (Futurism, 2017-03-01), https://futurism.com/softbank-ceo-the-singularity-will-happen-by-2047/, accessed 2017-05-02.

[8] S. Russell, P. Norvig, et.al., *Artificial Intelligence. A Modern Approach*, Third Edition (Prentice Hall: New Jersey, 2010).

[9] K. Schwab, *The Fourth Industrial Revolution: what it means, how to respond*, (World Economic Forum, 2016-01-14), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond, accessed 2017-05-02.

[10] H. Kagermann, W. Wahlster, et al., *Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0*. (National Academy of Science and Engineering, 2013)

[11] R. Leenes, F. Lucivero, 'Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design', *Law, Innovation and Technology (2014) 6(2) LIT 194–222*.

the most efficient and just in the context of singularity age's probability? In other words, the issue is whether humans are and will remain to be more efficient regulators than intelligent machines and if not, is it safe to delegate the regulation activities to that kind of artificial object (or subject).

The first part of the issue is too obvious to consider it in depth. Undisputedly, within the context of singularity scenario, only intelligent machines have the real potential to decide on thousands of issues within the fraction of the second; using the unbiased knowledge, wisdom and understanding of thousands of greatest minds; for a cost of a cup of tea. The second part of the issue is far more complex**.**

Singularity scenario may come with the success story of evolution and enhancement in all fields of human mental and physical activities. However it may also be a story of existential risk, that we have been warned about by the Future of Life Institute and by an open letter, signed by more than 8000 other leading opinion leaders and scholars in "ranges from economics, law and philosophy to computer security, formal methods and, of course, various branches of AI itself"[12]**.**

Naturally, besides the welfare enhancing technologies, the cyber security threats also evolve with the same exponential scope. Indeed, while one narrative touts the benefits of the greatest technological developments and bright future of cyber dependent opportunities, other warns the World of cyber-activism (hacktivism), cybercrime, cyber-espionage, cyberwar and cyber-terrorism[13]. Even cyber murder may become a reality since cyber-dependent medical technology is a likely target. The ongoing cyberwar does not require expensive soldiers, arms and ammunition. It is a war of sophisticated algorithms operating from advanced, lightning-fast computers. It is a war without any territorial and geographic borders. For these and other reasons cyber security is in urge of a Manhattan Project – a digital nuclear option, capable of swiftly inflicting grievous damage while simultaneously safeguarding the cyber systems of its motherland[14].

In sum, having introduced the concept of singularity age and related issues, the *problem* is that it is unclear what regulation framework should be used to regulate the cyber security in the context of emerging legal technologies thereof.

Therefore the *aim* of this paper is to develop the conceptual cyber-security regulation framework and evaluate it in the context of emerging legal technologies thereof.

Thus, the *object* of this research is regulation of cyber security

In order to achieve the aim of this research and to solve the problem, these *tasks* has been formed:

1) To uncover the *status quo* of cyber security problem
2) To develop the conceptual cyber-security regulation framework
3) To evaluate the proposed framework in the context of emerging legal technologies

Accordingly, three parts of this paper are presented below. The analysis of the *status quo* of cyber security problem is presented in the first part. The second part is dedicated to the development of the conceptual cyber-security regulation framework. Finally, in lieu of conclusions, the proposed concept is evaluated in the context of emerging legal technologies, thus contributing to the knowledge, wisdom and understanding of regulation issues in the context of technological evolution.

---

[12] *Research Priorities for Robust and Beneficial Artificial Intelligence. An Open Letter.* https://futureoflife.org/ai-open-letter (accessed 2017-05-02).

[13] B.B. Hughes, D. Bohl., et al., 'ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance', *Technological Forecasting & Social Change 115 (2017) 117–130*.

[14] D. Laton, 'Manhattan_Project.exe: A Nuclear Option for the Digital Age', *25 Cath. U. J. L. & Tech (2017).*

THE *STATUS QUO* OF CYBER SECURITY PROBLEM

It is beyond any reasonable doubt that cyber security of cyber ecosystem has become one the major threats to the World[15]. The exponentially increased use of software and digital services with asymmetrical distribution of security measures, possesses major economic and political threats. To name just a few, cyberwars, espionage, ransomware, DDoS attacks, blackmail and fraud, phishing, large data leaks, and other financially or politically motivated attacks have become an exponentially growing, unsolvable, everyday problem of law and economics. Cybercrimes differ from traditional crimes, because perpetrators are more difficult to track, economies of scale are larger and it is easier for cyber criminals to operate on an international scale[16]. The threat streams from private data of individual to the critical infrastructure and governments. There is no immunity. Indeed, the World has been hacked and the chances of being caught are small.

Some high-profile cyber-attacks are highlighting these risks and costs. In 2013 Target has lost approximately 40 million credit and debit card accounts, costing Target approximately $250 million. In 2014, a hack at Sony Corp. exposed Hollywood secrets. In 2015, the adult-themed, extramarital affair website Ashley Madison was hacked exposing the personal information of some 32 million users[17]. AdultFriendFinder followed with 412 million accounts loss in 2016. 1,5 billion accounts of Yahoo has been compromised in 2013 and 2014 attacks, LinkedIn has lost 165 million in 2012, Dropbox – 68 million in 2013[18], etc. The United States government has lost background investigation records of millions of current, former, and prospective federal employees and contractors, including the fingerprints of 5.6 million federal employees in 2014 attack that lasted for several months[19]. 2016 breaches also included the Department of Homeland Security and the Federal Bureau of Investigation[20].

According to "The Global Risks Report 2016," from the World Economic Forum, detectable crimes in cyberspace cost the global economy an estimated 445 billion USD in 2014[21]. There were no signs of slowing down in 2015 and a forecast for 2019 estimates up to 2 trillion USD[22]. The trends of cyber security incidents by attack type, time and impact were clearly summarized by IBM X-Force Threat Intelligence Index 2017 report[23] as in *Figure 1*:

---

[15] World Economic Forum, *The Global Risks Report 2016, 11th Edition* (2016), http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf , accessed 2017-05-01

[16] T. Kiseleva, B. Overvest, et al., 'Cyber Security Risk Assessment for the Economy', *CPB Communication, Dutch National Cyber Security Centre,* (2016, July 6).

[17] J.Heidenreich, 'The privacy issues presented by the cybersecurity information sharing act', *North Dakota Law Review, Vol. 91:395 (2015).*

[18] E.Palermo, P.Wagenseil, *The Worst Data Breaches of All Time*, (Tomsguide, 2016-12-14) http://www.tomsguide.com/us/pictures-story/872-worst-data-breaches.html#s21 , accessed 2017-05-01.

[19] See footnote 17.

[20] A.Kayastha, *Top 10 Security Breaches of 2016*, (Tufitech, 2016-12-27), http://www.tufitech.com/news/top-security-breaches-2016/, accessed 2017-05-01.

[21] See footnote 15.

[22] *Cybercrime will cost businesses over $2 trillion by 2019*, (Juniper Research, 2015) https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion, accessed 2017-05-01,

[23] Security Intelligence Staff, *IBM X-Force Threat Intelligence Index 2017*, (Security Intelligence, 2017), https://securityintelligence.com/media/ibm-x-force-threat-intelligence-index-2017/ , accessed 2017-05-01.

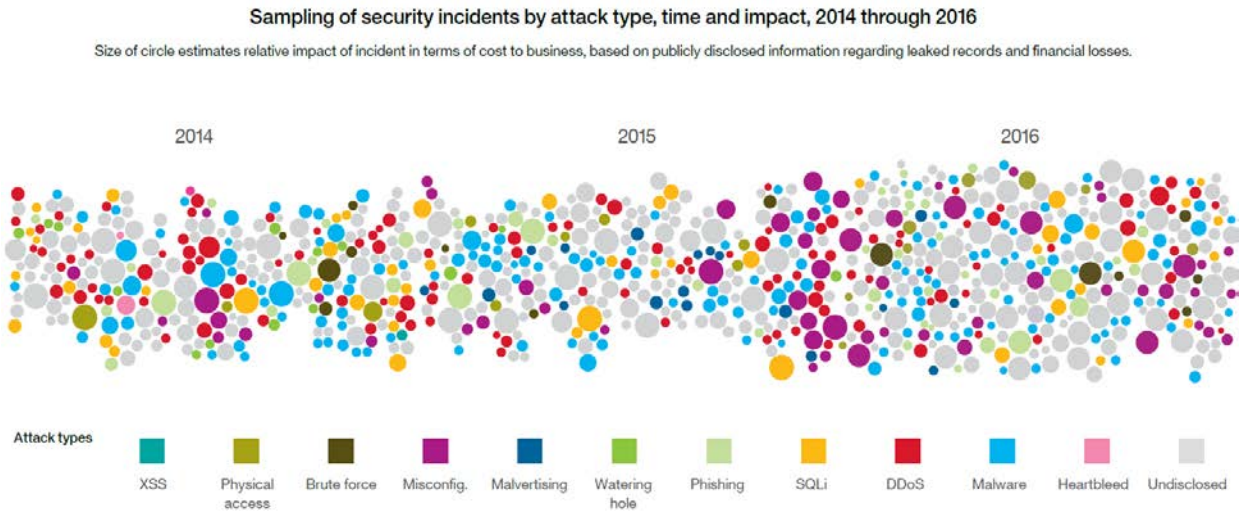

Figure 1: Cyber security incidents by attack type, time and impact (*source:* IBM X-Force Threat Intelligence Index 2017 report)

Nevertheless, the problem is much bigger. World is cyber dependent. Airports, cars, hospitals, stock markets, power grids are run by computers and these computers are shockingly vulnerable to cyber-terrorist attack. An attack of sufficient strength could destabilize a country's economic or military apparatus without the need for armed conflict. This requires a completely different framework for prevention or response than one for kinetic warfare, where physical actions are taken against physical targets. That is not to say that casualties in cyberwar are impossible. Cyber attacks on power grids and communications have the ability to cause kinetic effects directly, damaging physical infrastructure. For example in March of 2015, Iran launched a cyberattack against Turkey's power grid that shut down power systems in over half the nation's provinces[24].

