Law and Digitalisation: Rethinking Legal Services

EDITED BY RIIKKA KOULU & JENNI HAKKARAINEN

LEGAL
TECH
LAB .fi

2018

Law and Digitalisation: Rethinking Legal Services

EDITED BY RIIKKA KOULU AND JENNI HAKKARAINEN

Acknowledgments

First of all, the editors and the University of Helsinki Legal Tech Lab would like to thank the authors for the time and effort they put in to their papers.

In addition, we would like to thank the University of Helsinki, Faculty of Law and professor/former dean Kimmo Nuotio for assisting us with making the conference happen.

We would like to express our special gratitude for law firm Dittmar & Indrenius for their support in turning an idea of an event into reality and for their support with this publication.

For their effort in collecting and editing this publication, we would like to thank student volunteers Lila Kallio and Nazanin Gifani for their contributions in commenting on the papers in section III. Thank you Laurence Lawson, also a student volunteer, for proofreading all the articles. And lastly, thank you Legal Tech Lab's coordinator Aapo Asp for editing the layout.

Finally, a massive thank you to everyone who made the Law and Digitalisation conference happen. Thank you to the attendees, those who followed us via streaming, speakers, volunteers and Legal Tech Lab crew members.

RIIKKA KOULU & JENNI HAKKARAINEN
Legal Tech Lab, University of Helsinki

Conference sponsored by:

DITTMAR & INDRENIUS

LEGAL TECH LAB .fi

2018
University of Helsinki Legal Tech Lab publications

ISBN 978-951-51-4247-4
Print Veiters
Helsinki 2018

Contents

Foreword

‘Law and digitalisation’ is becoming a catch-word in the legal circles. It is a merger and we all read our own meanings into it.

Law and digitalisation sounds like future. Law, as we know it, will change when we learn to use modern tools in processing it. It will change. The question is rather: How will it change?

Universities should be places where the future is being made, or if not made, at least being discussed and theorized. Faculties of law tend to be somewhat traditional, as is the legal profession. It feels good to get rid of some of the dust.

In Fall of 2017 the weak signals had become louder, and the Faculty of Law of the University of Helsinki took the initiative to start a Legal Tech Lab in order to explore the field. We needed a host of collaborators since much of what was needed in this exercise had been developed if not completely outside, at least at the outskirts of the academia.

In the beginning we only had the idea and one person, Riikka Koulu, who had agreed to work on this idea. She was stunningly energetic. We were fortunate to get positive feedback from those

who knew more. The students also saw the chance to learn and do new things. The ball started rolling.

The idea was developed that we should try to set agendas. Our agenda became clear: law and technology should not be left in the hands of engineers only. We lawyers should try to learn enough to have our fingerprint in what happens.

This conference is now the launch of the Legal Tech Lab activities. It is the real litmus test. What we aim is actually not only to discuss the ways technological developments are transforming, and will transform legal practices. We wish to introduce a lawyers' professional and ethical perspective on this transformation.

Adoption of new technologies should always serve ethically sound purposes. We could, for instance, try to develop new tools facilitating access to justice. We could design technologies to help non-lawyers to get to their rights.

Already the first steps that we have taken indicate that this is going to be a long journey. With enthusiastic people the journey could be fun.

There is plenty of terrain to be explored. I'm glad that you are willing to join us in this effort. I wish you good luck, Legal Tech Lab, the entire crew, as well as everyone involved!

KIMMO NUOTIO
Professor, Former Dean of the Faculty of Law
University of Helsinki

I

Towards Legal Technology Studies

RIIKKA KOULU AND HANNA PAKASLAHTI[1]

Why We Need Legal Technology

1 INTRODUCTION

1.1 WHAT IS THE LEGAL TECH LAB?

During the last decade, the buzz around the law and technology field has increased exponentially. At times, the hype takes on optimistic tones, when technology is perceived to be the silver bullet that solves all the shortcomings of our justice systems.

1 Riikka Koulu is an assistant professor of Law and Digitalisation at the University of Helsinki and the director of the University of Helsinki Legal Tech Lab. LLM Hanna Pakaslahti is a project developer at the Lab. Koulu has contributed particularly to sections 1, 3 and 4 and Pakaslahti to section 2.

Occasionally and, it seems, more and more often, these conversations are tinted with apprehension and even warnings against the ethical consequences when technology is used in society's core areas, such as the legal system.[2]

What exactly does the digitalisation of law entail? Despite the rapidly growing body of literature on the subject, much remains unsaid and undiscovered. Some venture to predict the future of law by pointing out development trends, while others turn to history of technology to find answers. This much can be said: digitalisation of law in a multifaceted, ongoing, and highly complex set of related and unrelated phenomena. Some of the new legal technologies do contest the existing legal frameworks and conceptualisations, demanding reinterpretation and new governance models, whereas the use of other applications signify mainly new tools for the same tasks and fine-tuning of established legal practices, at most. In order to understand the ongoing transformation, we urgently need information that can be compiled only as a joint venture.

We need windows and glimpses to different worlds, academic research as well as practitioners' perspectives to the reality of this complex phenomenon. This need for information is the reason behind creating the University of Helsinki Legal Tech Lab in November 2016. The Legal Tech Lab's first public event and the unofficial coming out party was the Law and Digitalisation conference held at the University of Helsinki on June 9, 2017. This collection of articles and short essays you are holding is based on the topics discussed during that conference.

This introductory article presents the work and objectives of the Legal Tech Lab. It is argued here that we need new ways of doing legal science if we are to tackle the challenge posed to

2 Alex Campolo, Madelyn Sanfilippo, Meredith Whittaker, Kate Crawford, 'AI Now Report 2017' <https://ainowinstitute.org/AI_Now_2017_Report.pdf> accessed 15 March 2018.

the legal system by rapid technological innovation. The article consists of four parts in addition to brief concluding remarks. In the first section, we introduce the Legal Tech Lab and describe how different trends in the vibrant legal technology field came together in the 2017 conference. In section 2, we map out the possibilities to increase access to justice with the use of legal technology. Section 3 explains why, for this to succeed, we need more lawyers who have a deep enough understanding of technology and how this need intersects with the Lab's pedagogic objectives. In section 4 we demonstrate, how the potential of technology and the need for technologically inclined legal professionals can be incorporated into an emerging field of legal study, ie. law, technology and society studies. Here, we elaborate the core areas where research on these intersections are needed and present some remarks on the issue of methodology and interdisciplinarity.

Finally, we provide some concluding remarks that pave the road forward. The University of Helsinki Legal Tech Lab focuses on the intersections of law, technology and society. Research, experimentation and the resulting clarification of concepts and the following better understanding of the field are the main objectives of the Lab's research agenda. The Lab aims to increase awareness on the impact of technologies on law and to bring new insights and also critical views to the discourse on digitalisation of law in order to enable responsible digitalisation. The Lab combines academic research and teaching with experimentation and practical knowhow to create more agile ways to produce information that would serve more efficiently the needs of society and the legal profession.

The Lab consists of networks of research projects and researchers working on various areas of law and technology, most of whom are affiliated with the Faculty of Law of University of Helsinki. Within the university, the Lab is also a part of the

Helsinki Centre for Digital Humanities, the HELDIG community.[3] In addition to research networking, the Lab is a spearhead for external collaboration across disciplines, faculties, universities and outside of academia. Still, scientific inquiry into theories and methods legal digitalisation forms the Lab's core. Connections to non-academic actors from policy makers to legal practitioners are maintained through the Lab's Advisory Board and multiple contacts and collaboration with relevant stakeholders. Student engagement is encouraged by including a vibrant group of student volunteers in the Lab's daily activities and events. The Lab promotes an open science culture and societal dialogue on legal digitalisation through its activities. Where possible publications and research are online for easy and open access to all.

The Lab seeks to produce scientific knowledge about the digitalisation of law and to provide standards for responsible legal technology and policy recommendations. This task is divided into three steps. Firstly, we seek to define what digitalisation of justice entails and means by researching the changes affecting legal systems and the legal profession. This includes examining developments in the public services as well as extra judicial technological applications that have a direct or indirect impact on citizens and their legal rights for better or worse. We are also examining the profession as a whole but also from the point of view of different types of practising lawyers from the private and public sector alike. Secondly, we aspire to use and experiment with this information to formulate future best practices and guidelines for dealing with these changes. This is a complex task since the interests among different groups differ and the demands of law's end-users are not always easily met whilst also preserving the integrity of the core legal principles such as the

3 See, Helsinki Centre for Digital Humanities <https://www.helsinki.fi/en/helsinki-centre-for-digital-humanities> accesed 15 March 2018.

rule of law and due process. The third step is to develop concrete technological tools for legal practice that by design are adoptable and easy to use and thus facilitate better access to legal rights and just processes.

One of the Legal Tech Lab's objectives is to raise awareness of the need to shift the focus from the needs of legal institutions and established practitioners to the needs of law's end-users and how digitalisation of law can provide opportunities in this direction. The change of focus is needed, as the use of technology does not always comply with existing legal concepts and principles, regulatory frameworks or judicial redress mechanisms. If we are to take seriously the potential of legal tech to improve individuals' access to justice, we must look beyond these existing legal structures and find novel ways to provide legal protection in changing digital environments with the assistance of legal technologies. The Lab's work began with the Law and Digitalisation conference and, although many interesting topics were covered, equally as many still await for further dialogue. In this book, we discuss some of the themes raised in the conference and how these insights can be incorporated to the Lab's research agenda. This book attempts to paint a vivid and multifaceted picture of legal digitalisation and of the topics explored at the conference with the intention of introducing the reader to the diversity of discussions around the future of law. We hope that these insights on their part provide useful starting points for better understanding of the the different facets of this ongoing change.

1.2 THE LAW AND DIGITALISATION CONFERENCE 2017

The Lab sought to accomplish two distinct objectives by organising the Law and Digitalisation conference. Firstly, to act as a conversation starter and platform for discussion nationally, and secondly, to engage and spearhead in the international

discourse of theoretical foundations of the field of law and technology, the transformation of legal work and online access to justice. The conference was held at the University of Helsinki, Finland in June 2017. The event was one of the first of its kind in the Nordic countries.

The arising legal tech scene in Europe is about embracing dialogue between practitioners, academics and students.[4] It also aims to mix lawyers with startups and experts from different technological fields. The difficulty in this collaboration is that legal technology involves a massive variety of fields both in the meaning of legal disciplines but also such fields as computer science, data analytics, business management and service design. Attorneys, in-house counsels and policy makers all have different interests, needs and stakes in the development of legal technologies. This is why it is important to approach the issue through stakeholder models and themes based on interests of parties involved and not only by challenges associated to specific fields of law. A point of interest is that the Nordic legal cultures have traditionally emphasized the importance of the welfare state as the provider of legal rights and freedoms. This means that the public sector is a focal stakeholder in discussions over legal digitalisation.

How were these goals achieved in the Legal Tech Lab's first conference? By bringing as many stakeholders as possible to the university to an inclusive and neutral atmosphere to discuss what legal digitalisation in all its forms will constitute for the legal profession and the larger society as well. For a balanced approach it was important to not only discuss threats and challenges but also to highlight and explore the potential in engaging different new technologies to make law better. It is also important to

4 See e.g. Markus Hartung, Micha-Manuel Bues & Gernot Halbleib, Legal Tech: Die Digitalisierung des Rechtsmarkts (C.H. Beck: München 2018) ch. 1.1 Gedanken zu Legal Tech und Digitalisierung, 5-18.

clarify the nature of the claimed improvements and assess them critically before trying to implement any best practices. For example, the goal of the access to justice movement to make conflict management in society more user-friendly and more accessible both in cost and time seems to be achievable by utilizing different technology tools and online services. However, we need more discussion on the long term and overall effects before a conclusion of the pros and cons of legal technology in different cases can be made. Online dispute resolution and its promise, the expectations placed upon its impact and real life outcome will be discussed further in the next section.

The conference set out to ambitiously explore both the potential of technology for access to justice as well as the dangers associated with the unpredictable or still unknown effects of digitalisation. Dr Gavin Wood's presentation on the concept of allegality explored where decentralized ledger technologies enable complex networks of transactions without the maintenance of central authorities (law without the state); In this collection, key points of allegality are discussed in an article written by Jenni Hakkarainen and Nazanin Gifani, two PhD students affiliated with the Lab. The conference ended in a balancing presentation by Dr Gemma Galdon Clavell. Her message included words of warning against the loss of privacy, freedom of thought and unlimited corporate power - leading up to a call for action for sustainable digitalisation. She also encouraged us to think of technological threats in proportion to real life scenarios. An example she gave was autonomous cars; when discussing accidents where such vehicles have been involved in, the overall probable and far more important effect of an substantial increase in road safety because of abolished human errors is ignored.

This publication includes also an article on the outcome of the Disruption and Regulation panel that mapped out the transformation of the legal profession and examined how

development of legal tech is affected by the strictly regulated nature of legal services. The panelists represented a variety of legal professions. Partner and head of IPT of DLA Piper Finland Markus Oksanen provided the perspective of law firms, whereas CPO Hannele Korhonen from the legal tech startup Contract Mill brought insights into the startup scene. The potential and challenges associated with public software procurement were described by Marko Loisa from the Ministry of Justice. Fintech influencer Kirsi Larkiala presented views on financial technology, another strictly regulated field that is undergoing significant changes due to technology. Participants' discussion and conclusions are here described and compiled in a short article written by the panel's moderator Hanna-Mari Manninen from Dittmar & Indrenius Attorneys Ltd. Hannele Korhonen writes about the rise of the legal tech startup scene. Her article and topic are describing the other end of the continuum of changes in the legal landscape induced by technology, the introduction of new entrepreneurial and business models to the field. Marko Loisa then lets the reader in on what is happening in the Finnish Ministry of Justice in his article on how the public court system is developing new tools for digitalisation.

The conference also displayed its mission to include students as well as bringing all stakeholders to scientific events. A way to accomplish the pedagogical mission was the idea of organising a Call for Papers for the student panel designed for LLB and LLM students, which would give students interested in law and technology themes a prestigious venue to present their work. Among the applications, three winners were chosen to be coached to present their papers at the conference's student panel. The students continued working on their papers to produce articles for this publication. These papers include Kristina Svinhufvud's contract law article in which she discusses the regulation of autonomous algorithms from contract law perspective, using high-frequency trading as her starting point. In turn, Iiris Kestilä

evaluates the patentability of blockchains in light of the European Patent Convention. Alexandra Shtromberg's article deals with data privacy challenges of remote legal work.

Another concrete purpose the 2017 conference served was to bring forth and recognise the stakeholders interested and invested in legal digitalisation and the development of an inclusive conference platform to encourage dialogue in the spirit of open science.

1.3 WHAT HAS HAPPENED SINCE THE CONFERENCE OF 2017?

The conference was a coming out party for the University of Helsinki Legal Tech Lab. Since the conference, the Lab has established itself as a leading national actor as well as gaining international recognition in the emerging field of law and digitalisation. A key point during the The Legal Tech Lab's first year of operation was to provide understanding and an overview of the complex transformation brought on by legal digitalisation and to recognise what issues should be addressed and continued to be researched.

The Lab's pedagogical objectives are pursued continuously by involving students in all aspects of the lab's work, from creating events, assisting in research, raising funds and executing projects. Student volunteers work in teams and all projects are discussed in general meetings. The students' input is a valuable resource for the lab and the organizational hierarchy is kept to a minimum. Everyone has the power to impact the decisions and partake in discussions. This same inclusive and inviting spirit is why we feel that it is important to encourage and empower students to attend and contribute to scientific events early on. It is important to give students the chance to partake early on in legal technology discussions to ensure the vibrance and growth of the academic field. We are happy to say that the year after the

conference of 2017 it was often mentioned as the first encounter with the field of legal technology and also as the definite spark of interest to further explore this area of legal studies.

The Legal Tech Lab has expanded its outreach by collaborating with many different partners on different research projects as well as in organizing workshops, events and other activities to also developed further its goal of bringing experimentation culture and agile development to both research and teaching. By utilizing the inclusive low hierarchy working culture of the Lab and by reacting fairly quickly to invitations to participate we managed to reach a wide audience and to increase the societal impact and scope of the Lab. One concrete example of the experimentation culture that has previously been foreign to legal studies in Finland was the weekend-long Hack the Law! student hackathon in October 2017. The idea was to bring interdisciplinary student teams together to developed concepts and prototypes to improve citizens' access to legal information - a problem recognised through the Lab's empirical study questionnaire to 1000 Finnish residents.[5] In all its activities, the Lab emphasises the close connection between concrete legal tech development and scientific research on legal digitalisation.

5 Riikka Koulu, Jesse Heiskanen & Sonja Vainio, 'We Hacked the Law! - Oikeusjärjestelmän käyttäjäkokemusta parantamassa' [2018] Edilex <https://www.edilex.fi/artikkelit/18531> accessed 9 March 2018.

2 TOWARDS ACCESS TO JUSTICE WITH LEGAL TECHNOLOGY?

2.1 WHAT IS LEGAL TECHNOLOGY?

Legal Tech is a fairly new term and the overall terminology and taxonomy of terms are not yet clearly established. The discussion about law and technology, however, is not new. Already in the 1960s when automated data retrieval was yet to become a mainstream tool, the possible effects of information technologies and their application in legal processes were being discussed.[6] In spite of the newness of the terms used today we have decades of experience and research on the adoption of technology to legal processes using various different names and classifications. This section focuses on legal technology and discusses briefly the often-encountered assumption that the use of technology improves access to justice.

The broad definition of legal technology used in the Lab's work refers to information and communication technology (ICT) tools used in legal operations and decision making processes. These include but are not limited to software applications developed for legal practitioners, courts, government officials and legal research. Some examples can be found in case management systems, decision support tools, e-discovery and videoconferencing tools, virtual data rooms, risk assessment software, automated document generation as well as in smart contracts and predictive analytics, to name but a few. Some of these technological tools focus on automation of routine tasks, where others aim to provide new solutions for the shortcomings of national legal systems, as is the case with online dispute

6 For example: Robert A. Wilson, 'Computer Retrieval of Case Law' [1962] Southwestern Law Journal 409-438.

resolution which in some forms is pushing and challenging the boundaries of state-based jurisprudence.[7]

The use of ICT tools seems to be very impactful in areas that traditionally have not been classified as strictly legal processes. Naturally, the classification of what constitutes a legal process depends on perspective. In the Lab's comprehensive work, we are not referring to a strict legal definition of legal decision making, as might be the case if the perspective was of any specific field of law, but rather to all processes that are available to uphold and reach an individual's legal rights and others claims on them. It suffices to say that the greatest developments thus far for the laypersons have been in the area of accessing justice by technological means. Good examples include the DoNotPay chatbot for disputing parking tickets and different flight compensation services, such as AirHelp and Flightright. These same areas are underserved by the legal profession and public courts simply because it has been too expensive and/or time-consuming to address them. Another question can be posed. Is it actually justice that is accessed or just better information or a more convenient path to already existing legal remedies? The terminology used adds to the confusion and is not consistent throughout the field yet.[8] Clarification of some terms is attempted in this article as well as addressing the issue of access more thoroughly.

One may thus argue that when we talk about legal technology, legal tech in short, the more important term of the two to define is in fact 'legal'. What do we define as legal and how the definitions differ depending on the perspectives, i.e. from citizen to legal

7 See more, Koulu, Heiskanen & Vainio 2018 (n 5). Also, Riikka Koulu, Dispute Resolution and Technology: Revisiting the Justification of Conflict Management (COMI 2016). For more information on definitions and examples of legal technology, see Hartung 2018 (n 4), 9.

8 For example: Riikka Koulu, 'Missä viipyy välimiesmenettely', Defensor Legis 2017, 647-660, 649.

professional. Scalable technological solutions such as chatbots are a simple and often effective way to increase access as well as the experience of having access.[9] From the professional point of view of a lawyer, these tools can hardly even be described as legal services as they actually do not include any actual case specific legal advice.[10] Some services can be described as more administrative procedures[11] or customer complaint management.[12] However, using these methods may solve a legal issue, an access to rights issue more effectively even if the process used can not strictly procedurally be categorized in any traditional way. So lawyers are blind to the legal issues that are usually not handled by the legal profession and tend to think in terms of how issues would be analyzed in court or by a judge. However, most issues for laymen, and you could even say end-users of the legal system, never end up in court. For the end-users of the legal system, i.e. laypersons, any issue where their legal rights are challenged and they find themselves at loss with available remedies is a legal issue.

A prominent example of access to justice is Online Dispute Resolution, ODR, a branch of conflict resolution that focused first on processes and services provided online using various ICT tools to resolve conflicts that, for most part, arose in e-commerce and were difficult to resolve otherwise because of the distance between parties, possibly situated in different jurisdictions, and the relevantly low financial interest at stake.[13] The discussion around ODR has evolved into a nuanced approach that takes into

9 Hanna Pakaslahti, The Costs of Resolving Conflicts Online (University of Helsinki Legal Tech Lab 2018) 63, forthcoming at: <www.legaltechlab.fi>.
10 This discussion is related to the French legal tech startup Demander Justice, which is discussed in further detail in section 3.
11 Taina Pihlajarinne, Riita verkkotunnuksesta: UDRP-menettely vaihtoehtoisena riidanratkaisuna (University of Helsinki Conflict Management Institute 2007)
12 For example eBay see Koulu 2016, 147.
13 See for example Pablo Cortés, Online Dispute Resolution for Consumers in the European Union (Routledge Research in IT and E-Commerce Law 2010) 51-56.

account a number of challenges and also advantages of speeding up and altering conflict resolution with the use of technology.[14] Also different modes of enforcement as deciding factors behind the success and failures of different models have been studied.[15] Further, there are significant differences between processes that were originally developed with human offline interaction in mind and were later partly or wholly made available online or even automated, and processes that are designed from the start particularly for online use.[16]

One of the key assumptions of at least early ODR was that it would make the processes much more affordable for not only users but also for providers to offer. There was a boom of private ODR services in late 1990s. However for a number of reasons only a few actually became profitable and survived. The promise of profitably produced[17] high quality universally standardised[18] private online dispute resolution seems elusive at the moment and this may be a reason behind the increasing interest in digitalisation of public services and resolution

14 See e.g. Ethan Katsh and Janet Rifkin, Online Dispute Resolution: Resolving Conflicts in Cyberspace (John Wiley & Sons, Inc. New York, NY, USA 2001).

15 Cortés p. 82,204, Thornburg p. 106, Kaufmann-Kohler and Scultz, 223-233. For a comprehensive look at enforcement mechanisms see Koulu 2016.

16 Dispute Resolution System Design is a field of it's own. See closer, Ethan Katsh and Orna Rabinovich-Einy, Digital Justice: Technology and the Internet of Disputes (Oxford University Press 2017).

17 In early 2017 ODR provider Modria announced that the highly acclaimed ODR platform cannot be profitably upheld. See closer, <https://www.legalfutures.co.uk/latest-news/pioneering-odr-platform-to-rein-in-ambitions-after-commercial-setback> accessed 9 March 2017. Modria has recently pivoted towards offering its solutions mainly to courts, see <https://www.tylertech.com/solutions-products/modria/history> accessed 9 March 2017.

18 For example, one problem UNCITRAL's work on ODR rules encountered was the contrasting opinions of different jurisdictions towards pre-trial arbitral clauses in business to consumer disputes. See e.g. Riikka Koulu, 'One Click Too Much? Thoughts on UNCITRAL's Work on ODR Rules', (Cyberjustice Laboratory Blog 12 March 2015) <http://www.cyberjustice.ca/actualites/2015/03/13/one-click-too-much-thoughts-on-uncitrals-work-on-odr-draft-rules-part-ii/> accesed 15 March 2018.

methods and developing private services to aid access to already available public services. In the following section we explore how technology can indeed help in increasing access both to legal services and legal information.

Apart from the underlying funding issues, trust has always been a big issue in successful conflict resolution. The citizens simply trust, in general, governmental and public bodies more when it comes to solving disputes and guaranteeing due process. Trust is central also in other legal tech applications. If used "under the hood" to speed up labor intensive tasks in law firms newer technologies will probably not pose an immediate problem since clients are not necessarily fully aware of or interested in the tools used to get the job done. However as soon as technology is used to replace direct human contact or judgement altogether aversion to use such methods and tools may indeed arise. The growing awareness of technologies inherent biases and questions about algorithmic fairness are unsolved issues in the way of adopting more technology to crucial legal processes. In the next chapter we will explore this topic further.

2.2 HOW CAN LEGAL TECHNOLOGY IMPROVE ACCESS TO JUSTICE?

One arising issue when talking about legal technology is always its disruptive effect on the legal market and established models of providing legal services. However a legal system is not an open market and it is governed by its own, yes indeed, laws. These laws have an profoundly limiting effect on using possibly disruptive technologies and alternative service models. Providing legal services is still far more regulated than many other industries and engaging in public dispute resolution processes such as courts is regulated even more so. Technologies' disruptive properties and the potential embedded in their use for transforming legal practices is closely connected with the applicable laws of each

jurisdiction. If technological solutions are used directly to replace legal professionals and existing business models, they must be compliant with the regulatory limitations on the provision of legal advice.[19] There is a need for legislative reform on legal services in case we hope to encourage the development of truly alternative models of legal services.[20] One can argue that because of existing regulation, from a societal point of view, the most impactful legal tech is manifested today in areas that are not traditionally serviced by legal professionals and thus do not fall into the scope of any legislation pertaining to the legal profession.[21]

With the regulatory limitations of legal services in mind, in which cases does technology actually increase access to justice? A good example can be found in the different flight passenger right applications where you get to claim your compensation from an airline in cases where EU or American federal sanctions apply.[22] A number of these services are available for the consumer and they service a field where the airline-denied claims have been far too difficult because of the relatively small value of the claims compared to costs of going to court. In some countries the airline passenger claims are handled free of charge by consumer authorities but even this process is often thought ineffectual and slow in handling these cases. Another example

19 The regulation has an outward aim of safeguarding legal subjects and their access to legal redress by providing minimum standards for quality of legal advice. However the actual effect of regulation is that some of the services and processes are of no help to the citizen because of high cost or other difficulties in access.

20 Joanna Goodman: 'The UK Legal Tech Scene' in Hartung, Bues, Halbleib (eds) 2018 (n 4). Joanna Goodman argues that the rise of legal tech evident in the UK was in fact the result of opening up the legal services market with the 2007 Legal Services Act and the introduction of Alternative Business Structures (ABS) as means of providing legal services.

21 Thomson Reuters 'Movers and Shakers: UK Lawtech Start-ups' (2017).

22 E.g. AirHelp <https://www.airhelp.com/en/know-your-rights/> accessed 9 March 2018 and FlightRight <https://www.airhelp.com/en/know-your-rights/> accessed 9 March 2018.

could be the chatbot for disputing parking tickets; DoNotPay[23] is an effective yet simple solution to aid consumers in accessing already existing public recourse in a more user-friendly way.

These access services are a natural development on the continuum of digitalisation of dispute resolution after it has become apparent that placing legal services online is neither simple nor necessarily cost efficient. At the moment, as far as ODR is concerned, the most viable and at the same time also the most user friendly business models private providers employ are the ones that aid users in negotiations and later connect users to public dispute resolution or to services provided by legal professionals. On the same note, another growing trend is legal design which emphasizes the importance of thinking about the end user in all processes and applications in the legal field. This is revolutionary in a sense that many legal processes are in fact constructed for legal professionals, not the actual end-users.[24] Design thinking starts by examining the needs of the user and brings forth the human and not the technology as a starting point for change. The most successful legal tech applications have embraced and utilised this approach to the fullest.

In contrast to the undeniable success of user-friendly legal tech, there is growing concern over the lack of transparency of some of the technologies used, especially when used in the core fields of law such as the criminal courts. In Wisconsin a concerned citizen filed a claim where he demanded to be presented the exact decision making algorithm of a software used by the court in his criminal case. This software called Northpointe COMPAS is used in assessing the defendants risk of renewing a crime and it is aiding the sentencing determination made by the judge.

23 see DoNotPay <https://www.donotpay.com/parking/> accessed 9.3.2018.
24 Helena Haapio, Next Generation Contracts: A Paradigm Shift (Helsinki, Lexpert 2013) and Stefania Passera, Beyond the wall of contract text. Visualizing contracts to foster understanding and collaboration within and across organizations (Aalto University publication series DOCTORAL DISSERTATIONS, 134/2017).

The Wisconsin Supreme Court, the highest instance to rule on the case, denied to defendants claim and rejected the due process argument used. The court argued that although the software produced only assessments related to groups of people similar to the defendant, sufficient individual consideration of the case is given by the judge who is at liberty to deviate from the computer generated assessment. More interestingly the Court acknowledged the proprietary nature of the software and the provider Northpinte's right to withhold information on the algorithmic decision making process based on those grounds. The Court's decision is criticized among other things because it places too much confidence in the judge's' ability to assess possible shortcomings of said software and to give proportionate weight to the assessments in sentencing.[25]

Using technology and design may well be the key to increasing citizens' access to justice and improve overall legal protection provided by the states. On one hand, this might mean better legal tools, applications and services but also better access to legal information, which is the necessary first step towards demanding legal protection. On the other hand, there are a lot of ethical implications involved that are emerging after the first optimistic wave of belief in technology's capacity to enhance legal services such as dispute resolution services. The ethical implications are manyfold and not always straightforward. The previously almost uncritical and positive view on the capabilities to use technology in producing ever more efficient time saving tools and applications has shifted towards a more cautious opinion that includes an understanding of some of the threats as well. Especially machine learning algorithms and the much discussed issue of automation bias, where algorithms reproduce

25 see 'State v. Loomis Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing' (Harvard Law Review 10 March 2017) <https://harvardlawreview.org/2017/03/state-v-loomis/> accessed 8 March 2018.

discriminative structures of their training data, are a cause of concern particularly within legal applications.

It has also proven to be extremely hard to predict future developments on the field of legal digitalisation. As discussed, ODR was heralded early on to revolutionize dispute resolution completely and render judges useless. It has not quite turned out to be the success story that it was predicted to become. a major reason was the inability to forge a sufficiently comprehensive universal agreement on the rules to be applied to online methods of dispute resolution and another was maybe that such rules and regulations were attempted to be incorporated into a existing legal system too early on and without sufficient evidence on the viability of the chosen model.[26] There seems to be a very fine line between over and under regulating possibly disruptive legal technologies.

To be able to steer clear of such complications and even mistakes in being able to fully utilize the potential of digitalisation of legal services and practices we must combine multiple fields of research and expertise.

It is imperative that lawyers and policy makers work together with and utilize the knowledge and working methods of computer scientists, designers, psychologists and social scientists among others. And there must be a specific emphasis in educating law students to be better able to work in and with interdisciplinary teams.

26 For example, the EU has sought improved access to justice for online disputes through the introduction of ODR Regulation and the Commission's ODR platform, which directs the complaints filed on the platform to national ADR schemes. Despite these efforts, consumers have not used the platform in great numbers, which raises the question of the system's shortcomings. See e.g. Riikka Koulu: Improving Consumer Protection through Technology: The Challenge of Compliance, in Immaculada Barral Viñals (ed), Conflict resolution with consumers: from ADR to ODR (Reus: Barcelona forthcoming 2018) 173-192.

