Tanel Kerikmäe *Editor*

Regulating eTechnologies in the European Union

Normative Realities and Trends

Springer

Regulating eTechnologies in the European Union

Tanel Kerikmäe
Editor

Regulating eTechnologies in the European Union

Normative Realities and Trends

Springer

Editor
Tanel Kerikmäe
Tallinn Law School
Tallinn University of Technology
Tallinn
Estonia

ISBN 978-3-319-08116-8 ISBN 978-3-319-08117-5 (eBook)
DOI 10.1007/978-3-319-08117-5

Library of Congress Control Number: 2014942452

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

In March 2014, I had the opportunity to visit Tallinn Law School, Tallinn University of Technology, Estonia, as an invited guest lecturer.[1] While there, I was fortunate to meet with several of the authors of the chapters contained in this book. What became clear to me during my visit was that Tallinn Law School is *avant garde* in identifying and addressing legal issues relating ICT and its global applications in eGovernment and related fields. This book was written by a wide range of international Ph.D. students and young scholars who were supervised by Prof. Tanel Kerikmäe and Prof. Katrin Nyman-Metcalf, reflecting the global and integrative nature of the scholarship and academics of Tallinn Law School. This book reflects the authors' keen grasp of the complex technological and legal landscape, as well as their ability to clearly present real-world solutions.

Although Estonia only reestablished its independence in 1991, it has become a leader in eGovernance, and in particular eVoting. Because of its unique position as a relatively small country, establishing itself in the European Union and in the world digital market, it optimized its litheness to swiftly and effectively implement eGovernance technologies, together with associated legal and regulatory schema. Estonia truly is at the forefront of the development of eRegulation, eGovernment, and ePrivacy, in Europe. It has been holding eElections since 2005—the first in the world, and a model for other systems.

This volume of thoughtfully presented and exhaustively researched chapters present both optimistic views of the future of ICT-related technologies in government functionality, as well as often dystopic views of the hazards and potential dangers of the same technologies. The authors carefully lay the groundwork for their discussion (in the chapter entitled, "The Fragmented Securitization of Cyberthreats," Agnes Kasper gives one of the best accounts of the history of the internet, the world wide web, and cybercrime that I have yet encountered) and methodically reason through the benefits and potential concerns for each topic.

[1] Ms. Powers' visit was co-sponsored by the Center for International Legal Studies, Austria, and Tallinn Law School, Tallinn University of Technology, Estonia.

What is made clear by this body of work is that ICT and the Internet are rapidly becoming an integral part of worldwide regulation, governance, and business. While the U.S. is perceived as being at the technological forefront of emerging technologies, including e-technologies, the European Union and its more active members, in particular Estonia, is making significant headway into such areas.

This book is a must for anyone working in the legal field of cyberspace. Each chapter is worth contemplating and includes specific recommendations for legal practitioners willing to stand up to the challenges. Further research and regulations are required to enable eGovernance to achieve its multiple goals of accessibility, transparency, and increased participation, while at the same time preserving individual privacy and security. Potential uses as well as potential liability for ICT-based government systems are addressed in this book, and the authors offer specific proposals for ensuring that the rights and privileges afforded by the Internet are preserved without compromise.

Take your time to read these chapters not only for the substantive information, but also to generate new ideas about how to approach contemporary, cutting-edge issues in the Internet era. Then, use this information and these suggestions to make a difference in the world.

Elizabeth E. Powers
Attorney, Silicon Valley Law Group, Silicon Valley, CA, USA
Professor of Practice, Leavey School of Business,
Santa Clara University, CA, USA

Contents

Contributors

Johan Axhamn Faculty of Law, Stockholm University, Stockholm, Sweden

Dr. Mindaugas Bilius Law Faculty, Vytautas Magnus University, Kaunas, Lithuania

Pawan Kumar Dutt Tallinn University of Technology, Tallinn, Estonia; Estonian Business School, Tallinn, Estonia

Prof. Dr. Edita Gruodytė Law Faculty, Vytautas Magnus University, Kaunas, Lithuania

Kristi Joamets Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia

Agnes Kasper Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia

Prof. Dr. Tanel Kerikmäe Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia

Prof. Dr. Ülle Madise Institute of Constitutional and International Law, University of Tartu, Tartu, Estonia

Mari Männiko Law Firm LEXTAL, Tallinn, Estonia

Dr. Alexander Norta Faculty of Information Technology, Department of Informatics, Tallinn University of Technology, Tallinn, Estonia

Prof. Dr. Katrin Nyman-Metcalf Tallinn University of Technology, Tallinn, Estonia

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

Maria Claudia Solarte-Vasquez Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia

Dr. Ermo Täks Faculty of Information Technology, Department of Informatics, Tallinn University of Technology, Tallinn, Estonia

Priit Vinkel Ragnar Nurkse School of Innovation and Governance, Tallinn University of Technology, Tallinn, Estonia

Introduction: E-Regulation in the European Union—Normative Realities and Trends

Tanel Kerikmäe

Digital divide is the main obstacle in achieving the goal of eEurope. Multi-speed European Union (EU) becomes a reality when comparing Estonia and Nordic countries in general with some others. This fact was clearly reflected at the first international conference "Nordic Digital Agendas Day 2014" in Tallinn by the Estonian President, Toomas-Hendrik Ilves. The decisive factors and also key elements for success in Estonia have been psychological readiness and advanced technological basis. Being at the forefront has been based on the so-called "no-legacy policy", the rule that, as stated by Taavi Kotka, the Estonian government CIO requires that "no vital information system in Estonian public sector can be more than 13 years old". At the same time, the legal framework to legalize, licence and control technological advancements takes time. This is, most likely, another crucial problem of not having an effective eEurope today.

The EU has several advantages with being, at least in several regions, very much seen as an avant-garde. This is directly related to EU's perspectives in the competitive world as a wrestling scene with the economical giants such as the USA, China and India. E-services are usual parts of everyday life for many of us. When I spoke in Central Asia about my daily activities, such as mobile parking, prefilled tax declarations and other eGovernment services,[1] it was heard as a fairy tale by locals. The digital divide is getting bigger not only in the world but also within Europe. It seems that the technological advancements are also directly in interdependence with democracy where the inclusiveness and transparency are unavoidable. In North Korea, phones were banned in 2004, allowed now, but with no possibility to call abroad or use internet. Can you imagine this in Europe? One of the reasons of different appetite in seeking for new technologies is also derived from the level of economic welfare of the country or region. Also within Europe, the richer countries stress the need for welfare services and technology (going beyond eGovernment), while others are just discovering the magic of e-voting.

[1] See: https://www.eesti.ee/eng/services.

T. Kerikmäe (✉)
Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia
e-mail: tanel.kerikmae@ttu.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_1

Being the flagship in some areas is wonderful but the concern is how can we reach eEurope? The Estonian government is already advertising the successful eState to a new level, to ensure greater security related to data and information systems. There is an idea of the "Data Embassy", server rooms in the territories of partner states that would allow to create CloudEstonia: dispersing all data necessary to run Estonia all over the world (population register, business register, e-health system, judicial system, etc.). CloudEurope seems to be rather vision of the future.

However, there are very concrete steps taken by the EU to be eEurope which makes me believe that we are getting closer to democracy and rule of law through the new dimension. As the EU is often a cumbersome machinery, we cannot still underestimate relevance of regional cooperation. Recently, the prime ministers of Estonia and Finland signed (electronically) a memorandum of understanding in developing national data exchange services. However, one of the crucial questions is—how to familiarize eEurope for all its citizens? According to Yin-Jeou Wang from the Danish Agency for Digitization, the main approach should be "digital by default". He, while still calling them crazy ideas, suggests that eGovernance should be made mandatory for citizens and businesses in Europe. Further he states that we should make the whole European business lifecycle digital (starting with the public sector and invoicing). There is also the question of being more cost-effective: acting this way, it is expected to save up to 10 billion Euros per year. On the opposite side, Magnus Enzell from the Swedish government believes that citizens cannot be forced but rather should be included in the path of becoming eCitizens. He suggests the principle titled "digital when possible but personal when needed" led by the idea of "efficiency drive".

Alright, how would all of this influence the law and regulations? The Norwegian representative at the aforementioned conference, the high-level public official Jan Hjelle, believes that removing unnecessary regulations is one of the main purposes of eGovernance. Thus—new technologies should not make legal framework more complicated but rather vice versa! Is that possible when one takes a glance at the "wall of text" of soft measures and initiatives in the EU, comprising hundreds of thousands of pages. This is not even law that should be the next step! Many countries admit that so-far-made actions are risk-based innovations, there are no stable and sustainable platforms and there must be better risk assessment. I believe that legal regulation is the channel to balance or adjust market-based solutions with eCitizen's Europe.

Dear reader, right now you hold in your hand a compilation of articles (or maybe look at the screen when reading our eBook version) initiated by Tallinn Law School, Tallinn University of Technology. Just a few words about the contents. The first chapter maps the main dilemmas and principles for regulating eEnvironment in the EU and demonstrates how complex and far reaching the issue actually is. In the EU, endless piles of agendas, overlapping priorities and non-coherent terminology can astonish even cold-blooded lawyers. Yes, we are trying to follow the massive flow of innovative ideas and settle them to the "right" format of new legal space. The "wall of text" comprised of agendas, initiatives and strategies that are so-far-inevitable part of European bureaucracy is not always easy to grasp from the legal perspective. After making a concise overview of e-regulation

areas, existing legal basis and soft measures of the EU, I and my colleague Pawan Kumar Dutt propose that certain principles should always be taken into account with emphasis on the electronic identity of stakeholders, user-centricity, compliance of new regulations with rule of law and human rights (privacy) but also with interoperability that requires to alter the substance of e-regulation. Also, there is a need to recognize the dissimilar flavour of the new type of legislation accompanying rapidly developing technologies. Although controlled by the EU constitutional law, it should be rather led by clearly identified principles than remain purely norm-oriented. The big gap in digital divide among the EU Member States makes the idealistic "technologically neutral" regulation to be a mission impossible at least for a while. However, we believe that the methodological approach proposed in the first chapter would become a basis of future discussions when arbitrating problems of tailoring the e-regulation to the EU traditional legal universe.

One of the most well-known and a popular area assumed to be "thirsty" for new legislation is considered to be e-governance. Professor and Head of the Chair of Law and Technology at our law school, Katrin Nyman-Metcalf still, warns that there should not be separate legislation in addition to existing one as the parallel systems are creating risks rather than benefits. This would also be a way to diminish the influence of "luddities", (a term that comes from the age of industrial revolution and labelled English workers who destroyed the machinery that was believed to be a threat to their jobs). According to the author, the legal system should be able to absorb e-governance, so that it would not need to change totally. Prof. Ülle Madise from Tartu University and a colleague from Tallinn University of Technology are discussing another exciting area—namely electronic voting, on the basis of best practices and experiences of Estonia over six elections. The chapter includes a section of parliamentary debates, describes technical solutions and provides statistics to measure success of the elections.

Addi Rull from our law school and two talented colleagues from the Department of Informatics present a paper on dilemmas related to public databases and recommend "software-agent-enhanced" privacy protection policy. The authors open the world to technological solutions supporting public databases. The chapter concludes with the argument that the introduction of software agents "only partially resolves all problems related to traffic inspection" and suggests an introduction of intelligent software agents instead. Johan Axhamn from Lund University recognizes that the copyright issues on the internet are getting considerable and discusses recent cases from the European Court related to internet linking and meta search engines, focusing on the concept of "new public". A legal practitioner and Ph.D student Mari Männiko from the Estonian law firm Lextal analyses the frames for intermediary service providers' liability exceptions in the light of the e-commerce directive. A colleague from Tallinn Law School, Kristi Joamets, screens the EU digital development from the angle of free movement of civil status document and detects that civil status registration is, although used from ancient times, by its nature, dynamic and dependent on societal needs but also from digital tools available. Kristi believes that Estonian best practises in the field can be used as a sample all over the EU.

A promising legal scholar, Agnes Kasper, provides two chapters both linked to cybersecurity. The first chapter titled as "The Fragmented Securitization of Cyberthreats" focuses on theoretical assumptions, international cooperation and comparative analysis and concludes with categorizing legal responses to cyber threats and recognition for the need of "truly international regime in the future". The next chapter concentrates on emerging technologies in the field, namely Smart Grids and Big Data. The respective new EU directive is carefully screened and analysed. The issue is continued by representatives from our cooperation partner institution—Vytautas Magnus University Profs. Edita Gruodyté and Mindaugas Bilius. The Lithuanian scholars start with the fact that global cybercrime is the biggest underworld industry and provide critical comparative analysis of normative text, including the respective EU Directive. A good colleague and Ph.D student, Maria-Claudia Solarte Vasquez, concentrates on the possible strategies for cross-border consumer redressed in the EU, namely Alternative Dispute Resolution and its electronic format, Online Dispute Resolution. Again, as in several chapters, the principles are featured as a priority when introducing conflict management, i.e. values such as cooperation, empowerment, self-reliance, effectiveness and regulatory dynamism are the prerequisites for success. The book is completed with conceptual contribution on the very essence and associated risks of eDemocracy and eCitizen written by my colleague Pawan Kumar Dutt and the undersigned. The European and American approaches are opposed and compared. Also, as on previous pages of the book, the problem of accommodating the legal space with the new eLegal space is revisited. The metaphor-based model called "Trishanku effect" is figuratively used to explain the relation between reality and eReality.

"No-legacy principle", introduced in the beginning, is a gorgeous doctrine for sustainable development technology that would be good for the whole of Europe. But it also affects legal thinking. Lawyers are certainly far more conservative than technologists and visionaries. There is also a reason—one of their mission is to keep the society stable and secure for everyone who is loyal to the common values. These values, principles of law, should be recognized in eEurope. Let me end with another metaphor from the Estonian epic. Kalevide the leader of all Estonians was killed by his own sword, following the curse of the vengeful Finnish smith. In this case, Kalevide himself, misled and careless, asked to kill himself. The sword that was programmed with such a mystical and complicated password can be seen as mistreated technology, it led to the accident by which the legs of Kalevide were cut off (a symbol of stopping the progress) and the great hero died as he did not act wisely, did not consult anyone and remained egocentric until the inevitable end. Sad, he even did not seek the advice of lawyers!

Our hope is that beside the electronic divide, the discipline-based divide disappears with time and engineers, and IT gurus and lawyers are not seen as distinct tribes but as (potential) members of a friendly community that has clear vision, and is based on interoperability. As Hart (2012) supposed—we think and talk of justice according to law. So, which one prevails in case there is an evident conflict—conservative law or urgent need for technological advantages when both are seeking for better life with some stability and equal treatment? Which one

is more "real" if this question can be presented at all? By Josef Bleicher (1982), "technology is not a mere application of knowledge for a given purpose, and neither is it a neutral phenomenon; it is rather a process of realization, of making real something that, as the structure of nature is real but has remained hidden, undiscovered". We understand that a law should be able to meet the needs of developing world by its core principles. Can we, then, assume that *lex iniusta non est lex* maxime would be the case in new context, i.e. the positive law or even not sufficiently mature principles used-so-far should be reviewed. It is a fact that the industrial age changed the regulation. Alice Rawsthorn (2014), world famous design critic, concludes that the law needs, again, radical alterations in new digital age. However, the lawyers are the ones who cannot be ignored, but as my colleague, Prof. Nyman-Metcalf emphasizes that there is a need for continuous legal research. I believe that today, we have to make a significant effort to shape the legal space with the new technologies. The law, although it needs adjustment, remains to be a symbol for equal treatment, just and fair world. New generation of lawyers are those who know the past but understand the future.

I would bow down in front of all my colleagues and friends who contributed to the current book that is hoped to become a ship of the foundation in establishing eEurope in accordance with Rule of Law, legal certainty and justice. Special thanks to my colleague and friend Dr Archil Chochia who, being an eEditor, i.e. sending enormous amounts of emails to the authors reminding them their duties, encouraging them and myself, was an invaluable promoter of the book. I hope sincerely that Europe can lead this process and the current book, initiated by a small group of legal scholars from Tallinn University of Technology, can inspire as many as possible.

References

Bleicher, J. (1982), *The hermeneutic imagination: outline of a positive critique of scientism and sociology* (p. 13). London: Routlege & Kegan Paul.

Hart, H.L.A. (2012). *The Concept of Law* (p. 7). Oxford: Clarendon Press.

Intervjuu Alice Rawsthorn'iga (Tanel Veenre) at Müürileht, April 2014, p. 30.

Conceptualization of Emerging Legal Framework of E-Regulation in the European Union

Tanel Kerikmäe and Pawan Kumar Dutt

Abstract The article is focusing on emerging legal e-environment that comprises of legal acts regulating a field that can be administered by electronic means (eTechnology). The reasons behind various and sometimes overlapping and complex EU initiatives and agendas are analysed with the attempt to have an academic insight into the e-regulation and to establish a firm and more systematic approach for future studies in the field. The author maps the current situation, refers to the challenges related to e-regulation and discusses the need for characterising the e-legislation as a set of new type of rules. The stakeholders and e-identity, e-citizenship e.g. digital citizenship are discussed from the angle of e-regulation as a new qualitative level of EU law. It seems that today, some of the areas of e-regulation are well developed, and some of the areas still remain wishful thinking or are developing slowly in terms to be regulated electronically. The digitalization and e-regulation in terms of harmonization depend on the capacity of EU Member States in terms of electronic divide. Another challenge is the distinguishable nature of e-regulation normative status that should be taken in account when designing the new constitutional law and future for EU. As a conclusion and taking account of the interoperable nature of e-regulation, the author presents a list of policy stages that should be used when drafting and assessing EU level e-regulation.

T. Kerikmäe (✉) · P.K. Dutt
Tallinn University of Technology, Tallinn, Estonia
e-mail: tanel.kerikmae@ttu.ee

P.K. Dutt
e-mail: pawan.dutt@ttu.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_2

1 Preface: Competences of European Union in the Main Areas Related to eEurope

Digital Single Market: Articles 4(2)(a), 26, 27, 114 and 115 of the Treaty on the Functioning of the European Union (TFEU).

Digital agenda: Although Article 173 of the TFEU provides a legal basis for an EU industrial policy, the treaties do not contain any special provisions for ICT. However, the EU may undertake certain actions within the framework of sectoral and horizontal policies, such as competition policy (Articles 101–109 TFEU); trade policy (Articles 206–207 TFEU); trans-European networks (TENs) (Articles 170–172 TFEU); research and technological development, and space (Articles 179–190 TFEU); and the approximation of laws (Article 114 TFEU). Articles 28, 30, 34–35 (free movement of goods, including audio–visual products); Articles 45–66 (free movement of people, services and capital); Articles 65–166 (education, vocational training, youth and sport) and 167 (culture) TFEU are also key for a digital Europe.

Development and dissemination of ICT: The EU intends to promote the development and dissemination of new information and communication technologies (ICT), in accordance with Articles 179 to 180 of the TFEU.

Possible e-voting of European Parliament: TFEU art 223 (1)

2 "Wall of Text" Behind the E-Regulation: Initiatives and Agendas

The idea of building a digital knowledge-based information society was drafted into the *e*Europe action plan back in 1999, the main purpose of which was to make information technologies widespread across the EU, while promoting a socially cohesive, not divisive and integrated, not fragmented Union, or simply put—to bring Europe online.[1] The distinct features of the advantages of information society noticeable in all eEurope action plans as well as in the Digital Agenda stressed as endeavours for the EU can be seen as key features of why we can benefit from e-regulation[2] and digital market.[3]

---

[1] COM(1999) 687: Communication of 8 December 1999 on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000—eEurope—An information society for all.

[2] E-regulation, in terms of this article means the legal act regulating a field that can be administered by electronic means.

[3] Digital market is subdivided to many sub-areas. Beside e-invoicing, quite a recent initiative is e-procurement (strategy was elaborated only in 2012) which "refers to the use of electronic means by public sector organisations when buying supplies and services or when tendering public works".

The first *e*Europe initiative introduced in 2000 sought to promote information society and encouraged to start taking advantage of what it had to offer in many aspects for the advancement of higher employment, growth and productivity.[4] Europe was seen as having the potential, but it was not moving fast enough towards the digital age. The ten key objectives of the first action plan trying to improve the situation included among other things cheaper internet access, acceleration of e-commerce, e-participation for the disabled, healthcare online and government online. Given initiative, the first of this kind to promote the benefits of information society, aspired to carry "every citizen, home and school, every business and administration into the digital age and online," or to the "new economy", as the initiative referred to, while enhancing the digital literacy and promoting social inclusions as well as social cohesion.[5]

The *e*Europe action plan recognized that the uptake of internet usage in the United States at the time had led to direct creation of millions of new jobs and the endorsement of digital technologies to productivity growth and reduction in regulatory barriers. Even though the action plan saw Europe as a leading example in the mobile communications and digital TV, the uptake of the internet was relatively slow, and the public sector was not seen as enabling the development of online services at a pace it was expected. Therefore, first *e*Europe initiative sought to bring everyone online and to make the internet usage as commonplace as possible.

The importance of digital advantages was more emphasized in the succeeding initiative *e*Europe 2002,[6] which, along with the upcoming *e*Europe initiatives, formed an integral part of the Lisbon strategy's very ambitious plan "to become the most competitive and dynamic knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion."[7] In order to put the aforementioned ambition into practice, a comprehensive eEurope action plan was needed, which would combine the *e*Europe initiative, the communication *strategies for jobs in the information society* with coordination based on benchmarking the national initiatives. More concisely put, the *e*Europe 2002 focused on creation of a knowledge economy, an information society for all, so as to increase EU's competitiveness, while as in the first initiative, the improvement of the employment situation and greater social cohesion were mentioned as crucial to the success of the knowledge-driven economy. *e*Europe 2002 further emphasized that the initiatives' goals would go beyond Europe's borders and contribute to the growth of a strong and proactive global policy in the information society.

---

[4] To become familiar with the history of European Commission actions since 1980s in promoting a stimulation of the public sector to make its information available for re-use, see: Janssen and Dumortier (2003).

[5] See COM (1999) 687: *e*Europe.

[6] COM (2001) 140: Commission Communication of 13 March 2001 on eEurope 2002: Impact and Priorities A communication to the Spring European Council in Stockholm, 23–24 March 2001.

[7] Lisbon European Council 23 and 24 March 2000. Presidency Conclusions. Accessible: http://www.europarl.europa.eu/summits/lis1_en.htm.