These cyber security risks of cyber dependency raise two main challenges for the legal systems tailored to regulate the 'real world' behaviour. These are the jurisdictional fragmentation and attribution of behaviour. The first one follows from the global nature of cyberspace. Jurisdiction of a sovereign state is limited and protected by rules of customary public international law. The latter follows from the problems in determining the responsibility for harmful conduct in cyberspace. The asymmetry of the cause-effect relationship in the internet does not allow distinguishing with ease between participants standing behind an attack – an individual or a government[25].

Typical attempts to improve cybersecurity through regulation involve enhancement of capabilities to collect and share information about cybersecurity threats. However, cybersecurity regulation takes place within complex ecosystems, where stakeholders from diverse societies, having distributed responsibilities, diverse problems and challenges, make it difficult to initiate collective action. Therefore, cybersecurity is the sea of paradoxes, where the choosing of one direction can be at the expense of another direction, while the obligation of government is to go both ways[26].

The major cyber security paradox stems from the classical tension between security and privacy. In order for governments to ensure cybersecurity, they need to access the data of individuals

[24] See footnote 14.
[25] A. Appazov, *Legal Aspects of Cybersecurity*, (Justitsministeriet, Copenhagen, 2014).
[26] H. Bruijn, M. Jansen, 'Building cybersecurity awareness: The need for evidence-based framing strategies', *Government Information Quarterly 34 (2017) 1–7.*

and organizations for surveillance purposes. That is, capability to preclude or react to the cyber-attack increases as privacy barriers decrease. Therefore security and privacy are opposite vectors, although the obligation of government is to ensure both. The heated discussion about the legitimate balance between national security and information privacy, intensified by the Snowden leaks, has been going on for several years.[27]

Another important paradox stems from the realization that the same data that can be used to improve the quality of life can also be used against citizens, as was revealed by Snowden and other whistleblowers. Bruijn[28] classified some of other most common cybersecurity policies – making paradoxes in accordance to the policy issues they emerge from. What is the desired level of protection of systems? How much (cross-border) collaboration is necessary to fight cybersecurity? Who to fight to? What is the right amount of spending on cybersecurity? What is the right level of visibility? Who should ensure the cybersecurity of systems? Thus, cyber law is a new, complex and greatly diversified field of law.

The European Commission has also expressed understanding that there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of cyber incidents spanning across borders, and in terms of private sector involvement and preparedness[29]. To help address this, the 2013 EU Cyber Security Strategy asks The European Union Agency for Network and Information Security [30] to "encourage good practice in information and network security" to assist and support Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure. Thus, 18 European Union Member States have published National Cyber Security Strategies as a key policy feature, helping them to tackle risks that have the potential to undermine the achievement of economic and social benefits from cyberspace[31].

However, despite the high-sounding wording of the strategies, growing amount of cyber security cases and research in the field, the problem is far from solved. Cyber attacks remain among the biggest threats to people, businesses, governments and other institutions. Moreover, the technology upon which all these strategies and security tools are developed might very soon be outdated. It is expected to meet 2020 with 24 billion interconnected devices, with different security techniques and policy requirements applied by producers, thus making security challenges more difficult to fulfil as it is hard to develop a generic "one fits all" security strategy or model[32]. Clearly, the cyber-dependent World needs the Cyber Manhattan Project.

Since security and privacy are at the opposite ends of the same problem, the digital nuclear option may be developed either from the perspective of security or privacy.

---

[27] S.Schuster, M. Berg, et al., 'Mass surveillance and technological policy options: Improving security of private communications', *Computer Standards & Interfaces 50 (2017) 76–82.*

[28] See footnote 26.

[29] High Representative of the European Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, (Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. JOIN(2013) 1 final - 7/2/2013).

[30] The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens (www.enisa.europa.eu)

[31] European Union Agency for Network and Information Security, *An evaluation Framework for National Cyber Security Strategies*, (2014).

[32] A.R. Sfar, E. Natalizio, et.al., A Roadmap for Security Challenges in Internet of Things, *Digital Communications and Networks, http://dx.doi.org/10.1016/j.dcan.2017.04.003*

The first option involves a breakthrough in computing power and intelligence of the technologies used for security of data-driven world. However, such evolution would also open new possibilities for the development of hacking tools, as faster and smarter technologies will be accessible to the wrongdoers too. Moreover, technological singularity may not be reached in another 30 years. Therefore, security perspective option will not be accessible soon enough and (most likely) will not diminish the cyber security risks at the speed and scope needed for it to be treated as a nuclear option.

The second option is to reinvent the privacy law. This perspective has some major deviations from the technological advancement option described above. Security and privacy are opposite vectors, thus abilities to preclude or react to the cyber-attacks increase as privacy barriers decrease, even with the *status quo* in computation power and intelligence of the technologies. However, technological advancement is exponential, while the development of privacy law remains linear and slow. Thus the governments are urged to find a way for self-governance or to speed up, at a major scale, the regulatory procedures and decisions thereof. Finally, the law may be changed with the stroke of a regular pen. Therefore privacy perspective option is accessible and it may diminish the cyber security risks even with the *status quo* in computation power and intelligence of the technologies. Moreover, it may solve an ancillary issue of the governance efficiency.

Of course, there is an undefined set of third options, encompassing a mix of both: advancement of technologies while sustainably reaching for a trust-free governance system that would allow decreasing cyber security related privacy barriers.

CONCEPTUAL CYBER SECURITY REGULATION FRAMEWORK

Economic theories are increasingly used to explain cyber-security problems. In this vain, the field has been studied using such concepts as behavioural economics, asymmetric information, externalities and market failures framework[33]. Based on these theories, many various new behavioural models, networks and action research methodological advances in cybercrime and privacy economics are developed[34].

According to the general theory of regulation, regulators should intervene where market fails, aiming to fix these failures[35]. Market failures and resulting costs are the centerpiece of Transaction Cost Economics – one of the dominant economic theories of the XXI century[36], having a single transaction as a unit of analysis. Transaction unit is described as a process of exchanging scarce

[33] N. Jentzsch, 'State-of-the-Art of the Economics of Cyber-Security and Privacy', *IPACSO - Innovation Framework for ICT Security Deliverable, No. 4.1 (2016)*; T.Moore, 'The economics of cyber-security: Principles and policy options', *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies Press. (2010)*; T.Moore, R.Clayton, R. Anderson, 'The economics of online crime', *Journal of Economic Perspectives 23(3): 3-20 (2009)*; H. Manshaei, Q. Zhu, et.al., 'Game Theory Meets Network Security and Privacy', *ACM Computing Surveys (CSUR), Volume 45 Issue 3, (June, 2013*).

[34] Id. N. Jentzsch.

[35] A.C. Pigou, *The Economics of Welfare*, Fourth Edition, (Macmilan & Co., London, 1932).

[36] For exhaustive analysis of the transaction cost theory, its elements and developments see, for example, S.Ruester, 'Recent Developments in Transaction Cost Economics', *EE2 Working Paper. Resource Markets. No. WP-RM-18, (2010), 1-47*; T.J.Macher, B.D.Richman, 'Transaction cost economics: An Assessment of Empirical Research in the Social Sciences', *Business and Politics. Vol. 10, No. 1, (2008), pp. 1-85*; I.Geyskens, J.B.Steenkamp, N.Kumar, 'Make, Buy, Or Ally: A Transaction Cost Theory Meta-Analysis', *The Academy of Management Journal. Vol. 49, No. 3, (2006), 519-543*; R.Carter, G.M.Hodgson, 'The Impact of Empirical Tests of Transaction Cost Economics on the Debate on the Nature of the Firm', *Strategic Management Journal. Vol. 27, No. 5, (2006), 461-47*, and others.

resources[37]. This exchange is a result of ones actions, caused due to some behavioral incentives (motives). Accordingly, transaction unit has its motive (incentive), action (manifest of the will through activity or silence) and result elements, as shown in *Figure 2*.

Figure 2. Transaction unit

.

