THE CHALLENGES, DANGERS, AND OPPORTUNITIES INVOLVED IN THE ENGAGEMENT BETWEEN TECHNOLOGICAL INNOVATION AND LEGAL REGULATION

Spyros-Nikitas Tsamichas // LegalTechnology
2019

UNIVERSITY OF MANCHESTER

The challenges, dangers, and opportunities involved in the engagement between technological innovation and legal regulation.

Introduction

The technological innovations of the 21st century in combination with impactful events at the capitalistic markets have altered the nature of the economy, services, and institutions rapidly. The above-mentioned set an unprecedented status quo, which needs to be legally regulated, in order to control the unpredictable development and application of technological advancements. The aim of this essay is to discuss the challenges, dangers, and opportunities involved in the engagement between technological innovations and legal regulation.

Industry 4.0

The reason people talk about a fourth industrial revolution known as Industry 4.0, it is mainly because of the emergence of artificial intelligence, the Cloud, Big Data a blockchain. Such technologies lead to a globally interconnected system, which aims for automation and data exchange. Briefly, the combination of these innovations enables the artificial collection, storage, and management of information, which is mainly used for/ services by the governmental, public, and private sectors. That is the part where the famous Latin aphorism which is attributed to Thomas Hobbes, "scientia potentia est", which means knowledge is power, became reality. By digitalizing private and public information, hence making it so easily accessible, a solid foundation was established for the creation of a new political and financial system.

Legal Regulation & Practical Application in the Legal Sector

The essential question is whether technology can be used to create a better system. Policymakers need to regulate expeditiously transformations of the financial system and technological sector, by relying on Regulatory Technology (RegTech) and Financial Technology (FinTech), which are based on information technology, by monitoring, reporting, and compliance.[1] The principal regulatory objectives of the policymakers aim for citizen protection, social/political/financial stability, prudential safety, soundness, market integrity, competition, and development.[2]

For example, the creation of Smart Contract Code and Smart Legal Contracts, create an agreement and a linguistic process, "whose execution is both automatable and

[1] D.W. Arner, J.N. Barberis, R.P. Buckley, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, University of Hong Kong Faculty of Law Research Paper (2016).
[2] Ibid.

enforceable, by computer, although some parts may require human input and control and by either legal enforcement of rights and obligations or tamper-proof execution respectively."[3] The aforementioned establishment was an effort to legally overwatch the blockchain system, by promoting exchanges (e.g. money, property etc.) in a transparent, conflict-free way.[4] However, there is highly critique over their means of application, since technological developments are leading towards a paradigm shift necessitating the reconceptualization of social and economic regulation.[5]

Currently, technology is "focused on the digitization of manual reporting and compliance processes, for example in the context of know-your-customer requirements with the least possible costs to the services industry and regulators."[6] Specifically, through Smart Contracts legal contracts can be expressed and executed in software, something that encompasses operational aspects that affect the legal written language.[7]

Furthermore, an increasing number of law firms have started applying artificial intelligence (AI), since its adoption boosts productivity and less monotonous tasks. In particular a few strong benefits of AI are legal research and due diligence, review of documents and contracts and prediction of legal outcomes in a short period of time. As long as such technologies are not used against clients, but mainly for better service and results, then the legal sector can evolve positively and be able to combat the following challenges and dangers of such innovations and focus on future opportunities.

Challenges

The challenges of this topic are based on the contradictory decision of the hierarchy of the society's priorities, like deciding whether national security is more important than individual privacy. For example, in order to detect possible terrorists, the State needs to inspect every move made by entities whose procedures and personnel are exempt from even remotely similar treatment, thus the promise of democracy and free markets rings hollow.[8] Unfortunately, even whistleblowers that uncover such misconducts, have to practice similar illegal techniques, like Julian Assange the creator of Wikileaks or Edward Snowden, who presented to the public undercover operations and classified information, such as the disclosure of global surveillance programs of

---

[3] C.D.Clack, V.A.Bakshi and L.Braine*, Smart Contract Templates: foundations, design landscape and research directions*, (2016).
[4] Terry Parker, *Smart Contracts: The Ultimate Guide To Blockchain Smart Contracts – Learn How to Use Smart Contracts For Cryptocurrency Exchange*!, (2016).
[5] Ibid.
[6] Ibid.
[7] J. Stark, *Making sense of blockchain smart contracts*, (2016), <https://www.coindesk.com/making-sense-smart-contracts>.
[8] Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information,* Harvard University Press, (2015).

the National Security Agency (NSA) and Central Intelligence Agency (CIA), the mistreatments during the Afghanistan war or the Guantanamo Bay, the corruption in Kenya and the hacking of political campaigns in the U.S.

