Tanel Kerikmäe · Addi Rull *Editors*

The Future of Law and eTechnologies

Springer

The Future of Law and eTechnologies

Tanel Kerikmäe • Addi Rull
Editors

The Future of Law and eTechnologies

Springer

Editors

Tanel Kerikmäe Tallinn Law School Tallinn University of Technology Tallinn, Estonia	Addi Rull Tallinn Law School Tallinn University of Technology Tallinn, Estonia

ISBN 978-3-319-26894-1 ISBN 978-3-319-26896-5 (eBook)
DOI 10.1007/978-3-319-26896-5

Library of Congress Control Number: 2016931858

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Foreword

The rise and rise of the Internet and the digital economy that it enabled had a profound and as yet not fully mapped out impact on our understanding of law and the limits of regulation. Its borderless nature (seemingly) undermined the central regulatory role that the nation-state had since early modernity. The disintermediation that it facilitated subverted existing hierarchies and disrupted well-established business models. We see this tension when the EU tries to subject Google to its data protection regime, when Uber and the sharing economy get into conflict with regulation aimed at traditional services or when peer-to peer file servers call into question the business model of the film industry, especially the practice to release films for specific geographic areas at a time. Information technology did, however, not only create novel legal problems; it also created novel ways of finding out about them. Historically, the World Wide Web was conceived as a communication tool between research institutions worldwide, and without any doubt cross-border, collaborative research benefited greatly from the sharing of data and ideas that the new technology facilitated. Academic knowledge production changed dramatically as a consequence. The ethos of the academy had always been one of disinterested search for the truth. The open sharing of results and ideas, the cooperation across national borders in pursuit of universal truths and allegiance to one's discipline rather than country, creed or race come naturally to such a world view. The new technology proved an ideal environment for such an ethos to flourish, often to the dismay of national governments which did not appreciate their researchers sharing such sensitive knowledge as, e.g., optimal encryption methods with the entire globe. While the eventual pushback was significant, it cannot be doubted that the mode of academic knowledge production changes dramatically through the WWW, making research more open, less parochial and more truly international.

If the Internet thus poses challenges to the international legal order that transcend the capacity of nation-states to regulate them, and if in turn research communities have formed through international collaboration that address the international nature of these problems by forming globally distributed research networks, where then is the place for collections such as the present book, which brings together research and researchers from a specific geographical region? Surely, the legal and technological problems that Estonia faces through the global information revolution cannot be substantially different from those encountered in the US, the UK, China or India? Surely, the geolocation of an academic is much less relevant than the issues s/he studies? In short, is there still a place for books like this that organise around a shared tradition, research culture and national experience rather than, thematically, around topics and questions? Anyone reading through this collection will answer this question with an emphatic yes. It is a display of a rich and varied research culture, substantially connected and interlinked with international debates and informed by international research efforts, sure, but it is also responsive to the particular intellectual traditions and local problems, ideas and solutions of Estonia.

The importance of these distinctive, local research cultures is difficult to overestimate. Technological monocultures are a main reason behind the vulnerability of the Internet to crime and attacks. When almost everyone is using a Windows machine, a virus that attacks this operating system has devastating effect. Similarly, when everybody, everywhere, thinks like Silicon Valley, every flaw in the model, any angle of attack, is multiplied in its effects. Legal systems and legal cultures, as Pierre Legrande observed in the context of the debate on European legal integration, are breeding grounds and test beds for new solutions, regulatory experiments and problem-solving strategies. If they are replaced by (legal, intellectual) monocultures, the diversity, and with that the robustness of the system against attacks, suffers. Only if we maintain the ability to develop and test new ideas in a competitive and diversified environment can we hope to find the answers to the pressing challenges of tomorrow.

In this collection, we can find excellent examples of the dialectic between global problems and discourses and local, specific and particularistic solutions. The paper by Sandra Särav and Tanel Kerikmäe on E-Residency and the Digital Identity Card is an example in point. Estonia is not only a country with an excellent IT infrastructure, where successive governments have pursued aggressively and successfully an agenda of digital growth; it also came up with a unique solution to open up this infrastructure to the world. From this, a new concept was born, the Estonian digital identity or an e-residency that grants its holder a number of rights and privileges unknown, in this form, anywhere else in the world. The intended result will be a massive migration of electronic services to Estonia, where people from all over the globe will be able to store, access and process their documents. At a time when concerns over large-scale migration in the physical world hits the news headlines in Europe once again, e-migration, if the pun is excused, is a novel and radical approach to share local infrastructure globally and to put counties that are geographically at the periphery of Europe at the very centre of its digital agenda. While there is much to be applauded and to learn form this novel approach to grant access to non-citizens to government-funded IT infrastructures, Särav and Kerikmäe's paper is far from self-congratulatory. Rather, it reminds the reader of the various ways Estonia is integrated into an international legal regime, in particular EU data protection law, and how despite the technological soundness of the approach there remain serious legal concerns if this solution as implemented is compliant with these international legal obligations. Lehte Roots and Costica Dumbrava, in their contribution on e-citizenship opportunities in the changing technological environment, take up this theme in their analysis of the changing nature of citizenship and belonging in a digital world. In their analysis, the Estonian e-residency approach can serve as a blueprint for a much more ambitious endeavour, the creation of a European e-citizenship and with that a European e-demos. As a Scot by adoption, I have to mention at this place that Scotland's revolutionary e-petition already now allows all EU citizens (and indeed everybody in the world, including the considerable Scottish diaspora) to become active participants in our political process, by forcing, potentially, Parliament into a discussion. Developments like this in Scotland or the ones described by Roots and Dumbrava for Estonia show once again how small countries at the geographic fringes of Europe can build on their history of geo-migration to lead the way in defining a new form of European identity, where physical distance becomes irrelevant.