Thus, market failures framework, developed mostly by Williamson[38], may be used for the analysis of regulation issues. The centrepiece of market failures framework is an illustrative proposition known as the Coase Theorem[39]. By using an example of crop damage caused by straying cattle, Coase proposed, that:

> *it is necessary to know whether the damaging business is liable or not for damage caused since without the establishment of this initial delimitation of rights there can be no marked transactions to transfer and recombine them. But the ultimate result (which maximizes the value of production) is independent of the legal position if the pricing system is assumed to work without cost*[40]

The theorem has been stated in numerous ways and is subject to an enormous amount of theoretical and empirical controversy[41]. The general claims of this theory may be summarized by (i) "efficiency hypothesis" i.e. regardless of how rights are initially assigned, the resulting allocation of resources will be efficient, and (ii) "invariance hypothesis", i.e. the final allocation of resources will be invariant under alternative assignments of rights[42]. In other words, under the assumption of zero transaction cost, the outcome of transactions will be efficient regardless the legal regulation. That is, if transactions are costless, the allocation of rights or obligations is irrelevant. The transactions will always be efficient, legal rights – perfect and legal certainty – absolute. Accordingly, if law is irrelevant and the outcomes of transactions are always efficient, the state of zero transaction cost also means the state without the need of laws and lawyers. The state of self-governance.

Realizing that such proposition is too naïve to consider seriously, the state of zero transaction costs has always been seen as utopic idea - "*a very unrealistic assumption*", according to Coase[43]. Indeed, neither science, nor fiction has ever demonstrated complete and persuasive view of what it would be to live in the world where there is no need to have legislative, executive and judicial branches of government. Thus, the real message of Coase was to study the World with positive transaction costs[44] – the World with the market failures.

---

[37] R.A. Posner, 'The Law and Economics of Contract Interpretation', *John M. Olin Program in Law & Economics Working Paper, 2nd ser, No. 229 (2004) pp. 1-51.*; O. E. Williamson, *Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization*, (London: Free Press, 1975).

[38] O.E.Williamson, 'The Economics of Governance: Framework and Implications', in Langlois, R. (Ed.). *Economics as a Process: Essays in the New Institutional Economics*, (Cambridge: Cambridge University Press, 1986).

[39] R.Coase, 'The Problem of Social Cost', *The Journal of Law and Economics. Vol. 3, No. 1, (1960), 1-44.*

[40] Id. pp 8.

[41] S.G.Medema, R.O.Zerbe, *The Coase Theorem, The Encyclopedia of Law and Economics*, (Edward Elgar Publishing, 1999)

[42] Id.

[43] See footnote 39.

[44] O.E.Williamson, S.Tadelis, 'Transaction Cost Economics', prepared for Gibbons R., Roberts J, eds. *Handbook of Organizational Economics*, (Princeton University Press, 2012), 1-55.

Transaction costs may also be seen as the difference between perfect world and real world. These costs have also been defined as the "*costs of running the economic system*"[45] and conceptually equated to "*frictions in physical systems*"[46], constituting the major economic efficiency problem[47]. Moreover, since efficiency and justice coincide in many ways[48], the transaction costs are a legal problem, too. Thus diminishing of the transaction costs is the prime aim of regulation and regulators[49].

In order to diminish the risks of these transaction costs in the future, transacting one has to invest in pre-transaction research, analysis of data and development the protection instruments (legal or physical). These costs of transacting are incurred *ExAnte.*

Of course, the more investments are made at the pre-transaction stage, the less is the risk of post-transaction breach. However, human body, mind and resources have their limits, which together with future uncertainty makes it impossible to determine complete set of risks and to employ preemptive means to avoid all of them. Moreover, every symbol or action (even silence) used in the pre-transaction process has its own hermeneutical risk, which might be the source of misinterpretation and hence error in the enforcement procedure. Lastly, pre-transaction investments are based on the assumptions about future events, which are impossible or too costly to determine with absolute certainty. Despite the fact that future risks are only probable, the investments in security measures are inevitable. Due to these shortages, the transacting one may decide to absorb the costs of incomplete transaction[50]. Accordingly, most of transactions are incomplete and not self-enforceable due to the risk of uncertainty, opportunistic behaviour of others or enforcement errors.

If *ExAnte* stage protection fails, the parties are forced towards the process of adaptation through the state enforcement tools and/or sunk cost. In any of the scenarios the parties suffer from failures of protection in pre-transaction stage. These are the *ExPost* transaction costs.

According to Richard A. Posner[51], Transaction Costs (*TC*) are the sum of *ExAnte* costs (*x*) and risk (*y*) that *ExPost* costs (z) might occur. Thus the sum of transaction costs might be expressed as:

$$TC = x + y * z$$

[45] K.J. Arrow, 'The organization of economic activity: issues pertinent to the choice of market versus non-market allocations', in *The analysis and evaluation of public expenditures: the PPB system; a compendium of papers submitted to the Subcommittee on Economy in Government of the Joint Economic Committee, Congress of the United States, 1, Washington, D.C.* (Government Printing Office, 1969), pp. 47–64.

[46] See footnote 38.

[47] C.Marinescu, 'Transaction Costs and Institutions' Efficiency: A Critical Approach', *American Journal of Economics and Sociology, 71 (2012), 254–276.*

[48] R.Šimašius, *Teisinis pliuralizmas*, dissertation, (The Law University of Lithuania. Vilnius, 2002).

[49] See footnote 39 and 44.

[50] K.Eggleston, E.A.Posner, R.J.Zeckhauser, 'Simplicity and Complexity in Contracts', *John M. Olin Program in Law and Economics Working Paper. No. 93, The Law School, The University of Chicago, (2000), 1-45.*; O.Hart, J.Moore, 'Foundations of incomplete contracts', *The Review of Economic Studies. Vol. 66, No. 1, (1999), 115-138*; C. A.Hill, 'Bargaining in the Shadow of the Lawsuit: A Social Norms Theory of Incomplete Contracts', *Minnesota Legal Studies Research Paper. No. 08-46, (2009), 1-38*; E.Posner, 'A Theory of Contract Law under Conditions of Radical Judicial Error', *John M. Olin Program in Law & Economics Working Paper. 2nd ser. No. 80. The Law School. The University of Chicago, (1999), 1-39*; R.A.Posner, 'The Law and Economics of Contract Interpretation', *John M. Olin Program in Law & Economics Working Paper. 2nd ser. No. 229. The Law School. The University of Chicago, (2004), 1-51*; E.Rasmusen, 'A Model of Negotiation, Not Bargaining: Explaining Incomplete Contracts', *Harvard John M. Olin Discussion Paper. No. 324. Cambridge, MA: Harvard Law School, (2001), 1-52.*

[51] Id., R.A.Posner.

In the zero transaction costs (ideal) world, there are no *ExPost* transaction costs ($y = 0$). In this case $y * z = 0$, thus there is no need of safety measures, thus $x = 0$ and $TC = 0$. Hence, transactions are self-enforcing; the demand for regulation and enforcement services disappears. The market is works without a cost and need for law or lawyers. However, since the zero transaction cost state is deemed to be utopic, a state without *ExPost* transaction costs ($y = 0$) means that protection in pre-transaction stage is absolutely complete, with perfect rationality and full certainty of a future. This is a complete pre-crime society.

In either way, costless society is indeed a very unrealistic assumption and variables that causes market failures has to be taken into account solving regulation issues. These variables (either *ExAnte* or *ExPost*) were identified and elaborated by Williamson[52] (and others) and may be summarized into such groups:

1) *Bounded rationality*, which describes the limited cognitive competences and lingual limits of people[53];
2) *Opportunism*, which describes the self-interested nature of people that is sometimes led by the element of the guile in transaction[54];
3) *Uncertainty*, which describes the future state of nature, price and demand levels, innovations, legal and behavioural instabilities and many other characteristics, which are unclear and which make it impossible to predict the outcome of one's promises[55]. Uncertainty and bounded rationality are sometimes characterized as informational and cognitive inability[56].
4) *Asset specificity*, which usually describes six types of specific assets[57] that create critical dependency on the scarce resources, and identity of the transacting actor[58].

Bounded rationality and uncertainty make it impossible to evaluate all the risks related to relevant transactions and safeguards at the *ExAnte* stage. Thus all transactions are incomplete[59]. Opportunism and asset specificity make all transactions not self – enforcing, which in turn creates the demand for government system (i.e. laws and lawyers). These transaction cost variables, causing the market failures and thus demanding regulation, may be visualized as in *Figure 3* below.

[52] O.E.Williamson, 'The Economics of Governance: Framework and Implications', in R. Langlois, ed., *Economics as a Process: Essays in the New Institutional Economics*, (Cambridge: Cambridge University Press, 1986).
[53] H. Simon, *Administrative Behavior*, (New York: Free Press, 1976), p. xxviii; also see footnote 36, and *Id.*
[54] see footnote 36, S. Ruester, and footnote 52.
[55] see footnote 52; and O.E.Williamson, 'Comparative Economic Organization: The Analysis of Discrete Structural Alternatives', *Administrative Science Quarterly, Vol. 36, No. 2, (1991), p. 76*
[56] F.S.Nobre, 'Core Competencies of the New Industrial Organization', *Journal of Manufacturing Technology Management, Vol. 22, No. 4, (2011), 422 – 443.*
[57] These are: (i) site specificity; (ii) physical asset specificity; (iii) dedicated assets; (iv) human asset specificity; (v) intangible assets; (vi) temporal specificity.
[58] See footnote 36, S. Ruester, and footnote 52
[59] See footnote 36, E.Rasmusen, and footnote 50, O.Hart, J.Moore, C. A.Hill.