The *e*Europe 2002 aimed at developing internet connectivity throughout Europe and set three key objectives to be achieved by the end of the year 2002: firstly, to promote cheaper, faster and secure internet; secondly, to invest in people and skills; and third, to stimulate the use of internet. Since "closing the digital divide"[8] between the Member States in terms of their digital development level was seen as one of the objectives, the initiative sought to develop a more equitable information society, providing similar development possibilities to all Member States. One obstacle that had emerged on the implementation of the goals introduced with *e*Europe was the fact that mere fragment of the actual potential of digital technologies was used even after the adoption of the first *e*Europe initiative.[9] It was seen that the much needed lead of public sector and politicians in providing guidance in the field was deficient. Therefore, the new initiative also emphasized the importance of the public sector to set an example in the required adoption of new technologies, which had been mentioned as one of the causes of adoption in the previous action plan. Even though the *e*Europe 2002 Impact and Priorities Communication mentioned notable progresses in number of internet users and increase in the adaption of digital technologies, the efficiency gains of adapting to technology were seen as minimal, since the potential exploited was trivial, as in 2000, only 25 % of internet users had *accessed* government websites, 10 % had submitted any forms via public websites and 5 % did online shopping on a regular basis; thus the need to build up consumer confidence was seen.[10]

Accordingly, even though only half of workers were using computers in their workplace and less than 30 % of EU households were connected to the internet in 2000,[11] these numbers were on the rise and the focus shifted to the integration of internet to citizens' everyday lives in order to increase the computer literacy in general. The *e*Europe 2002 initiative called the EU institutions and national public administrations to make an effort to embrace the benefits the information technology provides in order to create professional services for European citizens and business and to turn the use of internet-based services into an inescapable routine. The Commission further recommended to include activities that would encourage access to such services in every regional development plan. Such actions were deemed to be important as they were seen as both, tools for improving the transparency of the public administration, as well as tools aiming to engage the citizens in the digitalization process.[12]

Further, certain priority areas were revised within the *e*Europe 2002 framework. These were provided by the Stockholm European Council in order to strengthen

---

[8] The digital divide is a concept generally defined as an inequality in access and use of information and communication technologies (ICTs) between individuals, households, businesses, geographic areas and countries, and reflects a number of differences between and within countries (OECD 2001).

[9] See *e*Europe 2002. Impact and priorities. A communication to the spring European Council in Stockholm, 23–24 March 2001. COM (2001) 140 final, 13 March 2001. COM (2001).

[10] Ibid.

[11] Ibid.

[12] Ibid.

the key activities of *e*Europe and they were formed taking into account the already established *e*Europe 2002 strategy paper, discussions in Council Working Group on Information Society Services and in cooperation with Member States as well as the Presidency.[13] These priority areas were: adoption of regulatory framework for electronic communications, high-speed infrastructure (networks), e-Learning and e-Working skills (training of teachers, adapting school curricula, etc.), e-Commerce (implementation of the electronic signature and e-commerce Directives), e-inclusions, e-Government,[14] Secure networks and mobile communications.[15]

The next initiative, *e*Europe 2005,[16] was responsible for ensuring that information society applications and services would have increased participation by newly skilled citizens and businesses that were brought online as a result of *e*Europe 2002. The *e*Europe 2005 initiative's general objectives were endorsed by Seville European Council, where it was noted that the 2005 action plan would be "an important contribution to the Union's efforts to bring about a competitive, knowledge-based economy."[17] Thus, as it still formed an essential part of the Lisbon strategy, the new initiative's overall aim was to acquire a positive impact on growth, productivity, employment and social cohesion by obtaining increased connectivity with upgraded access possibilities to higher quality services by a maximum number of citizens and businesses based on a secured broadband infrastructure.

Since the former initiative had had an objective to provide certain basic administrative services via internet, and by the third quarter of 2002, all Member States had been able to transfer at least some of the services online, it might be said that the main objective of *e*Europe 2002 was achieved.[18] The new initiative hence stressed how the information society was to be seen as having gradually growing potential owing to new services, applications and other digital content accessible with multiplatform applications that were to open up economic and social opportunities improving market's productivity and thus society's quality of life if exploited fully. In addition to using a PC for access, *e*Europe 2005 proposed that other mediums, such as digital TV, third generation mobile telecommunications technology connections (3G) would make the usage of information and communication tools more attractive, especially when they were accessible via high-speed, continuous and secure broadband internet access.

---

[13] Ibid.

[14] The spelling of different e-solutions varies within different initiatives and strategy papers.

[15] See COM (2001), *e*Europe 2002, Impact and Priorities.

[16] COM(2002) 263: Communication of 28 May 2002 from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions—The eEurope 2005 action plan: an information society for everyone.

[17] See Seville European Council Presidency Conclusions. Accessed 21 December 2013. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/72638.pdf.

[18] See *e*Europe 2002 Final Report. Communication of 11 February 2003 from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions eEurope 2002 Final Report [COM(2003) 66 final Not published in the Official Journal].

Overall, *e*Europe 2005 brought more focused ideas to the information society, as it pursued to provide modern online public services, such as actions on e-Government, e-Health, e-Learning and e-Business by the end of 2005. The initiative had two groups of actions. The first aimed at providing services, applications and content to the consumer, these included public services as well as e-Business services; while the second focus was on the broadband infrastructure, enabling of which was seen as a task for the private sector (to whom the community was to secure flexible legislative framework); moreover, as the number of internet users was still on rapid increase, yet the action plan saw the consumer as still somewhat suspicious towards the privacy and security matters, the enhancement of security was another focus point under the second group of actions. Similarly, to previous initiatives, *e*Europe 2005 set forth certain key targets: connecting public administrations, schools and health care to broadband; providing interactive public services on multiple platforms, providing online health services; removal of obstacles to the deployment of broadband networks, review of legislation affecting e-Business; as well as creation of a Cyber Security Task Force. *e*Europe 2005 also strived to bring Member States to work with the commission for the purpose of achieving the *e*Europe objectives as they were the same for all members; and this with a purpose of creating a commonly coordinated approach to information society issues, where the exchanging of experience, both from success and failures, would be promoted. The latter actions were combined under a MODINIS programme, with a purpose of analysing the effects of the information society to economic and societal aspects, to disseminate (good) practices, promote synergy between Member States and improvement of network and information security.[19]

As with *e*Europe 2002, reviews of the *e*Europe 2005 goals[20] proved that the ambitions had been rather achievable. Among other things, the sought after expansion of broadband connections was a success as the number of connections almost doubled between 2002 and 2003; the initiative had set up an efficacious structure for creating a dialogue between countries at different level of the information society; moreover, certain new services, such as e-Government and e-Health enabled the Member States to work towards unified goals set by the initiative for common more successful market of digital services. Nevertheless, the expected private investment was not as high as expected. What is more, even though there was an increase in online purchasing and selling, majority of citizens were still afraid to

[19] See Decision 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 adopting a multiannual programme (2003–2005) for the monitoring of the eEurope 2005 action plan, dissemination of good practices and the improvement of network and information security (MODINIS).

[20] See COM(2004) 108: Commission communication of 18 February 2004 “eEurope 2005 mid-term review”.; and COM (2009) 432: Communication from the Commission of 21 August 2009 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Final Evaluation of the eEurope 2005 Action Plan and of the multiannual programme (2003–2006) for the monitoring of eEurope 2005 Action Plan, dissemination of good practices and the improvement of network and information security (Modinis) (Respectively the mid-term review and the review of *e*Europe 2005 Action plan).

bargain online as the internet was not seen as providing secure basis for financial transactions. The MODINIS programme also received a positive assessment, although certain studies under the programme did not have the expected impact as they were not sufficiently distributed nor clear enough.[21]

Following the *e*Europe initiatives, as the midterm review of the Lisbon strategy had revealed that there had been certain shortcomings in the expected results, the European Commission introduced a new, more concisely drawn strategic framework, "i2010—A European Information Society for growth and employment,"[22] which formed a part of the re-launched Lisbon strategy that had special focus on creation of a "fully inclusive information society based on widespread use of information and communication technologies (ICTs) in public services, SMEs and households."[23] Since the leap to digital information society had increased swiftly over the preceding years, bringing traditional content—movies, music and other media services—to digital formats, and had encouraged the development of new digital services compatible with multiplatform devices, the "smarter, smaller, safer, faster, always connected and easier to use," ICT was to be seen as a means of expected inclusion and digital reality pursued by the e-initiatives.[24]

For that reason, as the digital information society had become a more tangible notion, the technological changes called for proactive policies for the Member States, which would foster the policy convergence for a more common set of regulatory framework in order to enhance the open and competitive political economy, which would aim to achieve the revised Lisbon Strategy goals. Herewith, the i2010 initiative focused on ICT research and innovation, content industry development, the security of networks and information, as well as convergence and interoperability in order to establish a seamless information area via three priorities. Firstly, in order to achieve an open and competitive internal market without regulatory obstacles for information society and media, the *Single European Information Space* needed to be established, as it was already seen how intensely the ICT affected working conditions and social benefits of citizens and businesses: the i2010 brought faster broadband, promotion of legal and economic certainty to encourage new services and online content, interoperable services with multiplatform access with minimized security risks. Secondly, for the promotion of growth and continuous delivery of new jobs in the information economy, it was seen that

[21] See COM (2009) 432: Review of *e*Europe 2005 Action plan. Accessed 10 December 2013. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0432:FIN:EN:PDF.

[22] COM(2005) 229: Communication from the Commission of 1 June 2005 to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions entitled "i2010—A European Information Society for growth and employment".

[23] Presidency conclusions of the Brussels European Council (2005): http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/84335.pdf.

[24] See COM(2005) 229: Communication from the Commission of 1 June 2005 to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions entitled "i2010—A European Information Society for growth and employment.".

ICT needed more efficient *Innovation and Investment*; and thirdly, again to stimulate growth and employment issues, but in a way consistent with sustainable development, better public services and quality of life, an *Inclusive European Information Society* was to be created with ICT-enabled public services accessible by all and benefitting all.[25]

The Commission's communication on the main achievements of the i2010 indicates that perhaps i2010 was the success story according to the previously set goals—by the end of the period, all Member States had ICT policies that were seen as contributors to national growth and employment sought by the initiative, the number of people online on a daily basis had increased to 56 % by 2008; Europe saw itself as the world leader in broadband internet, market penetration for mobile phones was 119 % in 2009; moreover, the 20 benchmarked public services available online had become more mainstream and approximately 70 % of the EU businesses used e-Government services. Nevertheless, even though the goals were achieved to certain extent, the rest of the world was still moving faster, Asia was seen as the leader in innovative wireless broadband, the USA had moved on to social networking and new interactive web, while EU was still trying to bring the rest 44 % of people online,[26]—this data indicated that the ambitious Lisbon objectives were not achieved to extent expected.

As the Lisbon Strategy and its revision were depleted by the end of 2010, Europe 2020 with its newly formed Digital Agenda (DAE)[27] was introduced in May 2010, and it forms one of seven flagship initiatives contributing to the EU's smart, sustainable and inclusive growth. Given agenda, similarly to previous initiatives, has the general purpose of improving the economic situation and providing for sustainable market by delivering economic and social benefits and launching interoperable applications; however, the new digital society, based on technological developments, is expected to run on fast and ultra fast internet which would help to exploit ICT-enabled possibilities at EU and national levels. As the digital technologies have improved significantly and, according to the DAE, the digital economy is growing seven times faster than the rest of the economy, today's citizens and businesses ought to benefit from smart sustainable and inclusive growth more than ever before.

As a part of the Europe 2020 flagships, the Digital Agenda consists of 101 actions, which are divided into 7 pillars and the agenda has altogether 13 specific goals, such as having 50 % of the population by online, 20 % buying online cross-

---

[25] See COM (2005).

[26] See COM(2009) 390: Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions—Europe's Digital Competitiveness Report: main achievements of the i2010 strategy 2005–2009. Accessed 20 December 2013. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0390:FIN:EN:PDF.

[27] COM(2010) 245: Communication from the Commission of 19 May 2010 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—A Digital Agenda for Europe. Accessed 25 November 2013. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:HTML.

border, 50 % using e-Government services and to have 75 % of the population online by 2015.[28] The DAE sets forth that the impact behind services moving to an online world, can, amongst other aspects, contribute to easier access to public services, better health care, cleaner environment and better environment for businesses, while such aspects will increase the overall quality of life. However, certain obstacles are hindering the full implementation of the DAE: for one thing, in order to create a platform for common set of e-regulation, a digital single market must be achieved; yet, the EU has fragmented national digital markets moving at their own pace towards digitalization without noteworthy interoperability. Moreover, with over 99.9 % of homes having access to broadband of varying quality, the number of people online is bigger than ever before, yet 22 % of European citizens had never used the internet by 2012.[29] Throughout the *e*Europe and i2010 strategies, it was emphasized that as the full potential of the new technologies would be exploited, the sustainable and inclusive growth would be more tangible; nevertheless, even though the digital content is available in all Member States, regulatory barriers limit the free flow of e-services. What is more, the digital market might be said to face even more threats, such as the security questions were posed before, they are even more acute today, as malicious software distribution and online fraud has increased with the increase in use of online services. Hence, the aim of achieving a digital single market without regulatory barriers will not only be crucial for the success of the Digital Agenda, but is the only way of not failing that Europe 2020 initiative.

Overall, the key aspect of the e-regulation is information society with maximized utilization of online services for all, as introduced by eEurope in 1999 and still ongoing with the Digital Agenda. Since the 15-year-old *e*Europe can be marked as the threshold of today's Digital Agenda forming part of the Europe 2020 with the objective of exploiting ICT in order to enable the progress of the digital single market offering economic and social benefits to both citizens and businesses for smart and sustainable growth in a borderless digital environment, it seems that certain key aspects need to be reconsidered whether similar goals need to be set with each initiative without any of them proving to be thoroughly successful—today, we have most of the Europe online, yet we still do not have a socially inclusive and fully integrated digital market. The initiatives and agendas despite of good intentions behind have created a "wall of text" for those who should get benefited, also for lawyers who should try to predict which part of the "soft law" is relevant in interpreting *de lege lata* and *de lege ferenda*.

---

[28] Digital Agenda for Europe. A Europe 2020 Initiative. Our Goals. Accessed 25 November 2013. http://ec.europa.eu/digital-agenda/en/our-goals.

[29] Digital Single Market Online Content 2013 Data. *Internet and Skills.* Accessed 25 November 2013. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/DAE%20SCOREBOARD%202013%20-%203-INTERNET%20USE%20AND%20SKILLS.pdf Ecommerce Europe. Available at: http://www.ecommerce-europe.eu/home.

3 Unshaped Legal Framework of E-Regulation in Europe

There are several fields that the European Union wants to and ought to regulate by electronic means. There are countless strategies and legal acts that would enable the creation of electronic recognition systems, e-services and e-registers across Europe. The justification or appetence is usually deriving from the concept of digital market. As de Andrade puts it, "Electronic Identity (eID) is the backbone of modern communications and transactions in the digital world, as well as a key driver for the growth of the EU economy and the completion of the digital single market."[30] It is important to emphasize that the EU does have the necessary technology to fulfil the visions of e-regulation; however, it must be noted that the legal space is not ready to support these initiatives. Hence, the following section concentrates on legal challenges and maps the current situation in the field of electronic identity for Europe, as well as emphasizes the common principles related to legal regulation of electronic identity and focuses on the problems in differentiated regulation fields so as to shed some light on those challenges.

The idea of effective e-regulation is not a straightforward goal due to numerous reasons. To begin with, there are many fields that the EU wants to regulate electronically and even though some of those fields can be seen as interlinked, some are more advanced in terms of electronic regulation, while others are simply rather ambitious visions. The capacity and experience of Member States varies noticeably from country to country; for instance, the ID legal framework is a part of citizens' everyday life in some countries, whereas other countries remain unaware of the possibilities that the application of e-services can provide[31]; therefore it is still quite disputable how the Member States who have different expectations, different administration systems that do not overlap with EU visions of e-governance, could be able to focus on a unified European eID framework. Moreover, it is very difficult to systematize the e-regulation field because of different viewpoints: some authors propose an electronic identity to be the keyword for Europe [e-identification and e-authentication, e-signatures, a full scale common European electronic Identity Management (eIDM) system, European Information Society (EIS)][32]; others emphasize the digital single market as the platform for further electronic regulation; and some authors are stressing that the basis of "e-revolution" can only be achieved with supporting the technological operational systems. The challenge has been and will remain that of Member States' governments giving away certain control over their national high-technology markets in order to be competitive in a globalized digital economy as a single market.[33] However, the one aspect that all authors and strategists agree upon is the importance of competitiveness for Europe in the global economy.

---

[30] De Andrade (2013).

[31] There can be very specific problems that are derived from the specific domestic legal system, such as the field of public procurement. See for example, Poremska (2010, 2012).

[32] Please see 2015: A connected and diversified Europe. eIDM Vision Paper. Accessed 27 November 2013. http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR513.pdf.

[33] Shahin and Finger (2009).

Another challenge in seeing a bright future for the EU in e-regulation is the multilevel construction of it. Schartum calls it "interoperability,"[34] which means that e-regulation system consists of four different layers: technological, semantic, organizational, legal and political. A source of law has been a qualitative label for the legal norm for contemporary lawyers over the centuries. By Lamond, "[c]ontrary to Austin's conception of law, where all laws necessarily had one source (the sovereign), there can be separate sources."[35] One may claim that, first, the sovereign in the EU (e) decision-making process should be more widely defined; and secondly, these differentiated layers oppose the traditional law making. Schartum[36] brings forth the core problem which is the identification of the source of e-legal norm. It can be at least presumed that the relative slowness of achieving the e-EU is caused by the fact that many of the norms are rather inspired by other layers than the ones related to legal traditions. What is the *grundnorm* or legal principle that forms the basis for the creation of e-regulation? As there is no clear answer, one may see the potential threat for the so far relatively well-functioning and efficient legal system, at least from the point of view of lawyers. The problems are seen especially in the field of ICT sector where the lack of legal certainty is caused by fact that the rules are very case-specific[37] and do not always form the sustainable set of EU jurisprudence as a part of legal space.

One may claim that perhaps it is time for lawyers to leave the ivory tower and give up the traditional legal process of creating the legal norm. However, the legal definitions are traditionally different from technological and semantic notions. That is why, interdisciplinary thinking would become very serious challenge for the lawyers who see a "core characteristic of Europe's integration project"[38] as reliance of law. However, presuming that e-revolution in the EU legal space is motivated by integrationist objectives, the paradigm suggested by Joerges and Weimer i.e. "a shift away from hierarchical regulation" preferring "soft, flexible, decentralized, and experimental regulatory techniques,"[39] should fit the challenges of EU e-regulation. The sanctity of legal norms should probably be revised when stepping to the new area of e-regulation. Dynamic, deliberative and inclusive process of norm-making does not mean denying the rule of law.[40] As the EU constitutional law is in transitional period, one of the elements in building up the new constitution for Europe (being federalist or not) should take into account the special characteristics of e-regulation. De Visser, trying to find the common features

---

[34] Schartum (2011).

[35] Lamond (2013).

[36] Legal definitions and semantic interoperability in electronic government.

[37] See presentation of Inge Graef at Interdisciplinary Centre for Law and ICT (ICRI) "Achieving interoperability in the absence of standards: a new policy under the Digital Agenda?" Accessed 25 November 2013. http://www.eurocpr.org/data/2013/Graef.pdf.

[38] Joerges and Weimer (2014).

[39] Ibid, p. 303.

[40] Kerikmäe (2010).

of constitutional review in Europe, refers to Hoffman-Rien, a former judge of the German *Bundesverfashungsgericht*, who said, "[a] constitution is a nation's autobiography,"[41] constitutional conformity of the EU would be closer to perfect when taking into account the special characteristics of e-regulation. Therefore, the e-regulation should, despite of its innovative nature and despite of the fact that the efficiency of establishing supportive legal framework for e-regulation is an unavoidable tool to win the race of competitiveness with other big economies in the world, clearly be linked with the constitutional law of the European Union.

3.1 Electronic Identity for Stakeholders

In addition to the abovementioned, one of the crucial problems is related to the variety of stakeholders seeking to gain certain control in the e-regulation field (citizens, businessmen, service providers, data processors, Member States' governments, the EU itself), since it brings an obstacle for having a homogeneous view on the EU's electronic future due to the growing concern over privacy, which can be undermined by large number of stakeholders. Moreover, the structure of EU legal norms does not facilitate having an efficient e-regulation framework for the benefit of the consumer. For that purpose, a crucial principle emphasized by several authors is a rather recent phenomenon of user-centricity.[42] This principle of prioritising the end-user of the services is not clearly visible as different strategies of the EU rather emphasize the dimensions of e-regulation (research development, standards) that are not sufficiently linked with the consumer of the services.

E-governance is gradually gaining more popularity. Theorists of several disciplines are providing new concepts comparing different models and, in conclusion, strengthening the e-identity for governments, institutions and corporate enterprises. Identity assurance providers who have agreed upon the concept of e-governance are the "largest controllers of people's identity—provision of credentials, identification, authentication, and authorization."[43] Hoikkanen, Bacigalupo, etc., are proposing e-Identity as a new legal category. They argue that the new type of e-identity should not be state-allocated, but rather a user-chosen identity. They claim that there must be a right to identity which is closely related to anonymity, pseudonymity and the right not to be misrepresented (privacy). Identity management systems should avoid collusive behaviours between different service providers when dealing with citizens' personal data. The authors try to define main elements of the e-identity (a capital asset, public good, a cost) and foresee the main problem not in creating a legal framework, but rather making the citizens to be informed of their rights and obligations. From a legal point of view, the authors

[41] De Visser (2014).

[42] De Andrade (2013).

[43] Hoikkanen et al. (2010).

also provide a clear understanding of dimensions or levels, or categories, for which the e-identity can be used and determine such regulative levels. For example, they argue that soft law and alternative regulatory mechanisms could be extensively used to quickly achieve results and address the most evident legal gaps, while higher-impact solutions are developed.[44] This applies mostly to the individual self-determination as the variety of separable fields of activities cannot be exhaustively listed. The coherency and continuity of legal acts would rather be a task for Member States and the EU institutions in creating a digital single market with all of its deliverances.

One of the areas of promoting e-citizenship of the EU is electronic voting. This is also a field for teleological interpretation of existing constitutional law of EU. Kuzelewska and Kraśnica refer that the possible e-voting of the European Parliament can be covered by TFEU art 223 (1), which, beside of the "uniform procedure," states that the basis of the election system could also be built on "principles common to all Member States".[45] They are convinced that the e-voting (especially I-voting—which is internet-mediated version of e-voting) "seems to be the easiest way to unify various voting systems to the European Parliament". Even if the internet voting can have several models,[46] there are certain principles that should be guaranteed from the perspective of protecting the e-identification of any member of e-electorate. As explained by Radek and Petr,[47] the following principles must always be applied:

1. Participation in the voting process is granted only for registered voters.
2. Each voter has to vote only once.
3. Each voter has to vote personally.
4. Security and anonymity of voters and voting.
5. Security for the electronic ballot box.[48]

This discussion leads to the solution for solving the e-regulation puzzle using the principles rather than rigid legal norms as the e-identification does not concern only the EU citizens but also the migrants to EU. The issue here concerns the democratic control of information systems and the weak legal position of immigrants.[49] Besters and Brom believe that 'European migration policy is turned into a kind of "test lab" for new technologies'[50]; as it directly relates to identity of person (biometric identification, travel surveillance, and other legitimization methods of a person who wants to cross the border). Possibly this field of regulation is an outstanding example of the vagueness of the rights and obligations of an individual when

[44] Ibid, p. 7.

[45] Kuzelewska and Krasnicka (2013).

[46] Ibid.

[47] Šilhavy and Šilhavy (2008).

[48] Ibid, p. 141.

[49] Besters and Brom (2010).