The areas in which Big Data looms largest in our lives are reputation, search and finance. For example, credit card companies are currently able to decide whether to raise a couple's interest rate if they seek marriage counseling, without the cardholders being aware of such changes.[9] Moreover, websites like YouTube or Facebook algorithms have shut out channels and pages that promote conspiracy theories or right wing ideologies, like the channel 'Infowars' by Alex Jones, Milo Yiannopoulos[10] or the Greek political party Golden Dawn[11], despite being legally elected into the parliament. The above-mentioned actions matter because authority is increasingly expressed either by a company's board or autonomously algorithmically.

Furthermore, society is facing the problematic creation of monopolies by a minority of companies, like Google, Facebook or Apple which centralize various powers, by evolving and dominating in different sectors, such as source of information, social networking and communication. Such companies advertise products and news according to the users' data and cookies. Therefore, there is a justified feeling of aggressive antitrust enforcement in tech industries.[12] On the other hand such companies, due to their popularity, have the ability to promote global communication, information and awareness about social, political, financial and environmental threats.

Additionally, some countries trying to adopt a new legal system that will fight crime more efficiently, have started using AI robots as police officers, judges and juries, due to their impartiality and faster process and review of events. However, the fact that such projects are programmed by humans or that they do not own consciousness and the sense of fairness, equality and justice according to the current social standards, could create a huge problem in the decision of cases and who is opposing a threat.[13]

We cannot so easily assess how well the engines of legal processing, reputation, search, and finance do their jobs. It is practically impossible to test whether their judgments are valid, honest, or fair. The designation of a person as guilty, or a bad employment prospect, or a website as irrelevant, or a loan as a bad risk may be motivated by illicit aims, but in most cases we'll never be privy to the information needed to prove that.[14]

---

[9] Ibid.
[10] https://www.theguardian.com/technology/2019/may/02/facebook-ban-alex-jones-milo-yiannopoulos.
[11] https://www.euronews.com/2018/06/15/golden-dawn-gets-greek-parliament-ban-after-call-for-military-coup-
[12] Ibid.
[13] https://www.bbc.co.uk/news/av/technology-37749697/could-ai-replace-judges-and-lawyers
[14] Ibid.

Dangers

There are theories that argue that Government agencies, businesses, financial institutions and internet companies follow proprietary methods in order to keep their actions in secrecy under nondisclosure agreements, while the privacy of the individual is exposed, without him usually acknowledging it. This brings us to the following questions; that since all online actions are recorded, who has access to them, for how long, how they can use this data and what kind of authority should overwatch them.

Online users can apply anonymizing software at their devices, but this is a short-term solution. For example, browsing history and cookies can record users' actions and then through an algorithm promote relevant advertainments accordingly. Companies seek out personal details of potential customers' and employees', but they do not disclose to regulators information about their own statistics and procedures.[15]

The decline in personal privacy might be worthwhile in the name of national security or if it dealt with transparency from corporations and government. Unfortunately, security services, cameras, search engines, credit raters, major banks, and the take in data about us and convert it into personal files, scores, rankings, risk calculations, and watch lists with vitally important consequences, aiming to the overwatch of citizens or higher profit, like deciding whether they are a threat on unbiased reasons or the terms of credit and debt.[16] Modelling of online usage is even worse when unfair or inappropriate considerations combined with the power of algorithms create the failures they claim to merely predict, like considering individuals as security threat or credits risks by inaccuracies. Such errors could become systemic like the financial crisis of 2008.[17]

Unfortunately, the current legal system does not take proper measures to combat the threat of privacy. Specifically, the imposition of fines up to a few millions to Google and WhatsApp, which were found guilty by the EU for advertising violations and sharing personal information to third parties, [18] is not enough since such a financial loss is equal only to a few hours of their revenue. This failed model leads to minimal consequences to the companies responsible. The simply digitalizing analogue processes in a digital world could be described by inadequacy.[19]

It also demands an understanding of the companies that influence our government and culture. The infamous case of Cambridge Analytica scandal, which played a

---

[15] Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information,* Harvard University Press, (2015).
[16] Ibid.
[17] Ibid.
[18] https://www.theguardian.com/technology/2019/mar/20/google-fined-149bn-by-eu-for-advertising-violations.
[19] McKinsey on Digital Services, *Introducing the next-generation operating model*, 22 April 2018.

significant role in the U.S elections, proves that political campaigns apply such technologies, which enable them to combine data mining, data brokerage and data analysis with strategic communication during the electoral processes, without the public's awareness and permission.