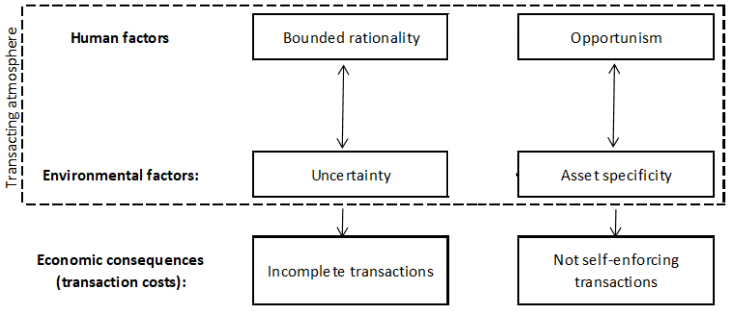

Figure 3. Transaction cost factors (adopted from Ruester[60])

Since the major task of regulation is to diminish transaction costs, with regard to *ExAnte* costs it implies the duty to foster access to data and computing power to process it (thus diminishing perils of uncertainty and bounded rationality). With regard to *ExPost* – the duty to foster accessibility to governance system and diminish dependency on scarce resources (thus diminishing the perils of opportunism and asset specificity).

Fixing of market failures is done through regulation – laws made by regulators using the powers delegated to them by the society. The discretion limits are usually analyzed through the lens of fundamental values of the society, such as right to life, liberty and pursuit of happiness (property).

Within the tri-tier institutional structure of society[61] and ontology of law[62], the conceptual holistic model of regulation, integrating fundamental values of society, transaction and variables of transaction cost, may be developed (see *Figure 4*).

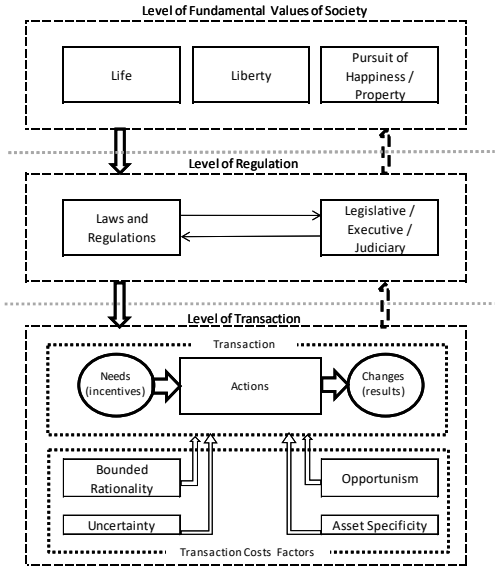

Figure 4. Standard model of regulation in theory.

[60] See footnote 36, S.Ruester.

[61] O. E. Williamson, ‚Transaction Cost Economics: How It Works; Where It Is Headed'. *De economist, Vol. 146, No. 1, (1998), pp. 23–58*; O. E. Williamson, ‚The New Institutional Economics: Taking Stock, Looking Ahead', *Journal of Economic Literature, Vol. XXXVIII, No. 3, (2000)*, pp. 595-613

[62] A. Vaišvila, *Teisės teorija*, (Vilnius: Justitia; 2004).

At the top level there are fundamental values of society. There the transition from fundamental values of society to the level of regulation and back is carried out. It means that fundamental values of society determine certain limits of regulatory discretion, however regulatory institutions (e.g. parliament, courts, etc.) may also transform the understanding of fundamental values of society.

The middle part of the model is the level of regulation, where regulatory institutions are forming regulatory measures and *vice versa* - the need for regulatory measures shapes the institutional setting. It encompasses the setting of laws and lawyers, i.e. the linear system of three branches of government with all the checks and balances. At the middle level the transition from the level of regulation to the level of transaction and back is carried out. It means that regulatory measures shape the market transactions. However, market is very dynamic, it is constantly innovating and therefore the regulation level is also under the direct influence of market transactions.

Lastly, the bottom part of the model is the place of the transaction and its cost variables, which, according to Williamson[63], are the reason for market failures. The everyday world is at a constant demand for regulation due to the market failures. Assumedly these failures result from the same transaction costs – inevitable part of the human nature to err. Standard model of regulation rests on human intelligence, which is limitedly rational, opportunistic, and performed under the uncertainty and asset specificity.

Furthermore, it is assumed that the standard model of regulation may fail in the four transition points between the ontological levels of law and institutions. First of all, the government may fail to interpret its discretion boundaries (values-to-regulation transition). Then government may abuse or fail to use its power (regulation-to-transactions transition). The third one involves the failure of government to interpret the market signals (transactions-to-regulation transition). Lastly, the powers given to government may be abused or failed to use for anchoring the fundamental values of a given society (government-to-values transition).

Assumedly these failures result from the same transaction costs – inevitable part of the human nature to err. Standard model of regulation rests on human intelligence, which is limitedly rational, opportunistic, and performed under the uncertainty and asset specificity. Human actors at the middle and bottom levels are behaving rather in the same intelligence and behavioural capacity, although with the different type of transactions[64]. In other words it doesn't matter how many cyber security agencies or super-agencies will be at the regulation level, as long as there are humans involved, the regulation will not be failure – free. In sum, the standard model of regulation in action may be presented as in *Figure 5*.

[63] See footnote 61.

[64] Bottom level is filled with the resource allocation transactions and middle level - with the state power transactions.

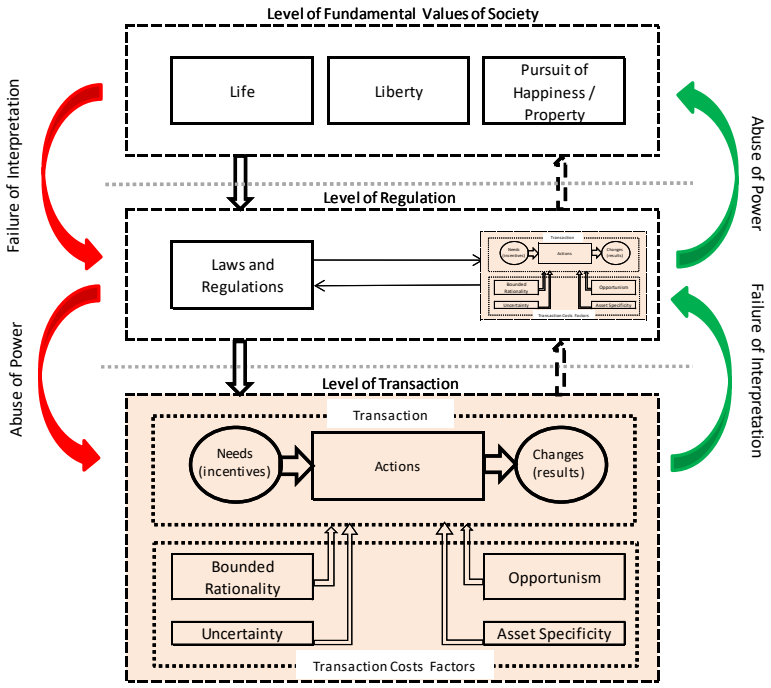

Figure 5. Standard model of regulation in practice

Therefore, it should be emphasized that most of the cyber security strategies and regulation models rest on the human reactions and decisions, integrating the risk of human nature to err. Indeed, only 48% percent of data security breaches are caused by acts of malicious intent. Human error or system failure accounts for the rest.[65] Verizon 2016 Data Breach Investigations Report[66] reveals that cybercriminals are continuing to exploit human nature as they rely on familiar attack patterns such as phishing. 95 percent of breaches and 86 percent of security incidents fall into nine patterns. Sixty-three (63) percent of confirmed data breaches involve using weak, default or stolen passwords. Most attacks exploit known vulnerabilities that have never been patched despite patches being available for months, or even years. In fact, the top 10 known vulnerabilities account for 85 percent of successful exploit. All findings boil down to the human element. Indeed, misaligned incentives of human being is more often a source of information insecurity, rather than the lack of suitable technical protections[67].

Unfortunately, most of the cyber defence systems tend to rely on humans who try to anticipate what the other human might do before they do it. However, neither kinetical nor digital firewalls will stop a determined hacker, exploiting vulnerabilities of the humans. Post-breach reactions also tend to rely on humans, who are dealing with jurisdictional fragmentation and attribution of behaviour. On either stage, government faces additional so-called "Going Dark" problem, which refers to situations in which government has legally obtained the right to search certain devices but has no technical

---

[65] B. Laberis, *20 Eye-Opening Cybercrime Statistics*, (Security Intelligence, 2016-11-14), https://securityintelligence.com/20-eye-opening-cybercrime-statistics/, accessed 2017-05-01.