3 WHY WE NEED LAWYERS WHO UNDERSTAND TECHNOLOGY

3.1 CHANGING LEGAL PRACTICES

As discussed in the previous section, it is not always straightforward to predict the success of different legal technology concepts and applications. Some applications are able to provide new tools to make access to legal help cheaper and more user-friendly, whereas others fail despite wide support from academics and policy makers alike, as the surprising lack of success many ODR initiatives have faced. Yet others might hinder transparency of legal praxis and reproduce the shortcomings of our justice system, as recent research on algorithmic decision making suggests.[27]

The responsible use of legal technology means that the ethical and legal consequences need to be addressed already when applications are conceptualised, designed, and implemented. This sets complex demands on the developers and demonstrates the risks of mostly business-driven development. The boom around legal tech has translated into increasing funding for technological innovation and the emergence of many legal tech startups, suggesting new business models and opening new, untapped markets. Despite many positive implications, there exists the danger of oversimplification if the legal system is perceived as legal markets. Law is one of the key operations of

27 For an overview, see Campolo et al 2017. Also, Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information (Harvard University Press 2016); from a computer science perspective, see Toon Calders and Indrė Žliobaitė, 'Why Unbiased Computational Processes Can Lead to Discriminatory Decision Procedures' in Bart Custers, Toon Calders, Bart Schermer & Tal Zarsky (eds.), Discrimination and Privacy in the Information Society (Springer: Berlin 2013) 43-57.

the society and nation-states have the primary responsibility to ascertain the respect of fundamental rights as the addressees of fundamental rights conventions, including the European Convention of Human Rights, which means that business-driven legal tech development alone is not sufficient to secure responsible legal digitalisation.

In addition to demanding developers to understand the ethical nature of legal tech, legal digitalisation is changing the nature of legal work. Especially business-driven legal tech development aims at transforming the legal profession by finding new untapped markets and building business models around such areas. Another linked but separate development is the increasing interest of governments in designing and executing new working methods for the courts and other public legal services. This means that the pressure to change is not created only by those outside the legal system but comes also from inside. However, one consequence of the external pressure is that the lawyers' hegemonic ownership of legal practices is slowly changing. Of course, this disintegration is not novel or solely technology-based but instead it is a combination of several factors, including those shortcomings presented by the ADR movement in 1980's, namely the ever-increasing price of litigation and growing number of self-representing litigants.

The impact of the legal tech scene on the legal profession can be exemplified with the hurdles created by a French startup Demander Justice, which was created in 2012. The web service provides easy-to-use forms for drafting legal claims, aims at reaching a conciliatory outcome with the other party and files the claim if no settlement is reached.[28] The service has given rise to several lawsuits, as the regional bar associations and later on the federal association le Conseil National des Barreaux have considered the service to provide legal counsel and thus being in

28 Demander Justice <www.demanderjustice.com> accessed 5 March 2018.

violation of the French lawyer monopoly, where only lawyers are allowed to represent clients. The tension between the startup and the legal profession has clarified somewhat, as the Parisian court le tribunal de grande instance de Paris, declared in its decision in early 2017 that the service does not violate the bar association's monopoly, as litigants are under no obligation to use lawyers to find the information provided by the service or to file the claims.[29] The experiences of the service, like those presented by access services described in the previous section, demonstrate how the legal system is a difficult environment to change and how new technological tools may easily lead to collisions between existing practitioners and newcomers.

The economic and qualitative change brought on by technology is often described through the model of disruption theory, which was developed in a 1995 business management article by Professors Joseph Bower and Clayton Christensen. The theory draws a line between sustainable and disruptive innovation and by doing so strives for describing why market leaders are often unable to perceive and invest in new technology trends and thus face the possibility of losing their market shares to newcomers better equipped at addressing the needs of future clients.[30] The disruption theory has since then quite rightly been criticised for its for oversimplifying the complex socio-legal aspects linked with technology development. Still, the theory is often used especially outside the academia and has at least in some aspects become the hegemonic discourse to describe innovation, and thus a sort of self-fulfilling prophecy

29 Vincent Monnier, 'Nouvelle victoire du site DemanderJustice contre les avocats' (L'Obs, 12 January 2017) <https://www.nouvelobs.com/justice/20170112.OBS3749/nouvelle-victoire-du-site-demanderjustice-contre-les-avocats.html> accessed 26 February 2018.

30 Joseph L. Bower and Clayton M. Christensen, 'Disruptive Technologies: Catching the Wave' [1995] January-February Harvard Business Review 1995 43-53.

of the startup scene. However, it is clear that no single model can accommodate the need for theory development on legal digitalisation, a point further highlighted by the nature of legal practices as a focal societal operation that impacts the rights and obligations of everyone.

3.2 LEGAL DIGITALISATION AS COLLABORATIVE EFFORT

Because of law's important social role and in order to alleviate the resistance to change and the tensions between new and old practices, responsible legal digitalisation can only be achieved by collaboration of all stakeholders. In simple terms, this means involving lawyers and legal scholars both in overall discussions on legal applications of information technology as well as in designing software architectures intended to be used within the legal system. Such collaborative approach could relieve the pressure on developers by connecting the knowhow of the legal profession with the forward-looking attitudes of the startup scene and thus help in avoiding the pitfalls of technology-driven development.Such collaborative schemes, however, require understanding and willingness to find a common language across professions, fields and disciplines. From the legal perspective, this translates into demand for lawyers who are able to relay to others how law functions and to evaluate which elements of the legal system exist for a reason and which are the result of organic growth over the centuries and serve no sensible function in the current legal landscape. This requires from layers the awareness to ascertain that technology is implemented into the legal system in order to improve access to justice, equality and transparency of legal decision making as well as the willingness to proactively look for solutions on how legal rights and values can be translated into better legal services.

Although practicing lawyers have been facing these growing demands for quite some time, the training of future lawyers

plays a focal role in enabling cross-disciplinary collaboration. In order to address the expectations of legal work in the future, the curriculum for legal education needs to include a strong focus on project management skills and on communication and team work. Also, legal education should stress interdisciplinary courses and thematic teaching instead of examining complex phenomena from the perspective one legal field at a time. Interdisciplinary courses provide law students safe environments to practice their abilities the explain the often nuanced logic of legal reasoning to others, which simultaneously forms the basis for reflections on future legal profession.

Needless to say, it is still unclear how technology is impacting the future of legal work and what skills will be required of lawyers on the long term. The impact of technology on legal profession has given rise to an extensive body of literature. For example, Professor Richard Susskind's work over the decades has discussed disruptive legal technologies as well as ongoing transformation of legal services and lawyers' work.[31] Also, Roland Voigl from Stanford Center for Legal Informatics CodeX describes the impact of predictive legal analytics have on the US Legal Market.[32] Additionally, Professor Frank Pasquale and Senior Systems Engineer Glyn Cashwell argue in their article on automation that the future of legal work is as much defined by the level of regulation or deregulation as it by automation of routine tasks.[33]

Legal practices have formulated around legal institutions, like law firms, court systems, ADR schemes, and government offices and international organisations. The legal profession and

31 Richard Susskind, Tomorrow's Lawyers. An Introduction to Your Future (Oxford: Oxford University Press, 2nd ed, 2017).
32 Roland Voigl, 'Changes in the US Legal Market Driven by Big Data/ Predictive Analytics and Legal Platforms' in Hartung, Bues, Halbleib (eds) 2018 (n 4), 53-65.
33 Frank Pasquale and Glyn Cashwell, 'Four Futures of Legal Automation' [2015] 63 UCLA Law Review Discourse 26-48.

legal institutions are entwined; lawyers' professional identity is central to the ways in which these institutions are operated, developed and organised. Also, legal institutions are central for governance models and also regulation is often formulated around these established legal structures. Traditional regulatory mechanisms and legislative technique do not always cater to the challenges presented by legal tech applications, as Professor Danielle Citron's early article on the negative implications of data-driven technologies on due process suggests.[34] This said, legal digitalisation needs to address these regulatory challenges, which is no simple task due to the diversity of applications, technological flux and complexity of regulatory principles such as technological neutrality.[35] In order to fully comprehend the possible consequences of different regulatory choices, it is necessary to formulate a comprehensive framework through collaboration of lawyers and other stakeholders. It is still unclear what the regulatory landscape is that is needed to enable responsible implementation of legal technology in different legal practices. Probably some legislative action is needed to safeguard fundamental rights and transparency, but regulatory choices and governance models should be based on a comprehensive understanding about the implications and legal scholarship alone is not sufficient means to provide this.

This leads us to the following. Lawyers play a pivotal role in preserving the ethical dimension of law and in safeguarding fundamental rights, access to justice and transparency. Legal digitalisation in its different forms provide multiple fora, where legal perspectives are needed to secure responsible implementation of technology, from software development and business management to established legal structures

34 Danielle Keats Citron, 'Technological Due Process' [2008] 85:6 Washington University Law Review 1249-1314.
35 Chris Reed, 'Taking Sides on Technological Neutrality' [2007] 4:3 ScriptED 263-284.

such as institutions and policy making. Due to the complexity of issues associated with legal technology, best practices of legal digitalisation are by definition a collaborative effort. This, in turn, calls for lawyers and legal scholars equipped with an in-depth perception of the socio-legal aspects of law, ability to conceptualise the impact of technology on legal practice and the ability to communicate these to others.

4 WHY WE NEED LAW, TECHNOLOGY AND SOCIETY STUDIES

In order to assess the need for legislative reforms, it is necessary to find ways to conceptualise new technologies from a comprehensive socio-legal perspective.This might prove out to challenge deep-rooted conceptualisations of legal scholarship. For example, retroactive control of legal tech applications through courts does not necessarily constitute a sufficient safeguard for the protection of fundamental values but instead a more proactive perspective is needed, calling attention for predictive justice.

Automation and legal applications of information technology have enticed scientific work over 70 years. Law, technology and society studies have roots in early work on jurimetrics that advocated the use of statistical methods for legal decision making from the 1940s onwards,[36] legal informatics that examines structures and applications of information within the legal sphere,[37] AI & Law, a subfield of artificial intelligence research

36 Lee Loevinger, 'Jurimetrics: The Methodology of Legal Inquiry', [1963] 28 Law and Contemporary Problems 5-35.
37 Bing Jon, 'Let there be LITE: a brief history of legal information retrieval' [2010] 1:1 European Journal of Law and Technology.

growing in importance since 1980s,[38] as well as research on legal issues of cyberspace that gained prominence after the World Wide Web commoditized the use of Internet.[39] More recently, scholars of technology-related legal research have come to describe their work as the loosely defined law and technology studies. Also, vibrant research traditions have developed around specific themes such as digital copyright and IPRs, privacy and data protection, surveillance and predictive policing, robotics and autonomous systems, biotech and cybercrime, to name but a few.

It would be dangerous to evaluate legal digitalisation as a straightforward process, instead it should be understood as a unity of complex and even contradictory phenomena that entwine with social and ethical implications. We need to define which questions we are asking. Legal digitalisation includes, at least, three different perspectives. Firstly, how new technologies challenge existing legal regimes, giving rise to new interpretative issues. For example, use of artificial intelligence in journalism raises questions about copyright of articles, liability of journalists and incentives of the media market. Secondly, use of technology in legal practices forces us to examine the future of legal work and the profession's role in the society. For example, introduction of alternative business models and the growth of the legal tech startup scene suggest that tailor-made legal work will become the exception rather than the rule of legal service provision. Thirdly, the introduction of new technologies enable us to address the shortcomings of traditional legal institutions and mechanisms in new interpretative situations, enabling the reassessment and also streamlining of legal structures formed over the centuries.

38 On early AI and law, see e.g. Bruce G. Buchanan & Thomas E. Headrick, 'Some Speculation About Artificial Intelligence and Legal Reasoning' [1970] 23:1 Stanford Law Review 40-62.

39 On legal rules on cyberspace, see e.g. I. Trotter Hardy, 'The Proper Legal Regime for 'Cyberspace'' [1994] 55 Pittsburgh Law Review 993-1055.

Technology has become ubiquitous, the scope and pervasiveness of technology use having increased significantly over the last decades. In light of this, it seems futile to limit scientific work to any given field, as digitalisation themes correspond with all legal disciplines. Furthermore, examination of technology-related phenomena should not be distanced from basic research on non-technology themes, as such technology-centric approach would carry a deterministic undertone that technology issues somehow differ from other legal research. This said, there is a need for developing a comprehensive framework for examining digitalisation of law. Such a framework needs to approach technology from a holistic yet context-conscious perspective and thus avoid two major issues of legal technology research.

Firstly, holistic approach is needed so that we can formulate an overview of multifaceted legal digitalisation. This comprehensive approach would also reflect the importance of a given technological solution against others and thus avoid the pitfalls associated with more fragmented perspectives. However, as the discussion in previous sections demonstrated, all technology applications cannot be discussed as coherent whole, as this would lead to extensive oversimplifications. Thus, holistic perspectives need to be supplemented with context-based approaches. Developing such a framework for legal digitalisation is out of necessity linked with socio-legal theories, as digitalisation issues have the tendency to aggravate and to bring fundamental questions of law to the forefront. Some of these fundamental questions are by definition practical and theoretical at the same time; for example, designing algorithmic decision support tools makes us wonder what legal reasoning truly is and to which extent it can be automated and translated into algorithms.

To conclude, an overview of legal digitalisation cannot be produced solely within legal scholarship but instead

interdisciplinary approaches are needed. This, in turn, requires methodological awareness and willingness to engage in discussions about common grammar, which can often be time-consuming and frustrating. Simply put, the biggest challenge is making law in action as well as law in books ready for interdisciplinarity. First step in this direction is to understand how different legal disciplines approach new themes that do not belong within any single field of law, and build on this to create a grammar for discussions with researchers from other social sciences and humanities as well as from data sciences. One possible way forward is to develop concrete use cases that can be recognised by all disciplines. For example, the use of data analytics in law provides one concrete example and the need for algorithmic transparency is a relatively easy to understand across disciplines.

Based on the observations and conclusions discussed earlier in this article, the Legal Tech Lab's early research has recognised five different areas of law and digitalisation, in which legal research is needed. These research areas are formulated thematically instead of doctrinally on purpose, as we perceive that in this way it is easier to pave the road towards interdisciplinary research initiatives. This taxonomy should not be understood as exhaustive, as its objective is to provide a thematically organised starting point for mapping out different intersections of law, technology and society. To this end, this taxonomy intentionally excludes doctrinal fields, although some fields of law can be situated more easily than others. Also, all areas include fundamental rights perspectives and they should be seen as overlapping, intersecting and inclusive. At the moment, these strategic areas are:

1) foundations of legal digitalisation,
2) algorithmic fairness and justice by design,
3) legal approaches to information,
4) societal change in institutions and profession, and
5) digital access to justice and governance.

Firstly, foundations of legal digitalisation addresses the vocal need for theory and method development that are necessary for the blueprint of digitalisation of law. This said, this focus area is closely connected with legal theory and plays a role in developing the general principles and concepts that can be used to describe the ongoing change. Foundations of legal digitalisation also forms the umbrella and the systemic starting point for more detailed research projects. In the end, all individual research projects as well as collaborative work within interdisciplinary research groups all contribute to this comprehensive framework. Secondly, algorithmic fairness and justice by design focuses on the often unforeseen consequences of algorithmic decision making and decision support tools within the legal system. Taking influences from computational modelling of law as well as system design, it is asked how legal protection, access to justice and fairness can be translated into software architectures. It is not possible to understand automation bias simply from the perspective of legal scholarship, as this requires insight into how algorithms reflect structural biases of their training data and how such shortcomings could be avoided. For example, removing possibly discriminating factors is not sufficient and bias in the formal sense of computer science differs from the term's socio-legal meanings.

As discussed above, algorithmic fairness is becoming an increasingly urgent theme to address both from social sciences and legal perspective as well as from data mining and computer science perspective. During the next three year period from 2018 to 2021 algorithmic fairness is at the core of the Lab's academic

work. For example, the Lab's researchers are currently examining possible uses of algorithmic decision making and automation within the public sector and mapping out the regulatory frameworks and challenges associated with these uses.

Thirdly, legal approaches to information evaluates different legal interests associated with information such as ownership, privacy and access. Data, in the meaning of vast digital amounts of information, has become significant in new ways and there is no legal conceptualisation that would take into account all the different interests and consequences linked with its increasing importance. An analysis that combines perspectives from competition law, legal informatics, governance studies and constitutional law, public law and EU law would provide an overview of the different legal interests linked with the use of big data. Also, influences from other social sciences are necessary, as they might provide different conceptualisations for a more nuanced approach to information, such as the idea that all training data is broken.[40]

Fourthly, changes of institutions and legal professions evaluates how the roles of established legal structures are changing due to legal digitalisation. This approach combines perspectives of procedural and administrative law as well as constitutional law with input from social sciences and future of work studies. Due to increasing pressure to digitalise legal services, the research area has close connections with practice. Perspectives from practising lawyers as well as established legal institutions and new actors, including inter alia in house lawyers, judges, law firms as well as the legislators and the legal tech startup scene are important starting points for assessment of the on-going digitalisation of law. Legal scholarship on the subject,

40 See e.g. Sarah Pink, Minna Ruckenstein, Robert Willim and Melisa Duque, 'Broken data: Conceptualising data in an emerging world' [2018] Big Data & Society 1-13.

however, is necessary to ascertain that digitalisation is not used simply as a facade of legitimacy for cost-driven legal reform but instead implementation of technology into legal practices is conducted with the objective of increasing access to justice.

The necessary first step towards towards an overview of these changes is to attain more information from different stakeholders in order to understand the reasons for and against adopting technological solutions for legal work. To this end, we are currently conducting an empirical study on lawyers' IT skills, implementation problems and overall awareness with the kind support of Finnish Lawyers' Association and the Finnish Bar Association. The preliminary results should be available at the end on 2018.

Finally, digital access to justice and governance examines the viability of existing legal concepts and safeguards in new digital environments. Drawing from constitutional law and regulation theory as well as from consumer law and law and economics, the focus area discussed issues related to regulating code, increasing significance of compliance, monitoring mechanisms and the implementation of legal safeguards.

It should be noted that neither the Lab's research agenda nor these strategic focus areas are set in stone. Instead, the Lab's inclusive culture and additional perspectives cumulated through open science methods enable continuous feedback and evaluation of research impact.

5 CONCLUSIONS

This article has striven for providing a brief overview of the status quo of legal tech, digitalisation of law and legal scholarship on these issues. In addition, we have highlighted the role the University of Helsinki Legal Tech Lab plays in remedying the severe lack of information on the implications these developments bring forward. The Lab strives for establishing the structures for research as well as public debate on the impact of legal digitalisation. One way to accomplish this is to recognise thematic research areas.

Potential and pitfalls of legal technologies need to be critically evaluated in order to establish best practices towards responsible legal digitalisation. Lawyers need to actively engage in development of new applications and to provide insight into values, human rights and legal principles as well as ethics and governance to the field, as otherwise there is the danger that legal tech is developed without access to justice in mind. Law is a core area of society, which means that increasing automation of legal practices affects the rights and obligations of potentially millions of people. Basic research is needed to find out what digitalisation of law means contextually and comprehensively and such enquiry needs to include all fields of law as well as other disciplines, as different legal tech phenomena do not follow such doctrinal distinctions. It is evident that most of these questions cannot be answered by legla scholarship only, which creates pressures for interdisciplinary research. In order to facilitate this dialogue, legal education needs to provide future lawyers with tools to engage in such work and understand the delicate interplay between law, society, and technology.

In light of this work, one core question is how to translate the values of justice and fairness into functional legal tech applications and how to develop legal redress and monitoring

mechanisms that safeguard these ideals when traditional structures are unable to do so. The need for algorithmic fairness has also its impact on the Lab's future activities, as the Lab's 2018 conference Legal Tech Con provides critical insights into legal uses of artificial intelligence.

JENNI HAKKARAINEN AND NAZANIN GIFANI[1]

Blockchain - an Outlaw by Nature?

1 INTRODUCTION

Every now and then an unusual event occurs that disturbs our daily lives or our society as a whole. This event might be as mundane as a car speeding down our home street; of course, this event can be restrained by the police imposing fines or criminal prosecution. Sometimes the unusual event can be more disruptive than just a car driving too fast. Modern technologies from machine learning to blockchain technology are forcing legal professionals and lawmakers to partake in much deeper discussion on how to provide the same safeguards in the virtual world as nation states have so far provided in the real world - speeding cameras, fines and sometimes even existing laws have proven to be insufficient to address many of the new challenges.

1 Jenni Hakkarainen is a LL.M graduate from the University of Helsinki, and a member of the Legal Tech Lab. Nazanin Gifani is a LL.M graduate and current PhD student at the University of Helsinki.

Reactions against revolutionary innovations such as internet or nanotechnology show that if society and its' values are at stake, law is chosen to be the primary source of balancing powers between what is good and evil.[2] It is relatively tempting to add blockchain to the list of modern, disruptive technologies that are challenging, if not society's core values, at least the current status quo, where nation states are considered the ultimate point of centralization and coercive power. This paper discusses the regulatory issues which arise from the widespread use of so called blockchain technology - a distributed and decentralised technology that is said to disrupt the markets and nation states' monopoly on coercion.

While nation states have engaged themselves in an ongoing debate over the controllability of this technology, the industry and blockchain community has raised more a complicated question; whether blockchain can be regulated at all. Accordingly, Dr. Gavin Wood, a blockchain and a smart contract entrepreneur has referred to blockchain a an allegal technology. Dr. Wood presented some of his views on allegality at Law and Digitalisation conference held at the University of Helsinki in June 2017. Allegality is not a word recognised by any of commonly used dictionaries, but Dr. Wood uses it to describe how decentralised technologies relate to law and legal framework. Decentralised technologies are, according to Dr. Wood, immune to law and to nation state centric coercion. Decentralised technologies, with blockchain here being a prime example, cannot be regulated with traditional legal instruments that are designed to target centralised systems and enforcement mechanisms that are traditionally dependant on nation state jurisdictions. Being allegal thus refers to a phenomenon that exists outside jurisdictions.

2 Kieran Tranter 'Nomology, Ontology and Phenomenology of Law and Technology' [2007] 8(2) Minnesota journal of law & technology 453.

Blockchain has been widely noted as a revolutionary and exceptional technology and, when talking about the most disruptive and innovative technologies of the 2010's, it is nearly impossible not to mention blockchain.[3] Its' regulatory averse nature has been one of the dominant narratives surrounding the blockchain hype since Satoshi Nakamoto first introduced this new technology.[4] Blockchain technology rapidly gained momentum and has ever since raised interest among citizens, private corporations and public governments mostly due to its' disruptive nature, promise of reducing transaction costs and its' ability to challenge some of the basic presumptions out economy leans on - the need for a trusted middleman and need for government centered enforcement mechanisms. Bitcoins' rapid price fluctuations, recent attacks towards various blockchain based networks, and industry's increasing interest in utilizing blockchain technology have paved the way for the debate over what kind of role law plays in this picture. Both public and legal discussion around blockchain has largely concentrated on regulating Bitcoin and other cryptocurrencies, whereas other blockchain applications, such as smart contracts, have not been thoroughly examined from a legal perspective outside academia[5].

This paper aims to discuss some of the main arguments put forward by Dr. Wood from a legal perspective. Our research question unfolds in two parts. First, we will ask if blockchain

3 Melanie Swan, Blockchain: Blueprint for a new economy (O'Reilly Media 2015). 5.

4 Satoshi Nakamoto is an alias, under which an article that first introduced a decentralized technology that enabled monetary transactions without a trusted mediator was published. In the article, Nakamoto does not refer to the technology by the name of blockchain, but instead used a term "chain of blocks". Rather, the name had been established later. Satoshi Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system'. <https://bitcoin.org/bitcoin.pdf>, accessed 12 January 2018.

5 Riikka Koulu 'Blockchains and online dispute resolution: Smart contracts as an alternative to enforcement' [2016] 13(1) SCRIPTed 61.

really is a force of nature, something that is uncontrollable and regulatory averse by nature? While cross-border technologies are usually regarded as difficult to control, existing regulatory means and mechanisms are providing some ways in controlling legal irritants and enforcing compliance.[6] We argue, that by locating relevant actors that exercise power and control in blockchain based networks, the narrative where blockchain is described as a natural force beyond any control is at risk of proving out to be a fallacy. As an example, we will look into how the biggest cryptocurrency, Bitcoin, is structured. Contrary to what is commonly believed, numerous different intermediaries are actually exercising control over Bitcoin network and over consumer actions.

Secondly, we ask, whether technological infrastructures are sufficient enough to safeguard individual rights. In the second part of the article, we argue that society's common interests still play an important role in safeguarding our core values and balancing divergent interests. Especially so, when technical infrastructure fails to provide sufficient trust and compliance, or when the technical infrastructure itself holds a risk for the misuse of power.

6 Nathan Cortez 'Regulating disruptive innovation' [2014] 29(1) Berkeley Technology Law Journal 177-179.

2 TECHNOLOGY AS NATURE - WHAT IS NATURAL ABOUT BLOCKCHAIN?

2.1 BLOCKCHAIN AS TECHNOLOGY

Before addressing what we find problematic in the concept of illegality, we will shortly explain what blockchain is and what are the qualities that supposedly make it regulatory averse. Our aim is only to provide an overall view without going into specific, technical details. In a nutshell, blockchain can be described as a cryptographically secured and decentralised record keeping system, a ledger. It provides the same record keeping functionality that traditionally has been entrusted to centralised architectures such as banks or internet platforms and public records such as land owning records.[7]

Joshua Fairfield has described blockchain as a public whiteboard that functions as a public ledger. For example, at a working place a common way of keeping record of who has bought coffee and coffee filters is a paper attached next to the coffee machine. Whenever someone brings in coffee they sign their names to the paper. Because the list is as everybody's sight anyone can just walk in and check if there are any free riders among the coffee drinkers.

Notwithstanding, the list can be easily modified and data can be removed or added by anyone who has access to the kitchen. In order to maintain trust for the record keeping system, it is crucial that modifications are subjected under strict, predefined rules. Blockchains' consensus-based record keeping system does just that and data can not be added without participants knowing and

7 See European Parliamentary Research Service (EPRS), How blockchain technology could change our lives (2017 PE 581.948) 5.

accepting it.[8] In blockchain architectures all participants, that is computers and their users, partake in accepting and validating new transactions or adding new data to the system. The entire transaction history is stored to each participant's computer.[9] The structure results in the decentralization of governance and data storage. If one computer is shut down, the rest of the network can still continue validating new transactions. If data was removed from one computer, all the other computers would still hold a perfect copy of the ledger.

Hence, in order to function, the system simultaneously relies on each and none of the participants. It should be noted, that even though most of the current blockchain debate circles around Bitcoin and other cryptocurrencies, the use of blockchain is not limited to financial services. Entrepreneurship around blockchain has been slowly increasing and some new service models, e.g. around sharing economy, internet of things and transportation has been developed.[10] Nevertheless, since the regulatory status of blockchain still remains somewhat unclear, businesses and individuals have been prudent towards adopting blockchain based products.

A distributed, cryptographically secure, peer-to-peer structure enables parties to engage in transactions without having to rely on a trusted intermediator to uphold trust - trust is allocated into technological infrastructure. Traditionally, trust between parties that remain unknown to each other is created, secured, and maintained by central authorities. Central banks mediate between transactions and maintain banking accounts

8 Joshua Fairfield 'Smart contracts, bitcoin bits, and consumer protection' [2014] 71(2) Washington and Lee law review online 36.

9 Aaron Wright and Primavera de Filippi 'Decentralized blockchain technology and the rise of lex cryptographia' [2015] 5-7, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664>.

10 Open data institute (ODI), Applying blockchain technology in global data infrastructure (2016 ODI-TR-2016-001) 10.

and also affect the value of money. Individuals exchanging money, investing into stocks or paying their debts trust their assets to central authorities. Whereas, bitcoins are not situated in an centralized account nor is it accepted as a tradable asset in most of the countries .[11]

The shifting of trust from government centered enforcement or centralized mediators into code is articulated to decrease the reliance on central authorities, eventually resulting in fully decentralised and democratised technology driven governance. With the rise of the so called 'smart contracts', blockchain based programmes that automate both the negotiation and execution of a contract, we seem to be one step closer to a cyber world where the role of nation states and public laws are reduced to a minimum.[12] In a cyber world run by smart contracts, technology provides a privatised normative structure, sustaining the features that are regarded as essential for functioning society and economy - trust, enforcement and certainty.

2.2 BLOCKCHAIN AS ILLEGAL TECHNOLOGY

As described previously, Dr Wood has argued that blockchain technology and smart contracts in particular are providing a framework where the system is not even able to care about outside interventions and constraints - such as law enforcement. The concept of allegality seems to suppose two things. Firstly, the technology itself is able to promote trust and form a basis for economic activity. Secondly, the technology itself is uncontrollable due to its technical qualities. As a result, blockchain is considered as a force of nature, a new kind of a natural law. Here, he makes a distinction between natural laws and artificial laws. Natural laws are scientific facts, that is, laws

11 Swan (n 1) 3.
12 Ibid. 16.

that are embedded in nature itself and therefore cannot be contested. As an example, one might argue that gravity does not exist, but nevertheless, jumping out from an 8th story window would still result in hitting the ground.

In his presentation, Dr. Wood characterised artificial laws as man-made laws. Laws are created and can be changed accordingly. The need for artificial laws spurs from practical needs - they govern interactions between entities and individuals, and provide predictability and certainty.[13] With blockchain, the distinction between natural and man-made laws becomes unclear. Perhaps blockchain as a natural order is situated somewhere between, let's say criminal law and gravity. Besides having the qualities of a natural law, blockchain has the same function as human made laws - it governs human relations and enforces behaviour. Here, Wood's idea resonates closely to that of Lawrence Lessig and code is law narrative. In the late 90's, Lessig introduced his infamous idea, that technical structures and software architectures hold same regulatory power in steering human behaviour as law, markets and social norms do.

Kevin Werbach, an assistant professor and a technology entrepreneur, among others, points out how tempting it is to see the claimed regulatory averse nature of blockchain as a democratic escape from where the government and traditional policy making has failed, or a clever way for app developers to escape compliance and liability.[14] Recently, public debate as to whether blockchain or blockchain based applications can or should

13 In this section we are referring to Gavin Wood's presentation held at the conference, Law and digitalisation in Helsinki at 6th June, 2017 <https://www.youtube.com/watch?v=Br2deynrxxQ&feature=player_embedded>. For short introduction on allegality: Gavin Wood, 'Allegality: Systems that can't care', <https://www.slideshare.net/gavofyork/allegality>. See also <http://gavwood.com>, accessed 19 February 2018.

14 Kevin Werbach 'Trust, but verify: Why the blockchain needs the law' [2017] Berkeley Technology Law Journal, forthcoming, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844409, 2.

be tied more closely under legislative control, has increased. Due to the rising popularity of different cryptocurrencies and their indistinct position as an investment instrument is putting pressure on governments to safeguard both fiscal interests and consumer protection. Confusion in the markets and in the regulatory sphere has also led some of the biggest internet service providers, with Facebook being a forerunner, to ban cryptocurrency add-ins to their services.[15]

If blockchain was truly illegal, this discussion about regulatory measures would be pointless. Since the debate if and how governments should react to this innovation is still ongoing, it seems that the allegality of blockchain is a concept that can be contested and should be examined more thoroughly. Next we will examine the technical structure of the most well-known blockchain based innovation, Bitcoin. In doing this we are hoping to show how the way these technologies are designed and structured, provide ways to for law or other accountability enhancing mechanisms to address, or compliment blockchain networks and applications.

2.3 SKETCHES ON BLOCKCHAIN ONTOLOGY

Blockchain's technical structure as decentralised, cross-border technology forms one regulatory challenge and poses a danger of falling into the trap of thinking that blockchain doesn't have any standard jurisdictional footprint. As previously described, it does not rely on one single entity or computer in order to

15 See e.g EU report on virtual currencies 2016/2007(INI). Recently at least Gibraltar has taken a "friendly regulatory measures" on some cryptocurrency activities, see Annaliese Milano, 'Gibraltar will take market-driven approach to ICO rules' <https://www.coindesk.com/gibraltar-take-market-driven-approach-ico-rules-officials-say/>, Dave Lee 'Facebook bans all crypto-currency adds' <http://www.bbc.com/news/technology-42881892>, accessed 20 February 2018.

function and continue to run its' programme.[16] Secondly, the ability of law to recognize blockchain-based applications such as decentralised organizations or cyber-assets as legal actors seems to be somewhat unclear. To put it in other words, they seem to lack legally defined identity. The situation with the legal status has been compared to the role of microfinance in the early 2010's, when microfinancing was referred to being an institutional legal no-man's land, where law is not establishing roles, restrictions or safeguards.[17] Next, we are examining these claims in more detail.