Opportunities

Despite the hidden dangers, the same innovations can be used to protect and advance the society. Specifically, directed at the right targets, data mining and pervasive surveillance might even prevent the kinds of terrorist or financial crises and massive misallocations of resources that have devastated the U.S and European security and economy over the past decade.[20]

Public values and restrictions in Internet, Campaign, Marketing and Finance companies should be promoted, by drawing on best practices in other, more regulated sectors. Regulators should be deploying technologically savvy contractors to detect and deter fraud, abuse, and unnecessary treatments.[21]

Surveillance technology should be used for transparency, by monitoring and containing governmental and corporate greed, waste, unfair competitive or discriminatory practices and misconduct. Public options in technology and finance would make our social world both fairer and more comprehensible.[22]

Public options in search and finance need to be developed to create spaces not only for transparency, but for intelligibility as well.[23] The development of financial technology, the rapid developments in emerging markets, and the recent pro-active stance of regulators in developing regulatory sandboxes,[24] represent the ability to transit from the current regulatory model to a safer one. RegTech has the potential ability to enable a close to real-time and proportionate regulatory regime that identifies and addresses risks, while facilitating far more efficient regulatory compliance.[25]

One of the most important issues is what kind of authority will be responsible for the control and overwatch of these technological innovations. In order to solve that, the European Union created the General Data Protection Regulation (GDPR), which aims

---

[20] Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information,* Harvard University Press, (2015).
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Pistor, Katharina, *Towards a Legal Theory of Finance,* Columbia Public Law Research Paper (2012).
[25] D.W. Arner, J.N. Barberis, R.P. Buckley, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, University of Hong Kong Faculty of Law Research Paper (2016).

to "fundamentally reshape the way in which data is handled across every sector, from healthcare to banking and beyond."[26]

Conclusion

The stoppage of the constant technological innovations is unavoidable, hence the social implications that they have created, need to be combated by securing a balance between privacy and openness. Demands for dignity, due process, and social justice are controversial, since there will always be holders of vested privilege who prefer not to share.[27] The transformative nature of technology will only be captured by a new approach that sits at the nexus between data, digital identity and regulation.[28] Citizens should not be part of a society where hidden data determine and manipulate the fates of individuals, businesses and financial theories like the "invisible hand". Therefore, currently the only solution is that all future applications of technological innovations should be written at the constitution of each company and be overviewed by a body of legal regulators in order to be approved by the court, rather than wait till implications and consequences start impacting the society.

[26] EU GDPR, <https://eugdpr.org/>.
[27] Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information,* Harvard University Press, (2015).
[28] D.W. Arner, J.N. Barberis, R.P. Buckley, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, University of Hong Kong Faculty of Law Research Paper (2016).

Bibliography

Alasdair Sandford, *Golden Dawn gets Greek parliament ban after 'call for military coup',* <https://www.euronews.com/2018/06/15/golden-dawn-gets-greek-parliament-ban-after-call-for-military-coup->

Alex Hern, Jasper Jolly, *Google fined €1.49bn by EU for advertising violations,* <https://www.theguardian.com/technology/2019/mar/20/google-fined-149bn-by-eu-for-advertising-violations>

Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P., *FinTech, RegTech and the Reconceptualization of Financial Regulation,* Northwestern Journal of International Law & Business, (October 1, 2016)

C.D.Clack, V.A.Bakshi and L.Braine*, Smart Contract Templates: foundations, design landscape and research directions*, (2016)

European Union General Data Protection Regulation, <https://eugdpr.org/>

Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information,* Harvard University Press, (2015)

J. Stark, *Making sense of blockchain smart contracts*, (2016), <https://www.coindesk.com/making-sense-smart-contracts>

Kari Paul, Kim Waterson, *Facebook bans Alex Jones, Milo Yiannopoulos and other far-right figures*, <https://www.theguardian.com/technology/2019/may/02/facebook-ban-alex-jones-milo-yiannopoulos.>

McKinsey on Digital Services, *Introducing the next-generation operating model*, (22 April 2018)

Nikolaos Aletras, *Could AI replace judges and lawyers?,* <https://www.bbc.co.uk/news/av/technology-37749697/could-ai-replace-judges-and-lawyers>

J. Stark, *Making sense of blockchain smart contracts*, (2016), <https://www.coindesk.com/making-sense-smart-contracts>

Pistor, Katharina, *Towards a Legal Theory of Finance,* Columbia Public Law Research Paper No. 12-323 (November 18, 2012).

Terry Parker, *Smart Contracts: The Ultimate Guide To Blockchain Smart Contracts - Learn How To Use Smart Contracts For Cryptocurrency Exchange!,* (2016).