Another contribution that expresses particularly well the importance of the local in a time of global threats is the contribution by Norta, Nyman-Metcalf, Othman and Rull that investigates the role of software agents as a tool against Internet scams. We may all have been at one time or the other at the receiving end of a social engineering attack—the sudden and unexpected death of an African dictator who left billions of pounds behind for us to collect, the corrupt bank official who promises a share in the riches of a deceased client with similar name as us or the damsel in distress who needs quick financial support in exchange for undying gratitude are just a few of the cardboard characters that flood our email inboxes or approach us on social networking sites. Can we outsource the handling of this modern-day scourge to computer programs that handle the nuisance on our behalf? The paper shows that these attacks, designed to hit thousands of targets worldwide, are particularly susceptive to a bit of "local knowledge"—for everyone who understands local customs, habits, way of speaking and doing things, they raise immediately warning flags. Because they are premised on a "one size fits it all" approach, they cannot respond well to specific forms of common knowledge or socially shared expectations. The paper gives a fascinating account of how such local knowledge, for instance about typical dating cycles, could be rendered computational to allow software agents to identify and protect against these scams.

The other papers contribute to the rich tapestry of IT law research in Estonia, with often surprising new solutions to problems that capture at the moment worldwide attention. Sepp, Vedeshin and Dutt tackle the thorny issue of IP protection in the age of 3D printing, developing a new solution, secure streaming, that bypasses through technological means the intricate legal issues that the new technology raises while preventing stifling overregulation and overprotection. They do not make an explicit connection to the paper by Särav and Kerikmäe, but we can wonder if between the two a new type of business model could evolve—3D printer farms, located in countries that benefit from a strong IT infrastructure and flexible IT regulation, could become the places where designs from all over the world are printed out and assembled into shippable objects.

How would the German designer of a 3D pattern pay for having it printed, on the request of his Australian customer, in Estonia? Ideally, in a closed system, with a cryptocurrency using a “smart” or “self-fulfilling” contract, thus creating a fully digital value chain. Kõlvart, Poola and Rull in their paper give an overview of the challenges to contract law that self-fulfilling or “smart” contracts pose. Self-fulfilling contracts have recently taken centre stage in the discussion on the AI and law interface, though one could argue that some of the conceptual issues that they raise are as old as the classical vending machine, which would “execute” the contract of buying a bottle of Coke by measuring the weight of the coin and, if appropriate, through a mechanical contraption release the bottle without human interference. More recently, this idea gained renewed interest through the success of using automated agents in contract formation and online auctions. At the same time, digital rights management can also be seen as an early digital form of smart contracting, where the rights transferred through the copyright licence are “self-enforcing” But it was only with the emergence of blockchain technology and cryptocurrencies that all aspects of a contract could become “self-fulfilling”. Where in the past humans were still needed to act on the required payment, we can now think of a transaction where all constituent parts are automated, automatic and digital: my CD player profiling my preferences, on that basis buying a music file from another machine, downloading the use rights of the cloud-based file and at the same time transferring the right amount of bitcoin to the seller. The blockchain technology that could one day soon enable these automated contract execution together with digital payment are discussed in the paper by Künnapas. He charters the new legal territory that we need to conquer and the radical challenges to contract law that this new technology poses. Comparing Estonian and UK responses to bitcoin, he reminds us also of the often overlooked issues in the debate, most importantly tax law. The ICT infrastructure that enables all this, after all, is also (partly) financed by our taxes, and global digital markets are particularly prone to separate the beneficiary from such an investment from the taxation that enabled it. The topic of smart contracts, arguably one of the most fascinating developments in recent years, is taken up; a final paper by Solarte-Vasquez, Järv and Nyman-Metcalf analyses the usability factors in smart contracting. As with many other papers in this collection, it shows the benefits of sustained and systematic cross-disciplinary research, collaboration between computer science and law. Their contribution centres around the “Proactive Law Movement”, a way to think about the relation between law and technology that has in recent decades gained considerable traction, particularly in northern European countries. While law is often (mis)perceived as the “spoilsport at the party”, the incessant raiser of objections, concerns and warnings that get in the way of exciting and beneficial new technologies, proactive law considers law as a beneficial and indeed creative force that increases value and opportunities for companies, individuals and wider societies.

Solarte-Vasquez, Järv and Nyman-Metcalf show how proactive law and transactional design can come together to assist technology-supported smart contracting and finish their analysis with a glimpse on a potential role for visualisation techniques, an avenue pursued, inter alia, by the multisensory law paradigm.