Law's effectiveness is partially associated with state's ability to enforce laws or otherwise nudge towards wanted behaviour. A presumption is that different actors comply with normative rules voluntarily. If error or misconduct happens, the nation states' legislative measures or enforcement are called to rescue. In order for the nation state to intervene, it has to locate the relevant actors who can be regarded as legally responsible or otherwise obligated. Effective means for nation states' to intervene and solve disputes is tied to territorial jurisdiction, thus making cross-border disputes arising in technical networks even more complex

16 In general, for one transaction to occur, 51% of the computers has to validate the transactions. This of course varies and the precise conditions under which a transaction can occur is defined in the source code. In addition, it is not always clear how the "mining power", that is the ability to partake in validating the transactions in the network, is allocated. Recent research shows, that due to procedural and economical preconditions, the mining power can in reality be centralized to a selected actors. See Primavera de Filippi and Benjamin Loveluck 'The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure' [2016] 5(3) Internet policy review 7.

17 David Lee Kuo Chuen and Robert H. Deng (ed.), Handbook of Blockchain, digital finance, and inclusion, vol 2 (Elsevier inc. 2017) 413. See also Frederic de Breuck 'The Blockchain Universe: The lawless no man's land', <http://blog.global.fujitsu.com/blockchain-universe-lawless-no-mans-land/>, accessed 11 March 2018.

to address.[18] In addition, law needs an addressee.[19] Locating the relevant actor is a prerequisite for seeking redress or placing enforcement. Intervention might be needed for example in order to stop an illegal program running or collecting taxes if so called initial coin offerings[20] should be regarded as traditional investment instruments. In summary, various blockchain applications seem to lack both defined and established legal personality and "a stop button".

Despite Nakamoto's supposed intention to introduce the world a monetary exchange machine that would not need a central authority to validate transactions and to create trust, some recent studies have drawn quite a different picture on Bitcoins functionalities. These studies have revealed a partly centralised and highly complicated structure of actors that underlie the Bitcoin infrastructure.[21] An actor or agency by its' definition means someone with a capacity to act and exert power. The definition is twofold. Firstly, an actor can be addressed and influenced on.

Secondly, an actor can use power in relation to other actors. We suggest that this notion of agency entails two important factors - technical infrastructures can be affected via these actors, but what is more important to notice here, since some actors in the network hold power over others, the power relations in the network get distorted. Due to the structural power asymmetries,

18 Koulu (n 4) 43.

19 Roger Brownsword 'Code, control and choice: why east is east and west is west' [2005] 25(1) Legal studies 9. Alexander Boer, Legal Theory, Sources of Law and the Semantic Web (IOS Press 2009) 91.

20 Initial coin offering (ICO) is an unregulated way of raising funds in the cryptocurrency marketplace. It can be seen as an alternative for initial public offerings (IPO). Usually in ICO's a crypto startup sells it's own cryptocurrency, accepting payments e.g. in other cryptocurrencies as Bitcoin or Ether. See e.g <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>, accessed 24 February 2018.

21 de Filippi&Loveluck (n 15) and Werbach (n 13) 24.

the question of whether to regulate or not becomes even more crucial.

Werbach points, that even though the technological structure of Bitcoin remains decentralised, to function properly, the actual exchange is governed by different actors and various points of control. With different actors, different problems might occur. Werbach thinks of blockchain networks as a series of concentric circles. The distributed ledger and decentralised consensus is at the heart of the system. On the next level, we have smart contracts and the source code that directs and executes the transactions. At the outskirts of the technical structure there are various different service providers. Bitcoin is tradable only via these service providers that act as mediators on the intersection between the cyber world and the "real" world.[22] Stepping into cryptocurrency world does not simply happen by turning one's computer on and going online, on the contrary. Even though value is stored in the decentralized ledger, it is accessed through centralized access services.[23]

Resulting, the maintenance and the use of Bitcoin do not solely rest on technological infrastructure. The technology is maintained and utilized by human actors such as developers, miners who participate in validating the transactions, wallet-developers, and, of course, individual investors that trade with Bitcoin. De Filippi and Loveluck have showed, that despite being an open source and a decentralised project, the maintenance of the source code rests on highly influential and small sized core developers, resulting to a partly centralized governance of the platform.[24] Instead of focusing on the seemingly difficult question of how to regulate blockchain, we could engage ourselves in asking how can we find intermediaries or other actors, and how

22 Werbach (n 13) 23-24.
23 Ibid. 27.
24 De Filippi&Loveluck (n 15) 7.

can we affect those actors. Hence, even though the technology itself may not be addressed efficiently, there are several points of control where it can affect human behaviour, starting from the design process and ending to consumers entering into blockchain networks. Influencing some or all of these actors can eventually result in affecting the underlying technology as well, but first and foremostly these actors are on a key position to provide and build safeguard mechanisms and accountability for the end-users.

The problem with focusing solely on regulating the technology itself is that it leads us into thinking that the technology itself would be allegal by nature. This echoes, what we think closely reminds a deterministic worldview. In technological determinism, technology is granted a position as the most powerful change agent in our society; technology determines our future and society has only a little to say about the effects technology has on us.[25] The deterministic view on technology reduces the role of humans in the process, and doesn't recognise humane and social processes that affect the development and adopting different innovations. Instead we argue that technology is both constructed by humans and utilised by human beings, as previously stated by many scholars within science and technology studies.

We have now examined the multilayered system that is required to maintain Bitcoin infrastructure and to allow monetary action taking place in the decentralised ledger. Even though blockchain as a technology can be difficult to regulate, it is by no means a natural force. Instead it is a man-made innovation and can be further developed and designed differently. In addition, most of the blockchain based applications consist of many different layers. These layers usually differentiate from distributed ledger technology and instead are highly centralised.

25 Marcella Atzori 'Blockchain technology and decentralized governance: Is the state still necessary?' [2015] available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713, 21.

Despite what being said here, the question of how to regulate or control blockchain technologies or blockchain economy is another issue. Nation state centric, traditional legislation seems to be dragging behind and it seems that the balance is slowly shifting towards "from bottom up" approach, where the relevant actors and stakeholders are taking more responsibility in securing safeguards with governance procedures instead of only relying on the code underlying these systems

3 CANNOT FIGHT THE MARKETS - RECENT DEVELOPMENTS IN BLOCKCHAIN ECONOMY

3.1 ECONOMICAL RESPONSES TO DECENTRALISATION - TRUSTING THE TECHNOLOGY OR TRUSTING THE INDUSTRY?

In this section we are discussing further the concept of trust and why is it crucial to critically assess how trust is built and maintained in technical infrastructures. Until now, trust has been a focal concept in an online environment for both consumers and businesses in developing and adapting new online services.[26] Lack of trust in online stores and legal enforcement to provide sufficient safeguards and conflict management mechanisms are some of the key issues European Union has tried to resolve with different legal instruments. The development of an unified online dispute resolution platform to ease consumer cross-border disputes (ODR) [27] and general data protection regulation (GDPR) to strengthen consumer trust are only a few examples of how

26 Koulu (n 4) 48.
27 Ibid. 43.

managing trust has become of a great importance in today online environment. Nevertheless, blockchain seems to be a game changer here. It is said to deliver complete trust and security outside current legal framework and legal enforcement. However, recent developments and economic signals have shown that the society or the markets are not only passively adapting this new innovation, but also shaping the technology and its' design.

Blockchain technology is by no means an unified technological innovation and since Nakamoto's paper it has been further developed. To put it simply, different blockchains are usually categorized into two types: closed/open blockchains and permissioned/permissionless blockchains. Open and permissionless blockchains are basically open to everyone, the participants jointly maintain its' operations and anyone may have a copy of the database. In closed and permissioned systems, a central authority usually restricts who can join the network and on what terms. Access to the data stored at the ledger is also restricted.[28] The latter type of blockchain basically results in adapting only certain elements of the technology, while compromising decentralisation at the expense of complying with the normative framework surrounding e.g. particular industry adopting blockchain based processes. Consequently, permissioned chains are often targets for a criticism.

If one has any interest in the development of cryptocurrencies, finance, or technology in general, it would have been impossible not to notice the headlines that are emerging in one's newsfeed. Deutsche Bank and IBM are experimenting with blockchain,[29]

28 Open data institute (n 9) 3.

29 https://www.db.com/newsroom_news/2017/deutsche-bank-partners-with-ibm-for-block-chain-based-shared-kyc-platform-en-11726.htmhttps://www.db.com/newsroom_news/2017/deutsche-bank-partners-with-ibm-for-block-chain-based-shared-kyc-platform-en-11726.htm, last visited 28.1.2018.

Estonia is building its e-citizenship services on blockchain,[30] in 2017 the European Securities and Markets Authority (ESMA) published a report on the use of decentralised ledgers in the securities markets[31]. It would be just plain stupid to suppose that governments and one of the biggest banks in Europe would just on one Sunday morning trust its' databases and procedures to a decentralized and uncontrollable network. When we are reading news about blockchains becoming mainstream, we are usually reading news about the adaptation of closed and permissioned blockchains.

Why are the economy and markets slowly pushing the development towards more centralised and controlled blockchains? When trying to answer this, we must take a step back and to look into law as a system, the functions of law, and the concept of trust. Are the signals we are now beginning to witness only due to economic structures and markets thriving towards more controllable and efficient economy, or is there a deeper need in the society for safeguards that the technical structures alone are not able to provide?

3.2 TRUST IN CODE OR TRUSTING THE CODERS?

Werbach, among other scholars, is arguing blockchain technology is good at validating transactions and thus can efficiently exchange value. However, executing transactions is not the same as creating trust between parties.[32] Werbach develops

30 https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/, last visited 28.1.2018.

31 European securities and markets authority (ESMA), The distributed ledger technology applied to securities markets (February 2017, ESMA 50-1121423017-285).

32 Werbach (n 13) 23.

the idea further by stating that trust always implies uncertainty and vulnerability. Blockchain has proven to be a relatively good system in validating transactions, but to create trust, one requires something more. That is where law comes to play as Werbach argues the following: "The limitations of the blockchain create problems when it is positioned as the sole guarantor of enforcement. Fortunately, there is a mechanism that can work alongside the technical trust architecture of the blockchain. That mechanism is the law".[33]

Still, what can go wrong? As pointed previously, in blockchain architectures, trust is allocated into technical infrastructure instead of institutions or human centric enforcement mechanisms. Because blockchains' functions result from its' source code, the trust is allocated to the different codes running blockchain infra, and in multilayered systems this basically means trusting all the different stakeholders making the transactions happening. We want to point out that code is nevertheless human made line of commands, following that a possibility for humane error is always present.

As Dr. Wood pointed out in his presentation, code is also always a set of predefined rules that determine future actions. The messiness of the real world and human interaction does not translate well into pre-defined, mechanistic rules. Human-made technology is vulnerable to technical errors, malicious attacks and exploitation. In 2017 several initial coin offerings built on a blockchain platform Ethereum were hacked, ending with most of the investors to lose their investments.[34] In June 2017 Bitcoin-community went through a lengthy debate over whether they should increase Bitcoins mining capacity. The debate resulted in Bitcoin dividing into two, thus forming two different

33 Ibid. 23.

34 For a short summary on the events see https://www.coindesk.com/hacks-scams-attacks-blockchains-biggest-2017-disasters/, last visited 12.1.2018.

cryptocurrencies.[35] The former example shows that despite being regarded and promoted as "a trusted and secure system", failures can and will occur and systems are being exposed to vulnerabilities. The latter suggests, that decentralised structure and democratic-like voting process does not always effectively resolve disputes arising from the community.

It can be argued that predefined rules are good at executing rules but not suitable for managing exceptions.[36] Even though pre-defined rules have proven to be efficient in executing tasks, their ability to react in humane or technical errors is weak. If, and when, an error or other breakage occurs a human intervention is needed in order to repair the program or solve disputes. Previous examples show how trust allocated in the infrastructure has proven to be a fallacy. Lacking a uniform protocol or procedures, exceptions are handled case-by-case, thus creating an insecure and unpredictable environment. Perhaps trusting technological systems and executing transactions by code also requires trust in effective, unbiased and accountable governance, which, for now, seems to be lacking in most of the applications and networks.

Economic incentives are showing weak signals that the industry itself is beginning to react on the demands of assuring compliance and trust not only with the help of technology. Being lawyers, we do want to discuss another important topic. The Laissez-faire situation wherein the protection of the weakest and the basic human rights is left to the markets does not sound like a sustainable or feasible option. Next, we will argue that regardless the development of the markets and widening social acceptance of different blockchain based applications, there

35 Laura Shin, 'What will happen at the time of the Bitcoin hard fork?', <https://www.forbes.com/sites/laurashin/2017/10/31/what-will-happen-at-the-time-of-the-bitcoin-hard-fork/#816480a337d4>, accessed 12 January 2018.
36 Izabella Kaminska, 'Blockchain's governance paradox' <https://ftalphaville.ft.com/2017/06/14/2190149/blockchains-governance-paradox/>, accessed 12 January 2018.

might still be a place for more traditional safeguards. Is there a need to add another level of trust, one that is being secured by law or governance, to compliment trust provided by blockchain?

4 UNFOLDING THE RELATIONSHIP BETWEEN LAW AND BLOCKCHAIN

4.1 INTERPLAY BETWEEN LAW AND BLOCKCHAIN - IS THERE NEED FOR REGULATION?

In this section, we would like to explore the role of law in blockchain. First, we will examine whether law could play a role in making blockchain more human-centric. As discussed above, software architecture and the markets regulate behaviour in cyberspace. We argue that although blockchain technology can help to deliver better legal services, they cannot fully replace the importance of legal mechanisms in the society. We ground this argument on an analysis of the shortcomings of blockchain-based currencies, we explain why blockchain should be regulated and essentially why there is need for law or more traditional control mechanisms to step in as governance providers.

As the debate around bitcoin shows, blockchain architectures alone cannot guarantee sufficient levels of legal protection, responsibility and equality. The power asymmetries that exist on Bitcoin are very telling. Despite their decentralised mission, blockchain networks are gravitating towards centralised structures, as the mining process used to verify transactions

and generate new currency units demonstrate.[37] Due to the difficulty value and high demand of computer power for mining and technological skills required, most individuals have limited possibilities to participate in mining.[38] As a result, two major trends have developed in mining which allows individual to combine resources to increase their chances of earning rewards. One of the trends is mining pools, that combine individuals' computing powers to increase their chances of earning new currency.[39] The organisers of these pools usually control the computing power and miners have no means to influence the mining. Although pools enable single miners to have a better chance of getting rewards as a result of mining, the sharing of reward portions does not follow a transparent or equal protocol.[40]

Moreover, as a result of the great interest of corporations with huge resources and money investing various mining server farms have developed which has led bitcoin towards centralisation.[41] Having access to greater computational power and resources enables these centralised bodies to gain more shares of bitcoin which eventually leads to centralisation of mining. Furthermore, a centralised network is more susceptible to security attacks and manipulation. It's not only the mining that can make people vulnerable to abuse. The accumulation of crypto-currency in hands of few big-money bitcoin players allows them to manipulate the market easily. Mike Hearn, one of the original developers who maintained the open-source code that runs the bitcoin peer-to-peer network has publically announced

37 Mining is a process through which transactions are validated through a chain of cryptographic puzzles which are solved by individuals called minor. To encourage participation of miners they are rewarded bitcoin as a result of solving crypto puzzle. See e.g. Ittay Eyal & Emin Gun Sirer, 1.

38 Alireza Beikverdi and JooSeok Song, Trend of centralization in Bitcoin's distributed network[2015], IEEE Conference Japan, 1-3 June 3.

39 Ibid.

40 Ibid.

41 Ibid.

that future of bitcoin is doomed. He observes that bitcoin has failed because 'the community has failed'. He writes "What was meant to be a new, decentralized form of money...has become something even worse: a system completely controlled by just a handful of people."[42]

The centralisation of bitcoin enables these powerful players to interfere with the process of recording new blocks, prevent other minors from completing a block, control the price and influence the market easily. Centralisation per-se is not alarming- it is basically almost what we deal with in every other organization- however, it is the centralisation of a network that claims to be decentralised and law-averse which is threatening. The emergence of new crypto-millionaires known as bitcoin whales who are not bound to any regulation and can easily influence the market and manipulate the consensus leaves single fishes in the sea vulnerable. This is not to say, that law single-handedly can solve these inequalities but rather it is to show that law is an essential regulator that should exist along with other regulators of crypto-world.

Although law cannot address all these shortcomings alone nor it can completely eliminate the role of other actors, regulation through law could bring certain safeguards that can create trust in blockchain. Generating trust might eventually encourages the use of the technology. The case of Bitcoin uncovers that although the currency is not regulated by law, it is controlled by market, private interests and through self-generated norms. These self-generated norms can have a huge impact on rights and obligations of the individuals participating in these networks. The effects of such self-generated norms and consensus based governance became apparent in the event that occured after so-called DAO hack, where a hacker drained nearly 44 Million

42 https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7, last visited 16.03.2018.

euros from a community built on blockchain based smart contracts. Through analysis of the DAO attack we try to examine possible downfalls of consensus based governance and how the governance through smart contracts will eventually face the same challenges of governance in real world.

4.2 GOVERNANCE THROUGH SMART CONTRACT

The DAO was created as a complex smart contract on the Ethereum blockchain as a venture fund with the aim of decentralizing the investments and codifying the rules and decision making powers. In 2017 the DAO was hacked, resulting for nearly 44 Million euros being drained from the community. This ensued to a conflict about redress mechanisms on how to react to the losses and errors found in the source code of the smart contract after the hacked was noticed. The events clearly depict the limitations of the blockchain architecture as a governance model.[43]

As a result of a hack, the Ethereum team proposed some options to redress the situation. Part of the community demanded that the system is reset to pre-hack status, others advocated the irreversibility of the code and argued that the community should just bear with the losses. As a result, the lead developer community introduced an update that some users implemented and as a result the network split in two. The group argued that the code is law and the original protocol of the DAO should remain unchanged under any circumstances.

The group that was willing to reset the system argued that human should have a final say through a social consensus.[44] A hacker should not be able to benefit from the manipulation of the system. It seems that both groups have worthwhile points.

43 See, https://www.coindesk.com/understanding-dao-hack-journalists/, last visited 23.03.2018.

44 See, https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/, last visited 23.03.2018.

What the first group argues is that in absence of any democratic mechanisms, changing the decentralised immutable smart contract as a result of an abuse in the system, might create a slippery slope and open the door for exploitation and ultimately reduce the reliability of the DAO. Nevertheless, the argument of the second group also address the functionality the system. If the main aim of the system is to act as venture fund and to provide a secure and transparent way of investment, then it should not remain passive in response to the loss of investment of people.

The repercussions of the DAO hack and the community's response underline the importance of predictable recourse mechanisms. As Economics Professor Avinash Dixit puts it, the legal system has traditionally provided the framework and guidelines for markets, which consists foremost of property rights, enforcement of contracts, and regulation of collective actions.[45] Dixit observes that 'no institution or system will prove perfect' and every system suffers from constraints of 'information, commitment, and rules of the political game.'[46] Dixit recognizes that the governance is not synonym to government and informal institutions by utilising the means available to them, can also secure these elements. Nevertheless, for a well-functioning market it is essential that this institutional equilibrium exists.[47] The split in the Ethereum DAO illustrates the need for legal governance. It demonstrates that preserving liberties and preserving the normal function of market requires a

45 Avinash Dixit, Governance Institutions and Economic Activity [2009] available at https://www.princeton.edu/~dixitak/home/PresAd_F1.pdf,1.
46 Ibid. 6.
47 Ibid.

point of control that is agreed on based on democratic processes.[48] This need can and should be addressed by different formal and informal institutions. What law in its traditional sense offers is a set of principles and mechanisms which allows resolving the disputes and reaching to the public choice in a democratic way which currently, the DAO lacks. However, we argue that one should not ignore the value that law brings in generating trust and protecting public choice. In the following section, we attempt to show how law can play a part in achieving good governance.

4.3 LAW AS A POINT OF CONTROL

Having demonstrated the vulnerabilities of blockchain and risks of lacking legitimate control mechanisms, in this section we would like to illustrate how legal mechanisms can fill the gaps in effective governance. One of the most important objectives of law is designing mechanisms that support the effective functioning of market and create a fair space of interaction. These mechanisms among all, include procedures for the conflict resolution in contractual relationships. Legal mechanisms introduce predictable course of action when contract can no longer offer a solution to the special circumstances. One of the criticisms of smart contract is lack of flexibility which can impact the stability of contracts in a long run.[49] Because code only can offer binary solutions it is often unable to respond to newly arising circumstances. Traditional legal mechanisms can

48 Also Lessig points out that the problem with regulation is not whether there should be a regulation, after all, it appears that we all agree that there are collective values that cannot be decided and enforced on the basis of private choice. The question, however, is who is going to regulate the cyberspace and how things should be regulated to achieve these collective ends without compromising freedom and liberties that cyberspace promises. See Lawrence Lessig, Code and Other Laws of Cyberspace[Basic Books 1999] 302.

49 Karen E. C. Levy, Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law [2017] 3, 1-15, 8.

offer established mechanisms that are essential for generating trust because they allow people to enter into the smart contracts knowing that, in face of a conflict, they are able to rely on law to provide a solution.

More importantly, legal systems are designed to protect public interest. Constitutions often design legislative mechanisms such as applying the norm of fairness and using committees and other stability-enhancing mechanisms to reach the public preferences.[50] Regulation of collective actions are very important function of law, because no matter what technological means are used to reach consensus, eventually conflicts of interests arise. Individuals will choose their immediate interest over the long-lasting interest. Atzori argues that the main reason that central authorities were established was to protect the common good and collective rights from 'transitory individual interests and from any reckless logic of profit'.[51] In fact, central government with the ability to rule and sanction is the result of 'historical process of emancipation from private powers.'[52]

Atzori tries to illustrate that security and freedom do not emerge in a society automatically, they are fruits of historical and social struggles that established processes that can produce and protect these values. She observes that a blockchain-based society is incomplete because individuals are not citizens and the 'law of might – or the laws of the market-' overrides the common good. [53] She describes a situation in which people in a decentralised society might build non-aggression pacts based on consensus to avoid conflicts. However, she notes that the consensus is not sufficient to solve the conflicts. She predicts that the need for security and 'the necessity to avoid fragmentation of society' at the end leads to the establishment

50 Farber & Frickey, p. 58.
51 Atzori (n 24), 21.
52 Ibid 24.
53 Ibid 23.

of a 'permanent point of control' and an intermediary which can maintain the security and order and resolves the future conflicts in a 'legitimate way.'[54] This creates a greater need for coordination between conflicting interest to protect consensus once reached. She asserts that 'It is this juridical and ethic process that transforms individuals into citizens.'[55]

Viewing the central authority as having the power of sanction as a point of control calls the Hobbesian notion of law to mind. The selfish human needs a balancer and a point of control because in face of a challenge, often, immediate interest prevails over collective ones. Moreover, power imbalance and information asymmetries that exist outside the code generate inequalities that influence the users of blockchain. Looking at bitcoin reveals that blockchain architecture is also vulnerable to manipulation and risk. The architecture of blockchain regulates our behaviour and so do people who have a greater power in utilizing this architecture. Recognizing these regulators of crypto-world is essential in determining how law can and should play a part in creating a fairer space of interaction.

5 CONCLUSION

In this article we have challenged the claim of blockchain being regulatory averse technology by nature and explored ways how to affect how blockchain based innovations are designed and how they are adopted and used in the society or markets. The current debate over blockchain seems to be circling around deterministic arguments that falsely point our perception into thinking that the technology itself would be distinct from human

54 Ibid.
55 Ibid, 24.

shaped environment. Nevertheless, the regulation of disruptive technologies is no easy task. The emphasis on different approaches aiming to regulate blockchain, is on regulating the technology itself. Whereas our suggestion is that the focus of the regulation should be on spotting the relevant actors that act as point of control and address or motivate them instead to incorporate safeguards and accountability in the system.

The article has also illustrated the role and function of law through providing safeguards and unfolding the vulnerabilities of Bitcoin and smart contracts. By analyzing the current status of Bitcoin, we have shown how market has shaped the technology and has pushed it towards centralisation. We have challenged the deterministic view on technology and have shown that market has not adapted to the technology blindly. Through addressing the vulnerabilities of blockchain and showing the shift of the currency towards centralisation we have tried to show that blockchain also creates its own threat to liberty. Law can, and should, play a part in addressing the inequalities and power imbalances that blockchain itself cannot overcome, thus creating trust where the technical system itself fails.

Finally, we have examined the idea that whether blockchain can replace the law. Through analysis of the ethereum DAO we have illustrated the need for institutional guarantees for proper functioning of market. Law protects our collective values that have been established through democratic decision making processes. In contrast, smart contracts create rules on a case by case basis and puts law in a free market where all the values bear the same weight. Hence, the immediate individual interest can easily override the collective ones. As a result, a holistic approach that takes into account interests, weaknesses and strengths of different actors that participate in maintaining both the technical system and the legal framework is needed in order to protect and safeguard the collective values we hold important.

II

Between Disruption and Regulation: How Digitalisation Impacts the Legal Profession

Between Disruption and Regulation – How Do Lawyers Face Digitalisation?

1 INTRODUCTION

Digitization in the legal field has been deliberate compared to for example financial services. However, the pace of digitalisation is accelerating also in law, and digitization is now evident throughout the legal ecosystem. This is largely due to possibilities offered by technology, but also due to pressure by clients and wider society.

Although digitalisation is here to stay also in terms of legal services, there is not much research on digitalisation and law. Observations on the phenomenon are therefore often made on a more general level. So is the case in this article, the purpose of which is to find out how lawyers face digitalisation and to examine the future of legal services.

This article is based on a panel discussion that was held in Legal Tech Lab's international conference "Law and Digitalisation – Rethinking Legal Services" addressing the tension between disruption and regulation. Consequently, this article is a

combination of opinions of specialists who work closely with digitalisation of legal services. These specialists include Hannele Korhonen (Contract Mill), Kirsi Larkiala (Global Top 100 Fintech Influencer), Marko Loisa (Ministry of Justice), Markus Oksanen (DLA Piper) and Suvi Uski (University of Helsinki, Someturva).

The structure of this article follows the structure of the panel discussion. First, in order to understand digitalisation of legal services, we ask what happens when disruption meets regulation in general. The next section provides an overview of lawyers as potential change makers. Following on, we address ways for the legal field to embrace technology and to use legal technology in practice. We also try to understand the boundaries for disruption. This article ends by thinking ahead to the lawyers' future – not forgetting the final words of wisdom.

2 LIVING BETWEEN DISRUPTION AND REGULATION

Disruption provides essentially more access to justice. This is probably the most significant consequence of disruption from a legal perspective. In other words, technology brings new opportunities and makes it easier for all persons and companies to have access to both legal services and legal knowledge. New tools, resources and knowledge are being introduced, which is important for the rule of law. At the same time, there are still barriers for people to get legal services. The world is more and more complex and the legal certainty goes further from the ordinary people. This is a problem and legal technology is providing an answer to the problem.

From a more practical perspective, living between disruption and regulation means that disruption is followed by regulation – and regulation needs to be followed by individuals and

companies using new technology. It has been said that there is a massive "regulation storm" as a consequence of disruption and digitalisation – and even more regulation to come because of the attempts to control disruption. This development can be seen as a circle for many companies: When companies try to comply with regulation, they implement compliance programs, which are often implemented with the help of automation. Consequently, compliance requirements deepen the need for technology and make companies to welcome regulation technology software.

In the financial industry, disruption is the beginning of a new decade which can be verified also by following what kind of vacancies there are open for lawyers in banks and insurance companies. Traditional service providers have to be aware of how regulation affects different structures and products offered to customers. On the other hand, there are lots of Fintechs - start-ups but also established Fintechs - that face the massive regulation looking from a more algorithmic, technology point of view. For all financial sector service providers disruption is also about contracts and how to co-operate with customers and each other in the changing world.

From a legal service provider's point of view, disruption means more advisory type of work. Essentially, the purpose of law firms has always been to help customers to interpret and deal with laws and regulations. Also, regulatory authorities are constantly seeing what can be done better and in a different way than before because of disruption. For example, judges are living everyday between disruption and regulation as they build up new IT-systems for the courts and prosecutors' offices, changing the whole working method of those authorities.

To summarize, living between disruption and regulation means, among other things, more access to justice, increasing regulation, new legal services and digitalisation of existing services. The good news is that regulation is not considered as negative or burdensome as one could think. This follows from

the market logic that regulated industries are more trustworthy than unregulated industries.

3 LAWYERS – CHANGE-MAKERS OR RISK MANAGERS?

Lawyers' traditional roles can arguable be said to be changing in the overall digitalisation development. It was not long ago when lawyers were considered mainly as conservative risk managers. What should we think of the new development?

First of all, when considering lawyers' changing role from the "traditional lawyers" point of view, it is important to remember that lawyers' role is not only to interpret law but also to interpret the society and how it changes. All lawyers should adapt their mindset to the change and rather be the ones changing the world than just observing the change around them.

In accordance with the aforesaid, lawyers should be change makers rather than risk managers. Managing risk is and will be important to lawyers, however, the world is changing and so should lawyers. The new generation of lawyers will make the change evitable, but it would be important for all lawyers to be part of the change.

Taking active part in the change is also much more interesting than just stand back and watch. In Silicon Valley, for example, many founder teams of legal technology start-ups include a person with a background in a law firm in addition to the technology specialists. The more modern and complex services are created, the more lawyers will be needed. Of course, the change challenges lawyers also professionally as it requires lawyers to understand and interpret regulation in the light of the new services.

Regardless of the lawyers' personal opinions, technology is and will be a vital part of their careers and everyday life. It is therefore also self-preservation to take a positive stand on the future. Being a change maker does not mean that everyone should be specialized in digitalisation. Adapting new methods is rather a question of attitude than anything else – the change can be made with small acts.

4 WAYS FOR THE LEGAL FIELD TO EMBRACE TECHNOLOGY

New technology is making an emergence into the legal profession in many ways. This is not only inevitable but also interesting, because historically the whole legal field (and not just the individual lawyers) has been change resistant, and legal services have been strictly controlled and regulated.

A large part of embracing technology in the field of law is about the social norms that are shared in the legal professionalism. It is about how new ideas are welcomed or how difficult problems are tackled in that specific group of people – in this case lawyers.

Embracing technology in the field of law is also a lot about focusing on solving real life problems in everyday work. What should or could be automated? Could technology bring something new to the way we complete our work? Developing helpful ideas for one's own use might turn out to be helpful for others as well and follow with great opportunities in the field of legal technology.

Thinking back, it can be said that the biggest legal technology innovation so far happened in the 1990's when the Internet was invented, and Google launched its search engine. Even though Google is not a legal information research tool, it has made also the life of lawyers easier, and the usability of IT-tools and systems

still plays a great role in the change in practice. For example, the importance of proper IT-systems in the public sector has not been highlighted enough.

In terms of legal technology today, there are many good examples of legal technology innovations in Finland: artificial intelligence (AI) technologies, strong IPR-sector and great start-ups in the technology field. Technologies relating to contract automation and contract review automation discovery type of services are not yet too common in the Nordic, but there are examples also of such services.

As there is a great need for technology also for legal advisors and compliance officers, "RegTech", the regulation technology software, should also be pointed out. RegTech means the use of technology to facilitate the delivery of regulatory requirements. As such, the combination of regulation and technology is not new. It is, however, becoming more and more essential as the amount of regulation rises and focus on data and reporting increases. It is also something that brings new aspects to law, education and lawyers' work – and it will play even more important role in the future.