[50] Ibid, p. 456.

standing alone in the middle of e-regulation. It may also happen in other regulation fields that the EU creates systems affordable and efficient to the EU itself, but the legal guidelines for the individuals are left unexplained. Therefore, the proud statement of Rossi from more than 5 years ago "[i]n the current stage of European integration, the question of what principles are really fundamental in the EU becomes increasingly important,"[51] should be taken very seriously in the new context. Legal certainty should not hide away even if the decision-making process is deviating from the traditional forms and the interdisciplinarity as a basis of composing the norm is more evident. As Howes warned us more than a decade ago: "There will be an expectation in the postmodern cyber-village that legal knowledge will be accessible, and that it will be both communal and personal, or interactive."[52] As in oral societies, the emphasis will be on conflict resolution that adapts standard laws to existing circumstances and norms.

One of the new terms in use is "digital citizenship" and an important element of this is Digital Access, or full electronic participation in society which can be identified with following ideas: "[t]echnology users need to be aware that not everyone has the same opportunities when it comes to technology. Working towards equal digital rights and supporting electronic access is the starting point of digital citizenship. Digital exclusion makes it difficult to grow as a society increasingly using these tools. Helping to provide and expand access to technology should be goal of all digital citizens. Users need to keep in mind that there are some that may have limited access, so other resources may need to be provided. To become productive citizens, we need to be committed to make sure that no one is denied digital access".[53] Besides of citizens' initiatives, there are also initiatives of business circles—one remarkable example may be e-commerce Europe that was founded by leading national e-commerce associations across Europe. E-commerce Europe represents 4000 + companies selling products and/or services online to consumers in Europe.[54] According to its president, François Momboisse, "[l]ast year, the e-commerce industry in Europe had a total turnover of € 358 billion and it was one of the few industries that grew with double digits."[55]

One of the sample fields in e-identification is certainly e-signature. Graux[56] presents a vision of IAS (Internet Authentication Service) in Europe, calling it a not-so-modest proposal. He proposes a new structure for e-authentication directive and envisages technical elements that should be adopted separately from other legal instruments. The author brings us an essential example that in fact relates to the

---

[51] Rossi (2008).

[52] Howes (2001).

[53] See Nine Themes of Digital Citizenship. Accessed 10 January 2014. http://digitalcitizenship.net/Nine_Elements.html.

[54] See Ecommerce Europe. Accessed 15 January 2014. http://www.ecommerce-europe.eu/home .

[55] See Ecommerce Europe. Accessed 15 January 2014. http://www.ecommerce-europe.eu/press/press-release-ecommerce-europe-proposes-a-one-stop-shop-for-policy-coordination.

[56] Graux (2013).

nature of e-regulation as a whole. It is a rapid development of technologies as Graux explains, despite attempts to identify e-authentication services within the directive, new services that derive from even more contemporary technologies may create "unforeseen complexities."[57] As in this case, also other fields of e-regulation are actually facing the same challenges. There is a choice whether to have an endless flow of new legal acts, taking into account every new technological possibility, or to rely on principles and formulate new type of legal rules that would allow certain undetermined nature of the legal act which in practice means that the so-called basic acts can be supplemented with decisions widening the scope of the legal act so that the initial goal of the act would not be damaged. It is a hard task and needs a shift in mentality that must be reflected by the strategies of e-regulation of the European Union.

3.2 Digital Divide and Other Challenges: How to Proceed?

The issue raised by Venturelli almost two decades ago—on "how the EU ought to approach the design of the information society: the liberal market model, the public service model, and the nationalist or culturalist model,"[58] is still topical. Further studies on classification of the e-regulation areas by variables such as (a) institutional space of activity (jurisdiction of General Directorates, in case of the EU), (b) identification of end-users, (c) legal bindingness and balance between *de lege lata* and *de lege ferenda,* may be rather helpful in categorising of the e-regulation. What we are missing today, is a systematic approach in the context of legal certainty and rule of law despite the fact that the visions and technologies are born before the norm regulating, or planning to regulate these. The current contribution is just a preliminary attempt to map the current situation, refer to the challenges related to e-regulation and discuss the need for characterising the e-legislation as set of new type of rules.

How should we treat the emerging need for e-regulation? Is it just a new quality in decision-making and implementation process? Is it a revolution in legislative process that also influences previously existing laws and regulations? Is it a chance to strengthen the supranational character of the EU, widen the scope of the EU competences, using the minimum standard principle—such as successful e-voting in Estonia would become a basis for European Parliament e-voting system? A solution-oriented approach would be the encouraging of "technology-free regulation"[59] that is free from detailed references to technology and is based on legal principles. It seems that *de lege lata* deriving from the Lisbon and post-Lisbon developments is not unanimous in that regard and several legal acts tend to be technology minded.

---

[57] Ibid, pp. 114–115.

[58] See Shalini Venturelli, "Inventing E-Regulation in the US, EU and East Asia: Conflicting Social Visions of the Internet & the Information Society" at Presented at TPRC 2001 29th Research Conference on Information, Communication and Internet Policy Alexandria, Virginia, October 27–29.

[59] Lusoli and Maghiros Ioannis (2009).

The epopeya of pre-Lisbon and post-Lisbon legal and political development has been criticized, and several authors are not convinced that the *de lege lata* gives us the best ground for a balanced and innovative European Union. As, for example, stated by Piotr Tosiek, "[t]he Treaty of Lisbon is after all the agreement relating to almost every sphere of activity of the European Union. In fact the construction of the European Union and its foundations are not reformed in a revolutionary way. This is only a short step towards identification of the *finalité politique*."[60] Thus, the first question from the angle of legal system per se should be—if the EU would use the e-regulation as a challenge to reform the whole system; or, the e-regulation remains a vision with "multi-speed" character, i.e. some of the areas are well developed, some of the areas remain wishful thinking and some of the areas are new and may have a chance to be regulated electronically. It would be useful to analyse e-regulation from the perspective provided by Alexander H Türk, who discusses the law-making processes of the post-Lisbon EU.[61] As the e-regulation, by nature is dependent on digital divide of Member States, the question is whether all acts that fall into the category of e-regulation can constitute "legislative acts" rather than "regulatory acts". The difference is that "legislative acts" are on the top of EU acts by their hierarchical status as the "regulatory acts" are rather non-legislative acts with general application. It would be the question of the efficiency of the eEurope, which way is the best to go. Also, what kind of procedure should be preferred here e.g. if the open method of coordination should be most effective in cases where the beneficiaries are the citizens and the society as this method is usually used when dealing with social policies, including information society. Another type of goals may be a basis to prefer EU agencies or even private actors as the e-regulation is also strongly related to the EU institutional development (e-governance) and business stakeholders (e-services).

Furthermore, the legal sanctity of e-regulation can be seen improper and "old-fashioned". As Stephen Laws states: "…legislative drafters have to do their job in the knowledge that politics cannot be eliminated from the legislative process, but need to be reconciled with the things required of the legal output."[62] He also points out that there are certain assumptions (such as human rights standards), but also certain temptations (such as to leave certain part of the work of a legislator to the practice).[63] This is a hermeneutic circle—the ECJ can ground their cases only to the legal frames; however, the cases will specify narrow and define vague and aspirational norms that are often existing in such complex and always developing system as the EU legal space is. Thus, we have to admit that the glorification of the "legal" nature cannot be absolute.

Even ultra-positivist Kelsen already claimed, that law does have a necessary purpose that aims at social peace.[64] However, the ideas behind e-regulation are rather

[60] See Tosiek, Piotr. "The European Union after the Treaty of Lisbon—Still an Intergovernmental System," p. 16. Accessed 16 November 2013. http://www.jhubc.it/ecpr-riga/virtualpaperroom/072.pdf.

[61] Türk (2012).

[62] Laws (2013).

[63] Ibid, pp. 95–97.

[64] Hart (1961).

presented from the angle of becoming more competitive, thus focusing to the success of the EU and somewhat ignoring citizens in Europe. The passionate and somewhat unrealistic purposes of hardly controlled reforms can be balanced with what Chiassoni, (inspired by Hart), calls "Nirvana principle," meaning that the "legal theorists" should adopt more modest, craftsman-like approach; they should aim at the formulation of (tentative and revisable) "cool definitions".[65] The e-regulation is an undetermined area that can be called a "development law" where the coexistence of law/nonlaw instruments are combined[66] and the balanced interests of different stakeholders and beneficiaries are taken into account to guarantee inclusiveness and higher motivation to contribute to the eEurope for the members of European society.

There are confusingly many initiatives that relate to the digital age, but which are not (yet) strictly regulated by norms. The diversity here would raise many eyebrows for those who need to become familiar with the e-regulation in a specific area. One of the historical examples would be International Society for Digital Earth (ISDE), the initiative that was initiated in 1988 by Al Gore. In Europe, the term digital earth is rarely used, but there are many developments that strongly relate to it. At the political level, the European Commission launched in 2010 the Europe 2020 Strategy with the aim to achieve innovation-led, sustainable and socially inclusive growth.[67] As the authors found after SWOT analysis, digital earth concept has certain strengths, such as having "a strong technological component, harnessing developments in internet technologies, data availability and visualization methods among others, and provides a flexible framework to adapt to evolving technologies,"[68] which leads to the assumption that the whole e-regulation area and digital market dimensions should be screened through the variables used for digital earth analysis. Again, one of the dilemmas, deriving from the discussion, is the collision of different perspectives, i.e. political versus academic versus a technological versus legal perspective. For the sake of efficiency of any e-regulation field, these perspectives should be separated and the synergies found so that the development strategies would not be disturbed by mixing the academic visions, technological possibilities, political wishes and legal reality.

At the same time, there are certain risks such as threat to privacy or preparing useful tools for terrorists or organized criminal groupings. This discussion is most visible when talking about digital security governance, a term that according to Quirine Eijkman can be defined as "the use of digital personal data for threat analysis on the basis of (automated) risk profiling—as it enhances terrorism risk management in Europe."[69] European security strategies emphasize that ICT increasingly plays a key role in preventing and anticipating threats such as "terrorism and cybercrime."[70] One

[65] Chiassoni (2013).

[66] Zumbansen (2013).

[67] Annoni et al. (2011).

[68] Ibid, p. 274.

[69] Eijkmann (2013).

[70] Ibid, p. 35.

of the problems is that terrorists themselves are believed to adapt to changes and to use of new technologies. Unregulated areas are usage of bitcoins and other digital currencies that can be used for criminal purposes. Significant risks are also related to the protection of vulnerable groups, children among them. As formulated by O'Neill, "[t]he trust-reinforcement measures proposed under initiatives such as the CEO coalition of internet companies and the EC strategy for a better internet for children tackle some of the most persistent areas of risk identified in the online world."[71]

That is why the rule of law and human rights form a relevant part of establishing new regulations. Even more, the prerequisite of the legislative drafting to enhance e-technologies and methods is that the common values of Europe should be clearly seen as a ground of these developments. To use the words of Eijkman, "recent developments suggest that the use of ICT in the fight against terrorism requires more political and public legitimacy."[72] This legitimacy is secured when the rule of law and human rights are prioritized already in the beginning of the process of an initiative that elaborates to the set of legal norms.

By American judge O'Scannlain, it is "better to be ruled not by a mechanical, impersonal code, but the virtuous and wise".[73] In his essay, he emphasizes the role of judiciary in guaranteeing the Rule of Law and makes a reference to the philosopher Leo Strauss who referred to the ideas of Plato in context of nonperfect nature of laws: "Rule of Law is inferior to the rule of living intelligence, because laws, owing to their generality, cannot determine wisely what is right and proper in all circumstances given the infinite variety of circumstances"[74] These arguments can be easily taken to the discussion of how to position e-regulation that has certain constitutional background, but is still constantly open set of legal norms due to the innovation and technological development. Is it that we are moving towards natural law? Is there a threat to allocate too much power to judiciary? At the same time, the technological details in directives can be very detailed and cannot be much interpreted. It seems that e-regulation in its very many variations is a tool for emerging constitutional law of the EU and legal principles that are consolidating the whole legal system and cannot be disputed. The e-regulation should find a link to the EU constitutional law with the extended principle of "Rule of Law". This would lead to the phenomenon called the principle of technological neutrality. Under this view, and according to Cockfield, "laws should normally be applied in the same way no matter what technologies are employed…"[75] However, the authors are not sure that the new technologies can always be suitable of being regulated by traditional doctrinal legal approaches. Therefore, special attention to some aspects is relevant.

Technology friendly EU should take a position that even if the rapid legal or judicial response to the technological advancements is assumed, the user-centricity

---

71 O'Neill (2012).

72 Eijkmann (2013).

73 O'Scannlain (2014).

74 Ibid, reference to Strauss (1987).

75 Cockfield (2005).

should be contested with the public interest. So far, the commission demonstrated its good will in moving towards balanced and careful approach as stating in its website: "To contribute to setting-up of a legal environment at EU level which is fostering the take-up of new technologies, and is compliant with the EU Treaty and general principles of law. First, provide an early assessment on regulatory need for new technologies (in compliance with the Treaty) in order to foster their take-up. Second, early advice on legal feasibility of research projects or their results contributes to the reduction in costs for research being stopped for legal reasons or law suits resulting from research. Third, provide advice whether the EU is competent to act."[76] The Commission also adds: new technologies (autonomous/cognitive systems, cloud computing, internet, etc.) often appear to lack a legal setting. Stakeholders have diverging opinions whether regulating new technologies resulting in a deviation from rules governing the non-digital world, is needed for take-up. As new technologies have an impact on human and fundamental rights, an early assessment of legal feasibility as well as advice on liability, privacy issues, data protection, etc. mitigates the risk of high engagement of resources in actions, which cannot be implemented.[77] What would be the best procedure to screen all these concerns? A commission established the European Group on Ethics in Science and New Technologies (EGE), in December 1997. However, several authors warned that "the constitutional status of the EGE is at best 'grey', given that it has no firm basis in the European Union's constituent treaties, or the legislative structures developed to enhance the legitimacy, transparency, accountability, representativeness, effectiveness and efficiency of the European Union's legislative and executive decision-making"[78] The website of the institution: One of the leading principles should also be a reducing the complexity of e-regulation and promoting an adaptive, efficient and flexible framework (as suggested by Australian Law Reform Commission).[79] Technology neutrality is a beautiful and simplified illusion, rather a goal than a principle. The balanced e-regulation should be tested not only by several revelations of Rule of Law but also by user-centricity and other more specific principles related to new technology regulation—we would call it a keyhole effect. There are two separate rooms—law and technology, but united by keyhole. As the communication gets more intensive, the usage of keyhole (principles) is a preparation stage in creation of key (technology neutrality) that fits exactly with the keyhole.

The digitalization and e-regulation in terms of harmonization can also be categorized by the capacity of Member States or even regions. It is important to stress that although innovative new initiatives might stand a better chance while treating

[76] Legal advice for emerging technologies. Available at: http://ec.europa.eu/dgs/connect/en/content/legal-advice-emerging-technologies.

[77] Ibid.

[78] Busby et al. (2008).

[79] Australian Law Reform Commission. Guiding principles for Reform. http://www.alrc.gov.au/publications/issues-paper/guiding-principles-reform.

Member States from egalitarian perspective, the resources and traditions of societies differ significantly. This fact is more understandable when we look at EU regulation areas that have history but where the e-regulation may be inserted to improve and develop the situation. One of the good examples can be agriculture and CAP, considered among most mysterious and controversial regulation fields in the European Union that actually deviates from the mainstream free market ideology. Labrianidis and Kalogeressis analysed the determinants of the use of high technology, and ICTs in particular in 10 European rural areas. The authors concluded that "[t]he differences observed paint quite a disappointing picture in terms of regional disparities, as well as progress towards ameliorating them. In the most developed countries—in our case Germany and the UK—rural firms appear to be more or less 'digital', while in the less developed ones adoption has been much slower."[80]Another research, conducted by Brandtzaeg, Heim and Karahasanović shows that Eurostat data about digital divide is not sufficient, and there are several ways in which people in Europe use the internet.[81] An overview of digital inclusion or e-inclusion is presented by Paul Timmers. His statement, dating back to 2009, that "as of today, however, there is no comprehensive approach to measuring the loss of social capital caused by digital exclusion,"[82] still remains topical today, 5 years later, when the situation is probably very different due to the development and importance of Web 2.0 in everyday life of European citizens.

The most innovative areas (e-health, telemedicine, etc.) are delicately dealt with in order to find a balance between the EU competitiveness as a whole and the internal free market principles. For example, the so-called "next generation access networks (NGA)", mostly used in fibre optics technology to enhance fixed wireless and mobile communication, in the European Union, need constant update in legal regulation. Baistrocchi's research paper stresses that the guiding ideology with NGA should be as following, "[c]ompetition where possible, regulation where necessary."[83] He has also pointed out that the EU policy is to find a balance between the competition and safeguarding the incentives for investment at the same time.

As to the Digital market (DSM), it was envisaged several years ago by European Policy Centre that "the next step should be to draw up a timetable to set out the concrete actions leading to a date in 2015 by which time the DSM should have been realized through implementing these policy recommendations."[84] Looking at this deadline and some of the recommendations, one can easily see that the vision has, in many respects, failed. We could for example see that the suggestion to "create a more effective pan-European approach to taxes, including an easily accessible single VAT registration system and a harmonized tax base," is not

[80] Labrianidis and Kalogeressis (2006).

[81] Brandtzaeg et al. (2011).

[82] Timmers (2009).

[83] Baistrocchi (2011).

[84] See European Policy Centre. Establishing the Digital Single Market: Policy Recommendations. Accessed 12 January 2014. http://www.epc.eu/dsm/6/Policy_recommendations.pdf.

implemented. Some of the recommendations, such as to "develop a new accounting standard which can deal with knowledge/intangible assets" is still under discussion and the respective Directive is not transposed by several Member States. That leads to the conclusion that the e-legislation should be rather principle based than norm-based. The Digital Europe Agenda is well analysed by the progress report 2011[85] and directs to the motivation of the European institutions and networks trying hard to reach the goals.

One cannot underestimate the initiatives that originate from Member States. In the end, the political will of the stakeholders is a decisive factor. One of the newest innovations related to e-regulation is the European Cloud Computing Strategy.[86] T.H. Ilves, President of Estonia—a member state that is probably the most e-governance and eEurope minded, is a Chair of the Steering Board of the European Cloud Partnership. He recently stated that, "the European Union, like most of the world, faces economically challenging times. In such times, it becomes all the more important to recognize and seize new and unique opportunities to drive growth, stimulate innovation, and to provide benefits to citizens, businesses and public administrations."[87] From the strategy paper, it reads that the expected cumulative economic effects of cloud computing between 2010 and 2015 in the five largest European economies alone is around € 763 Bn.[88] The cloud economy is growing by more than 20 %[89] and could generate nearly € 1 trillion in GDP and 4 million jobs by 2020 in Europe,[90] with the support of the right policy framework. As the technological challenge is new for many, it is stressed that in regulating the area, one of the main goals is "establishing a shared understanding of regulatory and legal norms". At the same time, it is recognized that in this area, the EU cannot stand in isolation and therefore another relevant principle—recognizing the international environment, is emphasized, by stating that, "solutions should be based on best practices, favouring internationally recognized norms and standards wherever possible."[91] In conclusion, instead of somewhat hectic and suspicious e-Europe, there must be a clear EU initiative to demonstrate that the e-regulation is based on common principles of the Union Member States, and can therefore be an underlying platform for more efficient legitimization of the technological advancements. Legal certainty would encourage citizens to become European e-citizens and to invest and allocate

[85] See E-Europe Programs Advance. Special Report (2012).

[86] See the European Commission's communication on "Unleashing the Potential of Cloud Computing in Europe", Brussels, 27.9.2012, COM(2012) 529 final. Accessed 20 November 2013. http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy.

[87] See Establishing a Trusted Cloud Europe. A policy vision document by the Steering Board of the European Cloud Partnership.

[88] See Centre for economics and business research (2010): The cloud dividend report.

[89] See IDC Worldwide Cloud Black Book, 4Q 2012 update, April 2013.

[90] See IDC (2012): Quantitative estimates on the demand for cloud computing in Europe and the likely barriers to take up.

[91] Ibid.

resources of Member States into development in the field. Need for courageous and methodologically firm action by the EU is, for example recently analysed in telecom and electronic services. By melody, "the model of direct European Commission intervention on matters that affect EU policy and its many information society initiatives may be only way forward"[92] to achieve common market in the field.

4 Conclusion: Methodogical Approach for Better E-Regulation

The development of any e-regulation despite of its area should be encouraged by TFEU title I that lists the EU competences, but also furnish *Article 7*: "The Union shall ensure consistency between its policies and activities, taking all of its objectives into account and in accordance with the principle of conferral of powers". It would be suggested that the methodology in drafting and assessing legal acts covered by e-regulation should be overwhelmingly identical. The following list of policy stages is inspired by the methodology used in the field of e-signatures[93] and can be used, taking into account the interoperability of the nature of e-regulation, and can be used in any but especially developing area of preparing EU level e-regulation:

1. Analysis of the competences of the EU in the field, agendas, initiatives;
2. In case of new areas, the link between proposed e-regulation and common values of Europe, e.g. Rule of Law and human rights should be assessed, careful analysis of what extent the new e-norm would change the *lege lata*;
3. Assessment of the draft e-regulation from the perspectives of technological, semantic, organizational, legal and political layers, recognizing the special character of e-regulation;
4. Assessment of rights and obligations of electronic identity of stakeholders to guarantee the principle of user-centricity and the legal certainty in general;
5. Economic assessment, risks and obstacles for further development;
6. Analysis of the digital divide among Member States and have two category of e-regulation sets: a) based on minimum standard; b) based on multi-speed concept of Europe: the selection of *avangarde* EU countries for a deeper focus and feedback;
7. The context of reference for the area related market in Europe and in global context;
8. Characteristics and policies of supply-side actors;
9. An overview of the supply-side offering;
10. Characteristics of demand-side;

[92] Melody (2013).

[93] The new legislative proposal for electronic identification and eSignatures, European Parliamentary Research Service. Accessed 16 December 2013. http://epthinktank.eu/2013/11/05/the-new-legislative-proposal-for-electronic-identification-and-esignatures/.

Following these steps would break the "wall of text" of countless strategy documents and lead to the EU policy and legal actions for realistic (implementable) and efficient e-regulation, proper decision-making procedure can be selected due to the factors identified using the aforementioned methodology.

It is a fact that e-environment is a growing phenomena and it needs careful maintenance by those who wish to use it for better Europe. However, the dilemmas related to special character of e-regulation are not yet seriously theorized. Today, we face sometimes overlapping and complex EU initiatives and agendas, the concepts of Digital Europe, eEurope, e-citizen, e-commerce, etc. are not always linked and categorized with sufficient clarity. In conclusion, the challenges related to e-regulation and need for characterising the e-legislation as set of new type of rules is an open question for many. At the same time, the stakeholders would benefit from roadmap, legal certainty and clearly determined e-identity. It is assumed that the harmonization in the field of digitalization and e-regulation depends on the capacity of EU Member States who face the problems of electronic divide. Systematic and methodologically grounded approach of EU e-initiatives and e-regulation would benefit the situation and hearten the emerging generation of skilful e-lawyers and specialists.

References

Annoni, A., Craglia, M., Ehlers, M., Georgiadou, Y., Giacomelli, A., Konecny, M., et al. (2011). A European perspective on digital earth. *International Journal of Digital Earth, 4*(4), 271–284.

Baistrocchi, P. A. (2011). Competition and regulatory principles for next generation access (NGA) networks in the European Union. *Computer and Telecommunications Law Review, 17*(6), 166–179.