The blockchain technology and the inherent transparency that it brings should facilitate also issues of evidence and proof if a contract fails, or in the case of fraud. Yet for the time being at least, difficult issues of electronic evidence mean that the best substantive laws for the online world will be insufficient unless enforcement catches up. This in turn shifts out attention to the issue of evidence and proof, all to often the poor relation in the discussion on IT law and Internet regulation. Agnes Kasper and Eneli Laurits in their chapter give a broad overview of the various challenges that collecting on digital evidence still faces. They highlight in particular one of the perennial problems of all Internet law—how a private, commercial environment that is nonetheless based on a public infrastructure, and perceived by its inhabitants as a public space, can navigate the tension between private and public laws. This tension is normally discussed for substantive law issues: how can we regulate freedom of speech online when, from the perspective of the citizen, posting on a forum is an activity in a "public space" government by the constitution and its civil rights guarantees, yet from the perspective of the law it will be more often than not a private, commercial place governed by contract law, a shopping mall rather than Speaker's corner? Kasper and Laurits raise this issue in the context of the law of evidence and procedure. In the offline world, we give the police special powers to collect, curate and control physical pieces of evidence. In the online world by contrast, we (inadvertently, necessarily) give similar rights to system administrators and other private parties. What does this mean for the different forms of procedure, criminal, civil and administrative, and are existing legal frameworks that regulate the collection, analysis and admissibility of evidence that rely on a strict police/private dichotomy suitable for the Internet? While Kasper and Laurits give an overview of the issues that digital evidence and proof generate for the law, the contribution by Kristi Joamets focuses on one specific area, the question of digital marriages and divorces. Getting married or getting divorced are administrative actions that in the state of the twenty-first century, citizens expect increasingly to be supported, if not replaced, by online functionality. In 2007, there were predictions that two per cent of all marriages in the US would be conducted in virtual worlds by 2015, and while reality fell well short of this prediction, the concept of virtual marriage took hold. Less adventurous, even traditional marriages officiated by civil servants in brick-and-mortar registry offices increasingly rely on digital licences and certificates. This raises issues about data quality, security and robustness against fraud.

Throughout this introduction, we have seen the extraordinary range of topics that are addressed in this collection, from electronic evidence and the law of civil and criminal procedure to contract law, criminal law, tax law and intellectual property law. We have also seen how each of them is located in the intersection between different discourses, negotiating the tension between the global and the local, international and national, the technological and the legal. It is from these creative tensions that genuinely new solutions and approaches emerge. The papers give an account of the richness and interconnectedness of contemporary debates on cyber governance and technology regulation, and in a microcosm of a national research tradition also of the diversity of voices that need to be heard to find sustainable regulatory solutions for our digital future.

Burkhard Schafer
Professor of Computational Legal Theory
University of Edinburgh
Old College, South Bridge
Edinburgh, UK

Director, SCRIPT Centre for IT and IP Law
School of Law, University of Edinburgh
Old College, South Bridge
Edinburgh, UK

Contents

Foreword v
Burkhard Schafer

Theorising on Digital Legal (Outer)Space 1
Tanel Kerikmäe and Addi Rull

"My Agent Will Not Let Me Talk to the General": Software Agents as a Tool Against Internet Scams 11
Alexander Norta, Katrin Nyman-Metcalf, Anis Ben Othman, and Addi Rull

E-Citizenship Opportunities in the Changing Technological Environment 45
Lehte Roots and Costica Dumbrava

E-Residency: A Cyberdream Embodied in a Digital Identity Card? . . . 57
Sandra Särav and Tanel Kerikmäe

Intellectual Property Protection of 3D Printing Using Secured Streaming 81
Paula-Mai Sepp, Anton Vedeshin, and Pawan Dutt

From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of *de lege ferenda*? 111
Kaido Künnapas

Smart Contracts 133
Merit Kõlvart, Margus Poola, and Addi Rull

Usability Factors in Transactional Design and Smart Contracting 149
Maria Claudia Solarte-Vasquez, Natalia Järv, and Katrin Nyman-Metcalf

Digital Marriage and Divorce: Legality Versus Digital Solutions 177
Kristi Joamets

Challenges in Collecting Digital Evidence: A Legal Perspective 195
Agnes Kasper and Eneli Laurits

Theorising on Digital Legal (Outer)Space

Tanel Kerikmäe and Addi Rull

> *Computers are unreliable, but humans are even more unreliable. Any system which depends on human reliability is unreliable.*[1]

Abstract Although we tend to agree that innovation makes us smarter, happier and more skilful, securing the process of developing and exploiting technology remains an essential issue. The authors analyse somewhat controversial developments through the viewpoint of legal theorists to find out how to balance the rule of law with the rapidly growing world of tech. What are the guiding principles that have to be followed in the context of unpredictable and socially untested advancements? What are the constitutional dogmas and doctrines that cannot be damaged when adopting the new inventions? Kerikmäe and Rull are convinced that creating a legal principle cannot be rooted in a specific technological advancement and the new technology is not assumed to change the common values. Customer's rights and "dehumanisation" perspectives are discussed in the light of "surveillance state" and "service state" policies. The chapter gives conceptual overview of the contributions in the book and concludes with the statement that "user-centricity" and the common values should be prioritised as once when space law suddenly emerged.

1 Who Determines the Principles of eRegulation?

New technologies are making us all smarter—thus, should we worry about combining the existing values to all-embracing dominance of tech? Despite of the prediction of one of the leading priests of technological singularity, Kurzweil, namely that "by 2045, we will multiply our intelligence a billion fold by linking wirelessly from our neocortex to a synthetic neocortex in the

[1] Myrphy/anonymous author at: http://www.murphys-laws.com/murphy/murphy-technology.html.