The focus in embracing technology should in the future be in creating possibilities to customers – take for example ODR, online dispute resolution. Regardless of whether the focus is on private sector or not, ODR is something to concentrate on. At the same time, it is important to understand that innovations come from the players on the market, not from the actual companies on the market. Co-operation is the solution, not competition.

New innovations require co-operation between all players in the field, including lawyers. It is crucial to communicate and work with each other to reach better results. This means lawyers need to start thinking outside the box and open up to new ideas. There is a lot to learn and embrace from the technology side – their agility to work, open-minded way of thinking and developing new ideas. The combination of technology, competitors, market

players and lawyers working on the background opens up a whole new field.

5 BOUNDARIES FOR DISRUPTION WITHIN THE REGULATED AREA OFLEGAL SERVICES

Boundaries for disruption in the area of legal services form a difficult question. Demarcation between disruption and regulation will without doubt be an eternal battle. The only clear answer seems to be that lawyers cannot control the legal field as they used to do.

Disruption is already changing the legal services traditionally offered by law firms. For example, law firms are not anymore a "one stop shop" for all legal work, as alternatives are offered by new types of service providers. In addition, disruptive technology is taking place at all ends of the spectrum. Digital communication, self-help and efficiency tools as well as artificial intelligence are each part of the change.

In order to avoid collisions in the future, law firms need to come up with creative solutions how to simultaneous serve their clients and handle the challenges caused by disruption. One way to differentiate from other service providers follows from regulation. Law firms, in particular attorneys, are usually under strict code of conducts and supervision, whereas consults, legal technology companies and start-ups are not. Of course, all operators have to work under mandatory laws and be liable for their actions but being a service provider subject to supervision might be an advantage in providing legal services.

In the age of disruption, lawyers can be seen as the last defenders of the rule of law. If nothing else, the regulated providers of legal services stand for ethical standards in a way no-one else can or

will. At the same time, supervised law firms might remind others that even in the non-regulated sector of legal services there are moral and ethical standards — and private and customary rules.

At the end of the day it is the client who makes the final decision on the future of legal services and service providers. The key in the changing field is trust between the client and the lawyer – not the law firm behind the lawyer or the technology. The importance of trustworthy relationships will stand out even more in the future and high ethical standards might form also a unique selling proposition.

New innovations will most definitely bring whole new aspects to this discussion. Sharing economy is one rather ongoing trend at the moment as well as blockchain technology. These two developments have and will change rapidly our way of living and will reflect also to the boundaries for disruption in the legal field.

6 THINKING AHEAD – LAWYERS' FUTURE

Coming back to individual lawyers, it has been said that lawyers could be replaced by artificial intelligence. Automation of the legal services will increase efficiency and save money but might also reduce work as technology will take care of tasks currently performed by lawyers. Advocates of artificial intelligence, however, argue that there might even be an increase in the workforce as technology makes legal services more affordable to ordinary people.

As it is to be seen that everything that can be automated will be automated, we should be prepared, but still welcome the change open armed. The change should be seen in a positive way, as less of the lawyers' time will be spent completing routine work. Focus of the daily work will change and can be integrated into the most essential tasks. Accordingly, in the best scenario,

both legal services and legal protection will be improved through automatization. Timing wise, lawyers' role as a trusted adviser will most likely not change in the near future, but automatization will be an evitable change which will happen sooner rather than later. Technology will develop throughout, but enormous changes, such as fully automated contracts which are readable only trough machines, might still take some time. When that happens, lawyers' role also in the contract world will rapidly change.

It is an interesting question how automatization will affect lawyers' work even in courts. It is not too far-fetched scenario that a court session would be held through digital applications. The court is still, however, quite conservative, so the first step could be for example providing tools to analyse case law. In this connection, it is not only a question whether lawyers are ready, but also whether the legislator is ready for the forthcoming changes. In any case, digitalisation offers endlessly opportunities and the change will be evident also in the public sector.

Predicting the future is difficult, but lawyers need to prepare themselves to the forthcoming changes. It is now even more important than before for lawyers to take care of professional development and respect their path. Lawyers' work might be more complex in the future or it might dramatically diminish, but part of the change will be people's attitude towards law – they will most likely feel more protected by law and trust the law more.

The changing work field will be interesting to all lawyers who are open for change. Standardized work can and will be automatized with the help of technology. However, part of the work will always be advisory type of work solving complex issues. This also means that part of the work will be taking care of and communicating with natural persons – which is perhaps the most interesting part of the lawyers' work.

7 FINAL WORDS OF WISDOM

In a world where change is the only constant, an article on disruption and regulation cannot end with any final truths. Instead, we all need inspiration. Accordingly, here is some food for thought for any lawyer's digital journey:

- Do not be afraid of new – instead, try something new today;
- Do not ask why – ask why not;
- Adapt to change;
- Learn to think a little bit more like a disruptor and less like a lawyer;
- Believe in yourself – justice is still made by people;
- Have curiosity about digitalisation;
- Learn to understand technology's impact on the elivery of legal services;
- Embrace co-operation in whatever you do – it will be the key to success;
- Take a lead and show good example to others;
- Legal technology offers endlessly opportunities – as your legal solutions can be made global so can your professionalism.

As the moderator of the panel discussion, I wish to present my warmest thanks to all the panellists for sharing their thoughts on digitalisation and caring for the future of the legal field.

HANNA-MARI MANNINEN
Partner, Dittmar & Indrenius Attorneys Ltd.

AIPA - the Project for the Digitalisation of the General Courts and Prosecution Offices in Finland

1 INTRODUCTION

Digitalisation is most of all a new way to do things. It´s also an attitude that we can do things differently. New technologies make digitalisation possible and give tools for making the change.

AIPA (Aineistopankki – Material Bank) is the project for the digitalisation of the Finnish prosecution offices and general courts (District courts, Courts of Appeal and the Supreme Court). The project´s aim is to get rid of paper in legal work altogether,

and change the working methods from those based on paper to those that are electronical. The change will be somewhat of a revolution in the way the courts and prosecution offices do their everyday work. As part of the project, a new IT-system is being built to support the digital working methods. The project is organized in the Ministry of Justice.

2 DISRUPTION IN THE WORK OF THE JUDICIARY

The courts and prosecution offices are most likely not the first thing which comes to mind when thinking who are the leaders of the digitalisation within the public sector. But that is exactly what we want to be in the AIPA-project. Not just an evolution, but a revolution of the working methods is the aim of the project.

How can we achieve this goal, which might seem a difficult one? Getting the legal professionals onboard as early as possible when planning the digital working methods is the key, we think. Also, the building up of the new IT-system has to be user based. Change management and the building up of the IT-system have to go hand in hand all the time.

3 MAKING THE CHANGE TOGETHER

The Ministry of Justice has made a strategic decision from the start of the AIPA-project to give the power to decide to the legal professionals, judges, prosecutors and secretaries, who work at the general courts and prosecution offices. The project office was built to be responsible for the whole project, both the change management and the IT-system. Concerning the IT-system, the

main responsibility on the project office is to make sure that it meets the criteria of the end users when it comes to usability and how it suits their work. In the project office there are 10 professionals from the courts and prosecution offices who work fulltime for the project.

To get the ball rolling and to start the change in the judiciary, the project has a network of over 200 change agents all around the country. The project office coordinates their change management done locally in their respective courts and prosecution offices. Already there are more than 100 different experiments ongoing, where the new digital working methods are practiced as part of the everyday work using the current technologies and possibilities the end users have. The results of the culture of experimentation have been very positive. The AIPA-project and it´s network of change agents even received the Kaiku-award for the new work methods in the year 2017 given annually to the best practices in the public sector in Finland. As part of the work of the change agents, a concept manual for the digital court proceedings has been published. The idea behind the manual is to collect the best practices of the different experiments done around the country and make them available to others.

4 AGILITY IN THE PUBLIC SECTOR

Agile project models are needed when building IT-systems that have strategic meaning and possibilities to enhance the way work is done in the general courts and prosecution offices. Traditional waterfall models have their place, but when talking about a large scale IT-system that is being built for a totally new way of working, the agile way seems to be the best way.

The legal experts in the project office work together with the IT-experts day to day. The judges, prosecutors, and secretaries work as Product Owners and constantly make decisions about the functions of the IT-system together with the IT-specialists. The Legal Register Centre has allocated some of it´s IT-experts to be part of the project from the customer´s side. Private IT-companies are chosen in procurement processes to do the development of the IT-system. Even though there are many different actors with different backgrounds working in the project, it´s important that everyone works for the same objective. In the AIPA-project we have found it useful that the whole project works in the same office space in ongoing cooperation to get the best results.

In the AIPA-project, the IT-system will be built gradually in parts. The first part of the system has been in use in the prosecution offices from February 2017. The feedback from the prosecutors has been positive when it comes to the usability and the way the AIPA-system supports their work. Next part of the IT-system will be taken into use in the year 2018. The whole project will be finished in the year 2021.

After the project, the development doesn´t stop but it will continue in maintenance. The digital working methods and the IT-system that will be built in the project will also build a base for future development. We have to be ready for the next steps, that will include the use of AI and sophisticated analytics tools, for example.

5 THE CUSTOMERS' POINT OF VIEW

How will the digitalisation of the judiciary affect the private people, companies and other customers of the courts and prosecution offices? The new digital working method and a modern IT-system that supports it will guarantee that the courts and prosecution

offices can guarantee a high level of legal security also in the future. There are budget pressures in the public sector and we have to take steps to ensure that the rights of private persons, companies, and organizations are met in a timely fashion and with a high quality, this also needs to continue going in the future. Applying lean-thinking and changing the working methods from paper-based to digital is one important way to ensure this. Our customers also have rising expectations when it comes to the possibilities to digitally be in contact with and to send and receive information from the judicial authorities. As part of the AIPA-project, there are plans to build new ways for our customers to be in contact digitally with the general courts and prosecution offices. Also, the hearings at the courts are changing. The digital court process will make it easier for the customer to be heard at the courts in some cases through electronic ways without having to be present at the court personally. The material in question will be seen in screens in the court rooms and the publicity of the hearings will be higher because of that.

The judges, prosecutors, other legal professionals and secretaries are through the AIPA-project change agents of the digitalisation for the public sector. Through their work in the project, there will be a positive impact for the whole society.

6 WHY SHOULD USABILITY BE AN ISSUE?

Should the IT-systems for the courts and prosecution offices be user-friendly? It is the work of civil servants that we are talking about here and, one might argue that the state should not spend it´s resources on getting their data systems easy to use. I have answered this question time and again during our project. This is something that the AIPA-project sees differently than maybe other projects have done in the past. From our point of view, “easy

to use" equals more efficient working. When the end users don´t have to spend their time trying to figure out the functions of the IT-systems or do unnecessary steps to get the work done, there will be more time for the most important work in the judiciary, that is legal decision making and tasks that directly support it. User-friendliness not only leads to more efficient working but is also one of the most important tools to get the judges, prosecutors and secretaries make a radical change in the way they work and switch to the electronic administration of justice.

When talking here about user-friendliness, I don´t only mean that the end-users functions in the IT-system should look modern and be pleasant to use. More than that, I mean that the IT-system should accommodate the work it was intended to be used for. We have to go the end users needs, not technology first. We are not making the IT-system user-friendly for ourselves but want to create better legal security for the customers of the courts and prosecution offices by switching to electronic working methods and having a modern data system that supports the new working methods. One can´t have more efficient working without an easy to use IT-system.

User-friendliness is even more important when talking about the new ways the customers can be in contact with the judiciary digitally. Here we have to consider the principle of access to justice. The new digital ways of communication between the customers and the judicial authorities, for example, portals for private people, companies and their legal counsels, have to be easy to use so people will understand their meaning and functions and can get to their legal rights. After all, the end users of the legal security that is created in the judiciary are the customers.

MARKO LOISA
Project director, Ministry of justice

Disruption in the Legal Sector Begins With Small Challengers

1 INTRODUCTION

If you ask any start-up about their "Why", their raison d'être, they most probably say they want to disrupt the market. For the relatively young legal tech industry this may be even more true than for some other more mature tech industries and, at least for me and our start-up, disruption is one of the core reasons why we exist.

The word disruption however seems somewhat inflated since everyone is doing it; or at least everyone is saying they're doing it. So, what does disruption actually mean and why is it important? Why does it necessarily start with small challengers?

2 WHAT IS DISRUPTION IN THE LEGAL DOMAIN?

Disruption is not the same thing as change as it goes far beyond doing things differently. By its core definition in economics, disruption relates to competition and survival or extinction in competition while theory of disruption aims to predict what competition does in response to existing services and products.

When explaining disruption, Harvard Business School Professor and theorist of disruptive innovation Clayton Christensen makes a difference between disrupting and sustaining innovations. Innovating is not something that only start-ups do, but big, established companies also innovate and develop their offering constantly by building better and better products. The issue with these innovations at big companies is that they develop faster than customers' needs, which leaves many customers unserved without suitable or accessible services or products. Disruptive challengers will then find these people or businesses and develop innovations that allow them access to the services and products as well. Disruptive challengers fight the sustaining giants, which are then gradually forced to either change or go extinct.

This is exactly what is happening in the market of legal technology and legal services as we speak. We are seeing the early signs of disruption. We see that big, established software companies that have existed for decades are offering products that are sophisticated, complicated and expensive – and beyond the reach of many. Similarly, we see that big, established law firms which have existed for decades are offering sophisticated and expensive services which are beyond the reach of many. These players are doing what they do best, charge high prices to their most demanding and sophisticated customers at the top of the market and make good profits while they're at it. At the same time we are now beginning to see that the market is open for

small challengers that will start from the bottom, looking for the unmet needs, unserved customers, and unproven opportunities. These small start-ups do what they do best, they dare to do things seemingly wrong, explore, and pay attention to the needs of those who have not been heard before and open-mindedly see where this development takes them.

3 SO WHY IS THIS IMPORTANT?

Disruptive businesses create much improved services and products and make it possible for a larger group of people and companies to use or otherwise benefit from technological development. Successful disruptive innovations force traditional businesses to change and this leads to technical progress. Typically disruptive innovations also mean that not only those who have the money and skills but also those with less money and less knowledge get access to the services and products they need.

For me, disruption within the legal domain means a profound change in the way legal knowledge is made accessible to all. We are all affected by our legal system everyday so we should all be able to access not only knowledge of the rules and processes we are subjected to but also knowledge of ways to work the system in our benefit. This is why it is important that at long last the legal industry also undergoing massive changes, i.e. disruption is emerging.

Disruption changes the dynamics of the legal industry so that the market will no longer be dominated by big law firms, but new companies with new scalable business models and new technology-powered products and services are winning more mandates. The legal industry is also no longer a lawyer monopoly for legal knowledge - we are already seeing how alternative

service providers are entering the market and shaking the status-quo.

Accessibility means that legal services are available at lower prices and thus accessible to more people. Your legal protection is not dependent on the depth of your pockets and, in addition to this, you no longer have to pay for the inefficiency that can be solved by technology. If you are a legal service provider, technology enables you to scale your business like never before making it also possible for you to provide services at lower cost and at lower price for your customers.

Disruptive innovations are inevitably developed to solve real-world problems with and close to the users. Small technology providers have a constant challenge to be able to meet and even exceed the user needs while big companies can develop services without any validation and then notice there is no market need for it and start over. Small companies cannot waste months and years behind their drawing boards speculating what works and what not, they need to quickly identify, address, and creatively address the real business problems. Resources are well spent.

It is important to emphasise that accessibility is not only a question about money, who can afford to pay for technology or services, but especially with technology it is also a question about usability, how simple and intuitive the technology is. New technologies will not become disruptive if they are not easy to use and thus accessible to all users, even lawyers. In our product development there has been one rule above all, if our product is not easy to use, it is not worth our effort. There is no point of developing and selling complicated technology to chronically busy lawyers. We have wanted to take the target even further, we believe that technology should not only make things easier but to bring joy to users.

Finally, on why disruption in the legal domain is important. Disruptive innovations make complex legal knowledge more simple and understandable to be able to serve the new target

markets. This approach, which builds products and services by first listening and empathising customers and by lawyer going to the customer, turns the table between legal service provider and customer completely by putting customer on the pedestal. My hypothesis is that legal design will be at forefront of the disruption.

4 WHY SHOULD YOU CARE?

If you are a lawyer, you can of course choose not to care, but do you really want to? The world is changing whether you want it or not, and at last the change is affecting also the legal industry on bigger scale.

Those who are early adopters and visionary are change makers, they can set the stage and not remain as mere bystanders. Lawyers should take the lead in innovations that help their work since they know their real-world problems the best. They can also excel in honouring the best practices of their business conduct in defining clear boundaries to disruption based on ethics and values like loyalty, independence, competence, confidentiality and trust.

This massive change that is brought by legal tech promises good things for your future if you are open and ready to let them in. You can let the machines do what they do best, handle routines and repetitive tasks while you are trained to and can do exactly those things where machines cannot go. You can do subtle and novel things and have real-life encounters with people. You can be more who you are and who you want to be, strategist, negotiator, advisor, developer - and also have life outside work.

5 WHY DISRUPTION STARTS WITH SMALL CHALLENGERS?

The previously cited Clayton Christensen's theory persuades that small challengers are inevitable for disruption. Successful companies simply fail to produce disruptive innovation since it is in their interest to produce better and better of the same with less defects and increase efficiency in all their doings. It is not in their interest to dedicate resources to try something different, to lower gross margins, smaller target markets and simpler products. Small challengers are the ones who have interest to fill in the gaps, they will gladly serve those who have not been served before.

Besides the economical logic of start-ups starting disruption, there are also other reasons why such fundamental change, especially in the legal domain, starts with the small. The legal domain by its nature resists change. At the core of the legal profession is the ability to see problems and risks everywhere and it is therefore very natural that lawyers step into new technology cautiously. Lawyers are not usually praised for being risk takers but rather for their ability to identify and avoid risks, while disruption inherently means risks and uncertainty.

Also, service providers dominating the legal market do not see the need to change or consider the change even relevant for them. Let us see someone else doing it first and we will follow if it pays off, some might think, and as long as billable hour sells, change may actually work against and not for these service providers. It is understandable and follows the logic of so many examples before - necessity is the mother of change. This is why it is important to have small pioneers who will make bold bets and who will take leaps of faith to get the train moving.

For these reasons, I argue that the forces leading to disruption in the legal domain happen outside big companies. Fundamental change happens first in law firms offering services to consumers

and small businesses and then the change moves up the industry. Similarly, in terms of legal tech providers, those serving small law firms will be on the driving seat of disruption. Luckily there are plenty of opportunities also for careful observers and hesitant big players to be part of the change and enjoy the ride. Everyone is invited.

HANNELE KORHONEN
Co-founder and chairman, Contract mill

III

Legal Education for the Next Generation

ILKKA TOIKKANEN[1]

Legal Tech Lab - the Student's Perspective

As a final year law student, I would be a total fraud to try and preach about the effects of legal digitalisation (though I can pretty convincingly use buzzwords and talk about Susskind et. al.). However, as one of the law students helping Legal Tech Lab take its first steps, I can tell you what it is like to be part of a group looking to understand those effects. I have had the privilege to see the initiative grow from an ambitious idea to what it is today. Since I admit being a bit sceptical at the beginning, suspecting that the Lab would turn out to be just another techy-hypey-start-uppy sprout of the Helsinki scene in its Slush hangover, and end up being maybe a Facebook group, I could not be happier that I was proven wrong.

From the start, that was our first falafel meeting in a restaurant near Porthania in January 2017, our director Riikka Koulu envisaged Legal Tech Lab to be something for the students. After all, we are the ones in the core of the conversation about

1 Ilkka is a LL.M student at the University of Helsinki, Faculty of Law

legal digitalisation, the ones "being replaced by AI" and "having to learn to code". That student empowerment has fortunately stuck around and formed the foundation, on which actual physical things, such as a successful conference (Law and Digitalisation – Rethinking Legal Services), a hackathon (Hack the Law!) and this publication, have been built. Even though I have been trying to slowly transfer towards the ranks of the alumni, I still have some insider information and can assure you, that the Lab has some really interesting things in the works.

The Legal Tech Lab aims to bring together stakeholders from both the private and the public sector, NGOs, academics, students, and anyone interested. The bottom line being that legal digitalisation should be a common effort. What we can do to further the transition to everything legal being digital, is to provide a forum for discussion for the groups involved and to produce information to facilitate as victimless and sustainable an evolution as possible. In the future, I hope this could, in practice, involve things such as telling the start-upper how to build her app in a way that does not go against the GDPR and the ePrivacy Regulation or how to make a public welfare service digital without violating the fundamental rights of the elderly, who do not know what an app is. Or it could be telling the lawmakers what kind of regulation (or lack thereof) could foster the creation of GDPR-compliant apps that can be used by grannies.

For a student volunteer the Lab life holds event organizing, drinking champagne, and eating pizza, publishing scientific, and not-so-scientific, texts and, for the most daring ones, giving different stakeholders talks about the Lab and the things we do. It also means meeting real-life legal professionals, who are interested in hearing how we, the Lawyers of Tomorrow (pun / cliche intended), see the future of the profession. Of course for us - the first batch of volunteers - the bottom-up orientation of the Lab meant that melding into the shadows in a conference room corner and getting a nice new bullet point for our CVs was

not an option. Since the Lab's crew was small but the things we wanted to do were not, all hands were constantly needed on the deck. Even though more volunteers are being recruited, the Lab's operations are growing in proportion. Thus, I would say that assessing by the study credit-to-work ratio, volunteering is not the smartest move, but on the other hand, the advocates of such ratio are not necessarily the ones the Lab wishes to reach.

However, because the fundamental reason for law students to study law still naturally is utility, be it money, social status or proving things to our demanding parents and entitled friends, volunteering in the Legal Tech Lab has to be competitive for us. And it is, believe me. The ideas and topics discussed in the Lab events and meetings are of course interesting, but the inclusive and supportive atmosphere of the crew is the main reason I enjoyed my volunteer experience. Such atmosphere, where there are no wrong or stupid answers, is ideal for a student trying to build his/her academic and professional self-esteem and identity. Especially, when there will be plenty of stupid and wrong answers in the life of a graduated lawyer giving real-life legal advice. The importance (for your mental health and your career) of meeting nice new people who are interested in the same niche of things as you, cannot be emphasized enough. That is particularly true when that niche happens to be something changing our profession as we know it.

What I, as a soon graduating Legal Tech Lab volunteer, wish is that the Lab will somehow stay in touch with its alumni. I have the feeling that among the volunteers will emerge a group of top academics and legal professionals occupied with the intersection of law and technology. We could serve as the antennae observing the technology related woes, wishes and discoveries of the legal community and help to steer the Lab and its new student volunteers in the direction where the action is.

IIRIS KESTILÄ[1]

Patenting Blockchain: Insights from the Perspective of the European Patent Convention

1 INTRODUCTION

During recent years the blockchain technology has gained the attention of a growing audience, including companies, start-ups and state authorities. For example, in 2015 NASDAQ announced to have been able to use its Nasdaq Linq blockchain ledger technology to successfully complete and record a private

1 Iiris is a LL.M student from the University of Lapland, Faculty of Law.

securities transaction.[2] In 2016 R3 Consortium and member banks announced to be working on a distributed ledger technology.[3] Blockchain has even been forecasted to be the next big technical revolution after Internet, although only time will tell what the technology in practice has to offer for large crowds.

As blockchain seems to be attaining more mainstream status among corporations, questions about intellectual property rights arise at the same time. During 2016 some of the biggest names in business have applied for blockchain-related patents for their innovations created using blockchain-related technology.[4] This has caused a great controversy, as blockchain has traditionally been considered as open and accessible technology, available for anyone to exploit. If these patent applications have success in Europe, any company or private person willing to enter the market must consider, whether rights to particular blockchain innovation already belong to someone.

Blockchain technology derives from the white paper published by pseudonym Satoshi Nakamoto, creator of Bitcoin, who coded the first implementation and then disappeared.[5] Reasons for this remain unknown. However, this has raised questions about whether blockchain can be patented in the first place, since the core of technology has been already made

2 'Nasdaq Linq enables first-ever private securities issuance documented with blockchain technology' (Nasdaq, 30 Dec 2015) <http://ir.nasdaq.com/releasedetail.cfm?releaseid=948326> accessed 15 Sep 2017.

3 Richard Gendal Brown, 'Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services' (R3, 5 Apr 2016) <http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services> accessed 15 Sep 2017.

4 Olga Kharif, 'Big Banks Are Stocking Up on Blockchain Patents' (Bloomberg, 21 Dec 2016) <https://www.bloomberg.com/news/articles/2016-12-21/who-owns-blockchain-goldman-bofa-amass-patents-for-coming-wars> acccessed 15 Sep 2017.

5 Satoshi Nakamoto could be a person or a group of people. The white paper behind Bitcoin can be accessed here: <http://nakamotoinstitute.org/bitcoin/> accessed 15 Sep 2017.

available to public.[6] This article aims to give insight on the patent eligibility of blockchain technology and what does that mean for software business in general. I.e. on what basis innovations built on blockchain could be granted a patent. However, drafting a patent application is not the intention here. As will be discussed, there is a certain divergence between purposes of use and practical implementations regarding blockchain applications. Therefore general guidelines for patenting issue are hard to give. The question of patenting blockchain is closely related to the old problem of patenting innovations based on computer-programs.[7] What this article also aims to find, is what kind of interpretations can be derived from the European Patent Office's (EPO) previous legal praxis and how do those comply with blockchain-technologies. These findings are applied to practice via case study.

Examination is done from the perspective of European legislation. Whereas blockchain-related technology could quite possibly be covered by other IPR instruments as well, such as copyright, trademarks and trade secrets, here the focus will be placed on patent protection available under the European Patent Convention[8] and praxis of the EPO. The focus is on the patentable

6 'A rush to patent blockchain is a sign of the technology's promise' (The Economist, 12 Jan 2017) <http://www.economist.com/news/business/21714395-financial-firms-and-assorted-startups-are-rushing-patent-technology-underlies> accessed 29 July 2017.

7 Term computer program is sometimes used overlapping with term software. Here software is considered to consist of computer programs, procedures, associated documentation and data. Question of patenting could be different between computer programs and software. See Rosa Maria Ballardini, 'Intellectual property protection for computer programs: Developments, challenges and pressures for change' (Hanken School of Economics 2012) 11.

8 The Convention on the Grant of European Patents of 5 October 1973 (the European Patent Convention, EPC).

subject matter.[9] Whereas it's true, that this subject has been already explored to some extent, interpretative problems remain in the EPO's practice regarding computer programs. It's probably safe to say that blockchain is not the last new, computer-based technology world is about to see upcoming years. Cases discussed in this article indicate, that computer programs have in fact entered the patentable subject matter to some extent. However, it still remains somewhat unclear, on what basis can programs be patented. Therefore it's necessary to continue this discussion.

2 BLOCKCHAIN VS. DISTRIBUTED LEDGER

To fully grasp the scope of possible IPR protection, first it is necessary to understand what blockchain is. The underlying, basic technology will be shortly discussed. However, this article is not meant to give specific, technical insight on the matter. As the overall discussion consists of multiple terms used to describe the technology, terms will be briefly visited.

Blockchain technology has been said to represent the next step in the peer-to-peer economy. Blockchain enables people to form an agreement, and record it in a secure manner. This is done by combining peer-to-peer networks, cryptographic algorithms, distributed data storage, and a decentralized

9 Innovations that are susceptible of patent protection are referred to as patentable subject matter. Art 52 sets the limits of patent eligible subject matter. 'European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application.' However, Art 52 also excludes some forms of invention from patentability.

consensus mechanism.[10] Blockchain itself is usually considered as a globally shared, transactional database.[11] Traditional use of blockchain means that everyone can read entries in the database by participating in the network. Changes in the database protocol can only be made by acceptance of all others.[12]

Blockchains are built of 'blocks', which can be described as datasets containing information about a number of transactions.[13] If two transactions contradict each other, the one that ends up being second will be rejected and not become part of the block. Linked to the preceding block a linear sequence in time is formed.[14] Every block also contains an answer to a complex mathematical puzzle, which are however easy to verify.[15] This way the data associated with the block is validated. Every computer in the network stores a copy of the blockchain. The computers periodically synchronize, to verify the transactions and to ensure that all of them share the same database.[16]

10 Wright Aaron and De Filippi Primavera, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (March 10, 2015) Available at SSRN: <https://ssrn.com/abstract=2580664> 4-5 accessed 29 July 2017.
11 Michael Crosby and others, 'BlockChain Technology: Beyond Bitcoin' [2016] (2) Applied Innovation Review 6, 7. See also 'Blockchain' (Bitcoin Foundation Wiki) <https://en.bitcoin.it/wiki/Block_chain> accessed 13 Sep 2017.
12 Riikka Koulu, "Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement", (2016) 13:1 SCRIPTed 40, 50 <https://script-ed.org/?p=2669> DOI: 10.2966/scrip.130116.40 accessed 13 Sep 2017.
13 Wright and De Filippi (n 9) 6.
14 Shackelford Scott and Myers Steven, 'Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace' (2016) 19 Yale J L & Tech 334, 4. See also 'Introduction to Smart Contracts: A Simple Smart Contract' (Solidity) <http://solidity.readthedocs.io/en/latest/introduction-to-smart-contracts.html#blockchain-basics> accessed 29 July 2017.
15 Koulu (n 11).
16 Wright and De Filippi (n 9) 6-7.

Alongside blockchain, the term distributed ledger is being used.[17] In 2016 R3 consortium, which is a collaboration by financial institutions, presented their idea of distributed ledger Corda.[18] Distributed ledgers usually consist of a ledger, which multiple parties use, and which is stored across multiple locations. Blockchain on the other hand, is usually considered to have all three of these things, but where they differ from for example Corda, is how much they share and with whom they share that. Transparency is often considered to be one of blockchain's greatest strengths. Allowing platforms to operate without a central validator turns them highly resilient. Sufficiently decentralized and incentivized it becomes infeasible to shut down the network or make unauthorized changes. The main difference between distributed ledger technology and blockchain is usually considered to be whether the participants are known to each other and whether the participation is permissionless.[19] Distributed ledgers overall might also make limitations to other

17 "Blockchain" is also alternatively referred to as "multiple distributed ledger technology" (MDLT), "distributed ledger technology" (DLT), "shared ledger technology" (SLT), "consensus ledger" technology, "mutual distributed ledger" technology or a decentralized or "distributed database." McJohn Stephen M and McJohn Ian, 'The Commercial Law of Bitcoin and Blockchain Transactions' (November 22, 2016) Uniform Commercial Code Law Journal, Forthcoming; Suffolk University Law School Research Paper No. 16-13, 6-7. Available at SSRN: <https://ssrn.com/abstract=2874463> accessed 29 July 2017; Angela Walch, 'The path of the blockchain lexicon (and the law)' (2016) 36 Rev Banking & Fin 713, 3; Colin Platt, 'Thoughts on the taxonomy of blockchains & distributed ledger technologies' (27 Feb 2017) <https://medium.com/@colin_/thoughts-on-the-taxonomy-of-blockchains-distributed-ledger-technologies-ecad1c819e28> accessed 7 Sep 2017.

18 Richard Gendal Brown, 'On distributed databases and distributed ledgers' (Gendal, 8 Nov 2016) <https://gendal.me/2016/11/08/on-distributed-databases-and-distributed-ledgers> accessed 29 July 2017.

19 Walch (n 16) 10; Martin Valendna and Philip Sandner, 'Comparison of Ethereum, Hyperledger Fabric and Corda' (2017) Frankfurt School Blockchain Center Working paper, 2-3 <https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6?platform=hootsuite> accessed 15 Sep 2017.

properties of traditional blockchain technology, used for example in Bitcoin.