Besters, M., & Brom, F. W. (2010). "Greedy" information technology: The digitalization of the European migration policy. *European Journal of Migration and Law, 12*, 455–470.

Brandtzaeg, P. B., Heim, J., & Karahasanovic, A. (2011). Understanding the new digital divide—a typology of internet users in Europe. *International Journal of Human-Computer Studies, 69*, 123–138.

Busby, H., Hervey, T., & Mohr, A. (2008). *Ethical EU law? The influence of the European group on ethics in science and new technologies 33 E.L. REV* (p. 803).

Cockfield, A. J. (2005). Towards a law and technology theory. *Manitoba Law Journal, 30*(3), 383.

Chiassoni, P. (2013). The model of ordinary analysis. In L. D. d'Almeida., J. Edwards & A. Dolcetti (Eds.), *Reading HLA Hart's the concept of law*. Oxford: Hart publishing.

De Andrade, N. N. (2013). "Electronic identity for Europe": Moving from problems to solutions. *Journal of International Commercial Law and Technology, 8*(2), 103–109.

De Visser, M. (2014). *Constitutional review in Europe. A comparative analysis*. Oxford and Portland, Oregon: Hart Publishing.

E-Europe Programs Advance. Special Report. (2012). *Journal of E-Governance. IOS Press*, 159–163.

Eijkmann, Q. (2013). Digital security governance and accountability in Europe: Ethical dilemmas in terrorism risk management. *Journal of Politics and Law, 6*(4), 35–45.

Graux, H. (2013). Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union. *Journal of International Commercial Law and Technology, 8*(2), 110–117.

Hart, H. L. A. (1961). *The concept of law*. Oxford: Oxford University Press.
Hoikkanen, A., Bacigalupo, R. C., Wainer, L., & Ioannis, M. (2010). New challenges and possible policy options for the regulation of electronic identity. *Journal of International Commercial Law and Technology, 5*(1), 1–10.
Howes, D. (2001). E-legislation: Law-making in the digital age. *McGill Law Journal/Revue de Droit de McGill, 47*, 39–57.
Janssen, K., & Dumortier, J. (2003). Towards a European framework for the re-use of public sector information: A long and winding road. *International Journal of Law and Information Technology, 11*(2). Oxford University Press.
Joerges, C., & Weimer, M. (2014). A crisis of executive managerialism in the EU: No alternative? In G. de Burca., C. Kilpatrick & J. Scott (Eds.), *Critical legal perspectives on global governances*. Oxford: Hart Publishing.
Kuzelewska, E., & Krasnicka, I. (2013). E-voting to the European parliament and the United States congress. An attempt of comparison. In E. Kuzelewska & I. Krasnicka (Eds.), *Elections to the European parliament as a challenge for democracy. European integration and democracy series* (Vol. 2). Warszawa-Bialystok.
Kerikmäe, T. (2010). Estonia as an EU State: Lack of proactive constitutional dialogue. In K. Topidi & A. Morawa (Eds.), *Constitutional evolution in central and Eastern Europe expansion and integration to the EU* (pp. 11–42).
Labrianidis, L., & Kalogeressis, T. (2006). The digital divide in Europe's rural enterprises. *European Planning Studies, 14*(1), 23–39.
Lamond, G. (2013). The rule of recognition and the foundations of a legal system. In L. D. d'Almeida., J. Edwards., & A. Dolcetti (Eds.), *Reading HLA Hart's the economic concept of law*. Oxford: Hart publishing.
Laws, S. (2013). Legislation and politics. In D. Feldman (Ed.), *Law in politics, politics in law*. Oxford: Hart publishing.
Lusoli, W., & Maghiros Ioannis, B. M. (2009). *eID policy in a turbulent environment: Is there a need for a new regulatory framework?* Edificio: European Commission Joint Research Centre (JRC), Institute for Prospective Technological Studies (IPTS).
Melody, W. (2013). Next steps in Europe's digital agenda. *Journal of E-Governance, 36*, 101–104.
O'Neill, B. (2012). Trust in the information society. *Computer Law and Security Review, 28*, 551–559.
O'Scannlain, D. (2014). The rule of law and the judicial function in the world today. *Notre Dame Law Review, 89*(3), 390.
Poremska, M. (2010). ICT in public procurement can lead to cybercrimes? *Masaryk University Journal of Law and Technology, 4*(2), 157–172.
Poremska, M. (2012). Electronic signatures and acts in electronic tools used on public procurement. *Masaryk University Journal of Law and Technology, 6*(1), 147–158.
Rossi, L. S. (2008). How fundamental are fundamental principles? Primacy and fundamental rights after Lisbon. *Yearbook of European Law, 27*(1), 65–87.
Schartum, D. W. (2011). *Legal and semantic interoperability as part of Government communication policy* (pp. 1–16).
Shahin, J., & Finger, M. (2009). The history of a European information society: Shifts from governments to governance. *Global E-Governance Series* (pp. 62–83). Amsterdam: IOS Press.
Strauss, L. (1987). "Plato", history of political philosophy 33. In L. Strauss & J. Corpsey (Eds.), pp. 74–75.
Šilhavy, R., & Šilhavy, P. (2008). Internet voting. *Masaryk University Journal of Law and Technology*, 137–146.
Timmers, P. (2009). Update on e-inclusion and e-accessibility policy at European level. *Journal of Legal Technology Risk Management, 4*(1), 15–33.
Türk, A. H. (2012). Lawmaking after Lisbon. In A. Biondi., P. Eeckhout & S. Ripley (Eds.), *EU law after Lisbon* (pp. 67–84). Oxford: Oxford University Press.
Zumbansen, P. (2013). Knowledge in law and development. In L. Amicorum., D. M. Trubek., C. de Búrca., C. Kilpatrick & J. Scott (Eds.), *Critical legal perspectives on global governance*. Oxford: Hart Publishing.

List of Other Documents

Australian Law Reform Commission. Guiding principles for Reform. Available at: http://www.alrc.gov.au/publications/issues-paper/guiding-principles-reform Centre for economics and business research (2010): The cloud dividend report.

COM (2009) 432: Review of eEurope 2005 Action plan. Accessed 10 December 2013. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0432:FIN:EN:PDF.

COM (1999) 687: Communication of 8 December 1999 on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000—eEurope—An information society for all.

COM (2001) 140: Commission Communication of 13 March 2001 on eEurope 2002: Impact and Priorities A communication to the Spring European Council in Stockholm, 23–24 March 2001.

COM(2002) 263: Communication of 28 May 2002 from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions—The eEurope 2005 action plan: an information society for everyone.

COM(2004) 108: Commission communication of 18 February 2004 "eEurope 2005 mid-term review".

COM(2005) 229: Communication from the Commission of 1 June 2005 to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions entitled "i2010—A European Information Society for growth and employment".

COM(2009) 432: Communication from the Commission of 21 August 2009 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Final Evaluation of the eEurope 2005 Action Plan and of the multiannual programme (2003–2006) for the monitoring of eEurope 2005 Action Plan, dissemination of good practices and the improvement of network and information security (Modinis).

COM(2010) 245: Communication from the Commission of 19 May 2010 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—A Digital Agenda for Europe. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:HTML.

Decision 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 adopting a multiannual programme (2003–2005) for the monitoring of the eEurope 2005 action plan, dissemination of good practices and the improvement of network and information security (MODINIS).

Digital Agenda for Europe. A Europe 2020 Initiative. Our Goals. Available at: http://ec.europa.eu/digital-agenda/en/our-goals.

Digital Single Market Online Content 2013 Data. Internet and Skills. Accessed 25 November 2013. Available at: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/DAE%20SCOREBOARD%202013%20-%203-INTERNET%20USE%20AND%20SKILLS.pdf.

Ecommerce Europe. Available at: http://www.ecommerce-europe.eu/home.

*e*Europe 2002 Final Report. Communication of 11 February 2003 from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions eEurope 2002 Final Report [COM(2003) 66 final Not published in the Official Journal].

*e*Europe 2002. Impact and priorities. A communication to the spring European Council in Stockholm, 23–24 March 2001. COM (2001) 140 final, 13 March 2001.

E-Europe Programs Advance. Special Report (2012).

E-regulation, in terms of this article means the legal act regulating a field that can be administered by electronic means.

Establishing a Trusted Cloud Europe. A policy vision document by the Steering Board of the European Cloud Partnership.

European Policy Centre. Establishing the Digital Single Market: Policy Recommendations. Available at: http://www.epc.eu/dsm/6/Policy_recommendations.pdf.

IDC (2012): Quantitative estimates on the demand for cloud computing in Europe and the likely barriers to take up.
IDC Worldwide Cloud Black Book, 4Q 2012 update, April 2013.
Legal advice for emerging technologies. Available at: http://ec.europa.eu/dgs/connect/en/content/legal-advice-emerging-technologies.
Lisbon European Council 23 and 24 March 2000. Presidency Conclusions. Available at: http://www.europarl.europa.eu/summits/lis1_en.htm.
Nine Themes of Digital Citizenship. Available at: http://digitalcitizenship.net/Nine_Elements.html.
2015: A connected and diversified Europe. eIDM Vision Paper. Available at: http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR513.pdf.
Presentation of Inge Graef at Interdisciplinary Centre for Law and ICT (ICRI) "Achieving interoperability in the absence of standards: a new policy under the Digital Agenda?" Available at: http://www.eurocpr.org/data/2013/Graef.pdf.
Presidency conclusions of the Brussels European Council (22 and 23 March 2005). Available at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/84335.pdf.
See COM(2005) 229: Communication from the Commission of 1 June 2005 to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions entitled "i2010 - A European Information Society for growth and employment".
See COM(2009) 390: Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions—Europe's Digital Competitiveness Report: main achievements of the i2010 strategy 2005-2009. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0390:FIN:EN:PDF.
Seville European Council Presidency Conclusions. Available at: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/72638.pdf.
The European Commission's communication on "Unleashing the Potential of Cloud Computing in Europe", Brussels, 27.9.2012, COM(2012) 529 final. Available at: http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy.
The new legislative proposal for electronic identification and eSignatures, European Parliamentary Research Service. Available at: http://epthinktank.eu/2013/11/05/the-new-legislative-proposal-for-electronic-identification-and-esignatures/.
Tosiek, Piotr. "The European Union after the Treaty of Lisbon—Still an Intergovernmental System." Available at: http://www.jhubc.it/ecpr-riga/virtualpaperroom/072.pdf.

Author Biography

Tanel Kerikmäe is a professor of European Law at Tallinn Law School, Tallinn University of Technology. The author is grateful to Sandra Särav, research assistant for her conscientious attitude and professional support.

Pawan Kumar Dutt is a lecturer in Tallinn Law School, Tallinn University of Technology and a doctoral student in Estonian Business School.

e-Governance in Law and by Law

The Legal Framework of e-Governance

Katrin Nyman-Metcalf

Abstract The article provides an overview of various areas of law affected by e-governance. e-governance is often approached as a technical issue, even if it is now mature enough for other aspects to get more attention. It is not unusual that legislators, regulators or others concerned concentrate too much on technological issues and presume that new rules are needed if new technologies are used. However, there should not be much separate legislation or regulation for e-governance, as this risks creating parallel systems rather than benefiting from efficiency gains. What is required is a profound analysis of existing legislation to identify whether and in what contexts new or amended rules may be required. With more and more novel information and communication technology (ICT) solutions for governance, it may get difficult to fit new phenomena into old rules through interpretation only. For example, e-signatures or other identification systems need to be regulated. It must not be forgotten that the perception of reliability and security of e-governance is important as people will not use service they see as insecure, which is why data protection is a priority. Technology and law should work together and complement one another, but the relationship may be less complex than it may appear to the non-initiated. The legal system must be able to include e-governance but does not need to change totally because technologies change.

1 Introduction: Setting the Scene

Introducing e-governance will reduce corruption (which computer asks you to slip 100 Euros under the keyboard before it performs a transaction?); it will make it easier for people including minorities, inhabitants of rural areas or the disabled to participate in political life; it will lead to efficiency gains and thus cost savings;

K. Nyman-Metcalf (✉)
Tallinn University of Technology, Tallinn, Estonia
e-mail: katrin.nyman-metcalf@ttu.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_3

it will help states attract investment; and it will support innovation. Just like that? There is no question that the buzzwords and general enthusiasm that one encounters in the debate on e-governance make it sound very attractive and the only reason it is not fully embraced everywhere appears to be that there are too many Luddites[1] in positions of power. On the other hand, against this enthusiasm, seeing automation and interoperability as a panacea for many ills are also those who—Luddite or otherwise—list at least as many negative features as the positive ones mentioned. What there is less of is a balanced debate "in the middle", where it is not an inherent fear of, or opposition to, new technologies that is behind the counter-arguments to e-governance, but instead reasonable questions concerning risks, bottlenecks or lack of popular uptake. Such arguments should be met with well-founded explanations and improvements, rather than just a blind faith in technology.

Various information and communication technology (ICT) solutions to facilitate governance at different levels have been developed over the past decades, with an ever more rapid development in recent years. There are many solutions that deal with matters of relevance both for public administration and electronic commerce, which has led to cross-fertilisation as well as to public private partnerships. The debate on e-governance tends to be led by technical developments and technical experts. To some extent this is natural, as the subject matter would not arise without technology. However, to a large extent, the issue has now reached such a level of maturity that in practice other disciplines like law, public administration, sociology and so on have at least as much to contribute. For successful e-governance, it is essential to determine what possibilities there are within existing legal and administrative frameworks to move to new e-governance solutions and what legal and structural changes are needed to support innovation. Law—in its regulatory role—is the background against which new developments should be evaluated, but law—in its facilitative role—is also the tool to be used for introducing the changes.

The legal side and social side of e-governance tend to be less well studied than the technical one. This is despite the fact that in many ways, the "soft" side of e-governance development may hold the key to it being able to meet the ambitious targets set for it. The recognition of what e-governance means is in many ways still in its infancy in many countries. At any internal or inter-ministerial working group, international forum or e-governance conference, one tends to meet predominantly IT technical people. This is the case even if the subject for the event is the legal and regulatory framework of e-governance. It is not unusual that IT departments are made responsible for questions of access to information or data protection. Even if the ICTs used are no longer very new, there is still a prevalence of the idea that technology should guide the regulation and those who understand technology are thus best placed to also deal also with the regulatory issues.

[1] A member of any of the bands of English workers who destroyed machinery, especially in cotton and woollen mills, which they believed, was threatening their jobs (1811–1816). Derogatory: a person opposed to increased industrialisation or new technology. http://www.oxforddictionaries.com.

This article discusses what the legal framework for e-governance should consider and contributes to the discussion on how to benefit from the possibilities offered by ICT solutions while not ignoring possible risks. The article hopes to support the factual and properly argued discussion that was called for above, by setting out what a sensible approach from the legal side to the introduction of e-governance should be. It will be shown that e-governance and its legal framework can be de-mystified and it is most useful if it is seen as an integral part of the governance of the state rather than as an alien phenomenon.

2 e-Governance as an Integral Part of Governance

2.1 What Is e-Governance?

There is no coherent terminology used for the various elements of e-governance, although with the spread of certain technical and legal solutions, such terminology is gradually being created. Even the term "e-governance" itself is not universally used in the same way. The Council of Europe in one of the relatively few international legal instruments on e-governance, Recommendation Rec (2004)15, refers to Electronic Governance or e-governance without a definition, but with an understanding that the term is self-explanatory.[2] The European Union (EU) provides a very short definition: "*e-government uses digital tools and systems to provide better public services to citizens and businesses*".[3] The World Bank is more expansive and links the benefits of e-governance to the definition: "*e-government*" *refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions*".[4]

The term e-governance is used interchangeably with "e-government", although governance is the preferred term, being wider. What is meant by either term is not always clear. Countries talk about introducing e-governance or e-government when they facilitate access to information by electronic means, even without any interactivity. The times are gone when a state would claim to have e-governance just by having websites for ministries, but looking at legislation related to e-governance, this still quite often only deals with rather basic use of ICT in public administration,

[2] Recommendation Rec (2004)15 adopted by the Committee of Ministers of the Council of Europe on 15 December 2004 and explanatory memorandum, www.coe.int.

[3] http://ec.europa.eu/digital-agenda/life-and-work/public-services.

[4] http://web.worldbank.org/ (e-government—Definition of e-government).

to facilitate administrative work.[5] In the absence of widely applicable international conventions or other such instruments, the development of terminology is likely to be patchy and it is quite possible that separate terms are used in parallel for the same thing—or the same term for different things. Globalisation, made possible to a new extent through ICTs, presents its own challenges.[6] Phenomena get instantly translated and transposed without it being clear what may have got lost in translation.

Electronic, e-signatures or digital signatures present one example of such confusion in terminology. The word "confusion" may be too strong, as in practice in most contexts, it is clear what is meant with the words and why one of other is used, but this is because of pragmatic use rather than a clearly agreed terminology. An electronic signature can include a digital signature as well as one made with some electronic device, like the pen-like devices to write on screens that are popular with delivery services or even signatures written with the mouse or keyboard to resemble traditional signatures. From a legal viewpoint, such signatures are not different from traditional ones: they require the presence of the person, and the item he or she is signing. It may be possible to copy the on-screen signature in an even easier way than a pen-and-paper one, which makes it less secure, but there can be ways built into the device to prevent this. A digital signature is something totally different. As the name implies, the information is broken down into digital format and can be read with the correct codes to re-transform the digital form to legible form. A digital signature requires codes of some sort, and there may be a device needed to create or transmit the codes. From a legal viewpoint, the digital signature looks different from the traditional one, which means that there must be special provisions in law that explain what a digital signature is and how it can be created. Such rules are found for the EU in Directive 1999/93/EC which is entitled "Electronic signatures".[7] Its content shows that what is intended here is a digital signature, but given the EU use of terminology, the term electronic or e-signature is indeed what has gained ground. The UNCITRAL Model Law from 2001 is equally entitled Model Law on Electronic Signatures,[8] although its definitions like those in the Directive show a more specific area of application, focused on what may be more adequately seen as digital signatures.

---

[5] For example, the French Ordinance on electronic interactions between public services users and public authorities and among public authorities (2005; *Ordonnance n° 2005–1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*,) http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006052816&dateTexte=vig; the Polish Act on the Computerisation of the Operations of the Entities Performing Public Tasks (2005, http://www.mswia.gov.pl/portal/pl/589/3886/Ustawa_o_informatyzacji_dzialalnosci_podmiotow_realizujacych_zadania_publiczne.html); the Swedish Open Government Action Plan, Bill 2009/10:175 *Public administration for democracy, participation and growth* (www.opengovpartnership.org/file/938/download).

[6] Schneiberg and Bartley (2008, pp. 38–39).

[7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L13/12, 19.01.2000.

[8] http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html.

2.2 The Basic Legal Framework of e-Governance

In all areas of technological change, there is an almost unanswerable question of what should come first: technology or law? It is unanswerable as it is impossible to regulate technology that we do not yet fully know, while it may be just as hard to change an established situation, so the only answer is that the two must go hand-in-hand. This, however, is much easier in theory than practice. In practice, legislators and regulators attempt to fit new phenomena into legislation and regulation created in a different situation.[9] This may work very well and is the way all developments of society—not just technological ones—have been dealt with. Law can be interpreted to fit another reality than that for which it was written. Still, the more complex and rapidly changing the reality gets, the more risks there are that the legal and regulatory system does not manage to keep up with developments, not least technological ones. The result can be over-regulation that stifles innovation or instead under-regulation that allows harmful lacunae to occur. The need to take the legal framework into account at an early stage of developing new models of e-governance is thus evident.

The key principle that should be followed in order to create a coherent legal framework for e-governance is simple: There should not be too many special laws, in order to avoid the creation of parallel systems. Only by integrating e-governance with regular governance at all levels can be a part of the state system and help obtain efficiency and other mentioned gains.[10] Instead of concentrating on the technologies used, the background to what kind of regulation to adopt should be the issues dealt with, the aspects of governance that are to be handled electronically rather than (just) in the traditional, paper-based manner. This apparently self-evident suggestion is surprisingly often not implemented in practice. The reason for this may be sought in the novelty of technologies and the various technical issues that need attention, together with the mentioned fact that often more technically trained professionals than lawyers or other social scientists are in charge of introducing e-governance.

Legal issues of e-governance cannot be seen as a single, unified area of law. Novel e-solutions may affect basic structures of governance and may have implications on basic rights, such as the right to privacy—formulated through the legal provisions on data protection. Amendments may be needed to administrative law, administrative and criminal procedure law, criminal law, data protection law, regulations of ministries and other official organs, communications law, competition

[9] Brownsword and Goodwin (2012, pp. 19–21).

[10] *Noting that e-governance is about democratic governance and not about purely technical issues, and convinced therefore that the full potential of e-governance will be harnessed only if ICTs are introduced alongside changes in the structures, processes and ways that the work of public authorities is organised,* Preamble, Council of Europe Recommendation Rec (2004)15, op. cit.

law, intellectual property law, etc. Organisational structures must be analysed to see whether they need to be changed, as issues of responsibility are essential. In practice, the question of organisational responsibility and what competence different bodies have are often the main issues to resolve in order to have successful e-governance.[11] Interoperability, one of the key advantages of e-governance requires cooperation. As the organs that need to cooperate are often at the same level, the question "who can tell others what to do" becomes essential. This is a good example of how the solution cannot look the same everywhere and how the key to the solution is not to be found in technology. The organisational structure must fit the country in question and be established by law, regulation and/or internal rules in whatever manner that fits the society.

In addition to law, various political and sociological questions on how to integrate e-governance in society are of interest. Disclosure of information by public bodies, requirements of transparency in decision-making processes, creation of a proper marketplace of ideas can be enforced or encouraged by law but can be made to work through ICTs.[12] There is a constant interplay between law and technology that lays the foundation for successful e-governance, making use of both areas to find the best solutions. This also speaks in favour of not having a lot of specialised legislation, as any very specific law risks becoming obsolete rapidly. The law should focus on the result to be obtained, the issue to be regulated, rather than on the technology.

2.3 e-Democracy

The e-elections—remote internet voting with binding results[13] to parliamentary, local and European elections[14]—that are held in Estonia since 2005 have attracted a lot of attention as the ultimate way to use modern ICTs for democratic participation. So far, no other country has followed the Estonian lead in this respect for national elections, although some local elections as well as special elections for different organs use similar methods, but most probably it is just a question of time before the system spreads, especially as the elections have been a success in Estonia with no reported problems.[15]

[11] Examples from e.g. Palestine—OECD (2011) esp. p. 12—or Sri Lanka, Hanna (2008, pp. 9–10) and Chap. 2.

[12] Morgan and Yeung (2007, p. 96).

[13] The term "e-voting" is used also for various kinds of machine voting, etc.

[14] http://www.vvk.ee/voting-methods-in-estonia/engindex/.

[15] For more details on this issue, see the article by Ülle Madise and Priit Vinkel in this volume.