T. Kerikmäe (✉) • A. Rull
Tallinn Law School, Tallinn University of Technology, Akadeemia tee 3, 12618 Tallinn, Estonia
e-mail: tanel.kerikmae@ttu.ee; addi.rull@ttu.ee

T. Kerikmäe, A. Rull (eds.), *The Future of Law and eTechnologies*,
DOI 10.1007/978-3-319-26896-5_1

cloud",[2] the questions related to reaching this nirvana status for mankind, i.e. securing the process of developing and exploiting technological hype, remain. These questions are mainly related to the question of citizens to become e-citizens (willingness), digital divide, clashes between stakeholders in the market and political arena and—the most intriguing—who decides what is wrong and what is right, i.e. what is legal and why.

In the previous book, "Regulating eTechnologies in the European Union",[3] edited by one of the authors and published last year (2014), the researchers had to admit that various EU agendas and initiatives are still shadowing the unshaped legal framework, proposed methodological approach for better regulation and emphasised the key element in this process—electronic identity for all stakeholders[4] that should rely on legally binding principles.

We may try to find hints from philosophers who have been worried of the nature of law in the context of changing society. However, it might even confuse Hobbs what kind of "new social contract" or "new deal" would be preferred by ePersonalities. The beautiful idea of having a legal system where a regulation is supported and screened by principles needs renaissance in the context of presumed unbalance between law and tech. Before discussing the institutional source of the principles, i.e. *pouvoir constitué*, the collisions behind "right and best" doctrines may arise. Thus, the ultimate distinction between policy and law as suggested by Kelsen in his *Reine Rechtslehre* is not possible anymore as technology develops so much faster than legislator can ever admit and Bentham's utilitarianism should be revisited.

The current collection of articles is Europe oriented and seeks the premature answer to the question: how should the EU legislator represent the interests of EU (e)citizen when regulating e-technologies, assuming that Steve Saxby might be right when saying that "we are in the middle of a global identity crisis"?[5]

As Semmelmann stresses, "different legal principles import different sorts of content into the EU legal system".[6] The author refers to different driving forces, prioritising

(a) rule of law (proportionality and legitimate expectation);
(b) governance (subsidiarity);
(c) fundamental rights (equality, dignity, privacy);
(d) economic policy (free competition).

The most relevant general approach is the rule of law. But what if we have to reconsider even the borders of our current understandings? A good colleague from Folke Bernadotte Academy (FBA) working group, prof. Krygier, suggests that—

[2] Ray Kurzweil's Mind-Boggling Predictions for the Next 25 Years, available at http://singularityhub.com/2015/01/26/ray-kurzweils-mind-boggling-predictions-for-the-next-25-years/ (accessed 15.09.2015).

[3] Kerikmäe (2014).

[4] Kerikmäe and Dutt (2014), pp. 28–29.

[5] Steve (2013).

[6] Simmelmann (2014), p. 321.

before putting the bridle for lawmakers—we should discuss “what we might want the rule of law for”.[7] The editors of the current book believe that “the EU’s legal framework has been based on economic rationalities rather that were only gradually and selectively replaced by a fully-fledged constitutional approach”.[8] It is true that the principles as such, frequently politically highlighted, are mostly not systematically positioned in the EU legal space. Often derived from the so-called primary treaty law and then specified by the CJEU, we may only assume the teleological nature of this process of interpretation—taking account also certain contradictions when mapping the development in case law.

However, the legitimacy of principles in the field of law and technology is something desirable when looking forward to strengthen the legal culture that may face unexpected technological challenges without fear of losing its normative character. Martin, explaining the scholarship of philosopher Raz, emphasises that for legitimacy, the rules (being in the form of norm or principle) must “be identifiable in a content-independent way”.[9] It means that the reason for interpreting or creating a legal principle cannot be rooted from a specific technological advancement but should embrace various aspects described above. Totally new and distinct principles, even if they meet new challenges in e-technologies, cannot be justified as the new technology is not assumed to change the common values but should rather be seen as a tool for applying these values. Legitimacy is secured when the rule of law and human rights are prioritised already in the beginning of the process of an initiative that elaborates a set of legal norms.[10]

Austin once determined the law as a tool for the sovereign and expects the citizens to follow the rules habitually. In case we admit that innovators are leading the process, they can be considered the new Leviathan. This is why many IT architects also suppose digital by default! Sometimes the aforementioned slogan is justified by the idea of distributive or social justice—which can also explain citizen–State (EU) relationship as a compensatory or trade-like phenomenon, i.e. individuals lose some privacy but get compensated by other means. For example, by Rudder, Facebook and Google are free services and can be seen as the recompense for taking away some privacy, although he also admits, it would be complicated to find a fair balance[11] between the power line of governments and citizens’ rights and obligations.

This approach would be opposed by the theorists who suggest that a coercive role of law (“sanctions” by Hart, the “minimum of liberty” by Kelsen) should derive not from interest groups but from the legislator. At the same time, the so-called technological neutrality principle, as an idealistic justification, means that despite of the type of technology, the principle can be applied to all of them and legal intervention is needed only if the stakeholder is abusing his/her rights.

[7] Martin (2008).

[8] Ibid., p. 322.