As said, terms blockchain and distributed ledger are sometimes overlapping. It has been argued that blockchain and distributed ledger technology are basically the same thing, and platforms such as Ethereum and BitNation are samples of distributed ledgers.[20] At other times the terms are taxonomically separated, whereas blockchain is seen as technology described in Satoshi Nakamoto's paper, de-centralized and permissionless, and distributed ledgers are spoken in the meaning of mainly commercial use, where participation is limited.

Here the combination of terms will be used. For example in case Goldman, Sachs & Co. the application has been filed for distributed ledger, which will therefore be used. While this question of terminology undoubtedly bears some significance in the context of patenting as well, it is not further inspected here. As patents are often granted for seemingly small innovations (especially in the field of software) the details in technology might turn out to be crucial. When addressing the question of whether blockchain or distributed ledger technologies can be patented, it should be noted that current platforms use a variety of cryptographic and consensus mechanisms.

20 Michael Mainelli and Mike Smith, 'Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)' (2015) 3(3) Journal of Financial Perspectives 3, 14.

3 WHAT DOES THE EPC SAY ABOUT THE PATENTABILITY OFCOMPUTER PROGRAMS?

In Europe patentability is governed by the European Patent Convention. Requirements for patentability are invention, novelty, an inventive step, industrial applicability and sufficient disclosure for inventions in all fields of technology.[21] Conflicts and controversy have surrounded the European treatment of business method and software patents. The EPC states that all inventions 'which are susceptible of industrial application, which are new and which involve an inventive step' shall be granted a European patent. However, certain innovations are excluded from the patentable subject matter "as such" by Article 52(2), including computer programs.[22]

While computer programs are not considered as patentable subject matter as such, it does not mean they would not be patentable under the EPC. A computer-implemented invention is one which involves the use of a computer, computer network or other programmable apparatus, where one or more features are realized wholly or partly by means of a computer program.[23] If the core of the invention rests on a computer program, it is not considered patentable. However, if a computer program forms only a part of the invention, that invention may be patentable as long as the other patentability standards are met as well.[24]

21 EPC, Chapter 1.

22 Robert Thomas and Larry A Dimatteo, 'Harmonizing the International Law of Business Method and Software Patents - Following Europe's Lead' (2007) 16 Tex Intell Prop L J 1, 8.

23 'Patents for software? European law and practice' (European Patent Office, 2013).
<https://www.epo.org/news-issues/issues/software.html> accessed 7 Sep 2017.

24 Roy J Rosser, 'European software patents: when a rejection is not a rejection' (2005) 24(1) Intell Prop L Newsl 25, 2.

Under the EPO's practice, in order for a computer program to be patentable it must provide a technical solution to a technical problem.[25] Items excluded by Article 52 are considered non-technical due to their abstract nature, and if a claim is directed to these "as such", it will be rejected.[26] Although other requirements have been defined in the EPC, invention is not, therefore requirement of technicality has been formulated via practice. Computer programs "as such" have not been considered technical.[27]

The problem with the evaluation of technical character is connected to the computer programs dualistic nature of being a writing but also having capability to act. Programs components have no physical implementation, unlike traditional technical inventions. The consideration is done between computer programs excluded from the subject matter and patentable computer-implemented inventions.[28] To cope, the EPO has on different times developed different approaches to address the question of technical requirement and patentable subject matter. These approaches will be shortly introduced next.

25 Rainer Oesch, Heli Pihlajamaa and Sami Sunila, 'Patenttioikeus' (3th edn, Alma Talent Oy 2014) 59.

26 Rupert A Knights and Craig A Redinger, 'Patent eligibility of software patents in the U.S. and Europe: A Post-Alice Consideration', (2015) 8 Landslide 42, 5.

27 Rosa Maria Ballardini, 'Intellectual property protection for computer programs: Developments, challenges and pressures for change' (Hanken School of Economics 2012), 564.

28 Anna Haapanen, 'Free and Open Source Software Licensing and the Mystery of Licensor's Patents' (Publications of IPR University Center 2017) 75.

4 THREE APPROACHES

4.1 TECHNICAL CONTRIBUTION

In 1986 the EPO Technical Board of Appeal delivered a decision in Vicom,[29] where several claims were first rejected for relating to unpatentable mathematical methods. In the decision by the Board of Appeal processes considered abstract were however distinguished from those that produce a technical effect, and are therefore patent eligible.[30] The Board concluded that 'even if the idea underlying an invention may be considered to reside in a mathematical method a claim directed to a technical process in which the method is used does not seek protection for the mathematical method as such'. Therefore, the process can be considered as an invention and patentable if "technical contribution" is made to the state of art.[31] Even if an item to which claim is directed would normally be considered patentable, it won't be accepted if the contribution to the art is non-technical. Claim to a computer containing a novel program could not be accepted merely due the computer's nature as a physical equipment. Technical contribution needed to arise from the novelty of the software.[32] The program was considered patent eligible if it brought some technical effect, which was the subject matter of the application and made a contribution to the state

29 T 0208/84/Computer-related invention/Vicom (1987) OJEPO 14.
30 Thomas and DiMatteo (n 21) 9.
31 "Generally speaking, an invention which would be patentable in accordance with conventional patentability criteria should not be excluded from protection by the mere fact that, for its implementation, modern technical means in the form of a computer program are used. Decisive is what technical contribution the invention as defined in the claim when considered as a whole makes to the known art." T 0208/84/Vicom (n 28) Reason 16; Ballardini (n 26) 565.
32 Keith Beresford, 'Patenting Software Under the European Patent Convention' (Sweet & Maxwell 2000) 37.

of the art.[33] Basically, if imagining the invention as a machine was possible, protection could be granted. This approach was problematic where the invention was essentially program-based.[34]

4.2 TECHNICAL EFFECT

In 1990's the EPO started to apply a new interpretative line, later termed 'technical effect' approach.[35] The former contradictions were dealt with the IBM decisions[36], regarding the distinction between an invention which can be protected in software/hardware terms and one which can be protected as software alone.[37] In the decisions, the Board of Appeal reconsidered the meaning of 'technical character'. While further technical effect was still considered necessary for the invention to be patentable,[38] The Board revisited its machine-metaphor, now shifting towards the conclusion that software itself can be 'machine-like', and thus of technical nature.[39]

The Board concluded that Article 52 exclusion is not applied when a computer program produces 'a further technical effect which goes beyond the "normal" physical interactions

33 David Bainbridge, 'Introduction to computer law' (4th edn, Harlow: Pearson Education 2000) 110.
34 Philip Leith, 'Software and patents in Europe' (Cambridge University Press 2007) 35.
35 Ballardini (n 26) 565.
36 T97/1173/Computer Programs Product/IBM (1999) OJEPO 609 and T97/0935/Computer Program Product/IBM (1999) OJEPO 609.
37 Leith (n 33) 31.
38 Andre J Porter, 'Should business method patents continue to be patentable?' (2002) 29 S U L Rev 225, 11-12.
39 Susan J Marsnik and Robert E Thomas, 'Drawing a line in the patent subject-matter sands: does Europe provide a solution to the software and business method patent problem?' (2011) 34 B C Int'l & Comp L Rev 227, 26; Leith (n 33) 33.

between program (software) and computer (hardware).'[40] The IBM decisions have been considered to confirm that computer programs were accepted as patentable subject matter once they had a 'technical character', which can be found in the further effect deriving from the execution of the instructions given by the computer program.[41]

4.3 ANY HARDWARE-APPROACH

More new case law has shown the change in the EPO's interpretative line. Cases like Pension Benefit[42], Hitachi[43], Microsoft[44] and Comvik[45] indicate that in order to decide whether a computer program has a technical character, the examiner must ask a question of 'whether the claim involves the use of or is to a piece of physical hardware, however mundane. If it is, Art.52(2) does not apply.'[46] Under this approach examiner must first ask whether there is an invention, and then ask whether the invention makes a technical contribution to the state of art.[47] Pension Benefit decision clarified the EPO's position on patenting business methods, which often overlap with computer programs. The claim was directed to a method and an apparatus, where the apparatus was a computer programmed to run the method. On the apparatus claim the Technical Board of Appeal considered

40 T97/1173/Computer Programs Product/IBM (n 35).
41 Ballardini (n 26); Kelvin W Willoughby, 'How much does technology really matter in patent law? A comparative analysis of doctrines of appropriate patentable subject matter in American and European patent law' (2006) 18 Fed Circuit B J 63, 18.
42 T 0931/95/Controlling pension benefits system/PBS Partnership (2001) OJEPO 441.
43 T 0258/03/Auction method/Hitachi (2004) OJEPO 575.
44 T 0424/03/Microsoft/Data transfer expanded clipboard formats (2006).
45 T 0641/00/Two identities/Comvik (2002) OJEPO 352.
46 Aerotel Ltd v Telco Holdings Ltd (2006) EWCA Civ 1371, [2007] Bus L R 634.
47 Ballardini (n 26).

that involvement of physical entity was enough to separate the claim from excluded matter.[48] Although the claim was accepted as Article 52 invention, the Board found that the apparatus did not meet the requirement of inventive step.[49]

Soon after launching any hardware-approach, the Board made a decision on Comvik case. In Comvik, an invention consisted of a mixture of technical and non-technical features. The existence of inventive step was assessed by taking into account all those features which contribute to technical character. Non-technical features could not support the presence of inventive step.[50] According to Comvik decision, the invention could include both technical and non-technical features, which however, should be first separated clearly. After that, assessing inventiveness could only be based on technical features.[51]

Hitachi decision on the other hand showed, that the relevant question is whether the claim as a whole identifies as technical. Hitachi involved a method claim for the automated auction method, an apparatus claim for running the auction via network, and a computer program claim.[52] The Board concluded that a method involving technical means is an invention within the meaning of the Article 52. When assessing subject-matter eligibility, the Board found that the claim including technical features such as a server computer, client computers and a

48 "An apparatus constituting a physical entity or concrete product, suitable for performing or supporting an economic activity, is an invention within the meaning of Article 52(1) EPC."; Kevin Afghani and Duke W Yee, 'Keeping it Physical: Convergence on a Physicality Requirement for Patentability of Software-Related Inventions Under the European Patent Convention and United States Law', (2008) 15 J Intell Prop L 239, 3.

49 Tanya Aplin, 'Patenting computer programs: a glimmer of convergence' (2008) E I P R 30(9) 379, 3.

50 Knights and Redinger (n 25) 5.

51 Ballardini (n 26) 27.

52 T 0258/03 Auction method/Hitachi (n 42); Marsnik and Thomas (n 38).

network, was to be accepted as subject-matter.[53] The method claim was not excluded for it involved apparatus, which were both analyzed.[54] The Board, however, found none of the claims patentable due to lack of inventive step.[55]

In Microsoft, the claim was directed to a computer-readable medium, which was considered as a technical product and therefore had technical character. Both method claim and program claim were considered patentable.[56] Although Microsoft was in line with Pension Benefit and Hitachi considering the any hardware-approach, the analysis of inventive step now departed. The Board did not treat the computer program as excludable prior art, as was the case with business methods previously.[57] When considering an inventive step, unlike in Pension Benefit and Hitachi, the solution was seen as new and non-obvious, without the Board setting out its reasoning.[58]

53 Alain Strowel and Sinan Utku, 'The trends and current practices in the area of patentability of computer implemented inventions within the EU and the U.S.' (A study prepared for the European Commission, 2016) 19 <https://ec.europa.eu/digital-single-market/en/news/report-trends-and-current-practices-area-patentability-computer-implemented-inventions-within> accessed 11 Sep 2017.
54 Vicki Salmon, 'Patenting computer software and business methods in the UK' (2007) 12(1) Comms L 18, 4.
55 Michael Q Lee and James Cross, 'Recent developments in patenting software and business method inventions in the US and Europe' (2005) 12 Andrews Intell Prop Litig Rep 13, 4.
56 T 0424/03 Microsoft (n 43).
57 Marsnik and Thomas (n 38) 29.
58 William Cook and Geoff Lees, 'Test clarified for UK software and business method patents: but what about the EPO?' (2007) 29(3) E I P R 115, 3.

5 ANY HARDWARE-APPROACH AND BLOCKCHAIN

The EPO's any hardware-approach indeed raises the question whether the "as such" clause has lost its meaning all together. When according to the current approach computer programs involving any type of hardware (even a general computer) are considered technical, and therefore accepted as patentable subject matter, computer programs do seem to become patent eligible. However, as mentioned before, assessment of inventive step can only be based on technical features. As was seen in Comvik, technical and non-technical features must first be separated.[59] On the other hand, in Microsoft the Board followed the approach set in Hitachi and accepted that the method was not excluded since it used technical means.[60] The technical – non-technical – dilemma still remains in the EPO's legal praxis, as can be seen for example in recent decision concerning user interface for an electronic trading system.[61] The claimed subject-matter was considered to be a combination of technical and non-technical features. The Board found that features in question relate to methods of doing business as such and thus constitute financial business aspects which per se are non-technical and therefore can not support the presence of an inventive step.[62]

Broadening the lines of patentability has caused concerns of any new, program-based innovation becoming patent eligible, to the point where operating in the field becomes extremely

59 Steve Hickman, 'Reinventing invention: why changing how we invent will change what we patent and what to do about it' (2009) 91 J Pat & Trademark Off Soc'y 108, 4.

60 Sigrid Sterckx and Julian Cockbain, 'Exclusions from Patentability: How Far Has the European Patent Office Eroded Boundaries?' (Cambridge Intellectual Property and Information Law vol 19, Cambridge University Press 2012) 89.

61 T 1930/13/User interface for an electronic trading system/ Trading Technologies International, Inc. (2017).

62 Ibid.

difficult, especially for smaller companies and private persons. Search for prior art in the software field has been considered lacking, while applications have been broad.[63] This has created a risk (if not already a concrete situation) of patent thicket.[64] In this situation companies will have to navigate through dense thicket of overlapping patent applications, which is likely to slow down innovation rather than encourage it. This is especially harmful to individuals and smaller companies who cannot afford to defend themselves against forceful licensing agreements as well as the harm for unknown infringement as a result of patent issuing.[65]

Debate on patenting blockchain runs heated, as companies have just started to express interest for the technology. Question at the moment seems to be whether blockchain can be patented in the first place. As the core of technology is part of public domain, the conclusion would be that only important changes and improvements can be patented. Therefore the question is not the patentability of blockchain as a field of technology, but different features gaining patent protection to the point, where the technology in fact becomes difficult to exploit. As will be discussed in Goldman Sachs case, for example the features concerning security seem to be popular subjects for patents corporations are filing at the moment.

So what is the subject of patent protection in the context of blockchain? These questions do not seem to differ that much from software patents in general. As history indicates, the inventions should be at least partially realized using some form of hardware. This should not be too difficult of a requirement. Discussed cases as well as the EPO's Guidelines show that a general computer is

63 Ballardini (n 26); Seong-Hee (Emily) Lee, 'Software patent eligibility – A call for recognizing and claiming concrete computer programs' (2013) 95 J Pat & Trademark Off Soc'y 402, 4.

64 Ballardini (n 26) 28.

65 'Patents' (Electronic Frontier Foundation) <https://www.eff.org/issues/patents> accessed 7 Sep 2017.

considered sufficient.[66] Based on applications filed for the EPO, majority seems to be directed for system and method-types of claims.[67] The interpretative problems visible in the EPO's history of decisions imply that essential question might be where is technicality found in claims.[68] Rather than can blockchain be patented, it should be asked, are blockchain patent applications technical in the meaning of the EPO's legal praxis? (Which will also answer the former question.) The next section aims to give insight to this matter by representing two examples of what could be considered patentable under the current any hardware-approach. However, as this article studies the patentable subject matter, it should be borne in mind that other requirements of patentability need to be met too in order for patent to be granted.

6 CASES

6.1 SLOCK.IT

One example of potentially patentable blockchain-inventions is a smart-lock-system established by German-based company Slock.it. Focused on blockchain- and IoT (Internet of Things), the company has among other things been developing locks

66 'A computer-implemented invention is one which involves the use of a computer, computer network or other programmable apparatus, where one or more features are realized wholly or partly by means of a computer program.' 'Patents for software? European law and practice' (n 22).

67 There are currently 45 applications that include term 'blockchain' in the European Patent Register, when this article is being written. 33 of these are for 'system and method'-claims. <https://www.epo.org/searching-for-patents/legal/register.html#tab-1Register> accessed 15 Sep 2017. On the other hand, the subjects of a claim could as well be for example different functions, databases or user interfaces.

68 Oesch, Pihlajamaa and Sunila (n 24) 91-92.

connected to the Ethereum-blockchain platform.[69] At the moment Slock.it's invention is still a prototype. According to the latest information beta-version will be published in 2018.[70] Although full operational service is still not available, Slock.it has worked with different companies integrating items to internet.[71]

According to the vision of Slock.it, smart locks could be opened or closed by smart contracts running on Ethereum platform. In this manner it would be possible to rent different kinds of items, such as cars or apartments. The owner of a lock could define a prize for the item available for rental, as well as a deposit. Using a mobile app the user pays the deposit by a transaction to the Ethereum blockchain, gaining the right to open and close the lock. Deposit is kept until the user returns the cryptographic key with another transaction. After that the deposit is returned to the user, minus rental fee. The payment is transferred straight to the owner of the item.[72]

Although Slock.it's hardware might serve as an example, it seems unlikely that Slock.it would aggressively pursue patents for it. Slock.it has joined The Open Innovation Network, which is an organization that licenses its global defensive patent pool in exchange for a pledge of non-aggression. Its members agree to refrain from using their patent portfolio against the Linux

69 Slock.it <https://slock.it/> accessed 11 Sep 2017.

70 Stephan Tual, 'Slock.it secures $2 million USD seed funding to build next-generation Sharing Economy Platform' (Slock.it, 29 Mar 2017) <https://blog.slock.it/slock-it-secures-2-million-usd-seed-funding-to-build-next-generation-sharing-economyplatform-b795c6d1a92d> accessed 11 Sep 2017.

71 Stephan Tual, 'Slock.it working with Microsoft to bring its Dapp to the Azure cloud' (Slock.it, 15 Mar 2016) <https://blog.slock.it/slock-it-working-with-microsoft-to-bring-its-dapp-to-the-azure-cloud-c7a39720fdb3> accessed 11 Sep 2017.

72 Tual, 'Slock.it secures $2 million USD seed funding to build next-generation Sharing Economy Platform' (n 69).

System[73], on which Slock.it's software is build on. The company has also emphasized a need to fix patent system. [74]

In the context of any hardware-approach, the EPO concluded in those well-known cases that for a computer-program to be accepted as an invention, involvement of a physical hardware was needed. Slock.it's advantage might be applying blockchain-technology to a clearly technical apparatus, which itself could be considered inventive. The smart lock might be an example of a type of invention that could bring blockchain-innovations to the scope of patentability. However, as mentioned earlier, patents are not granted only for inventions that are accepted as patentable subject matter. As was seen in Pension Benefit, the lack of inventiveness can also be an obstacle for patentability. Smart locks are not necessarily new inventions, although blockchain-based user-interface might be.[75] As was stated in Comvik, while the invention may include both technical and non-technical features, the assessment of inventiveness can only be based on technical features. If the essence of invention would be considered to reside on business method of exploiting locks in the context of sharing economy, the patent eligibility is more questionable.

Also, patents are not usually granted for game-changing new fields of technology, but rather somewhat specific features. The

73 Stephan Tual, 'Slock.it joins the Open Innovation Network' (Slock.it, 7 Jan 2016) <https://blog.slock.it/slock-it-joins-the-open-innovation-network-b291ca2ba270> accessed 11 Sep 2017.

74 Slock.it Founder Stephan Tual has referred to the article 'Time to fix patents' noting that patents need to be reformulated. See also 'Time to fix patents' (The Economist, 8 Aug 2015) <https://www.economist.com/news/leaders/21660522-ideas-fuel-economy-todays-patent-systems-are-rotten-way-rewarding-them-time-fix> accessed 11 Sep 2017.

75 Lately many smart-locks have entered the market; Brian Heater, 'August Home raises another $25 million as it expands service partnerships for its smart locks' (TechCrunch, 26 Jul 2017) <https://techcrunch.com/2017/07/26/august-home-raises-another-25-million-as-it-expands-service-partnerships-for-its-smart-locks/> accessed 11 Sep 2017.

fact that smart locks as a concept exist, does not necessarily mean that nothing alike could be patented. For example, already in 2002 Microsoft applied for a patent directed to somewhat similar encryption technique, as what would later on be the basis for blockchain-technologies.[76] The application was eventually refused for the lack of inventiveness. Still the decision cannot be interpreted as an indication, that no encryption technique would ever be patentable. What might be concluded is, that Microsoft's invention was considered technical and patentable "as such". This can be seen to indicate that rather than questions of subject-matter, the relevant question in many cases is the evaluation of an inventive step.

6.2 GOLDMAN, SACHS & CO.

In 2016 Goldman, Sachs & Co. filed patent application named "Systems and methods for updating a distributed ledger based on partial validations of transactions."[77] Goldman Sachs has been eager to file applications for new fields of technology, and in July 2017 the company was granted a patent for cryptographic currency called SETLcoin in US.[78] The application has been filed for the EPO as well, but is still pending.[79] Both of these applications can be seen as to indicate Goldman Sachs's interest to utilize blockchain-based technologies. This article studies the former application, although it seems clear, that two are

76 T 1568/05/On-disk file format for a serverless distributed file system/ Microsoft (2011).
77 EP16710594/ Systems and methods for updating a distributed ledger based on partial validations of transactions/ Goldman, Sachs & Co. (2017).
78 Patent published in USPTO database no 9,727,932 8.8.2017.
79 Status of the application on European Patent Register at the moment states 'communication of intention to grant the patent'. This means, that Goldman Sachs will likely get the patent should there be no opposition <https://register.epo.org/application?number=EP16710594> Database accessed 11 Aug 2017.

connected.[80] The application is filed for the systems and methods for processing financial transactions using a computer network that stores a distributed ledger, employing the distributed ledger to control visibility of transactions.[81]

As has been discussed earlier, when the core of blockchain-technology is part of a public domain, patents need to be filed for improvements and changes. Big banks seem to be going for the field of security, as alongside with Goldman Sachs also MasterCard[82] and Bank of America[83] have sought for patent protection in the context of transaction security. When comparing blockchain-platforms and distributed ledgers, this also seems to be the major difference.

Goldman Sachs's application raises the question about the EPO's position on method claims. In Pension Benefit, the Board concluded that 'where a claim is to a method which consists of an excluded category, it is excluded by Article 52(2), even if hardware is used to carry out the method'.[84] However, in Microsoft the Board stated that the method was not excluded since it used technical means, a clipboard memory.[85] The Board also considered the method steps to contribute to the technical character as they solved a technical problem by technical means where functional data structures were used independently without enhancing the internal operation of a computer system. This way the method steps could be considered when assessing

80 Also, it should be mentioned, that lately Goldman Sachs has published a section with the term blockchain on their website, see 'Blockchain – the new technology of trust' (Goldman Sachs) <http://www.goldmansachs.com/our-thinking/pages/blockchain> accessed 11 Sep 2017.
81 T 1930/13/User interface for an electronic trading system (n 60).
82 EP16787693/Method and system for gross settlement by use of an opaque blockchain/Mastercard International Incorporated (2016).
83 EP16865030/Block chain alias person-to-person payments/Bank Of America Corporation (2017).
84 Salmon (n 53) 3.
85 Aplin (n 48) 3.

inventive step using the Comvik approach.[86] According to the EPO's guidelines: 'A computer-implemented invention is one which involves the use of a computer, computer network or other programmable apparatus, where one or more features are realized wholly or partly by means of a computer program.'[87]

As typical to blockchain technologies, Goldman Sachs's application is based on an idea of a computer network. Therefore, the EPO's interpretative line leads to assume, that hardware-requirement might be met, and the invention in this sense be accepted as computer-implemented. Another question is the one of method claims. The approach in Microsoft leads to presume that the door to the patentability of basically any program has now been opened.[88] As method steps seem to be accepted as technical features in some cases (and in some cases not), the impossible task of defining technical and non-technical features still remains, making it hard to forecast the outcome of patenting processes.

7 COMPUTER PROGRAMS OR BUSINESS METHODS?

Schemes, rules, and methods of doing business are excluded from patentability in a same manner as computer programs.[89] As seen in especially the Goldman Sachs case, method claims often overlap with program claims. Nari Lee has described business methods as 'a process of converting abstract data to useful information, to be applied in business activities.' Also: 'A business method patent is a patent whose claims are directed to

86 Sterckx and Cockbain (n 59).
87 'Patents for software? European law and practice' (n 22).
88 Ballardini (n 26) 567.
89 EPC Article 52(2)(c).

a business method, regardless of the claim format.'[90] The EPO has offered one possible definition by stating that 'a business method is any subject matter that is more concerned with financial, interpersonal, and societal relationships than with engineering.'[91]

If the EPO's interpretative line has not been consistent with computer programs, same goes for business method patents. For example in Sohei/General-Purpose Management System case[92] the patent granted could easily be classified as a business method, and it is difficult to ascertain how the invention solved an "objective technical problem."[93] In Pension Benefit for example, the decision involved two core claims: one for 'a method of controlling a pension benefits program' and another for an apparatus programmed to carry out the same method. Patent applications such as Pension Benefit earlier, and Goldman Sachs' now have become common in a manner of constructing the claim to consist of the method implemented in a computer-readable-medium. This way it seems, that adding a computer-readable-medium clause to the application serves as some sort of "Get out of jail"-card, in fact expanding the patentable subject matter to business methods as well. Regardless of an apparatus these claims recite, what seems to be the underlying purpose is to gain protection for the functionality of a program itself.[94] Therefore, focusing on the recited hardware limitation may allow unduly overbroad software claims.[95] This creates a

90 Lee, Nari, The Patent Subject Matter Reconfiguration and the Emergence of Proprietarian Norms - The Patent Eligibility of the Business Methods (October 14, 2002). Available at SSRN <https://ssrn.com/abstract=400100> or <http://dx.doi.org/10.2139/ssrn.400100> accessed 29 July 2017.

91 Jason T Taketa, 'The Future of business method software patents in the international intellectual property system' (2002) 75 S Cal L Rev 943, 10.

92 T 0769/92/General purpose management system/Sohei (1996) E P O R 253.

93 Matthew E Fink, 'Patenting business methods in Europe: what lies ahead?' (2004) 79 Ind L J 299, 5.

94 Ibid.

95 Fink (n 92) 5.

threat of already disclosed technologies, such as blockchain, to become at least partially patent-eligible if used in the context of inventive method steps.

Especially mixed claims have caused problems, as those in particular have led to contradicting outcomes. When claims consist of both business methods and technically applied business methods, it becomes highly difficult to judge on which part of the claim should the evaluation of patent eligibility be based on.[96] Similar to computer programs, also methods of doing business are only excluded "as such".[97] As Comvik and Microsoft have shown, in some cases the method steps can be considered to contribute to technicality of an invention. This leads to assume, that inventions where inventiveness is only based on abstract part of the claim, might however be declined. What still remains, is the task of defining what features of the invention can be considered technical, and where does the essence of the invention lay

8 CONCLUSIONS

As discussed in this article, the question arising can be narrowed down to what is the basis of patent eligibility for blockchain technology and what should be concluded from the history of computer-implemented-inventions. It seems that although the current any-hardware approach has removed some of the previous problems[98], the vagueness of current legislation might still lead to a situation, especially with new technologies, where patent

96 Afghani and Yee (n 47) 66.

97 Elizabeth Bestoso, 'Financial business method patents: the trend toward invalidity under section 101' (2014) 86 Temp L Rev 369, 11.

98 The EPO's problematic approaches with technical contribution and further technical effect.

protection is either given freely for overlapping applications or where investments made on program-development are left under-protected. Nevertheless, contradicting outcomes create uncertainty for markets, possibly slowing down innovation.

Then what is the scope of patent protection for blockchain-technologies? This issue is connected to the historical context of computer-program debate, which provides some information on how computer-based innovations have been evaluated before. However, what this article finds, is that one unambiguous answer can not be given. The assessment of computer-implemented innovations has shifted from time to time, and different interpretations have been established within the same approach as well. Problems with blockchain-patents in the European context seem to arise especially from the nature of systems and methods-applications containing mixed features of engineering and business methods, as well as the difficulty of technicality-requirement.

What this paper advocates is reformulating the concept of inventive step and limiting the scope of protection for computer programs, an approach presented by Rosa Maria Ballardini in her doctoral thesis.[99] This approach would allow considering all the invention's technical and non-technical features when assessing the inventiveness, therefore creating a more coherent and transparent system. This way it would also be less likely that new technologies become monopolized due overly broad method-type of claims directed to the actual functionality and effects of an invention, rather than any specific technical problem.

99 Ballardini (n 26) 27.

As has been discussed, especially inventions with mixed features have proven to be difficult to address. This system would eliminate the impossible task of defining "technical" and allow inspectors to concentrate on whether the invention is actually inventive.[100]

This article presents only a few notions on the subject. As stated in the beginning, blockchain-technology has sometimes been compared to internet in disruptiveness. It turns out this seems somehow an appropriate description. Whereas blockchain lies on certain unique technology, the possible applications are numerous and the scope of patent protection is more likely defined by the utilization of that technology. In this sense, the question of patenting blockchain is not necessarily different from patenting issues regarding traditional software field.

100 Ibid.

ALEXANDRA SHTROMBERG[1]

Data Privacy Risks of Working Remotely as a Lawyer (on the Example of the GDPR)

1 INTRODUCTION

Remote working programmes for lawyers begin to change the legal working arena on the global landscape. In March 2017, Morgan Lewis & Bockius LLP launched a formal remote-working programme for associates, allowing them to opt to telecommute one or two days a week beginning in their third year to increase flexibility, quality of customer service and keep up with trends

1 Alexandra is a graduate of the University of Helsinki, Faculty of Law, and is currently studying at Aalto University.

of the corporate world.[2] Baker McKenzie and Jackson Lewis PC have simultaneously introduced own remote work programmes.[3] A recent Gallup poll has shown that remote working in the legal industry has increased from to 41 to 43 percent between 2012 and 2016.[4] We can even observe introduction of "virtual law firms" that unite attorneys working remotely.[5] In April 2017, Association of Finnish Lawyers has published results of the research on remote work in the legal field. According to the results, around 50% of the respondents have stated that remote work suits their work tasks. In private sector, around 18% of respondents take 3-5 days of remote work per month.[6] Moreover, each lawyer working at the office premises faces the same risks as a remote worker. For instance, data privacy threats inherent in remote work arise from using personal devices, accessing public networks and using shared printers. Similar risks are likely to occur when a lawyer goes on a business trip, takes the days off or working on assignments when attending conferences, university classes and other events. For these reasons, it is extremely important to mitigate risks of remote work by developing practices of safe management of electronic information and its physical copies in internal and external communications to comply with requirements of applicable data protection laws.

2 Melissa Maleske, "Morgan Lewis Launches Remote-Work Option For Associates" (Law360, 7 March 2017) <https://www.law360.com/articles/898960/morgan-lewis-launches-remote-work-option-for-associates> accessed on 25 May 2017.
3 Aebra Coe, "How To Make Working From Home Work For BigLaw" (Law360, 21 March 2017) <https://www.law360.com/articles/904229/how-to-make-working-from-home-work-for-biglaw> accessed on 25 May 2017.
4 Ibid.
5 Leigh McMullan Abramson, Do Lawyers Need Offices Anymore? (the Atlantic, 9 October 2015) <https://www.theatlantic.com/business/archive/2015/10/do-lawyers-need-offices-anymore/409417/> accessed on 25 May 2017.
6 "Etätyön määrä arvioitua pienempi" (Lakimiesliitto, 27 April 2017) <https://lakimiesuutiset.fi/etatyon-maara-arvioitua-pienempi/> accessed on 25 May 2017.