The Estonian e-voting system was examined by the Supreme Court in 2005,[16] following a complaint by the President in his role of examining constitutionality of legislation. The case centred on the principle of one person—one vote and if the e-voting ensured this. For details on the case, please refer to the chapter by Ülle Madise and Priit Vinkel in this book, but suffice to say here that the Court found that there was nothing in the system that compromised the principle of one person–one vote. Thus, the Supreme Court ruled that the system of e-voting appropriately balanced all electoral principles of the constitution.[17]

Even in Estonia where e-elections have been introduced and have steadily gained in popularity and where there have been no serious incidents to compromise them,[18] one of the main opposition parties (Keskerakond) campaigns to abolish them,[19] as it finds its electorate among less educated and older people, in areas where e-voting is less prevalent and thus hopes to gain points among its core electorate and at the same time hope to reduce votes for the opposition, as people who have got use to e-voting may not go out and vote in the traditional manner. The interesting part of this political campaign is that it can serve as an example of how matters actually unrelated to the technology of the e-service or made-up matters can be seized upon to exploit the fears people have when something is new and technically complex. The opposition party even made a complaint to the European Court of Human Rights regarding the e-voting in the 2011 parliamentary elections.[20]

e-democracy or ICTs as a tool for democracy is, however, a much wider issue than just internet-based elections. New examples are constantly arising in this context. As just a small snapshot from new initiatives reported in the same week in February 2014 can be mentioned a new and more comprehensive website for government information in India, Open Government 2.0,[21] the possibility to monitor

---

[16] Judgment of the Constitutional Review Chamber of the Supreme Court number 3-4-1-13-05, Petition of the President of the Republic to declare the Local Government Council Election Act Amendment Act, passed by the Riigikogu on 28 June 2005, unconstitutional," 1 September 2005. http://www.nc.ee/?id=823.

[17] Ibid.

[18] OSCE *Estonia Parliamentary Elections 6 March 2011 OSCE/ODHIR Needs Assessment Mission Report,* 10–13 January 2011, Warsaw 27 January 2011, http://www.osce.org/odihr/elections/estonia/75216, p. 6.

[19] As on example http://www.postimees.ee/1264298/keskerakond-e-haaletus-ei-vasta-pohiseadusele (e-voting is not in accordance with the constitution) 9 June 2013. An organisation has been set up especially to campaign against e-voting, this organisation (MTÜ Ausad Valimised) was fined for breach of the election advertising code in 2013, upheld by court in January 2014. (http://www.delfi.ee/news/paevauudised/eesti/mtu-le-ausad-valimised-trahvi-maaramine-jaabjousse.d?id=67583548) 9 January 2014.

[20] http://news.err.ee/v/politics/4ee0c8a2-b9c2-4d28-8ae4-061e7d9386a4. It was not possible at the time of writing to determine whether the claim has been dismissed or will be dealt with by the court, although formal requirements of the court and the nature of the complaint may likely lead to its dismissal.

[21] www.data.gov.in.

the South African parliamentary assembly work[22] and a new website for asking US elected officials questions via Twitter or similar[23]—these examples among other social development examples highlighted by the World Bank in their Social Development Newsletter as Highlights of Social Accountability.[24]

2.4 The Role of Legal Research

Lawyers started paying attention to electronic documents and electronic signatures already when these where quite new in the 1990s or even earlier, but only in a rather patchy and minimal way. It was understandable that at that time, the discussions had to be somewhat speculative as the issues analysed were often not used in practice.[25] The technological developments happened independently from any legal discussion: meaning that the technologies that were implemented and achieved practical utility were not (much) influenced by whatever suggestions lawyers had made. In the early 2000s, legal writers got more interested in the world of electronic governance and commerce, but as technology moved so fast, the writings tended to be reactive and post-factum.[26]

The early 2000s was also the time when different disciplines began theoretical attempts to understand the complex relationships between ICTs and social structures. Gil-Garcia writes that initially such research mainly took a linear perspective and assumed a unidirectional causality. This causality could go both ways: either ICTs were seen to have the capacity to transform organisations or organisational characteristics arrangements were responsible for the selection, design and use of ICTs. The realisation of the actual complexity and the multidirectional influences mainly came later.[27] Legal research was still less included in this process than other social sciences and even now, the legal research on "e-issues" is more prevalent on e-commerce and for example special consumer protection issues in that context than on the governance aspects.[28]

Technology continues to develop rapidly, and it is not to be expected or desired to reach some point where everyone can sit back and analyse the situation in a profound and relaxed manner. However, with e-services of different kinds having

---

22 www.pa.org.za.

23 www.askthem.io.

24 asksocial@worldbank.org 22 February 2014 Newsletter.

25 One example is Reed (1996).

26 Some examples include Brazell (2004), Mason (2003). Wang (2006) stands the test of time very well, as the article concentrates on the essential function of signatures and thus changing technologies do not affect the relevance.

27 Gil-Garcia (2005, p. 2), quoting in this context, e.g. Dawes and Pardo (2002) and Garson (2003).

28 Laudon and Guercio Traver (2013), Spindler and Börner (2010), Dickie (2005), Edwards (2005) as examples.

become such essential features of everyday life, there is more of an understanding of the fact that also legal and administrative systems must be adjusted properly and the people dealing with this properly included in the development process if the benefits of the technologies are to be fully enjoyed.

3 e-Identification

When concentrating on issues, the first question to be posed is whether there is any need for special legislation or amendments to legislation in order to introduce e-governance: whether existing legislation created for the pre-e-governance system leaves any gaps that cannot be filled through interpretation? The reason for such gaps would normally be that something in the electronic way of doing things is so different to how it is done manually, that rules not written for the technology do not include relevant aspects. As an example, it is not difficult to interpret documents to include electronic or paper documents, but it is not likely that the law would include definitions of signature creating devices in the non-electronic world, where this would mean pens. However, for an electronic signature, the device used for making it is relevant and may be what determines its validity.[29] In general, questions related to e-signatures or e-identification are an area where there is a need for special legislation or at least explicitly adapted legislation to ensure that the law fits. As the ability to identify oneself and give binding commitments via a signature is essential for any transactions in the electronic world, proper regulation of this issue is a prerequisite for functioning e-governance (as well as for functioning e-commerce). Not surprisingly, the absence of an e-signature is seen as a key obstacle to creation of e-governance when such a signature is not introduced early on in the process.[30]

Electronic signatures include all kinds of signatures that use electronic means, so this would also include the kind of electronic devices used by many courier firms to sign for parcels or scanned signatures. These kinds of signatures are rarely very secure and are thus suitable for the kind of transactions where the level of security does not have to be very high—comparable to situations in which traditional signatures are not verified by having to show proof of identity or where the approval shown by the signature needs to be confirmed later or similar. For a secure electronic signature, the digital signature using different keys—a private and a public one—is regarded the most secure. Certification authorities issue and control identification systems that help ensure the validity of the signature: that it is indeed made by the person who claims to do so.[31] Even without a global definition of e-signatures, the concept is to some extent harmonised, e.g. through an

[29] Article 2 Directive 1999/93/EC, op.cit.

[30] OECD (2011, p. 14).

[31] Wang (2006, p. 254).

UNCITRAL Model Law on Electronic Signatures[32] but also the UNCITRAL Model Law on Electronic Commerce from 1996[33] that includes provisions on acceptance of e-signatures, something that has been included in the legislation of states in a similar fashion.[34] The idea is simple but legally important: e-signatures must have the same force as regular signatures and such force shall be provided by law.

The traditional signature is something that we instinctively recognise and can describe for everyday use as well as in the legal system. A person signs his or her name, thus showing who he/she is and giving consent to something—be it buying, selling, applying or just wishing happy birthday. The further consequences of the signature depend on the context and the legal framework for that context, which means that the requirements and the effect of my signature on a contract selling real estate is quite different to those linked to the very same signature on a Christmas card. This is self-evident, but how to re-create this in the electronic world is not immediately evident, which is why the situation of having had very few legal definitions or explicit rules on signatures may not suit the electronic world. Wang makes an interesting exposé of legal definition of signature in law and case law of selected countries, showing that in general, it is only in situations outside of a usual context that it is necessary to define signatures—otherwise the legal system manages to rely on what is traditionally known and understood.[35] What is essential is the function of a signature: to authenticate a document.[36]

In common law countries, it may be easier to accept electronic signatures without special legislation to that effect than in civil law countries, because of the greater role of courts in shaping the law. However, Wang shows that the case law has not been uniform in its interpretation of electronic signatures of different kinds,[37] which indicates that legislative guidance may be needed also in common law countries.

For the legal system, the question of approving a signature or other identification should not be related to the form but to whether it is capable of fulfilling its function of authenticating something. Relevant in this context is whether the signature is susceptible to intervention, modification or technical compromise.[38]

---

[32] Op. cit.

[33] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.

[34] Malkawi (2007, p. 163).

[35] Wang (2006, pp. 255–263).

[36] Ibid. p. 256 and p. 271.

[37] Ibid. p. 257 (UK) and pp. 258–259 (USA). About the USA, the example of Wang of how a court in 1869 accepted exchange of telegrams as signatures, but another USA court in 1996 did not accept a fax (as it was only chirps and beeps) is an amusing as well as illustrative example of the difficulty in interpreting technology through the prism of law.

[38] This aspect has been recognised by courts as a reason for not accepting electronic means of signing. See Wang (2006, p. 259) referring to German court cases.

4 The e-Person: Protection of Personal Data

4.1 Data Protection and Access to Information

A very crucial legal area in the context of e-governance is undoubtedly personal data protection. Data protection is a topic of great and growing importance in the modern communications landscape.[39] The Charter of Fundamental Rights of the EU is the first major international convention to include a specific Article on data protection, Article 8. This right includes the right to access and rectify data about oneself and the need for control by an independent authority. Otherwise, Articles on protection of privacy are interpreted to include data protection (and the Charter includes also an Article on protection of privacy, Article 7). By mentioning it specifically, the importance of data protection not least seen against an increased use of ICTs is underlined.[40]

Data protection is linked to access to information although the legal frameworks are different.[41] Although there is a lot of academic research as well as practical studies (for example in the EU context) on data protection, while access to information tends to be studied especially in the context of democratic transition, the important link to e-governance is less well developed in academic and practical studies. Not least for the perception of e-governance and the trust in it, there must be careful consideration of data protection. This is highlighted the in relation to interoperability of databases, as any breaches of data protection in a situation of high interoperability could have widespread negative consequences. Access to information can be facilitated by ICTs to a much greater extent than what is done today. As protection of privacy (the underlying legal principle for data protection) is one legitimate reason to limit transparency and access to information, the development of any improved data access and data handling system needs to be evaluated with these different legal areas in mind.

For protection of personal data just as for other aspects of e-governance or use of ICTs, it should be the type of information, its content and not its form that determines the level of protection. It should be no more the technology used than it is the colour of the paper something is written on that decides what protection should be given. At the same time, ICTs and automated data processing have led to new issues as it is now possible to deal with such amounts of information as

[39] The EU is in the process of reforming its existing data protection provisions (found in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), with a view to making the rules more suitable for modern ICTs as well as to avoid the rather significant differences in interpretation and application that have occurred between EU Member States (which is one reason a Regulation is proposed instead of a Directive). See http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[40] Nyman-Metcalf (2014, pp. 28–30).

[41] Neither legal area is examined in detail in this article, as the size of the article does not permit that and in any case the interest in the current context is rather to point out the potentially relevant legal areas for analysis in the context of e-governance, not to actually conduct this analysis.

previously, with manual processing, would have been practically irrelevant as no sensible facts could be derived from it. ICTs can also create situations that allow for new types of violations of rights, like data protection rights.[42] Unsolicited communications is an issue that is different due to ICTs and needs attention in a different way that in the "non-e" world, related to the well-known area of consumer protection but with new issues[43] regarding protection of privacy and data protection.[44]

4.2 The Importance of Perception

In addition to the recognition that there may indeed be new situations—new types of information and thus new risks—another important factor is the perception of risk. People often mistrust new technologies and one reason people fear ICTs is the feeling of vulnerability of personal data. Caring about popular fears is not just something done to be nice to people: if there is a lack of uptake of e-governance solutions, these will be irrelevant, even if technically secure and efficient.

The danger people perceived with the gathering of data and identification online is that it may lead to identity theft.[45] Such perceptions cannot be ignored, regardless of whether real risks can be shown. There have been a number of high-profile cases of theft of identification details in recent years, most of these from commercial companies. As concerns private firms providing special security features as an element of secure e-governance, one issue to consider is that firms often have an interest in not reporting security breaches. This is bad for business, and it may be cheaper for firms to compensate customers than to make it very public that their systems are not secure—especially if there is a situation of developing novel solutions and attracting customers to these.[46]

The extent of identity theft varies a lot between countries, with those countries without solid identification systems—offline or online—evidently being most susceptible to such thefts; a danger that can be exacerbated with more electronic services whereas it is not shown that states with good identification systems and

---

[42] Gonzales Fuster et al. (2010, pp. 107–109).

[43] Examples include Directive 97/66/EC concerning Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector; Directive 2000/31/EC on Certain Legal Aspects of Information Society Services and Directive 2002/58/EC concerning Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.

[44] Nyman-Metcalf (2014, pp. 30–31).

[45] http://www.bbc.com/news/technology-18866347.

[46] Anandarajan et al. (2013, p. 53). The authors in their paper examine US legislation about data security breaches, comparing the laws of different states and making conclusions on what could be improved. The results are interesting and useful, but the limitation of legislation is the mentioned fact that if companies do not give required information, regulation cannot have its full intended effect.

practices in the pre-e world have suffered more identity theft after increasing electronic services. The problem appears to be more linked to ideological opposition to proper identification systems (for example in the UK).

Anandarajan, D´Ovidio and Jenkins state that "*Technology guards against crime by increasing the effort which offenders need to expend to reach their victims and carry out the crime*".[47] There are many ways in technology can guard against crimes, like firewalls to prevent illegal use of electronic data, filtering technologies, technologies to make illegal copying of copyright protected material more difficult and so on. However, technologies have to potential not only to guard against the increased risks that technology itself has brought about but also to make transactions safer in the electronic world than they can be in the traditional, paper-based world. The way in which transactions can leave a trace is one such example. This is very important from the data protection viewpoint and a feature of electronic databases that can be used to promote trust among the public.

Many breaches of the security of electronic data systems are due to non-electronic reasons like human error or carelessness.[48] Properly implemented electronic systems can help to prevent negative consequences by alerting to wrongful use.[49] When evaluating pros and cons of any new electronic system, the data protection aspect should be a key to the evaluation, establishing whether and how the system may interfere with data protection and as a second step, what safeguards are built into the system to avoid such risks or to keep any infringements within limits for what may be permitted and proportional.[50]

5 State Responsibility for Facilitating Access to e-Governance

5.1 The Relevance of ICT Law

Quite evidently, access to internet is a prerequisite for using e-services, whether public or private. The legal questions in this context are less evident, not least as they challenge division of roles in society. Simply put, there is a great responsibility on the internet service providers—who most often are private firms—as they are the link between the citizens and their possibility to communicate with

[47] Ibid. p. 53.

[48] Many examples can be seen at http://ico.org.uk/what_we_cover/handling_complaints.

[49] Anandarajan et al. (2013, p. 53).

[50] An example of such an evaluation is the "Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)" 18 July 2013. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18_Smart_borders_EN.pdf.

government. Private firms get a pivotal role concerning an essential underpinning of the functioning of the state and such responsibility must be executable. Regarding private services, it is a commercial decision for firms for example to determine when and to what extent to transfer to (only) online services and to ensure that people can use such services. As far as public services and e-governance are concerned, access to internet becomes a matter of concern for the state. The more a state makes use of e-governance, the more essential it becomes that the physical and actual access is guaranteed. It is no longer a matter just of internet access, but it must be of sufficient speed to allow for the use of services and be secure enough to prevent interruptions or loss of data.

Issues related to this are found in the field of law dealing with utilities,[51] like telecommunications,[52] and the issues are not new as such but similar to matters of universal service obligation—a well-known concept for utilities. Thus, there is a link between legal questions of e-governance and those of provision of essential facilities for e-governance: ICT law.[53] ICT law is close to competition law, indeed overlaps with competition law in many ways and/or can be seen as a branch of competition law to some extent: *lex specialis* to general competition law. e-governance shows the universal service obligation in a new light. This happens at a time when there is a discussion on whether the universal service obligation has a role to fulfil in a society with vigorous markets providing services without a need for regulatory intervention.

In the e-governance context, it is essential that the access to internet is real, meaning that just the possibility of physical access is not enough if people for some reason cannot use it. The reason may be cost or lack of knowledge. Suitable action is not easy to define as the level of personal involvement and preparedness of people themselves should play a part as well. If this is lacking, it is unlikely that a state can make many gains from introducing e-governance services as this system will just remain a parallel structure for some enthusiast. The facilitative role of law, as a means to affect behaviour, comes into the picture in this respect.

Determining whether and how to include facilitating e-governance as a factor in the ICT law discussion comes at a time of many changes to this area of law. New technologies and convergence of technologies have changed the traditional distinction between ICT and audiovisual media and also the terminology used for the laws: telecommunication law and broadcasting law have become ICT law and audiovisual media services law. Other challenges to communications regulation are posed by liberalisation and globalisation.[54] Although liberalisation and privatisation are often used together, they are different concepts with privatisation relating to ownership whereas liberalisation means allowing competition. The first

[51] Nitsche and Wiethaus (2012, pp. 409–414).

[52] Nikolinakos (2006, p. 181).

[53] De Muyter (2012, pp. 453–454).

[54] Walden (2001, pp. 2–5).

private telecommunications operator in Europe was in the UK in 1986,[55] so the process is quite new everywhere in Europe (not just in Eastern Europe that has experienced a lot of privatisation recently). Although the situation in the USA is different with a longer history of private operators, in much of the rest of the world the liberalisation process is rather recent and/or ongoing.

5.2 Competition Law

Aspects of competition law that are important in the communications field include the issue of undertakings given special rights (in the EU, Article 106 of the Treaty on the Functioning of the EU): competition should be limited only to the extent this is needed given the special nature, like universal service obligation.[56] This obligation aims to ensure access for all at affordable prices and the quality and availability of the service at all times. The influence of the universal service obligation should be limited, so there is no over-compensation, but compensation for real costs—allowing reasonable profit—for needed services.[57] What services are needed and to what extent is a matter in constant evolution to which increased e-governance can add an aspect. The promotion of new technologies may involve state aid, special rights or other measures to influence the market—if this is necessary.[58]

Utilities include apart from communications also energy, gas, water, post and others. Another special issue for such services is that they are dependent on networks: it is not possible to compete unless you have access to the network and it is not feasible for all operators to have their own networks. This is why the regulator must ensure interconnection and access to networks even if this should primarily be decided by the sector participants through negotiations and agreements between the parties. However, it will be ensured by the regulator, who will step in if the parties cannot agree, to make sure an agreement is reached and to solve any disputes.[59] Linked to this, in many instances, tariffs will be set or monitored by the regulator.[60] The law must give a clear mandate to the regulator for such work as it is interference with the business of private operators.

Market failure of a utility may have extra great effects, so there may be ways permitted to protect against this. In the e-governance, context in the extreme case failure of a service provider can mean inability to access e-governance services.

---

[55] Long (1995, p. 26).

[56] Case C-320/91 Corbeau and Case C-280/00 Altmark, European Court of Justice.

[57] Nihoul and Rothford (2004, pp. 596–597).

[58] Quigley (2009, pp. 319–320).

[59] Nikolinakos (2006, pp. 236–237).

[60] Nihoul and Rothford (2004, p. 396).

Utilities are often natural and historic monopolies, so it is likely there will be dominant firms or at least firms with significant market power. The existence of such firms from the competition viewpoint means that the pricing of both services and market access must be monitored and may be regulated. There may be an obligation to enter into contracts, both for consumers/users (given the essential nature of the services) and the competitors (for market access). In addition, there may be ownership restrictions to avoid concentrations and accounting rules with bans on cross-subsidising as well as special transparency requirements.[61] All this must work as a necessary backdrop against which e-government can be developed.

Issues of ICT law are rarely formulated academically or practically as questions linked to e-governance, but with the increasing importance of both areas such connections are likely to be more prevalent. The topical discussion on network neutrality is one such issue that has bearing on e-governance, as a development toward differentiation between conditions for different users of internet would lead to a need to evaluate how e-governance shall be seen in this context. Network neutrality is the expression used for the discussion on whether operators should have the right to apply different conditions to different users of their infrastructure or whether that would undermine the freedom of the internet and generally the principles that have made internet such a success.[62] Given the importance of e-governance, should this mean a right of priority for any e-governance services and should the internet service providers "subsidise" this activity through charging more from other users to keep the cost down for public e-services? What should be the situation if private firms provide e-services of a public nature or of public use, or indeed if services are "dual use"?

6 Concluding Remarks

Governments looking to introduce e-governance or academics researching it often ask the countries that have already introduced e-governance on a more advanced level to share their e-governance legislation or to provide information about costs of e-governance. Such apparently simple questions are not easy to answer, as a sign of successful e-governance is actually the absence of special laws or a defined cost just for e-governance. The aim should be that e-governance is an integral part of the governance of the state, helping to make all aspects of it more efficient, secure and user-friendly. To achieve this, it needs to be incorporated into most areas of law preferably in as seamless a manner as possible. At some point, e-services will replace traditional services but this when this point in time will occur cannot be predicted with certainty, as it depends on whether people not just have the (physical and practical) ability to use e-services but indeed do also use them.

---

[61] Nikolinakos (2006, p. 392).

[62] Schejter and Yemini (2007, p. 138).

In Estonia, in 2012, over 94 % of tax declarations were submitted via the electronic system,[63] the number is thought to have risen since. With such high numbers, it may be considered if other ways to submit should be maintained, but it is important even if just a fraction do not use the e-service to think also of these people. If other than electronic ways to submit something are abolished, there can for example be targeted assistance to people who have problems using the new methods. It is a delicate balance for a state to what extent it obliges its citizens to adapt and use new methods or if it leaves it entirely up to people to choose. Means of persuasion can be used, like in Estonia those who submit their tax declaration electronically get any refunds several months earlier than those who submit on paper. Internet banking uses similar incentives with less cost and faster transactions. It cannot be said to violate principles of good administration to change service delivery in a state, not just linked to ICTs but generally. States must be allowed to introduce reforms even if they are not universally liked. At the same time, the speed of change in modern society means that there is a real risk that some people are left behind, which a responsible democracy should prevent. Changes may prevent people from actually accessing the services and in such a case all the potential benefits of e-governance are not only not realised but new problems introduced. The transition to e-governance must be made in a suitable manner and at a suitable time, supported and enabled by the legal framework.

Concerning e-governance, the fact that services are not available without access to the necessary infrastructure should not be forgotten. Internet must be fast and secure enough to allow for all sorts of transactions, and it must be available to people at reasonable terms. This does not mean it has to be free, but its cost must be acceptable if people are to use e-services. Internet is the same whether used for public or private services, so there is a good opportunity to engage the private sector and make it cover some costs. There are many possibilities for this, whether by using the same certification services and security systems for, e.g., banking and government services or encouraging internet service providers (or other companies) to provide inexpensive or even (partially) free internet access. Cleary, the new e-environment for governance should inspire to new solutions not just on the technical side.

For people to embrace e-governance, they need to have trust in the services provided in a new way. The way to identify oneself electronically needs to be secure but at the same time user-friendly. Authorities need to be approachable and responsive electronically. When new ways of doing things, for example with e-signatures, are introduced, it should be possible to use such new means effectively. These statements underline that what is needed from the legal side is not complicated technical legislation (the presumed complexity of which may be the reason lawyers largely keep away from the e-governance topic!), but an overview of legislation to ensure that e-services are integrated, attention to e-signatures and other e-identities as well as attention to data protection.