[9] Martin (2014), p. 16.

[10] Kerikmäe and Dutt (2014), p. 24.

[11] Rudder (2014), pp. 235–237.

Would “after-adjustment” be a reverse *grundnorm* in the context of a tech regulation? Can it be seen as a self-regulation of the digital world? Martin, analysing the positivism, claims that law has relative autonomy and there are moral values leading the decision-making process of those who apply the law.[12] She asks two relevant questions: “Are we able to conceptualize law without contestable value-laden assumptions? Does an account of the nature of law inevitably rely on assumptions about the human condition?”[13]

Thinking about the history of law—the establishment of the first democratic state or the adoption of the first constitution by *populi* was, at this time, most likely severe violations of *de lege lata*, existing law. These acts were contrary to the beliefs of most of the legal scholars and rather seen as temporary outbursts caused by mismanaged kingdoms. However, the new order was justified only if *demos* agreed upon and obeyed the rules. Social need is a prerequisite of efficient technology and legalisation of new advancements depends on crucial stakeholders: eCitizen, eCustomer.

2 Two Colliding Perspectives: Customer’s Rights or Dehumanisation?

Leading authors in the field, Hoikkanen et al., are suggesting EU-wide regulatory infrastructure, mapping the multi-level potential policy responses to regulatory challenges.[14] The authors present several relevant choices to be examined when modelling the renewed, “technofriendly” legal space,[15] namely whether

(a) to opt out of general rules or from specific transactions;
(b) to identify “new legal categories” (such as eIdentity) that require special attention;
(c) to recognise that distinction of tech regulation derives primarily from stakeholder’s interests (citizens, customers, software developers, etc.), although there can be intersections of layers such as personal, group, space and infrastructure profiles;
(d) to admit the (changing) borderline between the eIdentity allocated by the State and so-called user-chosen identity, indicating clearly the need for a separate level of regulation.

Lips is further developing the concept of citizen (customer)–State/EU relationship as a crucial element in the era of ICT-enabled development and a wide range of public service environments.[16] She unlocks the eIdentity from the perspective of

[12] Martin (2014), p. 51.

[13] Ibid.

[14] Hoikkanen et al. (2010), pp. 2–3.

[15] Ibid.

[16] Lips (2010), pp. 273–289.

(a) what you are (DNA, fingerprints),
(b) what you do (click-behaviour),
(c) what you know (passwords), etc.[17]

Lips also compares the doctrines "surveillance state" versus "service state" with examples: in the case of the first doctrine, the approach of monitoring and social sorting is preferred; in the case of the other, the approach is based on holistic needs of service provision—and ends up with "fair state perspective" with emphasis on client focus and citizens' rights implications.[18] This fits with the theory of Gallings, who, trying to elaborate the minimum requirements of eIdentity management, proposes several safeguards to control state power and secure citizens' rights (authorised personnel, secured storage and handling of data, monitored process, etc.). The sample test question, for example, could here be the following: can the electronic trackers rather be developed to reduce police brutality or discover attempts for possible criminal activities by the citizens?

The EU has certain advantages and disadvantages when it comes to legal history. In the current context, the fact that it is derived from international public law and constitutional law of Member States and it is still a rather young legal system would be an advantage to regulate technological developments in combination with Digital Market and Citizens Europe, contrary to what the United States leading theorists are predicting on eRegulation and eIdentity management issues. Namely, Smedinghoff is quite convinced that the "federated approach" is possible with a focus on private legal framework due to jurisdictional varieties and conflicts and that public law in the field, being "unclear, ambiguous" (and that's why "inappropriate"), can only have supportive role in regulating the area.[19] This angle of view seems to be adopted by the US federal government, which seeks for contractual relationships when solving legal issues related to technologies.[20]

However, even if a fear that technophiles would replace our (offline) rights with digital rights is perhaps even overestimated, the question of endless interpretation of *de lege lata* vs. new digital legal space still exists. Law is a conservative phenomenon, and its developments should be grounded. The "dehumanisation of law"[21] is, a general problem, related to unexpected and unforeseen technological developments directly embracing ourselves. There have been attempts to create principles that are higher than the will of sovereigns in public international law (*ius cogens* or peremptory norms) such as the principle of *hostis humani generis* and universal jurisdiction when fighting against piracy. D'Amato, disappointed of attempts to create such

[17] Ibid., p. 276.

[18] Ibid., pp. 277–279, 285.

[19] Smedinghoff (2012), p. 537.

[20] See, e.g., Warren, Zach. White House to Seek Comment for Government Contractor Cybersecurity Regulations. Legaltech News available at: http://www.legaltechnews.com/id=1202733514159/White-House-to-Seek-Comment-for-Government-Contractor-Cybersecurity-Regulations#ixzz3hZVSK4Na (accessed 15.09.2015).

[21] Gervassis (2012).

supernorms in international law, states: . . . there are competitive, politically associated, heartless governments who may interpret peremptory norms as they wish (and as the international law is based on consensualism, others have at least consider any of this interpretations of non-democratic international society of States).

