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

http://www.springer.com/978-3-319-26894-1

The Future of Law and eTechnologies
Kerikmäe, T.; Rull, A. (Eds.)
2016, XI, 233 p. 20 illus., 14 illus. in color., Hardcover
ISBN: 978-3-319-26894-1