[63] http://estonia.eu/about-estonia/economy-a-it/e-estonia.html.

References

Anandarajan, M., D´Ovidio, R., & Jenkins, A. (2013). Safeguarding consumers against identity-related fraud: Examining data breach notification legislation through the lens of routine activities theory. *International Data Privacy Law, 3*(1), 51–60.

Brazell, L. (2004). *Electronic signature law and regulation*. London: Sweet & Maxwell.

Brownsword, R., & Goodwin, M. (2012). *Law and the technologies of the twenty-first century*. Cambridge: Cambridge University Press.

Dawes, S. S., & Pardo, T. A. (2002). Building collaborative digital government systems. Systematic constraints and effective practices. In W. J. McIver & A. K. Elmagarmid (Eds.), *Advances in digital government. Technology, human factors, and policy* (pp. 259–273). Norwell: Kluwer Academic Publishers.

De Muyter, L. (2012). Regulatory asymmetry? The competition between telecommunication operators and other ICT players. *Journal of European Competition Law & Practice, 3*(5), 452–464.

Dickie, J. (2005). *Producers and consumers in EU e-Commerce law*. Oxford: Hart.

Edwards, S. (Ed.). (2005). *The new legal framework for e-Commerce in Europe*. Oxford: Hart.

Garson, G. D. (2003). *Public information technology: Policy and management issues*. Harrisburg: Idea Group Publishing.

Gil-Garcia, R. (2005). *Enacting state websites: A mixed method study exploring e-government success in multiorganizational setting.* In Proceedings of the 39th Hawaii International Conference on System Sciences—2006 http://www.ctg.albany.edu/publications/journals/hicss_2006_enacting/hicss_2006_enacting.pdf.

Gonzales Fuster, G., Gutwirth, S., & de Hert, P. (2010). From unsolicited communications to unsolicited adjustments. In G. Gutwirth, Y. Poullet, & P. de Hert (Eds.), *Data protection in a profiled world* (pp. 105–117). Dordrecht: Springer.

Hanna, N. K. (2008). *Transforming government and empowering communities. The Sri Lankan experience with e-development*. Washington D.C: The World Bank.

Laudon, K. C., & Guercio Traver, C. (2013). *e-Commerce: Business, technology, society*. Boston: Pearson.

Long, C. D. (1995). *Telecommunications law and practice* (2nd ed.). London: Sweet & Maxwell.

Malkawi, B. H. (2007). e-Commerce in light of international trade agreements: The WTO and the United States-Jordan trade Agreement. *The International Journal of Law and Information Technology, 15*(2), 153–169.

Mason, S. (2003). *Electronic signature in law*. London: LexisNexis UK.

Morgan, B., & Yeung, K. (2007). *An introduction to law and regulation. Text and materials*. Cambridge: Cambridge University Press.

Nihoul, P., & Rothford, P. (2004). *EU electronic communications law. Competition and regulation in the European telecommunications market*. Oxford: Oxford University Press.

Nikolinakos, N. Th. (2006). *EU competition law and regulation in the converging telecommunications, media and IT sectors*. Alphen aan den Rijn: Kluwer Law International.

Nitsche, R., & Wiethaus, L. (2012). Competition law in regulated industries: On the case and scope for intervention. *Journal of European Competition Law and Practice, 3*(4), 409–414.

Nyman-Metcalf, K. (2014). The future of universality of rights. In T. Kerikmäe (Ed.), *Protecting human rights in the EU* (pp. 21–35). Heidelberg: Springer.

OECD. (2011). *Modernising public administration: The case of e-government in the palestinian authority*. Paris: OECD.

Quigley, C. (2009). *European state aid law and policy* (2nd ed.). Oxford: Hart Publishing.

Reed, C. (1996). *Digital information law: Electronic documents and some requirements of form*. London: Queen Mary & Westfield College.

Schejter, A. M., & Yemini, M. (2007). Justice, and only Justice, you shall pursue: Network neutrality, the first amendment and John Rawl´s theory of justice. *Michigan Telecommunications and Technology Law Review, 14*, 137–174.

Schneiberg, M., & Bartley, T. (2008). Organizations, regulation, and economic behavior: Regulatory dynamics and forms from the nineteenth to twenty-first century. *Annual Review of Law and Social Science, 4*, 31–61.

Spindler, G., & Börner, F. (Eds.). (2010). *e-Commerce law in Europe and the USA*. Berlin: Springer.

Walden, I. (2001). Telecommunications law and regulation: An introduction. In I. Walden & J. Angel (Eds.), *Telecommunications law* (pp. 1–15). London: Blackstone Press.

Wang, M. (2006). The impact of information technology development on the legal concept—a particular examination on the legal concept of 'signatures'. *International Journal of Law and Information Technology, 15*(3), 253–274.

Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience over Six Elections

Ülle Madise and Priit Vinkel

Abstract Remote Internet voting has been allowed in Estonia since 2005 in all types of public elections. The share of online voters has risen to 20–25 %. According to surveys, Internet voting slightly increases general voter turnout, contrary to common expectations does not favor well-educated young urban population and is politically neutral. Significant factors predicting the use of Internet as a voting channel are computer skills and trust. The constitutionality of online voting and of postal voting lends itself to similar analysis with the exception of Internet as a channel. We argue that Internet voting is constitutional, if reliable remote authentication, electronic voter roll, and control mechanisms preventing from any kind of manipulation are in place: the I-votes must be cast as intended, stored as cast, and counted as recorded. In an advanced information society, online voting could be even seen as a required means of guaranteeing universal suffrage and voting equality. On the other hand, the impact of remote e-services on human psychology and behavior needs further research. The results of such scholarly work might lead to new arguments in legal analysis as well.

1 Introduction

Estonia is credited as a front-runner country in matters of e-governance with its universal electronic key to all e-services (e-ID), digital signature, e-Health, e-taxboard, etc. According to the latest *Global Information Technology Report 2013*,

Ü. Madise (✉)
Institute of Constitutional and International Law, University of Tartu, Tartu, Estonia
e-mail: ylle.madise@ut.ee

P. Vinkel
Ragnar Nurkse School of Innovation and Governance, Tallinn University of Technology, Tallinn, Estonia
e-mail: priit.vinkel@ttu.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_4

Estonia ranks as the highest Central and Eastern European country, in 22nd place.[1] The use of electronic means for claiming different services has steadily risen in the country, and a large amount of e-services are provided both by the public and the private sectors. About 77 % of Estonian inhabitants aged 16–74 use regularly Internet and 80 % of households have access to the Internet.[2]

While, in many states, the first step toward some form of electronic vote was to use voting machines in polling stations in order to facilitate voting or counting, in Estonia, from the beginning, there was the aim of creating conditions for public and accessible remote Internet voting. Similar projects of introducing binding remote electronic voting for general elections have evolved the most in Switzerland[3] and Norway,[4] but also in Catalonia, United Kingdom, Finland, Canada, and other.[5]

I-voting has stood beside a number of other voting methods in Estonia since 2005.[6] For six times, Estonian voters have had the choice of casting a paper vote or vote over the Internet at parliamentary, municipal, and European Parliament elections.

The declared aim of the launching of online voting in Estonia was to increase voter turnout, which perhaps could be described more realistically as widening access possibilities and stopping the decrease in participation, especially among younger voters.[7] The participation rate at local government council elections in Estonia is usually ~50 % and at parliamentary elections ~10 % higher. Voter turnout never exceeded 70 %, even at the 1992 constitutional referendum. By facilitating electoral participation, it seemed likely that voter turnout, and hence the overall legitimacy of the results, would improve.

Another reason behind the I-voting project was the wish of exploiting the existing infrastructure more efficiently. The widespread use of the national e-ID card was vital for starting the Internet voting project, as only e-ID card owners had the option of voting through the Internet. In 2012, the national ID card celebrated its 10-year anniversary and currently 1.2 million people possess a valid ID card, of those 85 % are Estonian citizens; thus, most of the eligible voters (~1 million) hold the card.

Moreover, according to some commentators, an important factor explaining the possibility to launch totally new solutions like I-voting in Estonia is the smallness of the country.[8]

---

[1] See the World Economic Forum (2013).

[2] As shown by Eurostat (2013).

[3] They have had numerous trials both on cantonal and federal levels. For an overview, see Maurer et al. (2012) and Gerlach and Gasser (2009).

[4] Norway has used Internet voting in two elections. See the OSCE report on Norwegian parliamentary elections 2013 at http://www.osce.org/odihr/elections/109517.

[5] The concept on electronic voting harbors both machine e-voting and remote Internet voting. An overview of the use cases can be found in Barrat et al. (2012).

[6] For a complex overview of Estonian elections after the restoration of independence, see Heinsalu et al. (2012).

[7] See Drechsler and Madise (2004).

[8] For context, see Kalvet (2012) and Kattel et al. (2011).

2 Starting Out

In 2001, discussions among political and academic groups started about whether or not Estonia should introduce Internet voting. At the same time, the Ministry of Justice announced intentions to introduce Internet voting as soon as possible.

A political agreement was reached in 2002, and in 2003, the National Electoral Committee (NEC) started the electronic voting project. At the beginning of the project, the NEC involved as many IT security specialists as possible to elaborate a commonly acceptable approach and, thereby, raise public trust in Internet voting. Good cooperation between different parties, public or private, was crucial in launching the successful and apolitical I-voting project.

I-voting project's executive group was formed by NEC, a project manager was elected, and the roles between the NEC, executive group, and project manager were distributed. In accordance with the project organization, the NEC approved the more relevant decisions. The task of the executive group was to make proposals and recommendations to the NEC and control the achieving of set objectives. The project manager was in charge of the implementation of the project, and he summoned project groups formed by experts upon necessity, directed their work, and checked the results.

At this stage, the I-voting concept was essentially complete. After that, the security analysis of the concept was carried out by a working group formed of IT security specialists. Proceeding from the recommendations of the security analysis, changes were made to the concept and the document entitled General Description of Estonia's E-Voting Project was presented.[9]

Early in 2004, the technical description of the I-voting software was produced. In March 2004, three tenders were submitted and the NEC chose the Cybernetica Ltd as a software developer, a cooperation that has lasted until today. In autumn, the software was ready for the first public pilot. The pilot offered the possibility of I-voting in a Tallinn residents' poll, it took place in January 2005. About 703 voters were participated, and 697 votes were counted. The system worked without failures. After the pilot was completed, the I-voting system seemed in place and ready to be used in the local elections of autumn 2005.[10]

3 Laying the Legal Ground

3.1 Parliamentary Debates About I-Voting

The scope of the parliamentary debate before launching I-voting was quite wide, ranging from clear ideological questions to detailed technological issues.[11] The most discussed question was the exact meaning and purpose of the principle of

[9] Latest version available at www.vvk.ee.

[10] For detailed elaboration of project management, see Madise and Maaten (2010).

[11] See about the genesis of the Estonian I-voting project with references to the minutes of *Riigikogu* plenary sessions, party structure, etc., in Drechsler and Madise (2004).

secrecy. Other important questions were the digital divide and the value of the ritual of walking into a polling station.

In Estonia, as well as in many other countries that have created and allowed remote voting possibilities (e.g., postal voting), advance voting, and other supplementary voting methods to meet contemporary mobile voters requirements, voting at a polling division has virtually lost its significance as a ritual transforming people into a nation-state and the carriers of sovereign nationhood.[12]

In the discussion about the introduction of I-voting, classical arguments about conformity of the I-voting with the principles of fair elections including the reliability of electronic voting systems were changed, whereby one of the arguments against I-voting was that people who have no commitment neither to prepare themselves for election nor go to the polling station to execute their citizen's duty should not participate in governing at all,[13] which contradicts the axiom that the higher the turnout, the better.[14] Indeed, the discussions were dominated by clear liberal democracy approach in the way as Robert A. Dahl puts it: if we accept the desirability of political equality, then every citizen must have an equal and effective opportunity to vote and all votes must be counted as equal. Viable democracy requires not only constitutional right to vote but also factual freedom of information and expression, civic education, etc.[15]

The principles of free and fair elections—especially universal suffrage and equality—cannot be followed if electoral administration is not adapted to changes in the society.

The legislative process in the Estonian parliament concerning Internet voting has had three stages. In 2002, only the concept of remote voting possibility was adopted. The main idea was to have enough in the law to guarantee public funding for the early-stage project. In 2005, right before the first implementation at the local government council elections, detailed provisions were entered into electoral acts. In 2012, after five cases of using Internet voting in different elections, more precise and accustomed regulations based on the previous experience were adopted. Additionally, the concept of verification was introduced.

It is likely that while deciding whether to support electronic voting, political parties took into account the potential effect of remote Internet voting over their election results. Parties suppose that I-voting brings persons to vote who would by traditional means not participate, and additional votes will not be distributed proportionally among political parties. So it seems likely that increased turnout changes the share of votes between political parties.[16] Of course, such kinds of considerations contradict the principle of universal suffrage and are rare if at all

[12] About the importance of the voting ritual, see, e.g., Monnoyer-Smith (2006).

[13] For reasons of the attitude that it might be better for democracy if some of votes were not cast at all, see, e.g., Buchstein (2004, p. 55).

[14] Explaining electoral turnout is never a simple task, see, e.g., Rolfe (2012).

[15] Dahl (1998, p. 80 and p. 95).

[16] See Madise (2008).

publicly exposed. One hint to calculations of that kind could be the condition added to electoral legislation that I-voting cannot be launched before the year 2005. In 2003, Estonian people voted in a referendum on EU accession.

3.2 Teleological Interpretation of the Principle of Secrecy

According to the Estonian Constitution, members of the *Riigikogu*, as well as local government councils shall be elected in free, general, equal and direct elections, and voting shall be secret.[17] The same principles apply to European Parliament elections. There is no special regulation for I-voting in the constitution.

The secrecy of voting has traditionally been viewed in Estonia as the right and obligation to cast one's vote alone in a voting booth. In the case of Internet voting, the state is not in a position to secure the privacy aspect of the procedure. Legislators proceeded from the interpretation of the constitution according to which secrecy of voting; drawing on its two subprinciples—private proceeding of voting and anonymity of vote—is required to ensure free voting and is not an objective per se.

The voter's right to anonymity during the counting of the votes is guaranteed to the extent to which this can be secured in the case of absentee ballots by mail; the so-called system of two envelopes used for absentee ballots by mail is both reliable and easy to understand for I-voters (see Sect. 5.2).

Remote Internet voting requires rethinking the privacy principle. The principle of privacy is there to protect an individual from any pressure or influence against her or his free expression of political preference. Such teleological approach to the constitution was the basis of the I-voting provisions from the very beginning of the whole project. In addition to the teleological interpretation of the constitution, the Ministry of Justice, led by the liberal Reform Party, based provisions enabling Internet voting on the premise that the state has to trust the individual and avoid, whenever possible, interference with decision making at the individual level. The individual has to be aware of risks, i.e., technical risks, and he or she has to have the right to decide whether or not to use the Internet voting opportunity.[18]

This teleological interpretation of the principle of secrecy is clearly divergent from the traditional approach generally adopted in the scholarly literature. For instance, Buchstein[19] remarks that

> Mandatory secrecy is a principle which goes beyond constitutional law, its fundaments are based on the idea of auto-paternalism and it is understood as a mechanism of self-binding of autonomous citizens in order to avoid situations of external pressure or corruption. In this concept, it is not the individual him- or herself, but a warranted outside agent or authority – normally the state – that is responsible for providing the necessary means to allow for the secret ballot.

[17] Articles 60 and 156.

[18] See Drechsler and Madise (2004).

[19] In Buchstein (2004).

> Indeed, in many countries, the privacy of voting act is not required nor protected in such a strict way: the voters are not required to hide their choice and traditionally they do not; in some countries, proxy voting is allowed.

In Estonia, unlike in some countries, the fact whether a person entitled to vote did participate in voting or not is not regarded as a part of the principle of secrecy. The voter lists that contain information about participation and chosen voting method (voting on voting day or advance vote in or outside polling stations of one's place of residence, in case of advance vote paper ballot or I-vote) are preserved in an archive and can be used for research purposes. Researchers have made use of this possibility, including for the I-voting survey, what unfortunately weakened somewhat the public trust against I-voting. The fact that the official questioner had knowledge about the actual fact of I-voting made some people suspect about the secrecy of their voting decision. These suspicions were discussed in public media but due to satisfying explanation, the common trust was not harmed.[20] The explanation was that voters' lists have always had the stated information about who participated and what voting method was used. The voting decision itself has always been and will remain secret. There is no possibility to obtain any knowledge about how the voter voted.[21]

3.3 Virtual Voting Booth as a Required Guarantee for Free Elections

In order to guarantee the freedom of voting, I-voters were granted the right to replace the vote cast on the Internet by another I-vote or a paper ballot. However, this could be done only within the advance polling days. In case of several I-votes, only the last one is counted; in case of contest between I-vote and paper ballot, the paper ballot was counted. If several paper ballots are cast, all votes are declared invalid. Thus, the "one vote—one voter" principle is ostensibly guaranteed.

This approach caused perplexity among the audience of the report presented by Madise at the Worldwide Forum on e-Democracy in Paris in 2001, and even in 2005. However, at the International Seminar held in Bregenz in 2006, Norwegian scholars remarked *inter alia* that they had arrived at similar principles before obtaining detailed knowledge about the Estonian Internet voting system[22] and expressed clear support for the vote replacement aspect of this idea.

---

[20] The survey results are encompassed in the Council of Europe study report accessible here: http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/evoting_documentation/PDF-FinalReportCOE_EvotingEstonia2005.pdf.

[21] Due to the technical and procedural aspects explained in Chap. 4.

[22] See Skagestein et al. (2006).

Some months before the municipal elections in 2005, the President of Estonia brought I-voting provisions to the Supreme Court for constitutional review, arguing that the possibility to change I-votes gives advantages to I-voters in comparison with non-I-voters. I-voters can change their vote for an unlimited number of times but only during I-voting and advance poll days. The initial version of the I-voting law contained the possibility to change the I-vote with a paper ballot on the actual voting day. This provision was left out of the law, because this could have given real advantage to I-voters: they would have had the chance to change their election preference on Sunday after receiving additional information about candidates in the second half of the week. All voters who use advance poll possibilities (either paper- or I-voting) were now formally in the same conditions.

The Supreme Court Chamber of Constitutional Review pointed out that despite "virtual voting booth," there was no possibility of the voter affecting the voting results to a greater degree than those voters who used other voting methods. From the point of view of the voting results, this vote was in no way more influential than the votes given by paper ballot. According to the Estonian Election law, each voter shall have one vote.

The court said that this interpretation renders the principle of uniform elections a special case of the general right to equality. In the legal sense, I-voting is equally accessible to all voters. The ID card necessary for I-voting is mandatory for all inhabitants of Estonia; thus, the state has created no legal obstacles for anyone to I-vote, including to changing one's vote during the advance poll days. It is a fact that due to factual inequality the possibility to change one's vote through I-voting is not accessible to all voters can be regarded as an infringement of the general right to equality and the principle of uniformity.

The principle of equal treatment in the context of electing representative bodies does not mean that factually equal possibilities for performing the voting act in equal manner should be guaranteed to all persons entitled to vote. In fact, those who use different voting methods provided by law are in different situation. The guarantee of absolute actual equality of persons upon exercising the right to vote is infeasible in principle and not required by the constitution. The aim to increase voter turnout is without any doubt legitimate. The measures the state takes for ensuring the possibility to vote for as many voters as possible are justified and advisable. Another aim of allowing I-voting is the modernization of voting practices that coincides with the aims of I-voting listed in the OSCE Recommendation.[23]

According to the opinion of the Supreme Court of Estonia, the principle of freedom of vote gives rise to the obligation of the state to protect voters from persons attempting to influence their choice. With regard to that principle, the state has to create the necessary prerequisites to carry out free polling and to protect voters from undesired pressure while making a voting decision. In paragraph 30 of the aforementioned judgment, the Supreme Court maintains the following:

[23] Rec (2004).

> The voter's possibility to change the vote given by electronic means, during advance polls, constitutes an essential supplementary guarantee to the observance of the principle of free elections and secret voting upon voting by electronic means. A voter who has been illegally influenced or watched in the course of electronic voting can restore his or her freedom of election and the secrecy of voting by voting again either electronically or by a ballot paper, after having been freed from the influences. In addition to the possibility of subsequently rectifying the vote given under influence, the possibility of voting again serves an important preventive function. When the law guarantees a voter, voting electronically, the possibility to change the vote given by electronic means, the motivation to influence him or her illegally decreases. There are no other equally effective measures, besides the possibility of changing the vote given by electronic means, to guarantee the freedom of election and secrecy of voting upon electronic voting in an uncontrolled medium. The penal law sanctions have a preventive meaning but subsequent punishment - differently from the possibility of changing one's electronic vote - does not help to eliminate a violation of the freedom of election and secrecy of voting.[24]

The Supreme Court thus confirmed the constitutionality of one of the main premises of the remote Internet voting project. The concept of teleological approach and acceptance of the used methods of I-voting has stood the bar also in subsequent cases in the Estonian Supreme court.[25]

3.4 Second Round of Parliamentary Debates: Stored as Intended Verification of I-Votes from 2015

As in 2011 the percentage of I-votes had risen to almost a quarter of valid votes, Parliament decided to specify the norms of I-voting in electoral laws in order to improve the legitimacy and transparency of I-voting. Until 2011, the I-voting procedures had only very brief legislative regulations. Parliament established a working group that, in addition to detail procedures, had to propose a solution, how to raise auditability and how to verify the correctness of I-votes.

At the same time, technical community, which has been involved by NEC in discussions about the security of I-voting, came to conclusion that a new mechanism for some level of verification is needed, in order to detect malicious attacks on the I-voting system. NEC and electronic voting committee (EVC) have better options to discover attacks and react to those if I-voters, even a relatively small amount of them, verify their votes. If somebody finds out and reports to NEC or EVC that his/her vote is not stored correctly, measures could be taken immediately. If voters would only have access to their personal computers and use them for verification, no security could be achieved at all. Therefore, some independent

---

[24] Chamber of Constitutional Review of the Estonian Supreme Court, Decision Nr 3-4-1-13-05. See http://www.nc.ee/?id=11&tekst=RK/3-4-1-13-05 (in Estonian).

[25] Namely cases 3-4-1-10-11 from March 31, 2011, see http://www.nc.ee/?id=11&tekst=RK/3-4-1-10-11 (in Estonian) and 3-4-1-4-11 from March 21, 2011 http://www.nc.ee/?id=11&tekst=RK/3-4-1-4-11 (in Estonian).

channels like mobile phones or mobile devices, which are easily accessible by the voters, are needed for verification.[26]

In the end of 2012 Parliament adopted, the amendments to the electoral law stating that a new electoral committee—EVC—to be created for technical conducting of I-voting. The first elections where the EVC was active were 2013 local elections. The law also regulates that before every implementation the I-voting system must be tested and audited. Most significant change in the law was the statement that from 2015, voters have to have possibility to check that their vote has reached and is stored at the central server of elections and reflects the choice of the voter correctly.