[66] J. Brumfield, *Verizon's 2016 Data Breach Investigations Report finds cybercriminals are exploiting human nature*, (Verizon, 2016-04-27), http://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-0, accessed 2017-05-01.

[67] R. Anderson, 'Why Information Security is Hard—An Economic Perspective', *Proceedings of the 17th Annual Computer Security Applications Conference, 358–65 (2001). IEEE Computer Society.*

ability to carry out those orders of court[68]. Moreover, these problems and conflicts arise when government seeks to obtain information for the purposes of investigating or thwarting crimes, but cannot bypass the encrypted information even when it has the accompanying devices in its possession[69].

In order to overcome "Going Dark" problem, the government is using its powers to compel private companies to assist them in accessing encrypted devices. These attempts have caused extreme tension with regard to privacy and other backdoor problems[70]. This debate might be highlighted by example of the US Cybersecurity Information Sharing Act ("CISA"), adopted in 2015, which has established a core real-time cybersecurity information sharing framework between private entities and the federal government. While its goal may be commendable, CISA has been criticized by *inter alia* Apple, Google, Amazon and Microsoft mostly with privacy, civil liberties and transparency related arguments[71]. The recent FBI and Apple encryption dispute in the San Bernardino Case[72] has exposed the major critical arguments supporting both sides of the paradox. On one hand, government asked Apple to create a backdoor to the iPhone 5C used in a 2015 San Bernardino terrorist attack that killed 14 people and seriously injured 22. Apple appealed arguing that government is asking for something that is too dangerous to create[73].

These arguments were supported by many, including the United Nations High Commissioner for Human Rights, who warned the FBI that unlocking a Pandora's box possesses the potential for "extremely damaging implications" on human rights[74]. Indeed, the Snowden leaks and other total surveillance attempts[75] have clearly demonstrated that humans involved in regulation are also vulnerable to opportunistically misuse of the private information collected. That is, distrust in personal data mismanagement extends to governmental institutions, thus requiring for protection measures from human vulnerabilities.

Nuclear option in privacy law would require treating privacy not as a law, but rather as a privilege. This perspective would open all private data to the government until the privilege to be forgotten is earned through a trustworthy behaviour. This option would be in alignment with the very idea of opportunism, which describes the self-interest nature of people. Transaction cost theory is based on a presumption of opportunistic behaviour, since it is too costly (or even impossible) to determine in advance whether individual actor is capable of acting opportunistically or not. General law, however, is based on the presumption of honesty, which protects all the actors (including hackers) from intervention to their privacy, until there is enough proofs of actual or potential threat to security. Thus nuclear option in privacy law would bypass "Going Dark" problem and would ensure maximum security available with the use of status quo technologies.

---

[68] J. M. Traylor, ‚Shedding Light on the „Going Dark" Problem and the Encryption Debate', *University of Michigan Journal of Law Reform. Vol. 50:2 (2017).*

[69] Id.

[70] Id.

[71] See footnote 17.

[72] *USA v. In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300*, United States District Court, C.D. California, No. ED 15-0451 M 2016 WL 618401.

[73] See footnote 68.

[74] Z. R. al-Hussein, *San Bernardino Shooting: UN chief warns of implications of Apple-FBI row*, (The Press-Enterprise. Associated Press, 2016-03-04), http://www.pe.com/2016/03/04/san-bernardino-shooting-un-chief-warns-of-implications-of-apple-fbi-row/, accessed 2017-05-01.

[75] P. Laungaramsri, ‚Mass surveillance and the militarization of cyberspace in post-coup Thailand', *ASEAS – Austrian Journal of South East Asian Studies, 9(2), (2016), 195-214.*

However, this option would also require a trust-free governance of the data collected. A cryptographic governance system, which should be organized very much alike blockchain - both autonomously and in a networked-based collective (distributed) nature, without any point of central control or single point of failure. Such technology, merging a cryptography with governance on a digital platform, if possible at all, might lead to the trust-free governance, which embraces the emerging digital lifestyle. Intelligent machines can be trained to constantly analyze patterns in order to identify any deviation in it, much like a human counterpart does, just much faster, cheaper and in higher details of variations. Moreover, it may constantly use existing data to learn and enhance its functionalities and cyber warfare strategies. Using process mining methodology[76] for transaction pattern analysis, such system could be shown as in *Figure 6.*

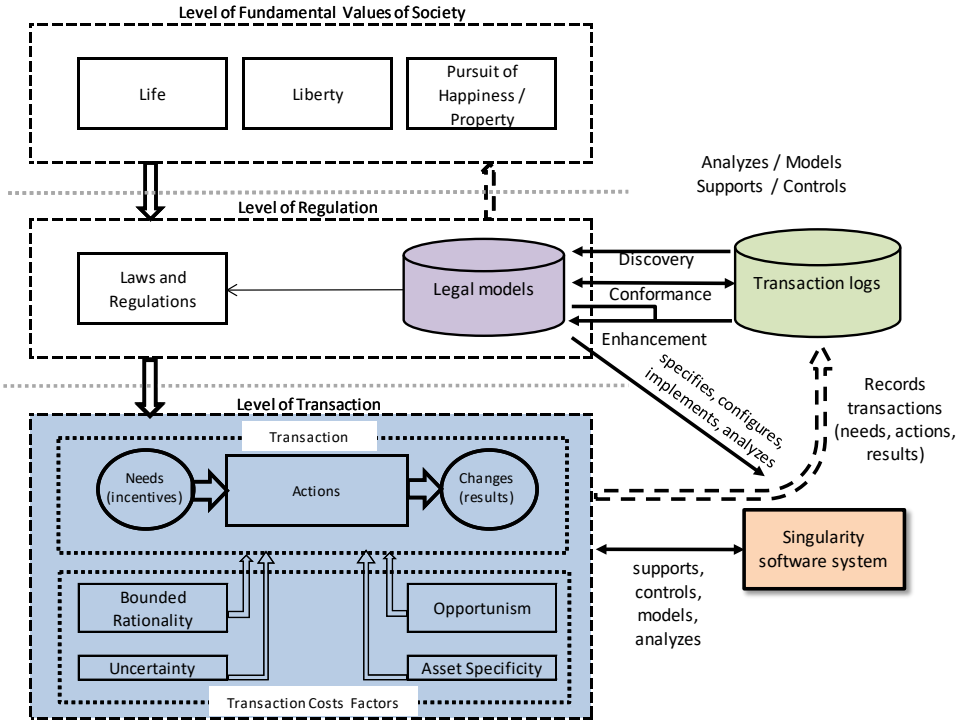

Figure 6. Conceptual failure-free regulation framework (SmartLaw)

Under this model all of the transacting data possible to collect under circumstances (from subjective to objective data) would go to the trust-free data base, supported and controlled by the trust-free software system. Trained within the standards of fundamental values (life, liberty and pursuit of happiness), it would autonomously analyze and model legal framework to prevent cyber security threats as much as possible, constantly learning and enhancing at the same speed and scope as the everyday transactions evolves. The law might become smart, i.e. individualized and constantly adopting in the real time situations.

This proposition is in line with the suggestion of that artificial intelligence presents a solution to the issues of human error and slow response time[77]. An artificially intelligent machine that is

[76] W.M.P. van der Aalst, *Process mining: Discovery, Conformance and Enhancement of Business Processe,* (New York: Springer, 2011), pp. 1-352; W.M.P. van der Aalst, et al., ‚Process Mining Manifesto', in *BPM 2011 Workshops proceedings. - Lecture Notes in Business Information Processing. Springer-Verlag, (2012), pp. 1-19.*

[77] See footnote 14

capable of autonomously learning and performing defensive and offensive strategies would be invaluable in the digital age. The issue remains – is the possibility of such framework a very unrealistic assumption in the context of developments in legal technologies?

IN LIEU OF CONCLUSIONS: THE GENESIS OF LEGAL TECHNOLOGIES

The rapid and exponential growth of data, its computation and storage capacity has led to the recent rise of legal technologies (LegalTech) and evolution of new search, drafting and control techniques. The trend of this industry is promising. The list of LegalTech companies on AngelList[78] has been extended from 15 companies in 2009 to 1532 companies in 2017. However, despite the recent industrial growth, the idea of artificial intelligence use in law is far from being new in the academic discourse.

Shortly after Konrad Zuse had built his first programmable computer in 1941, the idea of artificial intelligence began its shift from fiction to science. Started by seminal McCulloch and Pitt[79] paper "*A Logical Calculus of the Ideas Immanent in Nervous Activity*"; followed by "Turing test" [80] and Dartmouth Summer Research Project on Artificial Intelligence in 1956, the field of artificial intelligence studies has been widely accepted as a field of science rather than fiction, and has captured some of the greatest minds since. At the same time lawyers started their discussion on the use of artificial intelligence in law[81].