The aim of this paper is to explore the challenges remote work poses to data privacy regime of the business. It becomes especially important due to the recent strengthening of data protection requirements formulated in supranational laws (e.g., sources of the European law, such as upcoming European General Data Protection Regulation, the GDPR), national laws, non-binding international standards and ethical codes of conduct. My research will focus on the analysis of significant data privacy risks that are specific to routine working practices or are inherent to any work arrangements but are amplified in case of occasional or permanent remote work. Why remote work poses additional risks to lawyers' compliance with data privacy obligations? How can we classify risks of remote work to create risk prevention plans and raise personal "data privacy hygiene", in other words, make compliance with data privacy requirements imposed by aforementioned standards a daily habit?

I will address these questions in my paper. First, I will look into the essence of the remote work and the regulatory environment that shapes data privacy requirements for lawyers working remotely with focus on the GDPR. Secondly, I will introduce a data privacy risk assessment matrix that I have designed on my own. The matrix clarifies how different risks stemming from remote work can be distributed according to the probability level (how likely the risk is) and level of effort (amount of resources and time needed to mitigate it). The matrix helps to precisely assess data privacy risks arising from remote work in a specific company. Finally, the paper will discuss the knowledge tool box necessary for the lawyer to ensure working environment that is compliant with the GDPR, as well as address issues that should be addresses in employee trainings under the GDPR.

This paper provides a practically oriented approach to analysing data privacy risks created by remote work. Majority of the ongoing research focuses on analysing technological risks arising from data privacy breaches, ignoring analysis of

most common daily situations, such as working from home using personal devices or taking sufficient precaution when working in public places. One will more likely find an overview of practical guidelines in recent blog posts at the lawyer websites and pages of data privacy consultancies that are motivated to give practically implementable advice to a wide range of clients of different company sizes and spheres of activities. In my paper, I analyse these pieces of practical advice under the GDPR framework and, based on the provisions of the GDPR, match them against legal risks stemming from risky documentation storage and communication practices.

2 GENERAL TECHNOLOGICAL RISKS OF REMOTE WORK

First, it is important to identify what we understand by remotework in the framework of this paper. Defining scope of the remote work will help us to determine what additional risks it brings in daily working routine. This will help us to build a data privacy risk assessment matrix and further discuss the development of the knowledge tools for self-incentivised creation of a safe working environment.

For the aim of this paper, remote work includes any work that the employee conducts outside office premises with pre-arranged working environment. It includes working during commuting to or from office, when attending public events and working remotely from home. Remote working policies commonly define remote work as “working at a location other

than the employee's normal place of work which could be".[7] The European Framework Agreement on Telework highlights that telework (synonym for "remote work") does not necessarily mean working remotely for the whole span of working relationships. Namely, it defines remote work as "a form of organising and/or performing work, using information technology, in the context of an employment contract/ relationship, where work, which could also be performed at the employer's premises, is carried out away from those premises on a regular basis".[8] These vague definitions make it difficult for the employee to assess his or her own status of a remote worker and therefore comprehend connected risks. At the same time, employers due to a lack of time and resource are not able to focus on identifying risks arising from hybrid kinds of work (working partially remotely, partially from the office). All these factors highlight the necessity to consider different manifestations of remote work and its hybrid forms when assessing data privacy risks.

Remote work adds to decentralised and diffused working environment. It, in its turn, increases the need for confidential data protection and complicates the task of the IT department to manage an array of mismatched devices to reach the same levels of security.[9] Major security concerns of remote working are a lack of physical security controls, unsecured networks, infected devices on internal networks and external access to internal

7 See, for example, Policy and Procedure for Remote Working (the Crown Estate, April 2013) <https://www.thecrownestate.co.uk/media/5777/policy-and-procedure-for-remote-working.pdf> accessed 26 May 2017.

8 "Implementation of the European Framework Agreement on Telework. Report from social partners" (Social Dialogue Committee, September 2006) <https://resourcecentre.etuc.org/linked_files/documents/Framework%20agreement%20on%20telework%20EN.pdf> accessed 28 May 2017.

9 Top 10 Security Issues with Remote Employees (Kaseya Limited, 2017) <https://authanvil.com/blog/top-10-security-issues-with-remote-employees> accessed 26 May 2017.

resources.[10] In addition to complex technological matters, one should not also discount obvious risks such as stolen or lost mobile devices.[11] The vast academic discussion on the upcoming changes to the European legislation on data protection will hardly mention the risk of the cat jumping on the keyboard[12] (and probably pressing the "Send" button to send the client's personal information to the wrong recipient). However, this example can act as an illustration of diverse risks the remote worker may encounter while working outside the office.

To create effective policies and training materials for the employees, it is important to evaluate the impact of upcoming changes to the regulatory environment through the lens of the most common situations related to the technological risk, identify spheres and types of risks of data privacy breaches, as well as measures to mitigate these risks on the individual level. I will start first with analysing regulatory environment. This will help to identify status of persons involved in processing personal data and analyse their risks and legal obligations by critically assessing real working life cases from the perspective of GDPR compliance.

10 Murugiah Souppaya, and Karen Scarfone, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security" (U.S. Department of Commerce, 2016) <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf> accessed 26 May 2017.

11 Top 10 Security Issues with Remote Employees (Kaseya Limited, 2017) <https://authanvil.com/blog/top-10-security-issues-with-remote-employees> accessed 26 May 2017.

12 Carl Henriksen, "Top 10 security tips for remote and mobile working" (Oryxalign Blog, 11 April 2016) <http://www.oryxalign.com/top-10-security-tips-remote-mobile-working/> accessed 26 May 2017.

3 INTERPLAY BETWEEN GDPR REQUIREMENTS AND COMMON PRACTICES OF REMOTE WORK: CASE STUDY

Before proceeding to identifying concrete risks, I would like to provide a short overview of regulatory environment that affects data privacy standards that a lawyer shall comply with, especially when working out of office. It will also help to evaluate applicability of binding legislative provisions when analysing most common situations that a lawyer may encounter when working out of office. Data privacy legislation is experiencing significant changes now. In order to comply with strengthened requirements, it is important to assess how existing regulatory mechanisms shape remote work environment and professional obligations of a lawyer.

Regulatory mechanism model in the EU comprises of following:

- international standards
- European legislation (new General Data Protection Directive 2016/679, the GDPR);
- national legislation on data protection;
- regulations of professional communities (International Bar Association (IBA), local bars);
- local regulations of the companies (corporate codes of conduct, privacy and remote work policies).

First, I would like to take a brief look at international standards that are relevant for defining main concepts and principles connected with data privacy protection. ISO 27001 (the international standard that describes best practice for an information security management system) requires companies to develop a policy, operational plans and procedures to ensure information security

when using mobile computing and teleworking facilities.[13] In light of this, data privacy policy and compliance procedures should cover employees who both telework at the moment and who may telework, services available to remote workers, information restrictions, authorisation procedures, software specifications, integrity and confidentiality, maintenance guidelines, and active user education.[14] This standard provides a system for identifying information security risks and control sets to address these risks.[15] In general, a good policy should also state a clear prohibition on remote work in the absence of sufficient safeguards, detailed in the policy, specify different types of information that the employees process and describe process of breach reporting.[16] In further discussion in this paper, I will elaborate on what sufficient safeguards lawyers may employ, what stakeholders are involved in the process of creating these safeguards and what safeguards implementation measures lawyers should undertake.

However, ISO standards are voluntary and thus act as a "soft law" with a lack of formal legal effect.[17] In my paper, I will focus

13 See "ISO/IEC 27000 family - Information security management systems" <https://www.iso.org/isoiec-27001-information-security.html> accessed 26 May 2017.

14 Tim Godlove, "Improving Information Security for Teleworkers" (University of Fairfax, 2016) <https://www.ufairfax.edu/news/Improving-Information-Security-for-Teleworkers-20170113-0022> accessed 26 May 2017.

15 Paul De Hert, Vagelis N. Papakonstantinou, and Irene Kamara, The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection (Business Privacy Hub, 2014), p. 14 <http://brusselsprivacyhub.eu/BPH-Working-Paper-VOL1-N2.pdf> accessed 26 August 2017.

16 Mandy Laurie, "How to… balance the needs of remote working with data security risks" (People Management, 2009) <http://www2.cipd.co.uk/pm/peoplemanagement/b/weblog/archive/2013/01/29/how-to-balance-the-needs-of-remote-working-with-data-security-risks-2009-11.aspx#> accessed 6 August 2017.

17 Paul De Hert, Vagelis N. Papakonstantinou, and Irene Kamara, The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection (Business Privacy Hub, 2014), p. 6 <http://brusselsprivacyhub.eu/BPH-Working-Paper-VOL1-N2.pdf> accessed 26 August 2017.

more on binding legislation and namely upcoming GDPR for a couple of reasons. First, EU Member States shall transpose GDPR into their national laws by 6 May 2018.[18] Secondly, GDPR has a wider scope of application than one may think. It covers a wide scope of controllers and processors of personal data. Under Article 4 of the GDPR, a controller is a legal entity or a natural person that determines the purposes and means of processing personal data. A processor, in its turn, processes personal data on behalf of the controller. For example, a law firm can be both a data controller and a data processor. Namely, it would be the data controller in respect of the data about its own staff, but it will have a status of the data processor in respect of the personal data it processes for the benefit of its clients.[19]

Article 3 of the GDPR states that GDPR applies to the processing of personal data of data subjects located in the EU by a controller or processor not established in the EU in two cases. Namely, GDPR applies when processing activities of entities located outside the EU are related to the offering of goods or services to such data subjects in the EU or the monitoring of their behaviour within the EU. It evidences the wide scope of implementation of GDPR especially in case of law firms where it is difficult to avoid situations of consulting European clients, regardless of whether the law firm is located.

First, it is important to analyse briefly the role of the GDPR in regulating remote work. The GDPR makes the businesses review their approach to data protection governance and the contracts and other arrangements of sharing data with other

18 Reform of EU data protection rules (European Commission, 2017) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 26 August 2017.

19 See Are you a "data controller"? (Data Protection Commissioner) <https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm> accessed 26 August 2017.

organizations.[20] Under Article 4 GDPR, "personal data" means any information relating to an identified or identifiable natural person ('data subject'). The definition points to the possibility of "direct" or "indirect" identification. Thus, it comes as no surprise that a wide range of legal documentation the lawyers deal with fall under the scope of GDPR. Article 32 GDPR states that businesses involved in controlling and processing personal data are required to "implement appropriate technical and organisational measures". These measures should consider "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."[21] The price of failing to comply with the GDPR is high. Claims from data subjects are likely to add to the regulatory fines of up to €20 million or 4% of annual worldwide turnover claims.[22] When deciding on the scale of administrative liability, supervisory authority explores such factors as the effort of the controller or processor to implement precautionary measures and ensure secure data processing, mitigate the damage suffered by data subjects, as well as adherence to approved codes of conduct or certification mechanisms.[23]

Discussion so far shows that the GDPR raises data privacy standards for lawyers. For lawyers who work remotely occasionally or full time, complying with these raised standards will require

20 Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now (Information Commissioner's Office, 2016), p.1 <https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf> accessed 26 May 2017.

21 Rita Heimes, " Top 10 operational impacts of the GDPR: Part 1 – data security and breach notifications" (IAPP, 6 January 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/> accessed 28 May 2017.

22 Lorna Cropper, "Let the one year countdown commence" (Fieldfisher, 25 May 2017) <http://privacylawblog.fieldfisher.com/2017/let-the-one-year-countdown-commence/> accessed 26 May 2017.

23 See Article 83 of GDPR.

intensive preliminary preparations to maintain compliance with data privacy standards. Professional community sees GDPR as a threat remote work that involves a complex involvement of all kinds of devices that now should answer stricter standards.[24] In addition to that, lawyers are bound by ethical obligations of confidentiality that I will explore later in this paper when addressing individual data privacy awareness of a lawyer. All these regulatory tendencies make it especially important to focus on identifying, mitigating and eliminating risks of data privacy breach arising from daily routine. Following cases illustrate how common working practices may incur the data privacy breach.

SITUATION 1 - USING CLOUD STORAGE TO WORK OUT OF THE OFFICE

Such situations may involve cases when the lawyer uses the cloud storage to access documents provided by the client or one of the counterparties. It may also involve situations when the corporate network is difficult to access from out of the office, and the lawyer synchronises files on the cloud storage of his or her own choice to continue working on documents.

The GDPR requires any company choosing to process data in the cloud to ensure that the cloud provider offers sufficient guarantees to implement appropriate technical and organisational safeguards that meet GDPR requirements.[25] To meet these requirements, an employee needs to make sure that his or her employer has the right to audit the chosen cloud

24 Harry Leech, "Datasec to examine new EU law impact" (Independent.ie, 30 April 2017) <http://www.independent.ie/datasec/datasec-to-examine-new-eu-law-impact-35666738.html> accessed 25 May 2017.

25 Data privacy in the cloud. Navigating the new privacy regime in a cloud environment (Deloitte, 2016) <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-privacy-in-the-cloud-pov.PDF> accessed 26 May 2017.

provider, to perform necessary compliance checks and to receive necessary policies and procedures from the cloud provider.[26] In light of this, cloud storage use may create high risks especially in cases when lawyers work on massive due diligence projects using cloud storage provided by a client without proper analysis of its data privacy risks.

All this illustrates that lawyers should choose cloud storage providers on the centralized basis by decision of the management of the company. Discretion of the employee in using own favourite cloud storage tools may create significant risks of failing to comply with the GDPR requirements.

SITUATION 2 - CONNECTING HARDWARE TO WORK FROM HOME

Outside of the office, a lawyer would like to replicate the office environment. For instance, the lawyer may print documents to proofread them or use the USB flash drive to gain a fast access to the documents without using the cloud storage. Whereas rapidly developing technologies and software applications pose a new risk, using "older" office devices can also create risks of personal data leaks resulting from such common activities as using home printer to print work documents or saving work documents to the personal USB storage. In fact, papers stuck in printer that can be accessed by third parties or lost memory sticks may result in unexpected destruction of personal data or leaking personal data to curious third parties or even competitors. Thus, it is important to provide concrete illustrations of risks as they occur frequently but are still hardly identifiable due to becoming a part of daily working routine.

26 Antony Adshead, "The EU data protection reforms and cloud storage" <http://www.computerweekly.com/podcast/The-EU-data-protection-reforms-and-cloud-storage> accessed 26 May 2017.

Printers may pose such security risks as document theft or snooping (most likely to happen if printing happens in public places), unauthorised changes to settings, uncontrolled saving on the internal storage and more extreme cases of eavesdropping on network printer traffic and printer hacking via the network or Internet.[27] After the document is printed, its physical copy inherits the risk. A recent survey of 1,000 office workers has shown that 27 percent of office workers have thrown away printed documents without shredding, 24 percent have printed documents but left the copies in the printer tray and one in five have picked up someone else's documents from the printer.[28] The risks increase by multiple times when the printing happens outside the relatively controllable office environment. In fact, acquainting with data privacy instructions provided by the device manufacturers can help to identify and mitigate at list some of the risks.[29]

USB flash drives can also be a source of risk. When the Department of Homeland Security of the USA purposefully dropped data disks and USB flash drives in the parking lots of federal agencies and government contractors, 60 percent of the found objects were inserted into an agency or contractor network.[30] It shows that human nature traits such as curiosity

27 Eric Geier, "Your Printer Could Be a Security Sore Spot" (PCWorld, 25 April 2012) <http://www.pcworld.com/article/254518/your_printer_could_be_a_security_sore_spot.html> accessed 26 May 2017.

28 Wes Mulligan, "Is printing the biggest security threat for your business?" (SCMedia, 16 June 2016) <https://www.scmagazineuk.com/is-printing-the-biggest-security-threat-for-your-business/article/531565/> accessed 27 May 2017.

29 A Practical Guide to Print Security Ideal for Businesses of All Sizes (Canon) <https://www.canon-europe.com/images/ICO%20Canon%20Practical%20Guide%20to%20Print%20Security_tcm13-1000094.pdf> accessed 27 May 2017.

30 Steven Chabinsky, "Managing Thumb Drive Security Risks" (Security Magazine, 1 September 2014) <http://www.securitymagazine.com/articles/85768-managing-thumb-drive-security-risks> accessed 26 May 2017.

can easily create an additional risk of data privacy breach. Maintaining secure configurations and disabling autorun and autodisplay functions at computers is one of the strategies to mitigate the possible risks.[31] In general, it is advisable to minimise the use of USB flash drives to avoid spreading of malware and loss of sensitive information.

SITUATION 3 - USING UNSECURE MEANS OF COMMUNICATION

To speed up communication, the lawyer may be likely to use extra communicational channels in addition to Office 365 (or analogous software) preinstalled at the office computer. Such communication channels may include Messenger, WhatsApp, Slack and similar applications. When using innovative third-party applications which markets are boosting, users often do not understand thoroughly who is responsible for the applications they download and the personal data such applications use.[32]

Lawyers may communicate personal data through messengers by sending scanned documents, sharing contact details of the clients and discussing details of ongoing work assignments. They may take precaution by experimenting with data privacy settings of messengers they use at work. However, encryption services are not panacea now. In January 2017, a security vulnerability that can be used to allow Facebook to read encrypted messages has been found within WhatsApp messaging service.[33] Even if we assume

31 "USB thumb drive security best practices spelled out by NIST" (TechTarget, June 2010) <http://searchsecurity.techtarget.com/USB-thumb-drive-security-best-practices-spelled-out-by-NIST> accessed 27 May 2017.

32 Omer Tene, Privacy: The new generations (2011) 1(1) International Data Privacy Law 18.

33 Manisha Ganguly, "WhatsApp vulnerability allows snooping on encrypted messages" (the Guardian, 13 January 2017) <https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages> accessed 27 May 2017.

that the certain messenger has perfect encryption settings, there is still a question where the personal data collected by this messenger is stored. In January 2013, the Dutch Data Protection Authority (DPA) acting as a national supervisory authority issued a report that concerned appointment of data protection representative. In this report, DPA concretised WhatsApp's mechanism of collection and processing of user address book. [34] Namely, when seeking other users to message, a user of the app would grant it access to own list of phone contacts thus allowing WhatsApp to upload its users' contacts to U.S. servers where it cross-referenced this data with a stored list of existing users.[35] It is also important to remember that using WhatsApp (as many other messaging apps as well) means consenting to US terms of use and privacy policies. The GDPR does not allow enterprises to hand over data to WhatsApp without the client's consent.[36] This shows that the use of mobile phone application for the purposes of the work-related communications amplifies risks of unexpected data privacy breaches that are difficult to control for management of the law firms without an access to personal devices of their employees.

34 Cobun Keegan, Jeroen Terstegge "The WhatsApp wake-up call for companies doing business in the EU" (IAPP, 14 December 2016) <https://iapp.org/news/a/the-whatsapp-wake-up-call-for-companies-doing-business-in-the-eu/> accessed 27 May 2017.

35 Ibid.

36 Tobias Stepan, "Potential damages of using WhatsApp for business purposes" (Teamwire, 9 April 2016) <https://www.teamwire.eu/company/blog/potential-damages-of-using-whatsapp-for-business-purposes/> accessed 27 May 2017.

SITUATION 4 - USE OF "BRING YOUR OWN DEVICE" POLICY[37]

To make the working more efficient, the lawyer may need to use own private computer with preinstalled legal databases and mobile phone to improve communication. The lawyer may have to upload sensitive business data to the private computer when the work computer suddenly stopped working. That is how personal data leaves the controlled environment.

In situations when the lawyer needs to use own private computer, certain precautions that are generally applicable to working at public computers will be necessary. In the hectic moments, it is easy to forget about risks connected with storing vulnerable work-related data at the personal computer. Thus, it is important to treat personal computer as a public computer when planning data privacy measures. Precautionary measures include keeping screens private (positioning them away from other people and using privacy screen protectors), using "private browsing", never using "remember password" or "save information", and clearing browsing history and deleting any downloads before closing the browser.[38]

These examples showing the growing need of interaction between IT departments and lawyers, as well as the necessity to develop cross-disciplinary knowledge and training by professionals of both fields. As previous discussion has shown, trainings for lawyers should focus on technological implications of daily working routine and technological grounds on which legal standards are based. IT professionals, in their turn, should

37 "Bring your own device (BYOD)… at your own risk" (Privacy Rights Clearing House, 1 September 2013) <https://www.privacyrights.org/consumer-guides/bring-your-own-device-byod-your-own-risk> accessed 25 May 2017.

38 Carl Henriksen, "Top 10 security tips for remote and mobile working" (Oryxalign Blog, 11 April 2016) <http://www.oryxalign.com/top-10-security-tips-remote-mobile-working/> accessed 26 May 207.

keep up with changing data privacy standards to prioritise their working tasks effectively. It is especially important taking into consideration obligations of prompt reporting of data breaches under the GDPR. It is advisable to provide remote workers with technical support contact details, call-ins with managers, accidence reporting procedures and guiding handbooks to mitigate these risks.[39] These actions would need creating a strategy and prioritising the data privacy goals within the firm. Analysing the data privacy risks through the lens of the specially designed data privacy risk matrix will help to identify the directions of strengthening the data privacy regime individually and within the company.

4 PRIVACY IMPACT ASSESSMENT OF REMOTE WORK ACTIVITIES

Data protection authorities will have to be vigilant in monitoring compliance with the GDPR and applying the newly amplified range of possible sanctions in case if the GDPR requirements are violated.[40] Discussion so far has shown that remote work creates significant data privacy risks, as most daily practices of remote work related to document storage and communication with colleagues and clients can easily breach data privacy requirements imposed by the GDPR. Consequences of data privacy breaches that are difficult to control and mitigate promptly in the remote working environment include possible

39 Michael Cobb, "Assessing home offices for compliance with security teleworking policy" (ComputerWeekly, January 2012) <http://www.computerweekly.com/tip/Assessing-home-offices-for-compliance-with-security-teleworking-policy> accessed 26 May 2017.

40 Giovanni Buttarelli, The EU GDPR as a clarion call for a new global digital gold standard (2016) 6(2) International Data Privacy Law 77.

complaints, loss of clients, negative media coverage, reputational risk, damage claims from clients alleging a privacy breach and regulatory sanctions for noncompliance.[41] In order to prevent such risks and better identify its sources, employers and employees need to identify how these risks are linked to concrete business processes that entail dealing with personal data. To reach these goals, they should conduct privacy impact assessment (PIA) of their remote work environment. PIA is a methodology for assessing the impacts on privacy of different activities and processes, such as projects and services that involve processing personal information.[42] PIA can benefit the stakeholders in a number of ways. It can help to identify the correct people who could help in treating data privacy risks and who are actually the "risk owners" in the company.[43] It actually help to identify third-party suppliers whose activities also require PIA.[44] In case of remote workers, these third parties could be, for example, external consultants, software providers and partner law firms. It also in general helps to raise awareness about concept and importance of privacy compliance in business operations.[45]

There are certain advantages of using risk assessment approach to conduct PIA, especially when it comes to assessing the risks of remote work with the goal to find a balance between work efficiency and compliance legal requirements, as well as to consider interests of different stakeholders. A risk-based approach enables all stakeholders to identify the areas with

41 Thérèse Reilly, "Managing Privacy Risks with Telecommuting and Mobile Devices" (IAPP Canadian Privacy Summit, 30 April 2009) <https://iapp.org/media/presentations/09Canadian_Summit/handouts/Privacy%20and%20Security%20Risks%20in%20Telecommuting.pdf> accessed 26 May 2017.

42 David Wright, Paul de Hert, Privacy Impact Assessment, Privacy Impact Assessment (Springer 2012) 5.

43 Stephen Deadman, Amanda Chandler, "Vodafone's Approach to Privacy Impact Assessments" in Privacy Impact Assessment (Springer 2012) 297.

44 Ibid.

45 Ibid.

most significant risks and dedicate their resources to mitigation of these risks, ensuring a flexible and context-specific approach towards compliance.[46] In addition to that, this approach helps them to translate abstract concepts and goals into concrete risks and implementable mitigating controls and steps.[47]

In this chapter, I am going to analyse the risk assessment list that stakeholders involved in remote work can use for their privacy impact assessment. This list is based on the general research on privacy impact assessment and general cybersecurity provisions, primarily a practically oriented and an example-driven Guide to Cybersecurity issued by the Law Society of Scotland.[48] I have tailored it to specifics of remote work by investigating the common issues remote works that can be easily traced in professional blogs of lawyers and compliance professionals.

The GDPR highlights the need to assess risks levels from the perspectives of "likelihood" and "severity" of the risks to the individual (considering the nature, scope, context and purpose of the processing).[49] My risk assessment matrix is based on these provisions. It distributes different risks of remote work according to the probability level (how likely the risk is) and level of effort (amount of individual and corporate resources and time needed to

46 Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (Centre for Information Policy Leadership, Hunton & Williams LLP, 21 December 2016) 12-13 <https://iapp.org/media/pdf/resource_center/cipl_gdpr_risk_21_dec_2016.pdf> accessed 2 December 2017.

47 Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (Centre for Information Policy Leadership, Hunton & Williams LLP, 21 December 2016) 13 <https://iapp.org/media/pdf/resource_center/cipl_gdpr_risk_21_dec_2016.pdf> accessed 2 December 2017.

48 Guide to Cybersecurity (Law Society of Scotland, 2017) < https://iapp.org/media/pdf/resource_center/LSS-cybercrime-2017.pdf> accessed 2 December 2017.

49 Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (Centre for Information Policy Leadership, Hunton & Williams LLP, 21 December 2016) 28 <https://iapp.org/media/pdf/resource_center/cipl_gdpr_risk_21_dec_2016.pdf> accessed 2 December 2017.

mitigate it). There is a specific reason why I use "probability level" instead of "severity level" parameter that could be more obvious to use. Diversity of situations of data privacy breaches makes it difficult to assess the actual risk without knowing the nature and volume of information that has become subject to data privacy breach in the concrete case. Instead, the probability level helps us to trace how likely the data privacy breach is to occur without having to analyse material consequences of concrete data privacy breaches. Practicing lawyers (as well as professionals from other fields) can use this risk assessment matrix together with other matrixes that establish the hierarchy of risks based on the concrete examples of information.[50] The risk assessment list encompasses specific software risks and hardware risks, as well as risks stemming from common working routine practices. Common risks, such as careless use of passwords, are often surprisingly mundane but can compromise any security system.[51]

50 See "PII Risk Matrix" (IAPP) <https://iapp.org/media/pdf/knowledge_center/PII_Risk_Level_Matrix.pdf> accessed 6 August 2017.

51 Pasi Pyöriä, "Managing telework: risks, fears and rules" [2011] 34 (4) Management Research Review 393.

		LEVEL OF EFFORT		
		HIGH	MODERATE	LOW
LEVEL OF PROBA-BILITY	HIGH			
	MODE-RATE			
	LOW			

Table 1. Data privacy risk assessment matrix

The level of effort depends on the amount of procedures needed to mitigate the risks and the range of stakeholders involved. For instance, ensuring safe document storage practices of the client is highly complicated, as the lawyer cannot influence how those are regulated. In contrast, certain sources of risk lie more in the discretion of the individual person, not only the whole work team. Such are mostly situations of stealing data in such cases as getting physical possession of one´s computer, temporary access to one´s computer, commercial software keystroke loggers (e.g. third-party keyboard software that literally records all information that the user, for instance, types on the phone) and spyware in computer.[52] Risks of information stealing highlight the need for carefully planning physical storage of documents

52 Michael Caloyannides, Privacy protection and computer forensics (Artech House, 2004) 53.

and devices, as well as ensuring own precautions in accessing networks are among measures that lie partially within discretion of one person.

Success of these measures undertaken on the individual level is determined by the lawyer`s individual awareness of data privacy and ways to ensure it when communicating with third parties. In light of this, following remote work related activities can be analysed to complete the risk assessment list:

- Document storage practices of the client;
- Communication channels within own working team;
- Ensuring security of physical copies of the documents;
- Unreliable anti-malware protection (e.g. not covering all range of devices that an employee use during the work);
- Unsafe practices of using hardware (connecting printers, USB memorysticks);
- Unsafe network connection (e.g. using public Wi-Fi);
- Loss of working and personal devices (e.g. leaving them with out supervision when working in public places).[53]

In order to assess the probability level and level of effort, one can conduct peer-to-peer research (polling fellow law firms or major clients on common risks and data privacy attacks the incur) and carry out "IT audit" (identifying IT services that one relies on and assessing all IT equipment in active work-related use).[54]

This discussion has shown that risk assessment will help to identify a wide range of risks resulting from remote work

53 Guide to Cybersecurity (Law Society of Scotland, 2017) 10,12 < https://iapp.org/media/pdf/resource_center/LSS-cybercrime-2017.pdf> accessed 2 December 2017.

54 Guide to Cybersecurity (Law Society of Scotland, 2017) 14 < https://iapp.org/media/pdf/resource_center/LSS-cybercrime-2017.pdf> accessed 2 December 2017.

arrangements. The GDPR incentivises stakeholders to create risks mitigation strategies to avoid sanctions under GDPR and at the same time to take into account interests of employers and employees in a fair and a balanced way, and at the same time to balance the goals of maintaining compliance with the GDPR, ensuring efficient work processes.

5 EMPLOYEE TRAINING AND SELF-LEARNING OBLIGATIONS TO ENSURE COMPLIANCE WITH GDPR

In previous chapter, I have analysed the common data privacy risks stemming from remote work arrangements. It is necessary to highlight that these risks cover a lot of employees. One in ten companies with over 3,000 employees do not have a security strategy that covers remote work.[55] European Framework Agreement on Telework that we have already discussed before states that the employer is responsible for ensuring the protection of data used and processed by the teleworker for professional purposes and informs the teleworker in particular of any restrictions on the use of equipment and of sanctions in the case of non-compliance.[56] In practice, organisations show a lack of consistency in background screening of telecommuting employees and contractors.[57] The role of a lawyer as an employee

55 Jon Fielding, "Data on the move – the risks of remote working" (Global Banking & Finance Review, 4 April 2017) <https://www.globalbankingandfinance.com/data-on-the-move-the-risks-of-remote-working/> accessed 25 May 2017.
56 Teleworking (EUR-Lex) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Ac10131> accessed 27 May 2017.
57 Risk at Home: Privacy and Security Risks in Telecommuting (Ernst&Young) <https://iapp.org/media/pdf/knowledge_center/EYCDTRiskatHomePrivacyandSecurityinTelecommuting.pdf> accessed 27 May 2017.

in such situations is unique. In fact, the lawyer should take the active role of providing information and incentivizing mitigation of risks. This role is also prescribed by applicable professional codes of conduct. For instance, International Bar Association (IBA) requires lawyers to ensure maintaining of confidentiality and professional secrecy in respect of electronic communications, and data stored on computers. IBA also stresses the duty of lawyers to keep themselves informed of the required professional standards in order to maintain their professional obligations.[58]

When developing information security strategy, it is important to ensure own personal compliance with upcoming changes to the data protection legislation and general data privacy risks in general. This goes in line with both data protection laws and ethical obligations of the legal profession. I believe that this analysis will be especially relevant for in-house lawyers who are also responsible for ensuring corporate compliance at the firm, managing and self-employed lawyers, as well as any practicing lawyers and employees in general who operate personal data at their work. In my research, I would like to propose two ways of data privacy risk assessment.