The search for neutral and objective legislator in the era of technological triumph is somewhat similar to the *ius cogens* phenomenon. The creator of a discipline named social physics,[22] Alex Pentland from MIT, warns us that the revolutionary technology may also feed "the development of a "big brother" model, with government using the data but denying the public the ability to investigate or critique its conclusions".[23] To avoid cataclysms, he proposes "new deal on data" composing of three rights:

(a) right to possess data;
(b) data owner's control over the use of data;
(c) right to dispose or distribute your data.[24]

The author of the theory is convinced that securing these rights is not complicated. But one should not become worried about the technicalities and price of creating the enforcement mechanisms of these safeguards. The editors rather tend to agree with Haukamäki that "the aspect of social interaction must be on the agenda of social research" and "to practice Social Physics alone means dehumanization . . .".[25] In other words, legal theorists may get worried about anarchism, which gives the rights to people from an individualist point of view not from the angle of community, legal society or, more precisely, e-legal society composed of eRegulation.

There is a temptation to take both approaches and combine, balance them. Actually, it has been done already. The most comprehensive theory that combines different angles and approaches of law and technology is written almost 10 years ago by Cockfield and Pridmore representing the idea of "Synthetic Theory".[26] The authors claim that instrumental theories are idealistically focusing on technology as a "neutral tool" without taking account of social impacts.[27] The authors refer to the

[22] An Interview with Alex "Sandy" Pentland about Social Physics available at: https://idcubed.org/home_page_feature/an-interview-with-alex-sandy-pentland-about-social-physics/ (accessed 15.09.2015).

> "Social physics is a new, quantitative science of human society that can accurately predict patterns of human behavior and influence those patterns. Social physics helps us understand how ideas flow from person to person through the mechanism of social learning and ends up shaping the norms, productivity, and creative output of our companies, cities, and societies. Importantly, social physics also tells us how to deal with the privacy concerns raised by big data: by giving individuals more control over data that is about them."

[23] Pentland (2008–2009), p. 79.

[24] Ibid.

[25] Huhtamaki, Antti. Social Physics studies idea flow by big data. A critique of Alex Pentland's new book, p. 5. Available at: http://www.academia.edu/6508962/Social_Physics_studies_idea_flow_by_big_data._A_Critique_of_Pentlands_new_book (accessed 16.09.2015).

[26] Cockfield and Pridmore (2007).

[27] Ibid., p. 476.

idea that traditional approaches should be revisited time to time as technology changes the world and also the mentality of appliers. The authors indicate that new technologies are so different that they can be referred to as post-modernity phenomena.[28]

Authors in this book provide the insight to the discourse of cutting-edge technologies and law from several different angles. Topics discussed here are hotspots in the world of e-technologies. Novel concepts such as e-residency, smart contracting, use of secured streaming in 3D printing, smart agents and others offer opportunities that were difficult to imagine a few years ago, but they also pose challenges to regulators around the world. This is about taking the reader to unregulated territories.

Norta, together with his co-authors, explores the possibilities to use software agents to tackle Internet scams. The scenario of scam described in this chapter is a real-life case study experienced by Katrin Nyman-Metcalf. Scammers around the world have reached out to most of us. In most cases, people recognise a scammer, but many fall for a scam. As scams become more sophisticated, the risk of falling for a scam is rising. Authors suggest that a scam-filtering individual software agent able to recognise a fraud is a solution to the problem.

Särav and Kerikmäe discuss the implications of the concept of e-residency developed in Estonia. Several other countries consider similar developments while closely monitoring how Estonia handles the novel concept of attracting people around the world to benefit from Estonian e-services. We believe that this is just the beginning and soon we will see several countries advancing in the field of e-governance competing against each other in the offering of e-services to the world outside. This is part of a bigger phenomenon where blockchain technologies underlying cryptocurrencies are able to support decentralised autonomous organisations such as Bitnation (www.bitnation.co). These platforms demonstrate the power of social networks, peer-to-peer information production and crowd sourcing.[29] Multinational software companies and governments are investigating possibilities to use the blockchain technologies for governing purposes in the future.[30]

We are moving towards new governing ecosystems, and any new service or functionality developed contributes to the paradigm shift in many traditional practices. Joamets discusses the possibilities of digital marriage and divorce. She points to different legal issues that need to be solved before the digital solution can be legally ascertained. Kasper and Laurits cover the topic of digital evidence. This is an emerging field with many technological and legal challenges. States are increasingly in the need to secure the efficient collection of digital evidence as the use of digital technologies grows exponentially. Roots and Dumbrava discuss the possibility of the model of e-citizenship for Europe.

[28] Ibid., pp. 478–479.

[29] See, e.g., Benkler (2002a), pp. 81–107; Benkler (2002b).

[30] See, e.g., The Blockchain is a New Model of Governance. http://www.coindesk.com/consensus-algorithm-and-a-new-model-of-governance/ (accessed 13.09.2015).

Several chapters discuss smart contracting and smart property. Kõlvart, together with co-authors, brings out different understandings of smart contracting and outlines what is necessary for a smart contract to become a legal contract. Künnapas approaches the topic from the Bitcoin perspective, which has become highly controversial, because it is breaking the understandings of how monetary systems should function. There is a lot of legal uncertainty about cryptocurrencies. The blockchain technology may have proven already that a digital monetary system without a centralised state supervision is possible. Solarte-Vasquez et al. propose the concept of transactional design for conflict management and dispute resolution.