The works of Loevinger[82], Allen[83], Mehl[84], for example, could be regarded as the introduction to scientific and practical researches in this field, but the onset of application of artificial intelligence in law is usually related to the article by Buchanan and Headrick[85] "*Some speculation about artificial intelligence and legal reasoning"*

The practical experiments of synthesis of artificial intelligence and legal processes on the ground of these conceptual ideas did not take long. Such were the projects of McCarty[86] TAXMAN or Stamper[87] LEGOL. Of course, the interdisciplinary scientific researches continued developing in

[78] Legal Startups, https://angel.co/legal, accessed 2017-05-01
[79] W.S.McCulloch, W.H.Pitts, ‚A Logical Calculus of the Ideas Immanent in Nervous Activity', *Bulletin of Mathematical Biophysics, (1943), 115–133*
[80] A.M.Turing, ‚Computing Machinery and Intelligence', *Mind 59, (1950), 433–460*
[81] see for e.g. L.Loevinger, ‚Jurimetrics--The Next Step Forward', *Minn. L. Rev. 33 (1948), 455*; D.W.Allen, ‚Transaction Costs', in B. Bouckaert, G. De Geest, eds., *Encyclopedia of Law and Economics* (Chelthenham: Edward Elgar, 1999), pp. 893-925; L.Mehl, ‚Automation in the Legal World: From the Machine Processing of Legal Information to the Law Machine', *Mechanisation of Thought Processes (1958), 757-787*; B.G.Buchanan, G.Bruce, T.E.Headrick, ‚Some speculation about artificial intelligence and legal reasoning', *Stanford Law Review (1970), 40-62*
[82] L. Loevinger, 'Jurimetrics--The Next Step Forward', *Minn. L. Rev. 33 (1948): 455*
[83] A. E. Layman, 'Symbolic logic: A razor-edged tool for drafting and interpreting legal documents', *Yale LJ 66 (1956): 833.*
[84] See footnote 81, L. Mehl.
[85] See footnote 81, B.G.Buchanan, G.Bruce, T.E.Headrick.
[86] L.T.McCarty, 'Reflections on" Taxman: An Experiment in Artificial Intelligence and Legal Reasoning', *Harvard Law Review (1977): 837-893*
[87] R.K. Stamper, 'The LEGOL 1 prototype system and language', *The Computer Journal 20.2 (1977): 102-108.*

various directions. The works of Hafner[88], Gardner[89], Rissland[90], Sergot et al.[91] are considered to be influential scientific works in the area of artificial intelligence and law.

The International Conference on AI and Law (ICAIL) was started in 1987 and continued annually. At present it has become the main forum of application of artificial intelligence in law. These conferences resulted in establishment of the International Association for Artificial Intelligence and Law (IAAIL) and start of the Artificial Intelligence and Law Journal. It did not take long for the movement to involve not only the USA, but also Europe (e.g.. JURIX conferences), Japan (e.g., JURISIN workshop) and other countries.

Thus, academic discourse on artificial intelligence and law is celebrating more than 50 years of development. However, so far only primitive artificial intelligence systems have been found in legal practice. As Isaac Asimov has predicted with the punctilio of accuracy, **r**obots are neither common, nor very good in 2014, but they are in existence[92]**.** Thus the cognitive skills of superior level characteristic to the lawyer's profession are unattainable for the systems of artificial intelligence yet.

Nevertheless, the rapid technological development[93] and the current market trends (such as Google quantum supercomputer, digital copy of oneself[94], etc.) suggest that primitive artificial intelligence is gaining new properties and abilities that very soon will surpass their human counterparts. This process is accelerating. It is recognized in scientific literature that the latest technologies are and will continue changing the legal industry essentially.

Even with its limited capabilities the first generation of LegalTech has already disrupted the legal market[95] and applications for using artificial intelligence are rapidly growing. From a chat-bot that gives advice whether you have to pay your parking ticket[96], artificial intelligence enabled document creation or review[97], dynamic contracts or compliance management[98] to an algorithms that

---

[88] D.C. Hafner, 'Representing knowledge in an information retrieval system', in R.Oddy, et al., eds., *Information Retrieval Research*, (London: Butterworths, 1981).

[89] A. Gardner, 'The design of a legal analysis program', *AAAI-83, 1983.*

[90] E.L. Rissland, 'Examples in Legal Reasoning: Legal Hypotheticals', *IJCAI. 1983.*

[91] M.J. Sergot, et al. 'The British Nationality Act as a logic program', *Communications of the ACM 29.5 (1986): 370-386.*

[92] I. Asimov, *Visit to the World's Fair of 2014*, (N.Y. Times, 1964-08-16), http://www.nytimes.com/books/97/03/23/lifetimes/asi-v-fair.html , accessed 2017-05-01.

[93] L.Muehlhauser, A.Salamon, 'Intelligence Explosion: Evidence and Import', in A.Eden, et al., eds., *Singularity Hypotheses: A Scientific and Philosophical Assessment*, (Berlin: Springer, 2012), 15-42

[94] A.Sally, *Digital doppelgängers: Building an army of you*, (New Scientist, 2012) http://www.newscientist.com/article/mg21528771.200-digital-doppelgangers-building-an-army-of-you.html, accessed 2017-05-01.

[95] See for e.g. M. Bay, 'Survey Shows Surge in E-Discovery Work at Law Firms and Corporations', *Law Tech. News (July 6, 2012)*; E. Koblentz, 'Judge Carter OKs Peck's Predictive Coding Decision in 'Da Silva Moore,' *Law Tech. News (Apr. 26, 2012)*, W. D. Henderson, R. M. Zahorsky, 'Paradigm Shift', *A.B.A. J., July 2011*; D. R. Mountain, 'Disrupting Conventional Law Firm Business Models Using Document Assembly', *15 Int'l J.L. & Info. Tech. 170 (2007)*; E. J. Goldstein, 'Kiiac's Contract Drafting Software: Ready for the Rapids?', *Law Tech. News (May 18, 2012)* and others.

[96] See for e.g. DoNotPay, http://www.donotpay.co.uk/signup.php , accessed 2017-05-01; R. Price, *This chatbot fought parking fines and now it's helping refugees*, (World Economic Forum, 2017-03-07), https://www.weforum.org/agenda/2017/03/this-chatbot-fought-parking-fines-and-now-its-helping-refugees?utm_content=buffere3b83&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer , accessed 2017-05-01.

[97] See for e.g. Ironclad, https://www.ironcladapp.com/about, accessed 2017-05-01, Lawgeex, https://www.lawgeex.com, accessed 2017-05-01, G. O. Hernandez, *4 Ways Technology Is Changing Contracts*, (Legal Tech News, 2016-12-29), http://www.legaltechnews.com/id=1202775740310/4-Ways-Technology-Is-Changing-Contracts?rss=rss_ltn&utm_source=SocialFlow&utm_medium=LegaltechNews , accessed 2017-05-01, G. O. Hernandez, *Artificial Intelligence Has Found a Home in Contract Management*, (Legal Tech News, 2016-08-04), http://www.legaltechnews.com/id=1202764272201?back=law&slreturn=20170402123536, accessed 2017-05-01.

[98] See for e.g. SirionLabs, https://www.sirionlabs.com/, accessed 2017-05-01.

predicts decisions of European Court of Human Rights[99] or US Supreme Court decisions[100]. In 2012 New York District Court issued the judicial opinion in a pending federal case, Da Silva Moore v. Publicis Groupe, where the use of e-discovery has been officially endorsed in the US: "*Computer-assisted review appears to be better than the available alternatives, and thus should be used in appropriate cases.*"[101]

Accordingly, academically trained attorneys are increasingly being replaced by technology to analyze evidence and assess it for relevance in investigations, lawsuits, compliance efforts, and more[102]. For example Law firm Baker & Hostetler has announced that they are employing IBM's AI Ross[103] to handle their bankruptcy practice, which at the moment consists of nearly 50 lawyers.[104]

One of the primary reasons for such increase in LegalTech is due to the increased accessibility to neural networking models and other probabilistic algorithms. Further automation of law is streaming especially to quantitative legal prediction[105], machine learning[106], and other fields of scientific and practical legal problems. Professor Richard Susskind predicts unprecedented upheaval in a profession where the working practices of some lawyers and judges have changed little since the time of Charles Dickens. According to him, there will be anything dramatic, but there will be an incremental transformations in areas like the way legal documents are reviewed, legal risk is assessed and the way decisions are made[107].

Taking into account the probability that artificial intelligence might transcend the human one, the trend of legal technologies development allows to hope for a universal framework of cyber security regulation that would preclude perils of human nature to err and overcome problems of jurisdictional fragmentation and attribution of behaviour.

LITERATURE

1. A.C. Pigou, The Economics of Welfare, Fourth Edition, (Macmilan & Co., London, 1932).
2. A.M.Turing, ‚Computing Machinery and Intelligence', Mind 59, (1950), 433–460.

[99] S. Knapton, *Artifically intelligent 'judge' developed which can predict court verdicts with 79 per cent accuracy*, (Legal Tech News, 2016-10-24), http://www.telegraph.co.uk/science/2016/10/23/artifically-intelligent-judge-developed-which-can-predict-court/ , accessed 2017-05-01.