5.1 SECTOR-SPECIFIC ASSESSMENT

Analysing the data privacy assessment list and general analysis of obligations of controllers and processors under the GDPR has helped to identify four main segments of ensuring compliance with GDPR. I based my classification on the "Online Privacy Literacy Scale". This scale includes such spheres, as knowledge about the practices of institutions and online service providers,

58 IBA International Principles on Conduct for the Legal Profession (International Bar Association, 28 May 2011) < https://www.ibanet.org/Document/Default.aspx?DocumentUid=1730FC33-6D70-4469-9B9D-8A12C319468C> accessed 4 December 2017.

knowledge about the technical aspects of online privacy and data protection, knowledge about potential privacy threats and risks, knowledge about the legal aspects of data protection, awareness about privacy control strategies and ways to deal with privacy threats.[59]

Know-your-vendors. From Articles 28(1) - (3), 24(1), 29, 46(1) of the GDPR, it is evident that companies cannot simply outsource the data privacy obligations to their vendors. In other words, in case of violation caused by a vendor of an organisation (e.g. provider of a software for remote workers communication), organisation using this software will be liable.[60]

Know-your-colleague (identifying risky practices of your colleagues, e.g. co-employees, temporary staff, trainees, etc). Article 43 of the GDPR and Binding Corporate Rules (BCRs), a compliance mechanism developed by a multinational group of companies and referred to by the GDPR, require "the appropriate data protection training to personnel having permanent or regular access to personal data."

Know-your-technology (identifying technological risks of your own working habits). Obligation of technological awareness is based on the "privacy by design" principle as established by Recital 78 and Article 15 of the GDPR. This would also include assessment of applicability of "privacy enhancing technologies" (PETs) to daily remote work routine. PETs minimise personal information usage through anonymisation or pseudonymisation either online or offline, or collecting little personal information

59 Sabine Trepte, Doris Teutsch, Philipp K. Masur, Carolin Eicher,Mona Fischer, Alisa Hennhöfer, and Fabienne Lind, Chapter 14. Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS) 348-351 in Serge Gutwirth, Ronald Leenes, Paul de Hert (eds) Reforming European Data Protection Law (Springer, 2015).

60 Alexandra Ross, "A strategic approach to vendor-management under the GDPR" (IAPP the Privacy Advisor, 28 February 2017) <https://iapp.org/news/a/a-strategic-approach-to-vendor-management-under-the-gdpr/> accessed 4 December 2017.

from its users by anonymising or the pseudonymisation of personal data.[61] Protecting sensitive data can be achieved by combining fragmentation and encryption methods that provide data protection in stages of storage and dissemination by ensuring that no sensitive information is disclosed neither directly (i.e., in the database) nor indirectly (i.e., derived from other information present in the database).[62]

Know-ethics. It is important not to underestimate the role of compliance with ethical obligations. Namely, Article 35(8) GDPR highlights that the compliance with codes of conduct under Article 40 of the GDPR is taken into account when assessing the impact of the processing operations.[63]

I have developed a table to identify common issues, risk levels, key stakeholders and risk mitigation measures according to each identified segment. The table focuses on the self-control questions for the lawyers that would allow ensuring sufficient control checks at the various stages of data processing. The example questions are split across four spheres of sources of rules, requirements and expectations regarding data processing. Those spheres include interaction with external (primarily clients) and internal (primarily colleagues) stakeholders, exploring underlying technology risks and ethical implications of data privacy breaches (leading up to disqualification from the profession). It is especially important not to underestimate the role of compliance with codes of conduct.

61 Rebecca Wong, Rebecca. Data security breaches and privacy in Europe (Springer, 2013) 18.

62 Sara Foresti, "Preserving privacy in data outsourcing" (2010) 99 Springer Science & Business Media 86.

63 Felix Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost, "A process for data protection impact assessment under the European general data protection regulation" 26 in Annual Privacy Forum (Springer International Publishing, 2016).

The "Risk and effort" row helps to refer the content of the table to the content of data privacy matrix. Each sphere matches with measures to mitigate risks that would involve participation of third parties (see "Measures to mitigate risks" row). These measures are based on the knowledge that a lawyer can gain by raising awareness on his or her own, even without active involvement of the management. They encompass the variety of cybersecurity and data protection measures as advised by various thinktanks.[64]

64 Guide to Cybersecurity (Law Society of Scotland, 2017) < https://iapp.org/media/pdf/resource_center/LSS-cybercrime-2017.pdf> accessed 2 December 2017.

	Know-your-client	Know-your-colleague	Know-your-technology	Ethical risks
Example questions (based on situation analysis provided in chapter 3)	My client sends documents for due-diligence through Google Drive - what do I do? How can I assess privacy risks of provided data rooms?	How can I Communicate with my colleague during vacation? How to ensure secure team collaboration working out of office?	Why I should not print documents at home? How to use corporate VPN securely? Where to store documents outside the corporate local network?	How to ensure that my daily data storage practices do not breach regulations of professional communities I belong to? How can I learn from professional and ethical self-regulation in my field?
Key Sources of Information support	Compliance officers of the lawyer's employer and councel of the other parties	Employee training provided by HR and IT departments	Employee training provided by HR and IT departments	Training and education by local Bar association
Measures to mitigate the risks	Data privacy agenda in framework agreements, general T&C Data privacy related events for the clients (educational seminars, marketing newsletters)	Internal compliance training with follow-up testing of employee knowledge? Internal data privacy audits	Clarifying procedures of interaction between IT and other departments Running security checks on the devices provided to the employees	Training organised by professional communities Co-operation between businesses, local Bars and academid communities Integrating data privacy goals into the codes of conduct and policies

Table 2. Overview of the knowledge tools of the lawyer working remotely

This table shows the key requirements for lawyers in mitigating data privacy risks in working remotely. At the same time, the lawyer should be able to address critically the risks at the different stages of information processing from receiving materials to the client to the stage of archiving old documentation. These skills of critical self-assessment would help lawyers to actively engage in company policy drafting, internal and external data privacy trainings and developing interdisciplinary measures of mitigating data privacy risks in remote work (in cooperation with HR and IT). To be able to move to more specific assessment, the lawyer can adopt DPIA assessment approach as prescribed under the GDPR.

5.2 PROCESS-SPECIFIC APPROACH

Article 30 of the GDPR prescribes the controllers to maintain a record of processing activities, that will also include information on purposes of processing, categories of data subjects, indications of cross-border data transfers and, where possible, a general description of the technical and organisational security measures (including pseudonymisation and encryption measures and ensuring mechanisms "for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures").

Article 35(7) of the GDPR clarifies assessment scope, stating that data protection impact assessment shall contain inter alia description of processing operation, an assessment of the necessity and proportionality of the processing in relation to its purpose, as well as an assessment of the risks to the rights and freedoms of the data subjects. The assessment shall also address the relevant mitigation measures and safeguards with the focus on the interests of the affected individuals. These provision of the GDPR would allow the stakeholders (primarily, in our cases lawyers working remotely) to create an "inventory" of their

work processes by listing the situations of data processing, for example, based on case study analysed in chapter 3 of the paper.

6 CONCLUSIONS

The discussion has shown that recent and upcoming changes in the regulatory environment are increasing data privacy related obligations and risks of lawyers, especially in cases of remote work. In fact, remote work encompasses a wide scope of situations, ranging from working remotely on a full-time basis to working occasionally out of office due to traveling or a sick leave.

Remote work poses additional risks when the lawyer works outside the safe working environment without a pre-arranged technological setting and supervision of peers and IT department. Moreover, it will take longer time to mitigate consequences of any data privacy breaches without immediate guidance and technological support.

For these reasons, it is important to critically approach own working habits to be able to identify potential technological and regulatory risks under applicable legislation Overview of widespread situations of risky working behaviour related to document storage and work-related communications has helped to better comprehend the urgency of the problem especially in light of the upcoming GDPR.

After identifying possible risks of daily working routine, it is important to develop the strategy to minimise them. Data privacy risk assessment matrix has shown the importance of classifying the risks based on the level of the probability and level of the effort to mitigate them in order to effectively plan risk mitigation measures. To be able to mitigate the risks, the lawyer should be aware of the specific sources of risks of data privacy breaches relevant to processes that are specific to remote work or which

use is more frequent in cases of remote work. To be able to mitigate the risks, it is important to ensure following:

- Ensuring awareness of data privacy risks that are created by employees and vendors;
- Ensuring awareness of data privacy risks caused by purely technological factors;
- Ensuring compliance with professional codes of conduct (as also required by the GDPR).

Discussion in this paper has shown that the main concern and the burden of the lawyer lies within identifying highest data privacy risks in daily communication and documentation storage practices. Lawyers shall combine developing awareness of European and national data privacy laws with strengthening technological competence and management skills in the sphere of data privacy. Critical approach to daily working routine from the perspective of ensuring data privacy and active engagement of stakeholders (HR and IT departments, compliance officers of the companies, representatives of the local bars) would help to empower the knowledge of lawyers on maintaining and improving data privacy regime when working remotely.

KRISTINA SVINHUFVUD[1]

Is High Frequency Trading Potentially Unenforceable?

1 INTRODUCTION

The validity of some contracts is relatively straightforward. In most jurisdictions it would probably be clear that by the time an apple seller replies 'it's a deal' to an initial 'three red apples, please' by a buyer, a contract has come into being. 'Three red apples, please' would account for an offer made by the buyer and 'it's a deal' would be the seller's acceptance thereof leading to a binding contract.

Today, however, contracts rarely deal with as simple matters as buying apples at the market. The recent increase in using algorithms in contracting processes is one example of how more and more complex the contractual environment has become. What implications does the decreasing human involvement in

1 Kristina is a LL.M student at the University of Helsinki, Faculty of Law.

contracting processes have for contract law and, in particular, for the contractual notion of consensus ad idem? Are the traditional concepts and the existing rules sufficient to tackle the currently emerging challenges?

Equity market provides a prominent example of a complex and largely automated contracting environment. In equity markets trading happens in particular trading venues (e.g. London Stock Exchange) subject to special rules.[2] The rise of algorithmic and high-frequency trading has radically changed the trading practise making the contracting environment even more complex.[3]

Algorithmic trade refers to buying and selling securities in an automated manner by utilising mathematical models (i.e. algorithms), computers and telecommunications networks.[4] High-frequency trade (later on: HFT) is a subcategory of algorithmic trade. In HFT the analysis of the relevant data and the consequent trading based on the data happens at ultra-high speed, in only milliseconds. As the trading strategies developed by algorithms are more and more complex and the transactions occur extremely fast, the persons employing such high-frequency algorithms are practically unaware of what they are trading. In such a case, the algorithms obtain an autonomous role in the contract formation process. Today, high-frequency trading already covers a considerable proportion of equity

2 London Stock Exchange (LSE) is a regulated trading venue and the trading on LSE is not only subject to its self-regulatory regime but also to securities law regime, for instance. For more see the webpage of LSE <http://www.londonstockexchange.com/traders-and-brokers/rules-regulations/rules-regulations.htm> last accessed 13 August 2017.

3 See e.g. Securities and Exchange Commission (SEC), Securities Exchange Act Release (No. 34-61358, 75 FR 3594, 2010) 3606.

4 Andrei Kirilenko and Andrew Lo, 'Moore's Law versus Murphy's Law: Algorithmic Trading and Its Discontents' [2013] 27(2) Journal of Economic Perspectives 52.

markets: around 35% in Europe and 50% in the US.[5] It is thus no longer totally unusual to employ algorithms with autonomous character in the conclusion of contracts.[6] For the human being employing such an algorithm, it may be practically impossible to understand which steps the algorithm takes in order to reach certain result.[7] What implications does the use of more and more autonomous algorithms have for contract law?

Traditionally, in contract law for a contract to be valid there needs to be a meeting of the minds, a consensus ad idem. This paper will observe how law currently deals with the collision between the contract law notion of consensus ad idem and the use of autonomous algorithms in the contracting process. This paper gradually seeks an answer to the question might HFT be unenforceable due to the lack of proper formation of consent? In order to achieve specificity to the discussion the observations made are restricted to HFT taking place on London Stock Exchange. HFT, as an extreme example of algorithmic trading, will thus be used as a practical example on the basis of which the clarity of the current laws will be assessed. As the London Stock Exchange is subject to the laws of England and Wales, the analysis will focus on the English contract law.

5 ESMA has estimated that depending on how HFT is defined such activity would account for 24% to 43% of value traded: European Securities and Markets Authority (ESMA), High-frequency trading activity in EU equity markets (No. 1, 2014) 11; a more recent Deutsche Bank Research confirms that the share of HFT has settled to around 35% in Europe and 50% in the US equity markets: Deutsche Bank Research, High-frequency trading – Reaching the limits (2016) 2.

6 Lauren Henry Scholz has identified at least three areas where 'black box' algorithmic contracts are already in use: HFT, dynamic pricing practises and smart contracting (e.g. Ethereum). Lauren Henry Scholz, 'Algorithmic Contracts' Stanford Technology Law Review (forthcoming) 15-31 <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2747701> accessed 13 August 2017.

7 Scientists are currently trying to discover how software thinks through brain scan. See e.g. Aviva Rutkin, 'Brain scan for artificial intelligence shows how software thinks' New Scientist (20 February 2016) <https://www.newscientist.com/article/2077532-brain-scan-for-artificial-intelligence-shows-how-software-thinks/> accessed 13 August 2017.

This paper will start by describing the relevant contractual relations in the context of HFT. Then, the applicable Rules of the London Stock Exchange and the default rules of English contract law will be analysed in order to find out how they address the formation of consent when an autonomous algorithm is used in the contract formation process. Also, inspiration is drawn from the Electronic Commerce Directive even though its applicability to HFT is questionable. Finally, it is concluded that despite the degree of autonomy of electronic contracting agents (such as algorithms) highly varies, it seems that electronic contracting is currently regulated by rather generalised rules. This may lead to some specific issues being neglected. This paper suggests that one such issue might be whether the contractual consent is properly formed when electronic contracting agents with autonomous character are used in the contracting process.

2 CONTRACTUAL RELATIONS IN HFT – A SIMPLIFIED MODEL

As already described in the introduction, the contractual framework of HFT is not quite as simple as the contractual relation that emerges when buying apples at the market. When buying apples the contractual relationship usually simply emerges between the buyer and seller of the apples bought. When trading on stock exchanges the contractual framework is messier, however.

First of all, only members of the London Stock Exchange may trade on the Stock Exchange. The membership is strictly regulated in the Rules of the London Stock Exchange (later on: the Rules).[8]

8 The Rules G 1000, G 1010 etc. < http://www.londonstockexchange.com/traders-and-brokers/rules-regulations/rules-lse.pdf> last accessed 13 August 2017.

Those who are not members to the Stock Exchange may still get involved in trading via contracting with a broker or an 'agent'.[9] High-frequency traders are however normally members to the Exchange[10] and thus it is mainly the role of the clearing house that somewhat complicates the contractual relations. When buying a share, for instance, one does not actually conclude a contract with the person who is offering the share for sale. Without going into details, the buyer and the seller do not conclude a mutual contract but a clearing house acts as a counterparty to both sides of the trade.[11] This means that the imaginary contract between the buyer and the seller of a specific share is actually broken into two contracts – one between the buyer and the clearing house and the other between the seller and the clearing house (the so called novation process).[12] It becomes apparent from the Rules G 5100-5102 that all trading happening on the London Stock Exchange shall be cleared. In other words, the contract of sale of a share does not occur between the 'buyer' and 'seller' of certain share but via a counterparty being the clearing house.

The following paper will observe the contractual relation between the buyer and the seller of a security on London Stock Exchange. As it has just been explained there is actually no direct contractual relation between those two but the clearing house comes in between those two. Thus, such observation is somewhat artificial. In the following it will be focused on the legal problem related to consensus ad idem and the use of autonomous algorithms when trading on securities. For the sake of simplicity

9 On page 5 of The Rules.

10 Interview with Tommi Vuorenmaa, Doctorate in Economies/Econometrics, University of Helsinki (Helsinki, Finland, 15 March 2016). See e.g. Tommi Vuorenmaa 'The Good, the Bad, and the Ugly of Automated High-Frequency Trading' [2013] 8(1) Journal of Trading 58–74 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2088099> accessed 13 August 2017.

11 David Loader, Clearing and Settlement of Derivatives (Butterworth-Heinemann 2005) 35.

12 Ibid. 40-41.

one may imagine as if there would be a direct contractual relation between the 'buyer' and the 'seller' of a security as the underlying legal problem remains the same despite the involvement of the clearing house: is the person willing to buy a security validly agreeing to the contract of sale in case (s)he is using an autonomously acting algorithm in the contracting process. It does not make a difference whether the counterparty to such a contract is actually a clearing house or the 'seller'.

3 ANALYSING THE APPLICABLE RULES TO HFT ON THE LONDON STOCK EXCHANGE

Now the focus of this paper is turned to analysing the legal problem related to the formation of consent in HFT. As previously described, in HFT the trading algorithms make buying and selling orders autonomously and so quickly that it is practically impossible for human beings to understand in real time what is being traded, how much and at what price. In addition to the speed, the increasing complexity of the trading strategies developed by the algorithms, as well as the fact that the trading occurs in multiple asset classes and in multiple trading venues at the same time, make it even less likely that the person employing such an algorithm could realistically understand or predict what is and will be traded.

These observations lead us to the question whether then contracts concluded through such autonomously acting algorithms and without the real awareness of their employer are valid from the contract law point of view? In HFT the person in charge of the algorithm becomes aware of each particular transaction realistically only afterwards. How may the consent of the person using such an algorithm be attributed to the contract if the person is factually unaware of the existence of the contract?

And what if the person is not only unaware of but also unable to predict how the algorithm will behave?

In order to analyse these questions, let us move forward to observing what rules are applicable to the formation of consent in HFT taking place on the London Stock Exchange.

3.1 INTRODUCING THE REGULATORY FRAMEWORK

Three layers of rules have been identified that may be of relevance when analysing the enforceability of HFT from the perspective of formation of consent.

When it comes to the rules applicable to the formation of consent in HFT taking place on the London Stock Exchange (later on: LSE), the freedom of contract provides that there exists the self-regulatory regime of the LSE containing the most specific rules on how the trading shall occur.

The rules of the London Stock Exchange refer to the laws of England and Wales as default rules.[13] Consequently, on the second layer there exist the rules of the English contract law containing some more general rules on how the consent is formed.

United Kingdom is still for a while a European Union Member State and it is yet interesting to have a look at the Electronic Commerce Directive even though its applicability to HFT is not entirely clear.

3.1.1 THE RULES OF THE LONDON STOCK EXCHANGE

All trade occurring on the LSE is subject to its self-regulative rules contained in the Rules of the London Stock Exchange (The Rules) as well as to the even more detailed and technical guidebooks.[14]

13 On page 3 of The Rules.
14 The Rules 1023.

Those who wish to trade on LSE are subject to The Rules since they must either become members to the Exchange (and consequently directly obey the trading rules of the Exchange) or trade via a broker who is a member to the Exchange.[15]

The Rules state how the trading should occur on the Exchange and that trading which complies with the Rules shall be 'firm'.[16] In rule 2100 it is stated that '(E)ach order or quote submitted to the trading system shall be firm'. Rule D 2120 further specifies that '(T)he Exchange views all trade undertaken under its rules as firm'. Should something go wrong in the course of the submission of orders and other electronic messages to the trading system, rule G 2101 attributes the responsibility to the member firm to the LSE: 'Any obligations and liabilities arising from the submission of electronic messages and orders to the trading system under a member firm's trading codes are the responsibility of that member firm. The member firm shall, at all times, have sufficient order management systems, procedures and controls designed to prevent the entry of erroneous orders and quotes to the trading system'.

The Rules do not specifically address the formation of consent issue. If one concentrates on the rule '(E)ach order or quote submitted to the trading system shall be firm', one may read the Rules in such a light that, even if the electronic message or order or quote submitted to the LSE trading system was submitted by an autonomous algorithm, it shall be firm (or valid). One must note, however, that the Rules do not specifically discuss the use of autonomous trading agents when submitting orders. How broadly are the terms electronic messages, orders and quotes to be interpreted?

One may thus also come to the conclusion that the Rules do not address the issue of using autonomous algorithms for

15 The Rules G 1000, G 1010.
16 On page 35 of The Rules.

order submissions, in particular, but that they refer to electronic messages only in a generalised manner. In other words, is rule G 2101 sufficiently precise in the context of the problem setting of this paper or should one look for a more specific answer from the default rules? If the default rules would not seem to attach validity to contracts concluded through autonomously acting algorithms, might HFT be unenforceable? On the other hand, in Europe around 35% of equity trading occurs in the form of HFT.[17] Rule G 2101 concerns the submission of electronic orders 'under a member firm's trading codes'. One might also argue that as the use of autonomous trading algorithms (like in HFT) has become a common market practice, the Rules should be interpreted as also covering HFT.

In this paper HFT is used as a real life example of autonomous contracting algorithms in order to make the discussion more concrete. The analysis of the Rules shows that there remains room for interpretation and so there will remain until case law would hint to some direction.[18] When interpreting the Rules one would probably need to turn to the default rules of English contract law.

Yet, how about the use of autonomous algorithms in other contracting contexts where their use is not yet an established market practise and where no specific rules apply? In such a setting one would again need to seek for an answer from the default rules of contract law.

17 Ibid. 4.

18 There seems to be no case law on the HFT and contract law. See Lauren Henry Scholz, 'Algorithmic Contracts' Stanford Technology Law Review (forthcoming) 113.

The previous paragraph shows that when discussing the enforceability of contracts concluded via autonomously acting algorithms, at some point, one will have to resort to the default rules of contract law. This paragraph will present some the main points in the academic discussion on the use of autonomous algorithms in contracting from the point of view of English contract law (sometimes more generally from Common law perspective).

The early comments were presented already in 1996 by Allen and Widdison, when they concluded that 'the doctrine as it now stands would deny validity to agreements generated by an autonomous computer.'[19] They came to this conclusion as they found that in such a contract the requirement of an agreement, the required consensus ad idem (the meeting of the minds), is missing.

It is the minds of the contracting parties, namely the minds of the buyer and the seller, which must come to an agreement.[20] The English legal tradition (together with many other jurisdictions) uses the famous offer and acceptance -test in order to assess whether a meeting of the minds occurs.[21] In the test the court observes whether one party may be assumed to have made a firm 'offer' and whether the other party may be assumed to have 'accepted' the offer.[22] The test however only helps us one

19 Tom Allen and Robin Widdison, 'Can Computers Make Contracts?' [1996] 9(1) Harvard Journal of Law and Technology 49.

20 Michael Furmston (ed.), Chesire, Fifoot and Furmston's Law of Contract (16th edition, Oxford University Press 2012) 42; Tom Allen and Robin Widdison, 'Can Computers Make Contracts?' [1996] 9(1) Harvard Journal of Law and Technology 31.

21 Ibid.; Jan Smits, Contract law: a comparative introduction (Edward Elgar 2015) 41-42.

22 Michael Furmston (ed.), Chesire, Fifoot and Furmston's Law of Contract (16th edition, Oxford University Press 2012) 42.

step further in defining whether the meeting of the minds has properly occurred in a specific case. The second question that comes up consequently is, how can we define what is an offer/acceptance; how can we know what the offering/accepting party has intended?[23] The English legal tradition has chosen for an objective approach to defining intention.[24]

The objective approach to defining what constitutes an assent does not try to get into the minds of the contractors. A contract is not seen as a mental state but as an act being a matter of inference from conduct.[25] It is the external factors (such as behavior etc.) that represent the intent as opposed to the actual state of mind (which again is the starting point in the subjective approach adopted in the civil law tradition).[26] The requirement of consensus ad idem thus brings us to the core of the problem. Many have suggested that the use of autonomously acting algorithms in contracting may render the contract unenforceable

23 Michael Furmston (ed.), Chesire, Fifoot and Furmston's Law of Contract (16th edition, Oxford University Press 2012) 41; Tom Allen and Robin Widdison, 'Can Computers Make Contracts?' [1996] 9(1) Harvard Journal of Law and Technology 31.

24 Michael Furmston (ed.), Chesire, Fifoot and Furmston's Law of Contract (16th edition, Oxford University Press 2012) 41; Tom Allen and Robin Widdison, 'Can Computers Make Contracts?' [1996] 9(1) Harvard Journal of Law and Technology 31.

25 Michael Furmston (ed.), Chesire, Fifoot and Furmston's Law of Contract (16th edition, Oxford University Press 2012) 41

26 Ibid.

due to the improper formation of consent in such a case.[27] What seems to be of relevance in this perspective is the degree of autonomy of the used algorithm. As Allen and Widdison put it:

27 See e.g. Tom Allen and Robin Widdison, 'Can Computers Make Contracts?' [1996] 9(1) Harvard Journal of Law and Technology 49; Samir Chopra and Laurence F. White, A Legal Theory for Autonomous Artificial Agents (The University of Michigan Press 2011) 30-31; Emily Weitzenboek, 'Electronic Agents and the Formation of Contracts' [2001] 9(3) International Journal of Law and Information Technology 211, Lauren Henry Scholz, 'Algorithmic Contracts' Stanford Technology Law Review (forthcoming) <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2747701> accessed 13 August 2017; Christopher Poggi, 'Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation' [2000] 41Virginia Journal of International Law 266; Ugo Pagallo, The Laws of Robots: Crimes, Contracts and Torts (Springer 2013) 79-113, Anthony Bellia, 'Contracting with Electronic Agents' [2001] 50 Emory Law Journal 1092; Ian Kerr, 'Providing for Autonomous Electronic Devices in the Electronic Commerce Act 1999' Uniform Law Conference of Canada (Publication in the context of the 1999 Winnipeg MB Annual Meeting) <http://www.ulcc.ca/en/1999-winnipeg-mb/359-civil-section-documents/362-providing-for-autonomous-electronic-devices-in-the-electronic-commerce-act-1999> last accessed 13 August 2017; Jean-Francois Lerouge, 'The Use of Electronic Agents Questioned Under Contractual Law: Suggested Solutions on a European American Level' [1999] 18(2) Journal of Computer and Information Law 403-434; Christopher C. Nicoll, 'Can Computers Make Contracts' [1998] Journal of Business Law 35- 49; Emad Dahiyat, 'Intelligent agents and contracts: Is a conceptual rethinking imperative?' [2007] 15(4) Artificial Intelligence and Law 375-390; Donnie Kidd and William Daughtrey, 'Adapting Contract Law to Accommodate Electronic Contracts: Overview and Suggestions' [2000] 26 Rutgers Computer and Technology Law Journal 215; Stephen Middlebrook and John Muller, 'Thoughts on Bots: The Emerging Law of Electronic Agents' [2000] 56 The Business Lawyer 341-373; Steffen Wettig and Eberhard Zehendner, 'A legal analysis of human and electronic agents' [2004] 12 Artificial Intelligence and Law 111-135; Francisco Andrade, Paulo Novais, José Machado and José Neves, 'Contracting agents: legal personality and representation' [2007] 15 Artificial intelligence and Law 357-373.

'an autonomous computer is capable of altering its stored program and developing new instructions in response to information it acquires in the course of trading (…) it would be very difficult to characterize it as the embodiment or expression of human intention'.[28]

This quite striking approach has not been left without criticism. Lerouge is claiming that the conclusion taken by Allen and Widdison fails to properly take into account the objective theory of assent important in the English tradition.[29] Lerouge is worried that Allen and Widdison are 'trapped in a subjectivist approach of the meeting of minds' whereas the objective approach would seem to suggest that 'assent may be expressed in any way including via an electronic agent and the fact that the contractual theory (objectivism) does not require that a party must be aware of the exact time of the formation and content of the contract'.[30] Weitzenboek comes to a similar conclusion: 'what is relevant is that a person should be deemed to be expressing his assent by his conduct when using an electronic agent for the purposes of contract formation'[31] and thus 'it is submitted that the objective theory of contracting does provide a solution for giving legal validity to contracts carried out by electronic agents'.[32]

Others are however not convinced of the objective theory solving the doctrinal problem. Even though strongly criticised

28 Tom Allen and Robin Widdison, 'Can Computers Make Contracts? ' [1996] 9(1) Harvard Journal of Law and Technology 49.

29 Jean-Francois Lerouge, 'The Use of Electronic Agents Questioned Under Contractual Law: Suggested Solutions on a European American Level' [1999] 18(2) Journal of Computer and Information Law 416-417.

30 Ibid. 417.

31 Emily Weitzenboek, 'Electronic Agents and the Formation of Contracts' [2001] 9(3) International Journal of Law and Information Technology 225.

32 Ibid. 226.

by Weitzenboek[33], Kerr suggests that 'the objective theory of contract will not allow autonomous electronic devices to escape doctrinal difficulties: sophisticated technologies notwithstanding, electronic devices are not legal persons; they lack the intellectual capacity to intend legal relations and cannot meaningfully be said to enter into agreements voluntarily'.[34] Weitzenboek is however questioning the relevance of this statement as, in her opinion, 'the consent that is relevant is that of the person using the electronic agent, and not of the electronic agent itself'[35] (who is lacking legal capacity anyhow).

Chopra and White, in their more recent publication, are neither too eager to rely on objectivism in order to escape the doctrinal difficulty. They are even broadening the critic from Kerr's view that is only limited to autonomous computers. In their view one could not rely on objectivism either when it comes to using non-autonomous electronic agents, i.e. where computers are merely used as mediators in the trading process: 'Even with a relatively straightforward agent, without anything resembling autonomous behaviour, a "reasonable person" would not plausibly believe the principal (refers to the person employing the computer) "was assenting to the terms proposed by the other party".' [36]

33 Ibid.

34 Ian Kerr, 'Providing for Autonomous Electronic Devices in the Electronic Commerce Act 1999' Uniform Law Conference of Canada (Publication in the context of the 1999 Winnipeg MB Annual Meeting) 3 <http://www.ulcc.ca/en/1999-winnipeg-mb/359-civil-section-documents/362-providing-for-autonomous-electronic-devices-in-the-electronic-commerce-act-1999> last accessed 13 August 2017.

35 Emily Weitzenboek, 'Electronic Agents and the Formation of Contracts' [2001] 9(3) International Journal of Law and Information Technology 226.

36 Samir Chopra and Laurence White, A Legal Theory for Autonomous Artificial Agents (The University of Michigan Press 2011) 38-39.

Schulz uses the term 'black box algorithm' in this context and raises a serious concern on the enforceability of black box algorithmic contracts:

> *'Black box algorithmic contracts inherently introduce a gap between the objectively manifested intent of the party using the algorithm and what the artificial agent does. Unlike in typical contracts, where we assume that a "sophisticated party" knows what it is doing enough to bind and be bound, black box algorithms by definition engage in emergent behavior that cannot be anticipated by a principal. So that presumption of deference to general acts showing an intent to be bound, even of a sophisticated party using algorithms, must be relaxed in the case of black box algorithmic contracts, and this relaxed presumption could potentially result in a contract being unenforceable'.*[37]

Schulz seems to bring out a further point here: it is not merely the unawareness of the person using the algorithm what is problematic, but the person's inability to predict the behavior of such black box algorithms.

From the above-presented academic discussion one must come to the conclusion that if one looks at the traditional Common law contractual framework it remains unclear whether a contract concluded via an autonomously acting algorithm is enforceable.

37 Lauren Henry Scholz, 'Algorithmic Contracts' Stanford Technology Law Review (forthcoming) 109 <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2747701> accessed 13 August 2017.

European Union, to which the United Kingdom still at least for a while is a Member, has touched upon legal issues related to e-commerce in a bunch of regulatory instruments. In 2000 the European Union passed the Electronic Commerce Directive (2000/31/EC), later on: ECD.

Article 9(1) of the Directive provides that 'Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means'.

This provision first appears to attach validity to electronically concluded contracts, such as HFT. However, it is not exactly clear whether the example case of HFT would fall under the scope of application of the Directive as Article 9(2)(b) excludes contracts requiring by law the involvement of courts, public authorities or professions exercising public authority from the scope of application of the Directive. All trading on LSE shall be settled[38] and one might question whether the settlement procedure would fall under the exception contained in Article 9(2)(b). However, one may at least be inspired by the wording of the Directive and deduce the general spirit of the European legislator towards contract formation in the context of electronic commerce.