4 Technical Solution and Practical Experience

4.1 e-ID Card as an Universal Access Key to e-Services

Some of the biggest challenges in the sphere of e-Government are the reliable remote identification and authentication of citizens.[27] Simple password-based authentication methods are not secure enough.[28] Estonia chose the electronic ID card as main authentication tool. Although many states across the world already have some form of identity card schemes in place, few are based on electronic cards. However, in Estonia ID card, enabling secure personal authentication and digital signing, as well as the public key infrastructure (PKI) necessary for using ID cards electronically, had been developed already by the end of 2001.

Issued by the Estonian Government since January 2002, national ID cards represent the primary source of personal identification for people living within Estonia and are mandatory for all citizens and resident aliens above 15. The ID card carries two functions: physical identity as a regular ID and electronic identity that enables citizens to use the same card to electronically authenticate to Web sites and networks, and/or digitally sign communications and transactions as required.

Each card contains two discreet PKI-based digital certificates—one for authentication and one for digital signing. The certificates contain only the holder's name and personal code and have two associated private keys on the card, each protected by a unique user PIN. The certificates contain no restrictions of use: they are by nature universal and meant to be used in any form of communications, whether between private persons, organizations, or within the government. As mentioned before, the card can be also used for the encryption of documents so that only the person intended to view the document can decrypt it. This is an efficient means for secure transfer of documents using public networks. In addition to that, each ID card contains all data printed on it also in electronic form, in a special publicly readable data file.

---

[26] See Heiberg et al. (2010).

[27] See also Chap. 3 in Nyman-Metcalf (2014).

[28] See also Heiberg et al. (2012).

In 2007, a new e-ID solution was brought to the Estonian market: the Mobile-ID, where the mobile telephone (via its SIM card) acts as an ID card and a card reader at the same time. In addition to having the functionality of an ordinary SIM, a Mobile-ID SIM holds a person's certificates that enable providers of Internet services to identify the person and issue digital signatures. From 2011, Mobile-ID certificates have governmental guarantee and the solution can be used in Internet voting.[29]

4.2 Technical Measures Used to Ensure Voting Secrecy

One of the main interests of those interested in the security of Internet voting systems is the obvious contradiction of security and secrecy properties. On one hand, the votes must remain anonymous. On the other, voters must be identified in order to guarantee that only the eligible voters are able to vote and that they vote only once.

In order to understand how the I-voting system guarantees the secrecy and singularity of vote, we should describe shortly the envelope voting method used in Estonia for advance paper voting.[30] The latter gives the voter possibility to vote outside the polling station of the voter's residence in any rural municipality or city. A voter presents a document to be entered in the list of voters and then receives the ballot and two envelopes. The inner envelope has no information about the identity of the voter, and the ballot paper is put in it. The inner envelope is put into an outer envelope and the voter's details are written on it, so that, after the end of the advance poll, the envelope could be delivered to the voter's polling station of residence. There it is verified whether the voter has the right to vote; then, the inner envelope is taken out and put unopened into the ballot box. The two-envelope system guarantees that the voter's choice remains secret. Additionally, recording the data about envelope I-voting in the list of voters in the polling station of residence prevents voting more than once (Fig. 1).

Upon I-voting, a voter makes her or his choice, which is encoded (placed in a virtual inner envelope). Thereafter, the voter shall approve the choice through his or her digital signature, which means that personal data are added to the encoded vote (the outer envelope). The personal data and the encoded vote are stored together until the counting of votes on Election Day, with the aim of ascertaining that the person has given only one vote.

The personal data of a voter and the vote given by the voter are separated after the fact that the voter has given only one vote has been checked and repeated votes

[29] See also Heiberg et al. (2012), and for the statistical use of mobile-ID in elections, see http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics/.

[30] A system very similar to the advance voting procedure in Sweden (see http://www.val.se/pdf/Elections_in_sweden_2014_webb.pdf) and Finland (see http://www.finlex.fi/fi/laki/kaannokset/1998/en19980714.pdf).

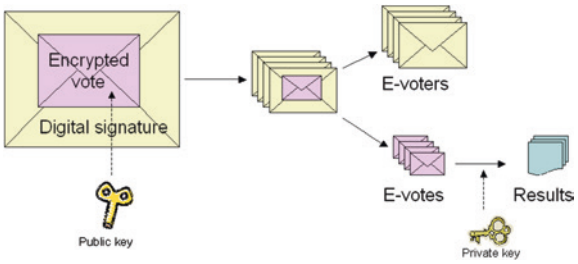

Fig. 1 Double-virtual envelope PKI-based method for I-voting

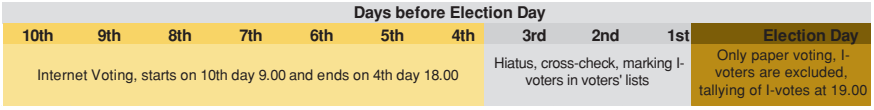

Fig. 2 I-voting event cycle

have been eliminated. It is then possible to open the inner envelope only after the personal data added to the encoded vote have been separated.

I-voting, like voting outside the polling station of residence, is possible only during advance polls. This is necessary to guarantee that, in the end, only one vote is counted for each voter. During the I-voting process, the voter's right to vote is checked. If the voter makes use of the possibility to replace his or her I-vote by paper ballot during the advance poll, then it has to be guaranteed that finally only one vote is counted. For that, all polling stations are informed of the I-voters on their voters' rolls after the end of advance polling and before the Election Day on Sunday. If it is found at the polling station that the voter has voted both electronically and with paper ballot, the information is sent to the central system and the voter's I-vote is cancelled by the EVC (Fig. 2).

Before the tallying of voting results in the evening of the Election Day, the encrypted votes and the digital signatures with personal data or inner and outer envelopes are separated. Then, all I-votes are opened by the EVC and counted. The system opens the votes only if they are not connected to any personal data.

4.3 System Architecture

The Estonian IT security experts in their security analysis[31] published in 2003 declared that in *practical sense* the Estonian I-voting system was secure enough for implementation. In absolutely secure systems, unexpected events are not

[31] Available at www.vvk.ee.

possible. One may dream about such systems, but they can never be achieved in practice.[32] This applies particularly to I-voting systems. Considering the security level of personal computers, it is impossible to design I-voting systems, which are absolutely secure for every user. The most important security goal of voting is not to affect the final results and not to abuse the principles of democracy. The single incidents with users are still important, but they do not have influence to the final result. Moreover, even in traditional voting systems, small-scale incidents are acceptable.[33]

I-voting part in the whole process of organizing elections is relatively small. The system uses existing information systems—population register as basis for voters' lists,[34] election information system of the NEC for the collection and publication of information on candidates, and voting results and the infrastructure of Certification Centre Ltd for checking the validity of the ID card certificates.

The main components of the Estonian I-voting systems are a stand-alone voter application for casting the vote; the vote forwarding server; the vote storing server; the vote counting server; and the monitoring (log-file) server.[35]

Asymmetric cryptography is used to guarantee the secrecy of votes. A pair of keys is generated for the system in a special hardware security module so that its private component never leaves it. The public component of the pair of keys is integrated into the voter application and is used to encrypt the votes. The private component of the pair of keys is used in the vote counting application to open the votes on the end of the Election Day. The NEC can decrypt the votes, i.e., use the private component, only collegially. After the end of the period of dealing with possible complaints, the private key is destroyed.

4.4 Users' Perspective

The Internet voting system takes advantage of the existing infrastructure and governmental databases. To vote electronically, a voter does not need to register himself or herself additionally. The voter needs an ID card and a computer connected to the Internet and with an installed card reader (not necessary if using Mobile-ID). The voter also needs PIN codes for authentication and signing. He can use the same tools for other transactions, including governmental e-services and Internet banking.

---

[32] As stated by Mägi (2007).

[33] See also Madise and Martens (2006).

[34] In Estonia, voters' lists are generated based on Population Register data, no separate registration procedures are necessary.

[35] More on the technical structure of the system can be found in the General Description (2010) at http://www.vvk.ee/voting-methods-in-estonia/engindex/reports-about-internet-voting-in-estonia/ and various technical documents (in Estonian) at http://www.vvk.ee/valijale/e-haaletamine/e-dokumendid/.

From the user's perspective, the voting procedure looks like this:

1. The voter opens the voting page www.valimised.ee.
2. The voter must choose how to identify him/herself (by using an ID card or Mobile-ID).
3. After that, voter inserts the ID card into the universal card reader and inserts PIN1 of the ID card or enters PIN1 on the mobile phone in case of Mobile-ID.
4. The server checks whether the voter is eligible (using the data from the population register).
5. The candidate list of the appropriate electoral district is displayed.
6. The voter makes his/her voting decision; the system encrypts it.
7. The voter confirms his/her choice with a digital signature by entering PIN2 of the ID card or Mobile-ID. The system checks whether the same person who authenticated him/herself during the start of the session gave the according digital signature. Also, the validity of the digital signature is confirmed by the validity confirmation server.
8. The system confirms that the vote has been stored in the vote storing server.

In the 2013 municipal elections, the NEC and EVC ran a pilot on verification: for the first time, voters had the possibility to verify whether their I-vote arrived in the central server as intended. In order to check the vote, voter must have a smart device (mobile phone or a tablet) that has a camera, Internet connection, and a special application downloaded from the Internet. Right after the voting procedure, a QR code will be displayed on the voting computer screen. The voter must now open the special application in the smart device and point the camera at the QR code on the screen. After reading the code, the application contacts the central server of elections and downloads the encrypted (secret) e-vote of the voter. In a few seconds, the voter's choice appears on the smart device screen and the voter can check whether his vote has reached the central server of elections and reflects the choice correctly.[36]

4.5 Impact and Analysis After Six Cases of I-Voting

The impact of I-voting and other important e-services (signing digitally contracts without seeing each other, etc.) on human behavior and psychology needs further research.[37]

[36] More on the pilot on I-voting Web page www.valimised.ee and on the Norwegian experience with verification see Ansper et al. (2009) and the OSCE mission report 2013 at http://www.osce.org/odihr/elections/109517.

[37] For a first insight with the topic, refer to Anu Realo's work in the latest survey by Trechsel and Vassil (2011).

So far, we can use statistics and the results of surveys conducted at European University Institute and Tartu University.[38]

One cannot avoid the question of whether Internet-based voting exacerbates the difference in representation possibility within social groups. What is clear is that Internet-based voting removes physical barriers hindering participation in elections of the aged, disabled or other groups with restricted mobility, or who have difficulty in attending polling stations (e.g., persons having tight work schedules or working, studying or traveling abroad, parents of small children, and persons living in regions with poor infrastructure), assuming, of course, that these people have access to the Internet.

Trechsel et al. concluded in their reports prepared for the Council of Europe following the experience of the Internet voting from 2005 to 2011 that education and income, as well as type of settlement, have been insignificant factors while choosing the Internet from other voting channels. One of the most important findings of the studies until the 2009 elections has been that it is not so much the cleavage between the Internet access haves and access have-nots, but clearly computing skills and frequency of the Internet use have been important predictors of choosing Internet voting. However, since 2009 local elections where more than 100,000 voters used Internet voting, those factors have faded away. Trust in the I-voting procedure has been throughout the years the most significant factor that directs voters' decisions to use or not I-voting.[39]

The actual impact of Internet voting on the change in turnout does not lend itself to objective analysis. One can determine the variations of turnout in different election years (comparing equivalent types of elections) and attempt to clarify the causes underpinning variations with the help of sociological studies. Perhaps, the most important question is what share of the electorate would not have participated in the voting, had the Internet voting opportunity not been provided. There is no really reliable way of obtaining empirical evidence. We must, therefore, come to terms with unverifiable claims made by the voters themselves. The only exception is the case when Internet voting is the only possibility for the elector to vote and he or she uses this possibility. For example, the local government council elections in Estonia do not provide for voting abroad by postal ballot or at a diplomatic representation. Nonetheless, they do envisage the possibility of voting on the Internet (Table 1).[40]

The most intriguing question for political parties is probably the impact of the use of I-voting on results. Although parties favoring I-voting have gathered through the years, most of the I-votes,[41] the studies show that left–right auto-positioning does not play any important role while choosing a voting channel.[42]

---

[38] For the full list of reports, turn to http://www.vvk.ee/voting-methods-in-estonia/engindex/reports-about-internet-voting-in-estonia/.

[39] See Trechsel and Vassil (2011).

[40] See Madise and Vinkel (2011).

[41] Ibid.

[42] In Trechsel and Vassil (2011).

Table 1 I-voting statistics 2005–2013

	2005 LE	2007 PE	2009 EPE	2009 LE	2011 PE	2013 LE
I-votes	9,681	31,064	59,579	106,786	145,230	136,863
Repeated I-votes	364	789	910	2,373	4,384	3,045
I-voters	9,317	30,275	58,669	104,413	140,846	133,808
I-votes cancelled by paper ballot	30	32	55	100	82	146
I-votes counted	9,287	30,243	58,614	104,313	140,764	133,662
Valid votes cast	496,336	550,213	396,982	658,213	575,133	625,336
% of I-votes	1.9 %	5.5 %	14.8 %	15.8 %	24.5 %	21.4 %
I-votes among advance votes	7.2 %	17.6 %	45.4 %	44 %	56.4 %	50.5 %
I-votes cast abroad	n.a	2%	3%	2.8 %	3.9 %	4.2 %

LE—local (municipal) elections
PE—parliamentary elections
EPE—elections to the European parliament

In 2005, the I-voting seems to have had a slight effect on the increase in the turnout of the voters who sometimes vote and sometimes not.[43] In 2007, already approximately 10 % of the questioned I-voters said that they certainly or probably would not have voted without having had the possibility to vote via the Internet. Trechsel and Vassil show (in 2011) that the percentage of the I-voters questioned who certainly or probably would not have voted without having had the possibility to vote via the Internet has risen to 16.3 %, which allows the conclusion that the overall turnout might have been as much as 2.6 % lower in the absence of such a method of voting. That is already a significant marker when one looks at the impact of Internet voting on the overall turnout.

Three cases of Estonian I-voting in 2013 (LE), 2014 (EP), and 2015 (PE) will also be analyzed by experts of the University of Tartu. This research offers unique prolonged insight into the development of such voting method throughout the years

Approximately one-fifth of the questioned non-I-voters pointed out that a reason for not I-voting was the sufficiency of the paper ballot system. Lack of trust with 3.2 % and absurdity of I-voting with 1.9 % were not dominant reasons. Prior to the actual I-voting, there was a concern that the possibility to change the I-vote is going to be misused. It was not the case. The general statistics shows that the number of amended I-votes was insignificant. As was noted previously, the improper influence of remote voters by others is a theoretical but potentially significant problem, although such threats are tolerated with vote by mail in numerous jurisdictions. If we consider the experience of voters in the I-voting experiences, we see that there is little evidence of coercion or concerns about privacy, based on voters' behavior. The small percentages of repeated votes as well

[43] See Breuer and Trechsel (2006).

as the significant increase on the total number of I-voters throughout the years indicate that the confidence in the existing I-voting system has grown.

The hypothesis that I-voting rewards advantages to urban electorate found no proof. Gender is not an important factor when choosing I-voting from possible voting channels. Age, on the contrary, is quite an important factor: most I-voters in all elections belong to the age group 18–39. Furthermore, an interesting analysis of the impact of I-voting on turnout and the role of voters who otherwise do not engage in public matters has been composed by Vassil and Weber.[44]

However, the legitimacy of Internet voting cannot be judged solely on the basis of its impact on political alienation. The legitimacy and constitutionality of Internet voting as well as its impact on democracy are only briefly discussed. It is too early to make strong statements on that topic—on one hand, the remote Internet voting experience has too thin a basis for that, and on the other, the socio-political environment is steadily changing.

4.6 Challenges: Transparency

How to create trust and guarantee the transparency of electronic voting? Although the risks mentioned above are handled, one should take into account that it is always possible to threaten legitimacy of the voting result without any objective cause. Therefore, it is crucial to shape I-voting procedures as transparent and simple as only possible and foresee several reliable control methods.

Simple methods have been used in Estonia to increase voter understanding and confidence on the I-voting system in an attempt to overcome any concerns about the lack of transparency and complexity. In all elections in which I-voting was used, prior to the voting period, the government allowed all individuals eligible to vote the opportunity to test out the I-voting system in order to encourage people to see how the system worked. This helped the voters detect any problems they might encounter before the real I-voting period started. In Estonia, the primary concerns among the country's election officials, outside observers, political parties, and citizens relate to the acquisition of the hardware and software needed to use an ID card on a personal computer, updating expired ID card or Mobile-ID certificates, and the renewal of PIN codes needed for electronic use of the ID card or Mobile-ID.

As an additional element of transparency, the number of I-voters who had cast ballots was updated regularly on the I-voting Web site. This very simple process allowed the wider national audience, as well as the political parties and media, know how many I-voters had voted and determine whether the trend in the number of I-voters casting ballots seemed reasonable. In the end, people were also able to compare the number of I-voters with the number of I-votes counted.

[44] See Vassil and Weber (2011).

In order to convince voters that their votes had been correctly registered, voters had an option to check whether their valid I-vote had been reflected on the polling lists on Election Day in order the prevent voting more than once. A second option for verifying the correctness of a valid I-vote was possible during I-voting period. If the voter decided to replace the I-vote with a new one, he got a notification of an earlier recorded I-vote.

4.7 Challenges: Observation

According to the Estonian electoral laws, all activities related to elections are public. Observers have access to the meetings of all election committees and can follow all electoral activities, including the voting process, counting, and tabulation of results. Internet voting has been no different. All significant documents describing the I-voting system were made available for all, including observers. In order to enhance the observers' knowledge about the system, political parties were invited to take part in a training course before each election. Besides political parties, auditors and other persons interested in the I-voting system also took part in the training, which was followed by surveys of concrete procedures that were necessary for a setup of the I-voting system. Observers were invited also to a test of the counting process.

Throughout the I-voting observation period of 1 month, the main observation tool was the checking of activities of the EVC against written documentation describing the necessary procedures. The key management function required extra attention, as the security and anonymity of I-votes was predicated on the encryption and decryption of votes. During the counting event—the highlight of the election period—the management of the systems' private key, which is the warranty of the electoral secrecy, was demonstrated to observers. This key, split in seven pieces, was hold by the NEC, and its members opened collegially the anonymous encrypted votes. The process of counting of ballots was conducted with observers able to watch all ballot counting activities on large screens in the observation area. The process was fully narrated, and observers were able to follow each step.

It is important that observers are deployed for a length of time necessary to allow meaningful observation. If some important stages influencing the correctness of final results have not been observed, the conclusions about the integrity of the system cannot be made. Especially for foreign observers, the length of the observation period appears to be a challenge. The OSCE did audits in the 2007 and 2011 elections and in its last report states "The OSCE in general found widespread trust in the conduct of the Internet voting by the NEC. However, /…/ more detailed and formal control of software installation and reporting on testing of the Internet voting system could further increase transparency and verifiability of the process."[45]

[45] The OSCE/ODIHR Election Assessment Mission Report, Estonia, Parliamentary Elections, March 6, 2011 is available at http://www.osce.org/odihr/77557.

4.8 Challenges: Validating the Voting Systems and Procedures

In order to validate the electronic voting system, certification procedures, testing, and audits should be considered. Currently, there is no domestic or international body that is able to certify the Estonian I-voting system. Estonia instead uses a system similar to that used in other countries (and similar cases), where the source code of the system is auditable and the operational procedures have been under keen supervision of auditors. System testing prior to elections is also an important part in order to control the functionality and accuracy by contracted testers, observers, and by public.

The Estonian I-voting system was developed with the underlying principle being that all components of the system should be transparent for audit purposes: procedures are fully documented and critical procedures are logged, audited, observed, and videotaped[46] as they are conducted. The procedure-audit,[47] conducted in every election, reviews and monitors security sensitive aspects of the process, such as updating the voters list, preparation of hardware and its installation, loading of election data, maintenance and renewal of election data, and the process of counting the votes.[48]

A common requirement is that the source code of a voting system should be available for public auditing. In Estonia, though, until 2013, the code was not universally available but one could access it if signing a NDA with the NEC. However, after the second legal debates mentioned earlier, in 2013, the source code of all central servers of the voting system as well as the software of the vote verification application was made available in Internet.[49] This is an important step for bringing more transparency and thus more trust toward the very concept of I-voting.

5 Conclusions

Estonia has been one of the first countries in the world where Internet voting with binding results has successfully been used countrywide. The whole Estonian electorate has had six times the possibility of casting the vote via Internet in local (2005, 2009, and 2013), parliamentary (2007 and 2011), and European Parliament elections (2009). Having I-voting constitutes a genuine qualitative change in the development of the electoral system and electoral administration. The Estonian I-voting experience shows that it is possible to ensure the conformity of remote I-voting with all constitutional electoral principles, including the principle of secrecy.

[46] Since 2013 also published on Youtube at http://www.youtube.com/channel/UCTv2y5BPOo-ZSVdTg0CDIbQ.

[47] The scope of the audit is to ensure the validity of performed procedures compared to the handbooks and technical documentation of I-voting. The audit is procured separately for every election by the NEC, the auditors must present a CISA certificate.

[48] See also Vinkel (2012).

[49] You can access the source code at https://github.com/vvk-ehk/evalimine.

The e-ID card, being a primary identification document in Estonia with its two mandatory functions—remote authentication and digital signature—as universal access key to all e-services has been the cornerstone of Internet voting. Reliable identification of the voter as well the anonymity of the vote and correct counting of the votes can thus be secured.

As long as universal Internet access and secure authentication of the voters is not guaranteed, the doubts related to the political neutrality of this technique will probably remain. Nevertheless, I-voting should be regarded as an essential public service in an information society. Issues related to voting machines (as faced in many countries like United States, Germany, or the Netherlands) should certainly not be extended to remote Internet voting.

In an advanced information society, online voting could be even seen as a required means of guaranteeing uniformity of voting. It gives access in elections to citizens who are temporarily working, living, traveling, or studying abroad. Therefore, it might be an important general e-service for guaranteeing free movement inside European Union. Would returning to the traditional voting channels harm free movement of Estonian people, goods and services inside EU?

The basic question in electoral administration no longer focuses on whether new technology developments are acceptable in electoral processes but rather on what kind of technology is suitable for any specific country, taking into account the political tradition and social culture, level of technological infrastructure, and the electoral system of the respective country. In the Estonian case, the preconditions were favorable and time was just right for introducing the most ambitious change in the nature of voting—voting over Internet.

References

Ansper, A., Heiberg, S., Lipmaa, H., Øverland, T. A., & van Laenen, F. (2009). Security and trust for the Norwegian E-voting pilot project E-valg 2011. In A. Jøsang, T. Maseng, & S. J. Knapskog (Eds.), *Lecture notes in computer science*, *5838, NordSec 2009, Oslo, October 14–16, 2009* (pp. 207–222). Berlin: Springer.

Barrat, J., Goldsmith, B., & Turner, J. (2012). *International experience with E-voting*. Washington: IFES foundation.

Breuer, F., & Trechsel, A. H. (2006). E-*voting in the 2005 local elections in Estonia: Report for the council of Europe*. Available at the Estonian National Electoral Committee website www.vvk.ee. Accessed January 2014.

Buchstein, H. (2004). Online democracy, is it viable? Is it desirable? Internet voting and normative democratic theory. In N. Kersting & H. Baldersheim (Eds.), *Electronic voting and democracy. A comparative analysis* (pp. 39–58). Basingstoke: Palgrave Macmillan.