[100] J. Wakefield, *AI predicts outcome of human rights cases*, (BBC, 2016-10-23), http://www.bbc.com/news/technology-37727387 , accessed 2017-05-01

[101] *Monique DA SILVA MOORE, et al., v. PUBLICIS GROUPE & MSL Group*, 868 F.Supp.2d 137 (2012), No. 11 Civ. 1279(ALC)(AJP). United States District Court, S.D. New York. June 15, 2012.

[102] E. Livni, *Your next lawyer could be a machine*, (World Economic Forum, 2017-02-06), https://www.weforum.org/agenda/2017/02/machines-could-soon-replace-lawyers?utm_content=buffer933aa&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer , accessed 2017-05-01

[103] Ross is built on IBM's cognitive computer Watson. It was designed to read and understand language, postulate hypotheses when asked questions, research, and then generate responses (along with references and citations) to back up its conclusions. Ross also learns from experience, gaining speed and knowledge the more you interact with it. ROSS monitors the law around the clock to keep up-to-date with developments in the legal system, specifically those that may affect your cases. See for more: http://www.rossintelligence.com/ , accessed 2017-05-01.

[104] C. de Jesus, *AI Lawyer "Ross" Has Been Hired By Its First Official Law Firm*, (Futurism, 2016-03-11), https://futurism.com/artificially-intelligent-lawyer-ross-hired-first-official-law-firm/ , accessed 2017-05-01.

[105] D.M. Katz, 'Quantitative Legal Prediction—Or—How I Learned To Stop Worrying And Start Preparing For The Data-Driven Future Of The Legal Services Industry', Emory Law Journal, vol 2013, no. 62:909, 2011.

[106] H. Surden, 'Machine Learning and Law', *Washington Law Review, Vol. 89, No. 1, 2014*.

[107] J. Croft, *Artificial intelligence disrupting the business of law*, (Financial Times, 2016-10-06), https://www.ft.com/content/5d96dd72-83eb-11e6-8897-2359a58ac7a5 , accessed 2017-05-01.

3. A.R. Sfar, E. Natalizio, et.al., A Roadmap for Security Challenges in Internet of Things, Digital Communications and Networks, http://dx.doi.org/10.1016/j.dcan.2017.04.003.
4. Appazov, Legal Aspects of Cybersecurity, (Justitsministeriet, Copenhagen, 2014).
5. B.B. Hughes, D. Bohl., et al., 'ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance', Technological Forecasting & Social Change 115 (2017) 117–130.
6. B.G.Buchanan, G.Bruce, T.E.Headrick, ‚Some speculation about artificial intelligence and legal reasoning', Stanford Law Review (1970), 40-62.
7. C. A.Hill, 'Bargaining in the Shadow of the Lawsuit: A Social Norms Theory of Incomplete Contracts', Minnesota Legal Studies Research Paper. No. 08-46, (2009), 1-38.
8. C.Marinescu, 'Transaction Costs and Institutions' Efficiency: A Critical Approach', American Journal of Economics and Sociology, 71 (2012), 254–276.
9. D. Laton, 'Manhattan_Project.exe: A Nuclear Option for the Digital Age', 25 Cath. U. J. L. & Tech (2017).
10. D. R. Mountain, 'Disrupting Conventional Law Firm Business Models Using Document Assembly', 15 Int'l J.L. & Info. Tech. 170 (2007).
11. D.C. Hafner, 'Representing knowledge in an information retrieval system', in R.Oddy, et al., eds., Information Retrieval Research, (London: Butterworths, 1981).
12. D.M. Katz, 'Quantitative Legal Prediction—Or—How I Learned To Stop Worrying And Start Preparing For The Data-Driven Future Of The Legal Services Industry', Emory Law Journal, vol 2013, no. 62:909, 2011.
13. D.W.Allen, ‚Transaction Costs', in B. Bouckaert, G. De Geest, eds., Encyclopedia of Law and Economics (Chelthenham: Edward Elgar, 1999), pp. 893-925.
14. E. J. Goldstein, 'Kiiac's Contract Drafting Software: Ready for the Rapids?', Law Tech. News (May 18, 2012).
15. E. Koblentz, 'Judge Carter OKs Peck's Predictive Coding Decision in 'Da Silva Moore,' Law Tech. News (Apr. 26, 2012).
16. E. Layman, 'Symbolic logic: A razor-edged tool for drafting and interpreting legal documents', Yale LJ 66 (1956): 833.
17. E.L. Rissland, 'Examples in Legal Reasoning: Legal Hypotheticals', IJCAI. 1983.
18. E.Posner, 'A Theory of Contract Law under Conditions of Radical Judicial Error', John M. Olin Program in Law & Economics Working Paper. 2nd ser. No. 80. The Law School. The University of Chicago, (1999), 1-39.
19. E.Rasmusen, 'A Model of Negotiation, Not Bargaining: Explaining Incomplete Contracts', Harvard John M. Olin Discussion Paper. No. 324. Cambridge, MA: Harvard Law School, (2001), 1-52.
20. European Union Agency for Network and Information Security, An evaluation Framework for National Cyber Security Strategies, (2014).
21. F.S.Nobre, 'Core Competencies of the New Industrial Organization', Journal of Manufacturing Technology Management, Vol. 22, No. 4, (2011), 422 – 443.
22. Gardner, 'The design of a legal analysis program', AAAI-83, 1983.
23. H. Bruijn, M. Jansen, 'Building cybersecurity awareness: The need for evidence-based framing strategies', Government Information Quarterly 34 (2017) 1–7.
24. H. Kagermann, W. Wahlster, et al., Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0. (National Academy of Science and Engineering, 2013).
25. H. Manshaei, Q. Zhu, et.al., 'Game Theory Meets Network Security and Privacy', ACM Computing Surveys (CSUR), Volume 45 Issue 3, (June, 2013).
26. H. Simon, Administrative Behavior, (New York: Free Press, 1976).
27. H. Surden, 'Machine Learning and Law', Washington Law Review, Vol. 89, No. 1, 2014.

28. High Representative of the European Union for Foreign Affairs and Security Policy, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, (Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. JOIN(2013) 1 final - 7/2/2013).
29. I.Geyskens, J.B.Steenkamp, N.Kumar, 'Make, Buy, Or Ally: A Transaction Cost Theory Meta-Analysis', The Academy of Management Journal. Vol. 49, No. 3, (2006), 519-543.
30. J. M. Traylor, ‚Shedding Light on the „Going Dark" Problem and the Encryption Debate', University of Michigan Journal of Law Reform. Vol. 50:2 (2017).
31. J.Heidenreich, 'The privacy issues presented by the cybersecurity information sharing act', North Dakota Law Review, Vol. 91:395 (2015).
32. K.Eggleston, E.A.Posner, R.J.Zeckhauser, 'Simplicity and Complexity in Contracts', John M. Olin Program in Law and Economics Working Paper. No. 93, The Law School, The University of Chicago, (2000), 1-45.
33. K.J. Arrow, 'The organization of economic activity: issues pertinent to the choice of market versus non-market allocations', in The analysis and evaluation of public expenditures: the PPB system; a compendium of papers submitted to the Subcommittee on Economy in Government of the Joint Economic Committee, Congress of the United States, 1, Washington, D.C. (Government Printing Office, 1969), pp. 47–64.
34. L. Loevinger, 'Jurimetrics--The Next Step Forward', Minn. L. Rev. 33 (1948): 455.
35. L.Loevinger, ‚Jurimetrics--The Next Step Forward', Minn. L. Rev. 33 (1948), 455.
36. L.Mehl, ‚Automation in the Legal World: From the Machine Processing of Legal Information to the Law Machine', Mechanisation of Thought Processes (1958), 757-787.
37. L.Muehlhauser, A.Salamon, 'Intelligence Explosion: Evidence and Import', in A.Eden, et al., eds., Singularity Hypotheses: A Scientific and Philosophical Assessment, (Berlin: Springer, 2012), 15-42.
38. L.T.McCarty, 'Reflections on" Taxman: An Experiment in Artificial Intelligence and Legal Reasoning', Harvard Law Review (1977): 837-893.
39. M. Bay, 'Survey Shows Surge in E-Discovery Work at Law Firms and Corporations', Law Tech. News (July 6, 2012).
40. M.J. Sergot, et al. 'The British Nationality Act as a logic program', Communications of the ACM 29.5 (1986): 370-386.
41. N. Jentzsch, 'State-of-the-Art of the Economics of Cyber-Security and Privacy', IPACSO - Innovation Framework for ICT Security Deliverable, No. 4.1 (2016).
42. O. E. Williamson, ‚The New Institutional Economics: Taking Stock, Looking Ahead', Journal of Economic Literature, Vol. XXXVIII, No. 3, (2000), pp. 595-613.
43. O. E. Williamson, ‚Transaction Cost Economics: How It Works; Where It Is Headed'. De economist, Vol. 146, No. 1, (1998), pp. 23–58.
44. O. E. Williamson, Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization, (London: Free Press, 1975).
45. O.E.Williamson, 'Comparative Economic Organization: The Analysis of Discrete Structural Alternatives', Administrative Science Quarterly, Vol. 36, No. 2, (1991), p. 76.
46. O.E.Williamson, 'The Economics of Governance: Framework and Implications', in Langlois, R. (Ed.). Economics as a Process: Essays in the New Institutional Economics, (Cambridge: Cambridge University Press, 1986).
47. O.E.Williamson, 'The Economics of Governance: Framework and Implications', in R. Langlois, ed., Economics as a Process: Essays in the New Institutional Economics, (Cambridge: Cambridge University Press, 1986).
48. O.E.Williamson, S.Tadelis, 'Transaction Cost Economics', prepared for Gibbons R., Roberts J, eds. Handbook of Organizational Economics, (Princeton University Press, 2012), 1-55.