Sepp and Dutt have written a chapter together with Anton Vedeshin, who is one of the founders of 3DPrinterOS. This innovative start-up company originating from Estonia develops the operating system for easy and secured 3D-printing. In the future, it may be comparable to what operating systems such as Windows, Mac OS and Android have done with computers and smartphones in terms of functionality and usability. 3DPrinterOS operating system is definitely a frontrunner amongst its peers, but this topic enters into the field of complex legal issues ranging from digital rights management to trademark, copyright and design laws. This chapter is by far one of the few to cover these topics comprehensively.

Today, e-technology and its legal regulation are often unbalanced. So-called e-regulation is left behind as "digital by default" is not really guided by overwhelming concepts that attempt to adjust the (soon)-to-be-true realities with the structural and systematic, sometimes idealistic, world of lawyers. At the same time, in few fields, the legislation is very detailed and does not reach the addressee, especially taking into account the digital divide in the world and in Europe. Seeking for principles, new social contract, *grundnorm*, utilitarism and trying to shape a somewhat conservative legal world with the digital world is a natural attempt to secure rule of law in the changing environment. This is what the current book is made for: the group of researchers, supporting e-development and innovation, remaining critical and analytical. We are trying to avoid the situation that was evident when the space law emerged. There is a certain similarity—unknown scope of issues to be regulated, fragmented and abstract legal acts (sometimes controversial in national level). Now, although the definition of outer space is still not uniformly agreed within international society, it has been concluded by Lafferranderie almost two decades ago that "the space law is no longer the sole prerogative of States".[31] For digital world, the whole development should also follow the ideal of "user-centricity" and the common values. We hope that the current book will wake up the spirit and mind of many, interested in the new era of regulation of e-technology.

[31] Lafferanderie (1997), p. 7.

References

Benkler Y (2002a) Intellectual property and the organization of information production. Int Rev Law Econ 22:81–107

Benkler Y (2002b) Coase's Penguin, or, Linux and the nature of the firm. Yale Law J 112(3)

Cockfield A, Pridmore J (2007) A synthetic theory of law and technology. Minn J Law Sci Technol 8(2):475–513

Gervassis NJ (2012) The dehumanisation of law: digital reflections. Eur J Law Technol 3(3)

Hoikkanen A, Bacigalupo M, Compano R, Lusoli W, Maghiros I (2010) New challenges and possible policy options for the regulation of electronic identity. J Int Commer Law Technol 5 (1):1–10

Kerikmäe T (2014) Regulating eTechnologies in the European Union. Normative realities and trends. Springer Verlag

Kerikmäe T, Dutt P (2014) Conceptualization of emerging legal framework of E-Regulation in the European Union. In: Kerikmäe T (ed) Regulating eTechnologies in the European Union. Normative realities and trends. Springer Verlag, pp 28–29

Lafferanderie G (1997) Introduction. In: Lafferaderie G, Crowther D (eds) Outlook on space law over the next 30 years. Kluwer Law International, p 7

Lips M (2010) Rethinking citizen – government relationships in the age of digital identity: insights from research. J Inf Polity 15(4):273–289

Martin K (2008) The rule of law: legality, teleology, sociology. In: Gianluigi P, Neil W (eds) Re-locating the rule of law. Hart Publishers, Oxford

Martin M (2014) Judging positivism. Hart Publishing, p 16

Pentland A (2008–2009) Reality mining of mobile communications: toward a new deal on data. In: Dutta S, Mia I (eds) The Global Information Technological Report 2008–2009. Mobility in a Networked World, p 79

Rudder C (2014) Dataclysm: Who We Are (When We Think No One's Looking). Crown Publishers, pp 235–237

Simmelmann C (2014) Legal principles in EU law as an expression of a European legal culture between unity and diversity. In: Helleringer G, Purnhagen K (eds) Towards a European legal culture. Nomos, p 321

Smedinghoff TJ (2012) Solving the legal challenges of trustworthy online identity. Comput Law Secur Rev 28:537

Steve S (2013) The CLSR-LSPI seminar on electronic identity: the global challenges. Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11–15, 2013. Tilleke & Gibbins International Ltd., Bangkok

"My Agent Will Not Let Me Talk to the General": Software Agents as a Tool Against Internet Scams

Alexander Norta, Katrin Nyman-Metcalf, Anis Ben Othman, and Addi Rull

Abstract This chapter takes as its basis an attempted so-called romance scam to evaluate a common modern communications phenomenon: the difficulty in evaluating human interaction online. Without having access to the kind of well-established, largely subconscious physical signals that we use to assess a situation in the offline world, extra vigilance is needed. The option of avoiding online communications is becoming increasingly unrealistic in personal as well as professional situations. The chapter examines whether, in addition to experience, training or personal characteristics, technology can help to avoid risks of misuse of personal data, fraud, extortion and so on.

We argue that the elements that arose suspicions in a sceptical and above-average vigilant Internet user can be generalised and instrumentalised through software agents. This would allow such agents to assist the user and raise the red flags where appropriate, even when the user herself may not detect the danger. Such software agents can be made required companions on cyber journeys, becoming an integral part of communication networks.