By doing so, one soon notices that the Directive does not address the particular problem related to using autonomous algorithms in the contracting process; the Directive does not provide a clear attribution rule attaching legal validity to those

38 The Rules G 5000; Jonathan Law and Elisabeth Martin (eds.), Oxford Dictionary of Law (Oxford University Press 2009) 506.

electronic contracts, in particular, in the conclusion of which the human involvement is minimal due to the remarkably autonomous role of the contracting algorithm.[39] It merely declares that the fact that a contract has been concluded through electronic means should not, as such, invalidate the contract.

In the explanatory notes of the initial proposal of ECD it was mentioned that the use of certain electronic systems, such as intelligent electronic agents, for making contracts should not be prevented.[40] One can only wonder why this aspect has been disregarded in the final instrument. Is the reason maybe the ignorance of the fact that electronic commerce concerns a broad variety of contracts in which an algorithm may be involved in various degrees? The ECD has indeed been criticised of the little influence it has taken from the other international instruments dealing with e-commerce and it has even been claimed to be of no value from the contract law point of view due to its vagueness.[41]

The ignorance of the regulator towards using autonomous algorithms for contracting is also prominent if one looks at how the United Kingdom has dealt with the implementation of Article 9 of the Directive. The United Kingdom has submitted that the electronic contracts had the same legal status as 'off-line' contracts under the laws of the United Kingdom already prior to the introduction of the ECD:

39 Samir Chopra and Laurence White, A Legal Theory for Autonomous Artificial Agents (The University of Michigan Press 2011) 63, 65; Sylvia Kierkegaard, 'E-Contract Formation: US and EU Perspectives' [2007] 12(3) Shidler Journal of Law, Commerce, and Technology 41.

40 Kierkegaard refers to COM (1998) 586 final at 42.

41 Christina Hultmark-Ramberg, 'The E-Commerce Directive and Formation of Contract in a Comparative Perspective' [2001] 26(5) European Law Review 2, 26; Samir Chopra and Laurence White, A Legal Theory for Autonomous Artificial Agents (The University of Michigan Press 2011) 63.

> *'The Act on electronic commerce and electronic signature provided for a general non-discrimination clause of electronic form and consequently electronic contracts. As a consequence where the written form was required by law, that condition could be met by an electronic form which was capable of being accessible and fit for later use. Some contracts (merely the same in ECD) however were excluded for being capable of conclusion in electronic form.*[42]

From the more detailed arguments submitted by the Law Commission in 2001 one notices that the Commission comes to its conclusion (that the current laws of the United Kingdom fulfil the obligation of Article 9) by merely considering whether the laws imposed some formality requirements which could be unfavourable to electronic commerce.[43] The use of autonomous algorithms and the consequent problem related to the possibly improper formation of consent is disregarded, however. This becomes apparent in the concluding remarks of the report where it is stated that 'statutory requirements for "writing" and a "signature" are generally capable of being satisfied by e-mails and by website trading (…) Because English law seldom imposes such form requirements in a contractual context, it is only in very rare cases that the statute book will conflict with the obligation imposed by Article 9 of the Electronic Commerce Directive'.[44]

The Law Commission emphasises in the beginning of the Report that any legal obstacle to electronic commerce should be removed as soon as possible and that the regulation should

42 European Commission, DG Internal Market and Services Unit E2, Study on the Economic Impact of the Electronic Commerce Directive – Final Report (2007) Part II – Appendix B, 287-289.
43 Law Commission, Electronic Commerce: Formal Requirements in Commercial Transactions (2001) paras 10.1–10.5.
44 Ibid.

even be such that it would 'anticipate' developments in trading practises.[45] Thus, somewhat contrary to the primary goals of the UK legislator, the position taken in the conclusion is limited to considering purely formalistic burdens on electronic commerce.

3.2 IS HIGH-FREQUENCY TRADING POTENTIALLY UNENFORCEABLE?

Thus, in the light of the foregoing, one is left with somewhat unclear answer to the very initial question: might HFT be unenforceable due to lack of proper formation of consent? Is the requirement of consensus ad idem satisfied in such a case? An easy answer would be to refer to the rule G 2101 of the Rules in conjunction with Article 9(1) of the ECD and to argue that they generally attach validity to all electronic contracts including HFT.

On the other hand, one can also claim that even though the Rules and the relevant legislation seem to grant validity to electronically concluded contracts, the default rules of English contract law make the picture messier. If the firstly discussed rules do not specifically deal with the consensus ad idem problem in case the contract is concluded via an autonomous electronic agent, one must turn to the default rules in this regard. As elaborated above, the Common law is not entirely clear on how it reacts to contracts in the conclusion of which an algorithm takes an autonomous role. In this light one could thus also conclude that HFT might be unenforceable.

45 Law Commission, Electronic Commerce: Formal Requirements in Commercial Transactions (2001) paras 1.1–1.5.

This second conclusion is quite frightening taking into account how remarkable role HFT has in equity markets. Also, why could not the use of such contracts move to other business fields, too, and even quite rapidly? How about the enforceability of such contracts that are subject to the default rules of English contract law, only?

4 THE WAY FORWARD?

The problem related to the notion of consensus ad idem only seems to emerge with such electronically concluded contracts in the conclusion of which the algorithm is taking a highly autonomous role. The assessed rules seem to refer to contracting 'by electronic means' in very generalised terms, but do not seem to take into account neither make any distinction on the basis of how autonomous role the algorithm is taking in the contracting process. However, the degree of autonomy seems to be of paramount importance when it comes to the notion of consensus ad idem; has the person employing such an algorithm properly consented to the agreement?

Interestingly, if one takes a look at the United Nations Convention on the Use of Electronic Communications in International Contracts, it states: '(A) contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.' (Article 12)

A preparatory document of the Convention reveals the motives of the drafters when it comes to the contents of Article 12. The Working group came to the conclusion that it was

necessary to add Article 12 to the Convention (in addition to Article 8 of the Convention being content-wise very similar to Article 9(1) of ECD):

> *'The current draft, however, went a step further and expressly recognized that data messages exchanged by automated information systems could generate binding obligations even without human intervention or review of those obligations or the actions that led to their creation. That was an important clarification that should be retained in the draft convention. The substance of the draft article was not already covered by draft article 8, paragraph 1, since it dealt with a particular category of data messages.'* [46]

Article 12 thus specifically addresses the issue of the lack of human intervention. What it is still silent on is the degree of autonomy of the contracting algorithm. From the consent point of view the case may be very different if the automated algorithm is very simple (easily predictable for its employer) or if the algorithm is a very complex and practically unpredictable 'black box algorithm'.

Today one cannot avoid hearing of artificial intelligence and the development of fully autonomous, even self-learning algorithms. It seems that this development has not been properly taken into account in the rules observed in the context of this paper. Contracting algorithms are by no means a homogeneous class but there exist endless amount of different kinds of algorithms used for different contracting purposes and their degree of

46 United Nations Commission on International Trade Law, Report of the Working Group on Electronic Commerce on the work of its forty-second session A/CN.9/546 (37th session 17-21 November 2003) 126.

autonomy varies.[47] It seems that the rules analysed in this paper are neglecting this heterogeneity. A very generalised rule is not necessarily sufficient to tackle the multidimensional problems related to the formation of consent in e-contracting.

The European legislator seems to have come to this conclusion too. Very recently, the European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) was adopted. Amongst other things, the resolution recognises the shortcomings of the current contract law framework and highlights the need for new, efficient and up-to-date rules that should comply with technological developments and innovations that have recently arisen and are used on the market (AG.).

Also the academia has made suggestions to overcome this contractual problem. In this paper it is not possible to cover the suggestions elaborately, but some of the ideas that have been presented include 1) the mere tool –approach, 2) different variations of agency approaches and 3) the possibility to grant legal personhood to electronic agents.

The mere tool –approach would not require legislative changes as according to it, electronic contracting agents would be continued to treat as a mere means of communication.[48] This approach would imply the ignorance of the more and more autonomous role that the contracting agents in reality have.[49] Some have also worked upon the idea of applying the principles

47 Samir Chopra and Laurence White, A Legal Theory for Autonomous Artificial Agents (The University of Michigan Press 2011) 30.

48 See e.g., Tom Allen and Robin Widdison, 'Can Computers Make Contracts? ' [1996] 9(1) Harvard Journal of Law and Technology 43; Samir Chopra and Laurence White, A Legal Theory for Autonomous Artificial Agents (The University of Michigan Press 2011) 36.

49 Ibid.

of agency law to electronic contracting agents.[50] Also, it has been discussed whether legal personhood could be granted to the electronic contracting agent.[51]

5 CONCLUSION

This paper has observed how the law currently deals with the potential collision between the concept of consensus ad idem and the use of autonomous algorithms in contracting. High-frequency trading subject to the Rules of the London Stock Exchange has been used as a practical example on the basis of which the clarity of the current laws has been analysed. One may conclude that the rules analysed are not crystal clear on whether a contract concluded via an autonomously acting algorithm is enforceable – at least there is quite some room for precision.

For instance, in the UN Convention on the Use of Electronic Communications in International Contracts it is specifically stated that the lack of human intervention in each individual transaction should not be an invalidating factor per se in the context of electronic commerce. This is one step closer to recognising that the legislator might need to address the decreasing human involvement in some contracting practices. The Convention however fails to take into account the heterogeneity of algorithms

50 See e.g. John P. Fisher, 'Computers as Agents: A Proposed Approach to Revised U.C.C. Article 2' [1997] 72(2) Indiana Law Journal; Samir Chopra and Laurence White, A Legal Theory for Autonomous Artificial Agents (The University of Michigan Press 2011) Chapter 1; or more recently Lauren Henry Scholz, 'Algorithmic Contracts' Stanford Technology Law Review (forthcoming) 134 <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2747701> accessed 13 August 2017.

51 See e.g. Tom Allen and Robin Widdison, 'Can Computers Make Contracts? ' [1996] 9(1) Harvard Journal of Law and Technology 35; Samir Chopra and Laurence White, A Legal Theory for Autonomous Artificial Agents (The University of Michigan Press 2011) Chapter 5.

used for contracting purposes and their varying degree of autonomy. What seems to be crucial from the point of view of the consent formation, is the predictability and complexity of the algorithm used and not merely the human involvement or their non-involvement. Of course, these two are strongly interlinked.

The academia has made suggestions to overcome this contractual problem. Some of the ideas that have been presented include 1) the mere tool –approach, 2) different variations of agency approaches and 3) the possibility to grant legal personhood to electronic agents.

The European legislator seems to have recognized this contractual problem, too. In February 2017, the European Parliament resolution on Civil Law Rules on Robotics was adopted. Amongst other things, the resolution recognises the shortcomings of the current contract law framework and highlights the need for new, efficient and up-to-date rules that should comply with technological developments and innovations that have recently arisen and are used on the market. It remains to be seen whether some legislation will occur in this regard.

The high level of autonomy of contracting algorithms is already the reality in equity markets. Why could not other business sectors employ such agents rather soon in the future, too? For instance, an e-agent could be developed (if it already has not) that could analyse your browser data and do your grocery shopping autonomously online based on the information retrieved from your data. In such a scenario the legal problem discussed in this paper would actualise again – potentially even in the context of buying apples.

IV

Law, Technology and Ethics

SUSANNA LINDROOS-HOVINHEIMO, JUHA KARHU[1]

The Past, the Present and the Future of Law and Technology: a Marriage or a Mismatch

1 INTRODUCTION

When considering technology in the 1990s French philosopher Jacques Derrida noticed that technology enables all kinds of things, mobility as well as speed. It even raises concerns of complete dislocation. Technology is not confined to a place or any specific space. Technology makes territoriality secondary,

1 Susanna Lindroos-Hovinheimo, Senior Lecturer, University of Helsinki; Juha Karhu, Professor (emeritus).

or in any case troubled, displaced and de-localized.[2] This analysis is sound still today. The law faces problems caused by an increasingly mobilized world where technology dislocates, delocalizes, and dispossesses people, activities, and even time. Legal problems slip through the cracks of established laws that are determined by territorially, by new combination of facts (contextuality), and by time. Legal problems evade the grasp of national legislators, the grasp of pre-determined facts and the grasp of our time as a prioritized period in human history.

Besides cracking the nucleus points of (old) law, technology can also enable understandings in the connections that bind us together. It can be either way, cracking and/or connecting, but there are structural shifts that technology brings about. Technology points towards virtual presence, that is, presence tainted by absence and by dislocation from presence; and, in emphasizing our not being-there, not being fully present on Earth, with our feet on the ground, not being fully bound to the present time, technology also may give rise to backlashes, among them a desire for rootedness in time and place. Such reactions may be visible as backlashes in societies where common mentality calls for a return to earlier, better rooted pasts when also time was still in its place. Lawyers are not immune to such reactions. A yearning for old times when the law of the land was easy, when facts were simply facts, and when everything could be tied to presence are not uncommon.

However, law has always included technology because there can be no law without technology. The origins of law as administration and organization of society coincide with the

2 Jacques Derrida and Bernard Stiegler, Echographies of Television. Cambridge (Malden: Polity Press 2002) 32-33, 57, 80-81. It is worth mentioning that the mechanisms and processes of dislocation were of key interest for Derrida in general. See for Jacques Derrida, 'Au-delà du principe de pouvoir' [2014] Revue Rue Descartes 3.

origins of written language. Law requires at least a pencil, or the land marking stick in the hand of an ancient Egyptian priest after the floods of Nile. Unlike a human sense of justice which is in our nature, there is no immediate law that would not be mediated by one technology or another. Nowadays there are more and more sophisticated technologies through which the law operates. They may produce new problems, but technology itself is not foreign, nor external, to law.

We get a kind of first answer: law and technology have always already been married.

2 HOW HAS TECHNOLOGY CHANGED THE LAW?

We want to start by taking a topical example, the European Union's new data protection regulation (GDPR) which will become applicable in May 2018. When looking at this field of legal ordering, which the EU is energetically advancing, it is not quite clear if there is any revolutionary new law emerging. It may well be said that the new Regulation is fairly old-fashioned as to its legal technique. It is still focused on the rights of data subjects, that is, individuals, whose privacy it rigorously seeks to protect. All personal data, be it processed by companies or governments, will generally need to be dealt with in a privacy-enhancing manner. If not, then fines apply. This logic resembles consumer law techniques.

It is of course a step towards curbing the power of multinational tech companies. But there is nothing in the Regulation, nor the case law of the European Court of Justice, which is already aligned with many principles of the Regulation, that would point to revolutionary regulatory techniques. Essentially, it's all about rights, and that's nothing new. Also, as a mode of governing in a

Foucauldian sense, the regulation represents an old-fashioned technique.

One could draw the conclusion here that the law – and legal thinking more generally – lags behind technological development. Instead of rights, especially individual rights, norms should regulate basic technologies (the codes), the interfaces between technology and human beings (cyborg), and most importantly the interrelation between non-human elements and protocols.[3] This may well be so, but it remains to be seen how much the Regulation might have indirect effect on such new contexts. After all, the Regulation is not yet applied.

Still, it is by no means clear that law needs to do cartwheels to keep up with societal development. The general logic of Western legal systems based on rights might well able to cope with this world and the next. Sometimes it is just as simple as the trams arriving. In Finland, we did not have legislation that would regulate tram traffic or the legal disputes caused by trams and other vehicles colliding. Still, it was hardly a problem to apply traffic rules for other vehicles and adjust them to fit trams. Law is a flexible thing. Legal interpretation and language make it so.

But why then all the fuzz about robotic cars? The fundamental options for the liable party based on traditional law seem to be manufacturer, seller, owner, driver, or society at large, with various combination of all of them. Basic options seem to be, like in nuclear power, either to wait for safety technologies to develop, or to further the implementation of new technologies through liability incentives, i.e. making the society at large liable in the last instance. Again, there is one obvious new starting point for conceptualizing liability, which is not visible for rights-centric law. The car itself could be set as the liable party. This would match the emerging philosophical and ecological ethics of material things, as well as from another point of view, the

3 See Mika Viljanen, 'Oikeutta kyborgeille' [2017] Lakimies 1.

enlargement of the group of possible rights holders under law. A distinction must be made with our tram example. In the case of trams there was no need for novel law because trams could be seen similar enough to trains as. In the case of robotic cars there are cracks (economically creative distortions) in the functional system of traffic (containing old law) which requires a novel solution. – Obviously and the legal story of liable cars could continue to insurance policies needed, and to questions about which involved actors have duties of care for the insurance, and lastly to which functional technical means would enable a direct coupling of insurance and the use of robotic cars.

Perhaps here is also a key to understand our example with data protection regulation. The problems connected to privacy and personal data protection today are not that different from the problems that we inherited from the 19th Century. This area of law has always been intertwined with technology. Some of the earliest legal cases from the US have to do with new technologies, for instance cameras, invading peoples' private space. There is a striking similarity with drones doing photographic scanning.

There are certainly also new issues to deal with now, and it would be foolish to assert that nothing has changed. Digitalisation has changed data in ways that move it beyond the control of ordinary citizens. Quantity (of possibilities of use) can become quality (in the eyes of law). These problems have very often the nature of the Magician's Apprentice. We should be able to control early on the emergence and use of new technologies – but in doing so we would have to give up some fundamental dogmas of existing law like the technology neutrality and the policy of advancing technological development. There is no societal faith anymore in the technological imperative ("all technological invention will be taken into use sooner or later"), but the road of regulation is not easy either. An illustrative example here would be Über. However, we want to refer to another example.

Jannice Käll's recent PhD from the University of Gothenburg[4] analyses the new functions of transportation markets. What happens increasingly often in transactions is that on the surface the focus may be on goods or services sold and bought. Beneath the surface level, however, the goods aren't anymore old-fashioned goods. They are various kinds of service platforms or algorithms. The law has problems keeping up with the regulation of such objects because they are not (only) physical or even immaterial objects in a traditional sense. Bruno Latour's ideas of actants and object-subject-networks has been used to help in unravelling some of the issues to which we already hinted earlier when speaking of cyborg law.

Law seems to enable dynamic thinking that makes it possible for law to deal with new objects, even though this may require a creative mindset. Of course we need to be aware of what we are saying. To argue that the kind of law that we have is already capable to deal with most things risks sounds like a wish that the law should stay as it is. A conservative hope coupled perhaps with nostalgia. Unfortunately, nostalgia is seldom very productive, even though it is popular. The sociologist Zygmunt Bauman writes in his latest book Retrotopia that old fears have gradually been replaced with new ones, and the contemporary mindset seems to be longing back to the old. Late modernity, or whatever we should call our present time, is characterized by a wish to go back. Back to when things were simpler and most importantly: back to the times that were less global. It is understandable that there is a longing for an era when national law could solve our problems and a time when objects were still tangible. This would be a time when 'portable data' was a newspaper under an arm instead of a metaphor.

4 Jannice Käll, Converging Human and Digital Bodies – Posthumanism, Property, Law (Göteborg: Department of Law, School of Business, Economics and Law, University of Gothenburg 2017).

Today one major challenge lies in the rich but also complicated ways that technology is intertwined with global capitalism and market developments. There is an increasing number of phenomena, objects and relations that seem to escape law, slip beyond the law. Both national and transnational legislators face these problems.

One reason for this escape takes the form of the disruption of traditional distinctions between the public and the private space. Dividing lines between the private and the public have been eroding for a while but they are being shaken up forcefully now because of social media. Again, it is hard to tell whether that the old public-private distinction cannot be amended in ways that fit our times – if indeed there ever was a clear distinction. But things are changing for sure. We detect cracks here as well. Perhaps a scale is evolving instead of the old distinction. On one end of the scale would be the core of authoritative public power, police, army, prisons, and courts, and on the other end purely private matters on the market and at home. In between these ends there are phenomena composed of both public and private elements, and activities serving both common good and private interests. Media is here a traditional example that social media is challenging: should we see social media as private rather than public? Also health care entails aspects of both public service and private business.

On the other hand, it is worth asking whether everything really needs to be regulated by law. This is no self-evident truth. Many areas of life have traditionally been beyond the law in the sense that they have not been subject to much regulation. Such areas can still function. If we want the law to be everywhere, we need to be able to argue why. Perhaps it would be helpful to make a distinction between phenomena that are beyond law and phenomena that are out of the reach of (old) law. Being beyond is showing a difference in the nature of the activity in question, and therefore lacking the reason of a regulatory policy. As

mentioned family and market are the prime examples here. But there is a growing number of phenomena that are simply out of the reach of (old) law but which would fit very well in the policies of modern societies. For example, corporate social responsibility (CSR) seems to be just outside the reach of (old) law, not beyond law. Most contractual issues relating to digital services' markets could be seen normal contractual questions, and the reason for them to be out of reach of, say, effective consumer protection is simply lack of "hooks" in the old ways of regulation (for example the traditional court system is not capable of offering effective legal protection anymore)[5].

3 DO WE NEED NEW KINDS OF LAWYERS? HOW CAN LEGAL EDUCATION FACE UP TO THE CHALLENGES? DO LAWYERS NEED TO KNOW HOW TO CODE?

A lawyer's job stays the same: to look after justice, the Rule of Law, democracy and the good of the society, and to enable economic and social interactions. Even in the era of technological development that pierces all areas of life, a lawyer does not become an engineer, as lawyers did not become economists either. But when matters that are regulated become highly technologized, it causes problems for legal thinking. Certainly such problems arise in data protection legislation today. The ideas driving the new Regulation mentioned above, such as subjects' right to control of data, or data portability and consent, are issues the solution of which are thoroughly technical in nature. Metaphorically, but perhaps also concretely: a lawyer can only say whether one click

5 See for example Riikka Koulu, 'Dispute Resolution and Technology: Revisiting the Justification of Conflict Management' [2016] Juridiska Föreningen i Finland 5.

or two clicks are needed but not block clicking to become means for consent! So the essence of the Regulation, the world that is being regulated, is pure technology. There seems to be only a minor role for lawyers, and never the main role.

On the other hand, a technologized world may require even more lawyering because so many things, issues, objects or whatever are now beyond the comprehension and the control of citizens. The task for looking after people's rights falls heavily on those with a legal education. This is arguably the ideology behind the EU's strong data protection law. The citizens need to be protected because in this area, similarly as in consumer law, they do not have the resources to protect themselves. Whether there is also an earnest will to control harmful and disempowering effects of global capitalism remains to be proved, though. Our hunch is that such goals are not very high on the regulatory agenda. It is worth remembering that in addition to the juridical law, there are also economic laws, which are even harder to handle. But our previous example of CSR shows also that "justice effects" can be produced with an effective mix of legal, economic, and social ingredients if there is enough popular support.

What we need are flexible lawyers, that is, lawyers with flexible minds. Lawyers, who are able to seek creative solutions. One prime example here is the use of block chain technology in contract planning and drafting to improve the integrity of the contract. We are already educating such lawyers. It certainly does not hurt that law students also study technology, economy, even coding if they so wish. Above all, they need to know the law and they need to know it well. They need to be able to adjust to its new constellations and to be able to use it in unforeseen ways. And what they especially need is an ethos that is not restricted to just this field of law or that kind of legal case. A broad and open mind is a prerequisite for a just mind.

BEATA MÄIHÄNIEMI[1]

Regulating Technologies by Law - From Ethics to Algorithmic Fairness

1 ETHICS AND AI

In the age of digitalisation one needs to rethink legal services to address the tension between disruption and regulation. In particular, legal technology challenges the current boundaries of law and redefines legal services.[2] There is therefore an urge to address the needs and perspectives to law and technology.[3]

1 Beata Mäihäniemi is a post-doctoral researcher at the Legal Tech Lab, University of Helsinki.

2 See e.g. Frank Pasquale and Glyn Cashwell, 'Four Futures of Legal Automation' (2015) 63 UCLA Law Review, 26 - 48.

3 Conference website can be found at <https://www.helsinki.fi/en/networks/legal-tech-lab/events/law-and-digitalisation-09062017> accessed 14 March 2018.

The Law and digitalisation conference organised by the Legal Tech in June 2017 acted as a platform for international discussion on foundations of the relationship between law and technology.[4] The conference aimed at answering the following questions: What are the boundaries of disruption within the regulated area of legal services? How should the legal field embrace technology? What follows from the paradigmatic change of the legal market?

It seems that the most reasonable way to address the relationship between law and technology is to place technology after social problems and not the other way around. Therefore, when attempting to legislate technologies, one should refer to already existing social values that would serve as boundaries for the application of technologies.[5] Commissioner for Digital Economy and Society Mariya Gabriel pointed out that 'to reap all the benefits of artificial intelligence the technology must always be used in the citizens' interest and respect the highest ethical standards, promote European values and uphold fundamental rights.'[6]

4 See the official website of the Legal Tech Lab <https://www.helsinki.fi/en/networks/legal-tech-lab> The Legal Tech Lab at the University of Helsinki focuses on law, technology and society and their interrelational impact to each other. Research, experimentation and the resulting clarification of concepts and better understanding of the field are the main objectives of the Lab's research agenda. The Lab attempts to increase awareness, create new insights and bring critical views to the discourse in order to aid regulatory decision making and development of better legal services. The aim is to combine academic research, studies and practical know-how and to create a new, more agile model that more efficiently serves the needs of society.

5 Gemma Galdon Clawell, 'Responsible Digitalisation: Fitting Ethics with Innovation' (Law and Digitalisation Conference, University of Helsinki, 9 June 2017) <https://www.youtube.com/watch?v=Br2deynrxxQ&feature=player_embedded> accessed 5 March 2018.

6 European Commission, 'Artificial Intelligence: Commission Kicks off Work on Marrying Cutting-Edge Technology and Ethical Standards' (Press Release, 9 March 2018) <http://europa.eu/rapid/press-release_IP-18-1381_en.htm?&locale=en> accessed 14 March 2018.

We should then aim at strengthening fundamental rights of citizens in the face of technology. For example, empowering the user of online services to decide which personal information they wish to share, could be replaced with collective values. Similarly, as 'digitalisation stops things, makes them impossible to forget',[7] the so-called 'chilling effect' of technologies should be minimised. 'Chilling effect' denotes the situation where users abstain from exercising their fundamental rights as many technologies expose actions of the user to wider, online audience (by e.g. means of recording).[8]

Therefore, although, it would be tempting to offer new technologies outside the law, law is able to offer 'the seatbelts of technological future'[9]. In particular, although it is easy to get excited about the possibilities of technology, one should bear in mind the need to limit the technology to minimise its harmful effects on exercise of human rights.

As AI 'cannot be accorded the moral standing of the human person and inherit human dignity,'[10] the relationship between AI and ethics should be embraced. The European Commission[11] has already created its own separate ethics unit as it realised that a number of technologies were in fact illegal in Europe. The European Group on Ethics in Science and New Technologies

7 Gemma Galdon Clawell, 'Responsible Digitalisation: Fitting Ethics with Innovation' (Law and Digitalisation Conference, University of Helsinki, 9 June 2017) <https://www.youtube.com/watch?v=Br2deynrxxQ&feature=player_embedded> accessed 5 March 2018.

8 Ibid.

9 Ibid, see also John Markoff. Machines of Loving Grace: The Quest for Common Ground Between Humans and Robots on values of the ones who create the legal system.

10 European Commission, Directorate-General for Research and Innovation, European Group on Ethics in Science and New Technologies, 'Statement on Artificial Intelligence, Robotics and 'Autonomous Systems' <https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf> accessed 13 March 2018.

11 The EC is also to present a comprehensive European strategy on artificial intelligence in the coming months.

(EGE)[12] is an independent advisory body of the President of the European Commission. The group has recently released the 'Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems',[13] which analyses among others questions about human moral responsibility.[14] Some of the questions to be asked are:

> *'How should moral responsibility be attributed and apportioned and who is responsible (...) for untoward outcomes? Does it make sense to speak about 'shared control' and 'shared responsibility' between humans and smart machines? Will humans be part of ecosystems of 'autonomous' devices as moral 'crumple zones', inserted just to absorb liability or will they be well placed to take responsibility for what they do?'*[15]

One way to translate ethics to technology is to conceptualise specific concepts such as algorithmic fairness, which relates to the behaviour of large digital platforms and data-driven technologies.

12 European Commission, The European Group on Ethics in Science and New Technologies (EGE) (Policies, information and services) <https://ec.europa.eu/research/ege/index.cfm> accessed 13 March 2018.
13 European Commission, Directorate-General for Research and Innovation, European Group on Ethics in Science and New Technologies, 'Statement on Artificial Intelligence, Robotics and 'Autonomous Systems' <https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf> accessed 13 March 2018.
14 Ibid..
15 Ibid.

2 ALGORITHMIC FAIRNESS AS A SEATBELT OF TECHNOLOGY

Dominant Internet platforms, such as "The Big Four" (Google, Amazon, Apple and Facebook), have practically become legal regimes in their own right, collecting and trafficking in information about their users. These data can be later on used as training data for machine learning algorithms that will further on reinforce the leading market position of such an Internet platform. Moreover, also the business interest in developing commercial AI raises the issue of ownership of data and the functioning of information markets, where access to public data suddenly becomes a valuable asset.

There is no established legal meaning of information and thus legal approaches to data-driven technologies are currently fragmented. Recently, the scholarly interest in legal dimensions of information has focused on data protection and the implementation of the EU's General Data Protection Regulation.[16] However, this narrow focus on personal data disguises the overall picture of the increasing social, commercial, and legal importance of information as the prerequisite of AI development.

One way to approach these issues by the legal system is by means of algorithmic fairness. The concept was developed as a response to recent advances in artificial intelligence, machine

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, 1–88.

learning, and data analytics. Algorithmic fairness[17] acknowledges the benefits of algorithms in improving efficiency and equity of decisions, however, it points out that they also raise ethical problems.[18] Therefore, such algorithms can e.g. 'amplify structural discrimination, produce errors that deny services to individuals, or even seduce an electorate into a false sense of security'.[19]

The biases created by algorithms have tremendous ethical implications. For example, a risk assessment tool used by the US courts to sentence defendants in criminal cases was found to be discriminatory. Despite this, the higher court considered the software's use to be in accordance with the defendant's due process rights, placing its trust in the ability of judges to evaluate the evidentiary value of the software's risk score. The judges, however, have little or no training or understanding in how such algorithms work, especially considering that the public courts do not necessarily possess access to the actual proprietary code. The example demonstrates the social importance of algorithms used in legal decision making.

Legal Tech Lab, in one of its project attempts to analyse the concept of algorithmic fairness. It then aims at conceptualising the growing importance of information used in AI systems from

17 See also Sorelle A. Friedler, Carlos Scheidegger and Suresh Venkatasubramanian, 'On the (im)possibility of fairness' <https://arxiv.org/pdf/1609.07236.pdf> accessed 8 March 2018; Susan Nevelov Mart, 'Results may vary in legal research databases' (March 2018 ABA Journal) <http://www.abajournal.com/magazine/article/results_vary_legal_research_databases/> accessed 9 March; Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson and Harlan Yu, 'Accountable Algorithms' (2017) 165 University of Pennsylvania Law Review, 633 – 705.

18 Sharad Goel, 'Algorithmic Fairness' <https://icme.stanford.edu/sites/default/files/algo-fairness.pdf> accessed 7 March 2018.

19 Nicholas Diakopoulos and Sorelle Friedler, 'How to Hold Algorithms Accountable' (MIT Technology Law Review, 17 November 2016) <https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/> accessed 1 March 2018.

the perspective of legal scholarship. This analysis has four goals. Firstly, it provides an overview of the legal, social, and ethical implications of using artificial intelligence, data analytics and machine learning in legal decision making. Secondly, the project examines the needs and responsibilities of different actors and interest groups. Thirdly, the project evaluates the potential of different governance models to secure algorithmic fairness. Finally, the project suggests algorithmic fairness as an emergent legal principle that should guide future policy making.

Consequently, the Legal Tech Lab has found it extremely relevant that the theme of the conference organised by the Legal Tech Lab this year in 2018 is then the use of Artificial Intelligence in the legal practice and decided to focus on legal, ethical and its practical implications towards the field. [20]

20 See the Legal Tech Lab's conference site at <https://www.helsinki.fi/en/conferences/legal-tech-con> accessed 14 March 2018.