49. O.Hart, J.Moore, 'Foundations of incomplete contracts', The Review of Economic Studies. Vol. 66, No. 1, (1999), 115-138.
50. P. Laungaramsri, ‚Mass surveillance and the militarization of cyberspace in post-coup Thailand', ASEAS – Austrian Journal of South East Asian Studies, 9(2), (2016), 195-214.
51. R. Anderson, 'Why Information Security is Hard—An Economic Perspective', Proceedings of the 17th Annual Computer Security Applications Conference, 358–65 (2001). IEEE Computer Society.
52. R. Kurzweil, The Singularity is near. When Humans transcend biology, (NY Penguin Group, 2005).
53. R. Leenes, F. Lucivero, 'Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design', Law, Innovation and Technology (2014) 6(2) LIT 194–222.
54. R.A. Posner, 'The Law and Economics of Contract Interpretation', John M. Olin Program in Law & Economics Working Paper, 2nd ser, No. 229 (2004) pp. 1-51.
55. R.A.Posner, 'The Law and Economics of Contract Interpretation', John M. Olin Program in Law & Economics Working Paper. 2nd ser. No. 229. The Law School. The University of Chicago, (2004), 1-51.
56. R.Carter, G.M.Hodgson, 'The Impact of Empirical Tests of Transaction Cost Economics on the Debate on the Nature of the Firm', Strategic Management Journal. Vol. 27, No. 5, (2006), 461-47.
57. R.Coase, 'The Problem of Social Cost', The Journal of Law and Economics. Vol. 3, No. 1, (1960), 1-44.
58. R.K. Stamper, 'The LEGOL 1 prototype system and language', The Computer Journal 20.2 (1977): 102-108.
59. R.Šimašius, Teisinis pliuralizmas, dissertation, (The Law University of Lithuania. Vilnius, 2002).
60. S. Russell, P. Norvig, et.al., Artificial Intelligence. A Modern Approach, Third Edition (Prentice Hall: New Jersey, 2010).
61. S.G.Medema, R.O.Zerbe, The Coase Theorem, The Encyclopedia of Law and Economics, (Edward Elgar Publishing, 1999).
62. S.Ruester, 'Recent Developments in Transaction Cost Economics', EE2 Working Paper. Resource Markets. No. WP-RM-18, (2010), 1-47.
63. S.Schuster, M. Berg, et al., 'Mass surveillance and technological policy options: Improving security of private communications', Computer Standards & Interfaces 50 (2017) 76–82.
64. T. Kiseleva, B. Overvest, et al., 'Cyber Security Risk Assessment for the Economy', CPB Communication, Dutch National Cyber Security Centre, (2016, July 6).
65. T.J.Macher, B.D.Richman, 'Transaction cost economics: An Assessment of Empirical Research in the Social Sciences', Business and Politics. Vol. 10, No. 1, (2008), pp. 1-85.
66. T.Moore, 'The economics of cyber-security: Principles and policy options', Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academies Press. (2010).
67. T.Moore, R.Clayton, R. Anderson, 'The economics of online crime', Journal of Economic Perspectives 23(3): 3-20 (2009).
68. Vaišvila, Teisės teorija, (Vilnius: Justitia; 2004).
69. W. D. Henderson, R. M. Zahorsky, 'Paradigm Shift', A.B.A. J., July 2011.
70. W.M.P. van der Aalst, et al., ‚Process Mining Manifesto', in BPM 2011 Workshops proceedings. - Lecture Notes in Business Information Processing. Springer-Verlag, (2012).
71. W.M.P. van der Aalst, Process mining: Discovery, Conformance and Enhancement of Business Processe, (New York: Springer, 2011).
72. W.S.McCulloch, W.H.Pitts, ‚A Logical Calculus of the Ideas Immanent in Nervous Activity', Bulletin of Mathematical Biophysics, (1943), 115–133.

CASES

1. *Monique DA SILVA MOORE, et al., v. PUBLICIS GROUPE & MSL Group,* 868 F.Supp.2d 137 (2012), No. 11 Civ. 1279(ALC)(AJP). United States District Court, S.D. New York. June 15, 2012.
2. *USA v. In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300,* United States District Court, C.D. California, No. ED 15-0451 M 2016 WL 618401.

SANTRAUKA

Singuliarumas yra suprantamas kaip laiko ir skaičiavimo pajėgumo momentas, kuomet dirbtinis intelektas tampa lygus žmogaus intelektui. Singuliarumas yra ekonominė teorija, kuri vis dar yra vertinama nevienareikšmiai. Neatsižvelgiant į tai, ar žmonija pasieks singuliarumą, ar ne, yra akivaizdu, kad precedento neturinti technologijų plėtra iš esmės keičia visas žmogaus veiklos sritis ir socialines institucijas, įskaitant ir teisę. Teisė turi būti suderinta su technologiniais poreikiais ir galimybėmis bei skatinti tvarų technologinį vystymąsi. Tam yra būtina peržiūrėti esamus reguliavimo modelius technologinio singuliarumo galimybių kontekste.

Akivaizdu, kad tik dirbtinio intelekto sistemos turi realų potencialą išspręsti tūkstančius teisinių klausimų per sekundės dalį, naudojant tūkstančių didžiausių protų žinias, už arbatos puodelio savikainą. Tačiau technologinė plėtra turi ir egzistencinių pavojų. Kartu su gerovę didinančiomis technologijomis, tuo pačiu greičiu plečiasi ir kibernetinio saugumo pavojus keliančios sistemos. Siekiant sureguliuoti kibernetinio saugumo pavojus, vien technologinės plėtros neužtenka, kadangi tiek puolimo, tiek gynybos technologijos vystosi lygiagrečiai. Kibernetiniam saugumui reikalingas radikalus "atominis" sprendimas.

Šiame straipsnyje yra nagrinėjama problema, jog nėra aišku, koks reguliavimo modelis turi būti naudojamas kibernetinio saugumo reguliavimui besivystančių teisės technologijų kontekste. Atitinkamai, šio straipsnio tikslas – sudaryti konceptualų kibernetinio saugumo reguliavimo modelį ir jį įvertinti besivystančių teisės technologijų kontekste. Tyrimo objektas – kibernetinio saugumo reguliavimas.

Siekiant nustatyto tikslo ir išspręsti problemą, buvo iškelti trys uždaviniai. Pirmiausiai yra apžvelgiama esama kibernetinio saugumo problematika. Tam yra pateikiama mokslinės literatūros ir praktinių kibernetinių incidentų atvejų analizė, išskiriant žmogaus klaidų reikšmingumą kibernetiniam saugumui. Toliau šiame straipsnyje yra sudaromas konceptualus kibernetinio saugumo reguliavimo modelis. Šio modelio pagrindu yra sandorių sąnaudų teorija ir šias sąnaudas lemiantys veiksniai. Apibendrinus esamą reguliavimo modelį ir jo trūkumus, šioje straipsnio dalyje yra sudaromas konceptualus kibernetinio saugumo reguliavimo modelis. Trečiuoju uždaviniu yra vertinama ar pasiūlytas konceptualus modelis yra galimas, atsižvelgiant į teisės technologijų vystymosi eigą.

Sprendžiant šiuos uždavinius nustatyta, kad vien technologinėmis priemonėmis sustabdyti kibernetinio saugumo grėsmes yra neįmanoma, todėl reguliuotojas neturi kito pasirinkimo kaip didinti saugumą mažinant privatumą. Deja, tačiau kadangi daugiausia kibernetinio saugumo grėsmių kyla dėl žmogaus klaidų, būtina sukurti autonominį modelį, kuris tvariai valdant asmens duomenis

maksimaliai užtikrintų kibernetinį saugumą. Technologijomis grįstas reguliavimo modelis leistų kurti, stebėti ir vystyti teisės sistemas taip, kad jos leistų užkirsti kelią kibernetinėms grėsmėms. Šiame kontekste apžvelgus teisės technologijų vystymosi istorija ir tendencijas buvo nustatyta, kad dirbtinio intelekto sistemos yra plačiai naudojamos ir vystomos teisės praktikoje, kas atitinka bendrą technologinio progreso kryptį link singuliarumo. Ši analizė leidžia daryti prielaidą, kad esant pakankamam technologiniam išsivystymui, toks reguliavimo modelis galėtų maksimaliai užtikrinti kibernetinį saugumą, tuo pačiu apsaugant asmens duomenis nuo žmogaus klaidų.

REIKŠMINIAI ŽODŽIAI

Reguliavimas, kibernetinis saugumas, singuliarumas, teisės technologijos, sandorių sąnaudų teorija.