1 Introduction

The West African scammer who targeted a Professor of Law and Technology in his romantic scam may not have made the most appropriate choice for his purposes but inadvertently provided an excellent case study of a common modern communications phenomenon: the difficulty in evaluating human interaction online. The story of an attempted romance scam can provide a good illustration to a problem that is

A. Norta (✉) • A.B. Othman
Department of Informatics, Tallinn University of Technology, Akadeemia tee 15a, 12618 Tallinn, Estonia
e-mail: alex.norta.phd@ieee.org; anis.ben@gmail.com, http://www.smarpshare.com

K. Nyman-Metcalf • A. Rull
Tallinn Law School, Tallinn University of Technology, Akadeemia tee 3, 12618 Tallinn, Estonia
e-mail: katrin.nyman-metcalf@ttu.ee; addi.rull@ttu.ee

T. Kerikmäe, A. Rull (eds.), *The Future of Law and eTechnologies*,
DOI 10.1007/978-3-319-26896-5_2

more and more important in today's Internet-dependent society, where so much interaction is done virtually. Many of us who frequently use electronic communication are aware of the risks of misuse of our personal data that we may be exposed to through virtual communication, social networks and other websites. We also know that being present in the cyberworld is essential for professional and personal reasons. Thus, an assessment has to be made of the risks and benefits. A factor to consider in this context is whether the technology can help us: if IT can mitigate the risks that using this same technology causes.

In the technology environment, traditional social norms and inherent tools to evaluate trust cannot work. Trust is, however, an important commodity for all kinds of interactions. Trust exists in different forms and contexts, like social trust, cultural trust, professional trust and so on.[1] The creation of online trust is of key importance. There are different possibilities to create such trust if technology is properly applied to assist with this. If the problem of scams due to insufficient trust mechanisms is solved on a meta level, this will lead to a positive chain reaction with the whole industry benefitting. Authorities would not need to ask for information from ICT firms—which has negative privacy implications—since the problem would not reach that far.

A sceptical cyberspace user, with good skills and awareness of threats, navigates the treacherous waters of the cyberworld in a cautious and careful manner. He or she notices warning flags that are raised by strange behaviour even without meeting or seeing the person in real life. For a less-skilled person or any person in a setting in which one is less likely to be suspicious, it can be problematic to estimate risks. We are used to noticing what someone looks and sounds like, how they make eye contact, how they answer to our questions and so on. When we interact through a computer, we lack that direct contact and do not even know if the picture we are looking at is the person we are talking to. There is thus a need for different signals to make us wary, but these should be reasonable so as not to hinder all normal interaction in cyberspace. In this article, we examine how technology can help to provide such signals. More specifically, we examine the use of agent technology.[2]

With the increasing role of the Internet for social interaction, there has been for several years an interest in technology to help match people and prevent scams. However, many of the algorithms used to establish characteristics for matching (people with other people or people with goods and services) are rather crude and do not really "understand" people. They can quite easily be manipulated. Collaborative filtering is a popular method used both by, e.g., Netflix for movies and by different dating sites. Constant development refines the algorithms, but what is

[1] The description of trust is inspired by the concept of economic, social and cultural capital discussed by Bourdieu (1986), pp. 241–258. The authors do not attempt to define the concept of trust in this chapter.

[2] The notion "agent" was first used in 1973, Hewitt et al. (1973), pp. 234–245. It is used, e.g., to predict the perception of consumers before the launch of new consumer goods. Gowda (2008), pp. 246–251.

much more difficult is to use technology not just to filter contacts but also to help against the various threats that online interaction may entail.

Given the potential grave impact of scams in cyberspace, the matter is of major legal importance. However, the law has proven to be an ineffective tool in cyberspace. The jurisdictional issue is one major reason for this, as actions and their consequences can be in totally different parts of the world.[3] This means that even if some behaviour is illegal, the chances of taking effective action may be so small that in reality it is the same as if there were no legal consequences imposed at all. This does not mean that there is no room for law. If it is possible to use IT to combat harmful behaviour, the law may be needed to ensure that such IT tools are actually used, obligating relevant websites to apply them. However, if and how legal obligation is the best way to do this should be examined—self-regulation or a business interest from the websites may be a more effective method.[4] If a climate of self-regulation can be created so that the different sites that enable communication as a matter of cause apply certain functions to prevent fraud, this can repair the negative effects of the feeling of impunity that is created by the inefficiency of the traditional legal system.

The importance of privacy and data protection law is growing with the increased use of the Internet in all kinds of situations. The Internet of Things will only exacerbate this, as the many location-based services have already done. Social networks add to the complexity as they rely on the responsible behaviour of users but with few tools to encourage such behaviour. New approaches are needed, and technology can provide important assistance in this respect.

2 Setting the Scene

The case on which this study is based took place during about 10 days in November 2014. The initial contact was made on LinkedIn. Whether this was a conscious choice or just a coincidence is not clear. On the one hand, it appears less suitable to use a professional network rather than a dating one for a romance scam. On the other hand, it is normal to connect with strangers on professional networks and many users may be less vigilant, as they are not looking for any intensive personal interaction and only post such information that they want to be in the public sphere. In this case, the intended target indeed presumed that the scammer was a connection of a connection or someone she briefly met in some professional context. After having accepted the contact request, the supposed US General wrote and said he had looked for a contact with the same last name, found the profile and “been swept away by the beauty”. This was somewhat unexpected on LinkedIn but amusing more than anything else. However, it already raised a small warning flag because

[3] Chawki et al. (2015), pp. 7–9, 20.

[4] Examples related to Nigeria in Chawki et al. (2015), p. 143.