Dahl, R. A. (1998). *On democracy* (p. 95). New Haven and London: Yale University Press.

Drechsler, W., & Madise, Ü. (2004). Electronic voting in Estonia. In N. Kersting & H. Baldersheim (Eds.), *Electronic voting and democracy. A comparative analysis* (pp. 97–108). Basingstoke: Palgrave Macmillan.

Eurostat. (2013). *Survey on individuals regularly using the Internet and on households—level of Internet access*.

Gerlach, J., & Gasser, U. (2009) *Three case studies from Switzerland: E-voting*. Internet and democracy case study series. Berkman Center Research Publications.

Heiberg, S., Laud, P., & Villemson, J. (2012). The application of I-voting for Estonian parliamentary elections of 2011 In: A. Kiyaias & H. Lipmaa (Eds.), *Postproceedings of the 3rd International Conference on E-voting and Identity, Tallinn, September 29–30, 2011. Lecture Notes in Computer Science, 7187* (pp. 208–223). Berlin: Springer.

Heiberg, S., Lipmaa, H., & van Laenen, F. (2010). On E-vote integrity in the case of malicious voter computers. In D. Gritzalis & B. Preneel (Eds.), *Computer security—ESORICS 2010: Esorics 2010*, Athens, September 20–22, 2010 (pp. 373–388). Berlin: Springer.

Heinsalu, A., Koitmäe, A., Pilving, M., & Vinkel, P. (2012). *Elections in Estonia 1992–2011*. Tallinn: National Library of Estonia.

Kalvet, T. (2012). Innovation: A factor explaining e–government success in Estonia. *Electronic Government, An International Journal, 9*(2), 142–157.

Kattel, R., Randma-Liiv, T., & Kalvet, T. (2011). Small states, innovation and administrative capacity. In V. Bekkers, J. Edelenbos & B. Steijn (Eds.), *Innovation in the public sector: Linking capacity and leadership.* Basingstoke: Palgrave Macmillan.

Madise, Ü. (2008). Legal and political aspects of the Internet voting: Estonian case. In J. M. Reniu (Ed.), *E-voting: the last electoral revolution* (pp. 45–59). Barcelona: Institut de Ciències Politiques i Socials.

Madise, Ü., & Maaten, E. (2010). Internet voting in Estonia. In D. R. Insua & S. French (Eds.), *e-Democracy: A group decision and negotiation perspective* (pp. 301–321). Berlin: Springer.

Madise, Ü., & Martens, T. (2006). I-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. In R. Krimmer (Ed.), *Electronic voting 2006* (pp. 15–26). Bonn: Gesellschaft für Informatik.

Madise, Ü., & Vinkel, P. (2011). *Constitutionality of remote internet voting: The Estonian perspective*. In *Juridica International*, *18*, 4–16.

Mägi, T. (2007). *Practical security analysis of I-voting systems*. Available at http://triinu.net/e-voting. Accessed January 2014.

Maurer, A., Spycher, O., Taglioni, G., & Weber, A. (2012). E-voting for Swiss abroad: A joint project between the confederation and the cantons. In *Electronic voting 2012* (pp. 173–187). Bonn: Gesellschaft für Informatik.

Monnoyer-Smith, L. (2006). How I-voting technology challenges traditional concepts of citizenship: an analysis of French voting rituals. In R. Krimmer (Ed.), *Electronic voting 2006* (pp. 61–68). Bonn: Gesellschaft für Informatik.

Nyman-Metcalf, K. (2014). E-governance in law and by law. The legal framework of e-governance. In *E-technology in the EU: Normative Realities and Trends.*

Rolfe, M. (2012). *Voter turnout: A social theory of political participation*. Cambridge: Cambridge University Press.

Recommendation Rec. (2004). '*Legal, operational and technical standards for I-voting' of the council of Europe*. Available at http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/key_documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf. Accessed January, 2014.

Skagestein, G., Haug, A. V., Nødtvedt, E., & Rossebø, J. (2006). How to create trust in electronic voting over an untrusted platform. In R. Krimmer (Ed.), *Electronic voting 2006* (pp. 107–116). Bonn: Gesellschaft für Informatik.

Trechsel, A. & Vassil, K. (2011). *Internet voting in Estonia: A comparative analysis of five elections since 2005*. European University Institute 2011. Available at the Estonian National Electoral Committee website www.vvk.ee. Accessed January, 2014.

Vassil, K., & Weber, T. (2011). A bottelneck model of E-voting: Why technology fails to boost turnout. *New Media & Society,* 1–19. Accessed 23 Jun 2011

Vinkel, P. (2012). Internet voting in Estonia. In p. Laud (Ed.), *Lecture notes in computer science, NordSec 2011, Tallinn, Estonia October 26–28, 2011* (pp. 4–12). Berlin: Springer.

World Economic Forum. (2013). *The global information technology report 2013*. Available at World Economic Forum website http://www.weforum.org/reports/global-information-technology-report-2013. Accessed January, 2014.

Towards Software-Agent Enhanced Privacy Protection

Addi Rull, Ermo Täks and Alexander Norta

Abstract The ability to control the use of personal information is part of the right to privacy. With higher digitalization than ever, the lack of control is an essential privacy issue discussed extensively. Estonia is a unique society in terms of the highest level of digital public services available for a citizen, enabled by the omnibus X-Road infrastructure and personal identification solution developed some time ago. The technology has certain security elements essential for the protection of privacy. However, there are no technical measures to achieve better control over the subsequent use of personal information once it has been obtained from a database. We suggest a task-oriented approach to be exercised in the retrieval of personal information. This can be accomplished by using agent technologies. The aim of the technology is to control access to personal information so that a public servant only obtains a citizen's information limited to the performance of her particular task. In other words, the information system, with the help of a software agent, shall supply a public servant only with the information necessary for performing a decision concerning one citizen. Such enhanced control over the use of personal information contributes to better privacy protection. The prospect addresses the prevention of the misuse of personal information as well as the enforcement of data protection laws. The chapter is an introduction to the discourse of agent technologies and law together with a conceptual example for a possible technological solution in the police work of Estonia.

A. Rull (✉)
Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia
e-mail: addi.rull@ttu.ee

E. Täks · A. Norta
Faculty of Information Technology, Department of Informatics, Tallinn University of Technology, Tallinn, Estonia
e-mail: ermo.taks@ttu.ee

A. Norta
e-mail: alex.norta@gmail.com

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_5

1 Introduction

Continuous increase of the use of public databases poses new challenges. The European agenda to re-use information collected into public databases is the policy aimed at utilising information for the creation of economic and social benefits of a society.[1] The expansion in the area of public services immediately raises the question whether the protection accorded to individual privacy is adequate. Limiting the amount of data to be collected and used is a principle by which the protection of privacy can be better ensured, but there is a growing need for data in order to be able to create new public services. With the amount of data growing it is equally important to focus on the quality of data stored in databases and on the way it is used by public officials when they make decisions concerning an individual. In other words, it is important to consider the relation of the information available in a database to the decision to be made by an official. If an official has access to information which is unnecessary for the decision-making or it is wrong, then this may have unwanted influence on the decision. Although there are data protection laws, the access to information and how it is being used is often difficult to control.[2] This is not because of the lack of rules, or inability to trace enquires by log files, but because there are so many databases, so many different tasks to be performed by so many officials, and no efficient way of controlling the access to and the use of data. Daniel Solove wrote about Computer Databases and Metaphors of Information Privacy in 2001 and called it the aggregation problem.[3] He used Kafka's The Trial metaphor to explain that the information about a person circulating in databases lives the life of its own which is difficult or impossible to control. This may bring about unwanted decisions affecting the life of an individual.

The problem of aggregation can be explained by several scenarios. An official may have access to information unnecessary for the decision-making, but the decision is affected by this information, and this decision is the source of information for another decision made by another official. Or wrong information about a person may be accidentally recorded in a database, which is a source of information for several other databases, and several decisions are being made based on this information and subsequently recorded in various databases. Aggregation is caused by automated, semi-automated or human actions in the decision-making process. An action as a part in the process is not a problem if it can be corrected before the decision is affected, otherwise the sequence of actions causes the aggregation.

One way to tackle the problem of aggregation is to sustain better control over the use of personal information. Alan Westin wrote in 1970 that "[p]rivacy is the claim of individuals […] to determine themselves when, how, and to what extent information

[1] E.g., Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information; see also HOMER Report 2013, Janssen and Dumortier 2003, pp. 184–201.

[2] See Männiko 2001 for a comprehensive overview of privacy and data protection laws in Estonia.

[3] Solove 2001, pp. 1413–1434.

about them is communicated to others".[4] His description of privacy is more relevant than ever, given the vast development of information technologies over past decades. The discussion in the following does not seek to define privacy or to analyse data protection laws, which is an ongoing debate and research amongst many academics.[5] Instead, the motivation of the discussion is to offer novel ideas how better control over personal information could be achieved with the help of 'agent technologies'.[6] The reason to explore technologies subsides in the conviction that there are not so many other efficient and purposeful options left to solve the problem. There is the omnibus data protection regulation at all levels: international, regional (EU) and domestic. Further harmonization may be imminent and the continuous improvement of laws remains to be the objective,[7] but it does not seem to be the solution for the enforcement problem. Every day numerous misuses of personal information which people do not know about take place. If one knows about a misuse and decides to pursue a case, then most of the time the cost of proceedings calculated in terms of time, money or stress exceeds possible moral or pecuniary relief granted. For this reason most people do not react to relatively minor acts of unnecessary uses or misuses of personal data.

The following provides an insight to the use of a database in the police work in Estonia. We describe problematic uses of personal data and discuss violations based on the case law. The underlying problem is the lack of control over the use of personal data. We suggest using agent technologies independently or in combination with the legislation. The discussion of these possibilities is on a conceptual level. Practical solutions are yet to be developed.

2 Public Registers in Estonia

There are approximately 600 public registers in Estonia.[8] Population Register is one of the main databases containing information about citizens and foreigners living in Estonia.[9] The increase of the number of enquires made to this register from

[4] Westin 1970, p. 7.

[5] The concept of privacy has been discussed by many know authors e.g., Alan F. Westin; Judith Jarvis Thomson; Richard Posner; Robert Bork; William Prosser; Ferdinand D. Schoeman; Raymond Wacks, Daniel J. Solove.

[6] Nwana 1996, pp. 1–40. A software agent is a computer program that acts for a user or other program in a relationship of agency, which derives from the Latin *agere* (to do): an agreement to act on one's behalf. Such "action on behalf of" implies the authority to decide which, if any, action is appropriate.

[7] See e.g., Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 2012/0011 (COD), Brussels 25 Jan 2012.

[8] Administration System for the State Information System RIHA https://www.ria.ee/administration-system-of-the-state-information-system/. Accessed 22 Mar 2014.

[9] See information about Population register at https://www.siseministeerium.ee/35796/. Accessed 22 Mar 2014.

42.1 million in 2012 to 55.8 million in 2013 indicates the growing use. According to the Estonian Statistics Agency, the number of people living in Estonia is 1,311,870, which means more than 40 enquiries per person. Institutions that enquire most include the Police and Boarder Guard Board, notaries, courts and local administrations.

A person can check for enquiries by entering www.eesti.ee and making the enquiry about enquiries made to certain registers, for instance, the registers related to the Citizenship and Migration Board. The enquiry shows when the enquiry to a certain register happened, the number of the file this enquiry relates to, the name of the institution, the ID and the position of the enquirer. In some instances, a person can easily assume reasons why enquiries have been made, because this may be related to the visits or applications made by the person to public institutions.

Many registers retrieve information from the Population Register. Chapter 4 of the Population Register Act provides the composition of data recorded in the Population register.[10] Name, date of births, citizenship, marital status, postal address, or person's legal capacity, ethnic nationality and identification documents are examples of data contained in the database. The population register contains basic information about a person. Other registers contain specific information depending on the purpose of the register. For instance, Car Register contains information about registered cars in Estonia and the E-health system contains medical information about diseases diagnosed, medicine prescribed, etc.

Some registers like the Population Register, the Environmental Register, the Marital Property Register, and the Register of Economic Activities are regulated by laws. Most registers are established by regulations on the bases of delegations prescribed in laws. For instance, the statute on the maintenance of the police database, which is called POLIS,[11] is established by the Minister of Interior by regulation. This delegation is derived from the paragraph 13 subsection 1 of the Police and Boarder Guard Act.[12] These legal acts are publicly available and provide detailed information about public databases. The transparency decreases the risk of the arbitrary use of data by the state. In case the violation of the use of personal data occurs then it is possible to resort to data protection and penal laws for a remedy.

At least two databases in Estonia cannot be studied on the same bases as other public databases. There is nothing that can be learned about the database by the Estonian Internal Security Service called KRISTI. The database was publicly mentioned by the parliament member who was the member of the Security Surveillance Authorities Select Committee.[13] This is a parliamentary committee which exercises supervision over the legality of surveillance activities of the

[10] Population Register Act RT I 2000, 50, 317; RT I, 22 Nov 2013, 2, Chap. 4.

[11] Police and Boarder Guard Act RT I 2009, 26, 159; RT I, 02.07.2013, 18, § 8 (2).

[12] Ibid. § 13 (1).

[13] Security Surveillance Authorities Select Committee http://www.riigikogu.ee/index.php?id=42701&parentid=34615. Accessed 24 Mar 2014.

Security Police Board as well as the Police and Boarder Control Board. The existence of the database is certain, because one of the main functions of the Estonian Internal Security Service is to collect information for the prevention and combating activities directed against the state.[14] Most probably, this is not the only classified database in Estonia. We assume also that the Ministry of Defence or the Defence Forces have a database for military intelligence purposes.

Another database, occasionally discussed in public media, is called KAIRI.[15] The Estonian Police and Boarder Guard Board operates KAIRI that is linked to the general police database called POLIS. KAIRI is not entirely classified, but the documents regulating its use are not accessible to the general public. Nevertheless, several court cases include references to these documents. There are reasons for keeping the rules of the use of the database and its content secret, because it is being used in daily police work. KAIRI contains data collected during crime investigations and surveillance operations.

2.1 Database KAIRI

One of the problems identified in cases related to KAIRI shows how information retrieved from the database is not used for the performance of a public duty, but for a personal interest. Yet, instances discussed amongst people who have been stopped by the traffic police over the years suggest that sometimes the decision-making based on the information available in the database may be biased. Also, the quality of information collected into the database has been criticised. Similar problems may arise with other databases.

Every year, thousands of people are stopped by the traffic police, because they have been found guilty for misdemeanour. The mistakes are mostly over speeding, driving without fixing a safety belt or violations related to different traffic signs. The fines are calculated on the bases of fine units whereby one unit equals four euros. If a person is driving a car with the speed of 65 km/h in the area where the limit is 50 km/h then the excess speeding up to 20 km/h is punishable by a fine of up to 30 fine units i.e. 120 euros.[16] A police officer has other options. He may warn the driver and let him go. Cautionary fine is also a possibility, but it is applied when the over speeding is registered by speed cameras.

---

[14] See information available at https://www.kapo.ee/eng. Accessed 24 Mar 2014.

[15] Authors are responsible for any incorrect assumptions made in regards to the database KAIRI, because we have had no chance to study the database and the documents related to it. Information related to the use of KAIRI is a state secret. However, any possible mistakes discovered would not make our suggestions and conceptual discussion obsolete, because the ideas we propose for achieving better control over the use of personal information can be applied in multiple instances in different spheres of life in relation to other databases.

[16] Traffic Act RT I 2010, 44, 261; RT I 14.02.2014, 3, § 227 (1).

Oral warnings and cautionary fines are not recorded in the Punishment Register. If a person is punished for over speeding, then the misdemeanour is recorded in the register. Misdemeanour is substantially different from criminal offence. Paragraph 3 of the Penal Code provides that the punishment prescribed for a misdemeanour is a fine or detention and for a criminal offence it is imprisonment or pecuniary punishment.[17] The future of a person is only affected when the punishment is recorded, because it has a bearing in instances where a person is found guilty for an offence the second time. Often the past behaviour is taken into account and the second punishment is more severe. Punishments recorded in the Punishment Register can also be seen via KAIRI, probably, because the data is regularly synchronised.

A police officer uses a radar speed gun and stops a car when the over speeding is registered. He walks to the car and asks the driver to come to the back seat of the police car. A small mountable device with a screen similar to GPS car navigation device below the radio or the air conditioning unit enables the person sitting in the back seat to peak and see what is on the screen. The police officer uses the device to access KAIRI or POLIS. Firstly, the driver has to be identified. The information on the driver's identification document is compared with the information retrieved from the database. Then the police officer raises a discussion about the over speeding, asking questions in order to understand why the speed limit was not followed. Did the driver know that he was over speeding, why did he choose to drive at the speed above the limit, did he see the traffic sign, etc. The police officer has to make a decision based on the information received from the driver, taking into account the past behaviour. Often the police officer reminds the driver of the punishments recorded in the past. The record of punishments is the important source of information, because it is reliable. The truthfulness of the answers of the driver is more difficult to evaluate.

The police officer exercises the right of discretion to make the decision. The driver may be given a warning or a fine in between 12 and 120 euros[18] if the over speeding was up to 20 km/h in the area where the speed limit is 50 km/h. If the driver does not have an earlier record of misdemeanours, then he may be given a warning or a low fine. In case the driver has a record of over speeding or something else, then higher or maximum fine is an option.

A problem arises with the information accessible to the police officer. The full record of criminal offences and misdemeanours is accessible, whereas the limitation period of the execution of the decision in regards to misdemeanours is one year.[19] The Punishment Register Act provides that after a year the record of the misdemeanour has to be deleted from the register and archived.[20] Similarly, different types of criminal offences have archiving deadlines.

---

[17] Penal Code RT I 2001, 61, 364; RT I 14.01.2014, 10, § 3 (3), (4).

[18] Ibid. § 47 (1).

[19] Ibid. § 82 (1) 3.

[20] Punishment Register Act RT I, 21 Mar 2011, 3; RT I, 13 Dec 2013, 15 (hereinafter as Punishment Register Act) § 24 (1) 1.

Punishment Register was made publicly accessible in 2011 with exceptions related to minors and archived offences. The archiving procedure was further improved in 2013. The rule was that the calculation of one year after which a misdemeanour would have been archived elapsed and started again when the same person received another punishment within this timeframe before a year passed. The dependency of one misdemeanour to another in the calculation of one year was abolished. The Punishment Register held approximately 600,000 records of 250,000 thousand people excluding criminal offences of 22,500 people. Approximately one third of the adult population had public records of offences. Since misdemeanours older than one year are now archived, the number of people with punishments is considerably lower. It is unclear whether the whole catalogue of offences is still synchronised with KAIRI or the archive is excluded.[21] If the archive of misdemeanours cannot be studied via KAIRI, which we do not believe to be the case yet, then this only solves a part of the problem. Records of criminal offences have longer archiving deadlines, and if these records can still be studied in instances when this information is unnecessary for the decision-making, then biased decisions cannot be ruled out. Paragraph 20 of the Punishment Register Act regulates the right to obtain archived data. Clauses 3 and 7 of the subsection 1 of the paragraph 20 suggest that data can be obtained for the purpose of criminal investigation or surveillance activities.[22] KAIRI is the database used for these purposes.

The question raised is whether the police officer who retrieves the record of punishments via KAIRI disregards the information he sees about misdemeanours older than one year? It is known from the practice that police officers raise the discussion about older punishments which should not have the bearing on the decision. Even if they do not discuss the relation of past offences to the situation yet to be decided, it is impossible to know what they think while screening the history, including possible criminal offences.

Suppose a driver has records of punishments for over speeding older than one year and he is caught again. The police officer checks the record and must understand as if the driver has no valid punishments for over speeding. Shall he give the warning or a low fine, which seems appropriate, or a high fine, because in his mind the information seen suggests that the driver has the recidivist behaviour and deserves to be punished?

[21] Since authors did not have a chance to study the architecture of the police databases, then it is unclear how exactly data collected from different databases is recorded in KAIRI. It may be that data is not recorded in KAIRI, but KAIRI functions as an access filter showing data which is available in different databases. Nevertheless, authors are sure that somewhere in this chain the cache of data, which is a copy of the data originally recorded in different databases, is created. Therefore, this does not change the objective of the discussion of how it would be possible to eliminate the creation of cache and how it would be possible to achieve better control over the use of personal data regardless of the possibility that our assumptions about the system architecture may be wrong.

[22] Punishment Register Act. § 20 (1) 3, 7.

KAIRI has another problem related to the quality of data recorded there. KAIRI includes a wide variety of information about a person. A lot of it is retrieved from other registers. For example, it includes information about car registration, immovable property, family relations, offences, etc. If this information had to be enquired from different databases each time there is a need for that, then a lot of time may be lost in critical situations. KAIRI also includes information that does not exist in other databases. Surveillance information is recorded there, but also information about ties a person has with criminals or people who are suspected of criminal activities. Even gossip and unverified statements are known to be found there. The collected information in KAIRI is categorised based on how trustworthy it is. Unreliable information existed in 2011 when the Security Surveillance Authorities Select Committee raised the issue of legality and purpose of such information and ordered the police to clear the system of unreliable data. The extent of the improvement remains unknown. The question remains what exactly is the purpose of recording unreliable data? Hints are useful when the police officer is looks for leads to work on a case. However, wrong information is detrimental to the investigation of a case.

2.2 Case Law

Police officers have misused personal information in several instances. Three Supreme Court cases deal with the fact that personal information retrieved from KAIRI was not used for the performance of public duties, but it was transferred to people outside the police force who did not have the right to access the information.[23]

Directive of 14th of June 2004 by the Director General of the Police and Boarder Guard Board established the procedural rules for KAIRI. The Director General exercises the right to regulate the collection of data on the bases of the Government of the Republic Act.[24] The non-disclosure obligation of the police officer is specified in job descriptions and in § 26 of the Personal Data Protection Act, which requires persons who process personal data which become known to them in the performance of their duties to maintain the confidentiality.[25] The violation of the non-disclosure obligation is criminalised. § 157 of the Penal Code provides that the disclosure of personal information obtained in the course of professional activities is punishable by pecuniary punishment or 3 years imprisonment.[26]

The definition of the private personal data is provided in § 4 of the Data Protection Act. The Supreme Court has stated that the definition of private

[23] Estonian Supreme Court cases 3-1-1-81-08; 3-1-1-25-12; 3-1-1-56-13.

[24] Government of the Republic Act RT I 1995, 94, 1628; RT I, 27.12.2013, 33, § 73.

[25] Personal Data Protection Act RT I 2007, 24, 127; RT I, 30.12.2010, 11, § 26.

[26] Penal Code RT I 2001, 61, 364; RT I 14.01.2014, 10, § 157.

personal data should not be treated narrowly. It includes any factual information concerning the life of an individual. For instance, one's address is a personal data although it may be possible to obtain it from publicly accessible registers such as the Register of Economic Activities in Estonia.[27] Either the person has given the consent to make the address publicly available or it is a precondition for a certain activity. Economic activities require that a person has publicly available address, as it helps to achieve certainty in the business environment. Another example is the Traffic Registry. It is not possible to identify the owner of the car in Estonia, because the car registration information is not publicly available. Car registration and address information can be obtained from KAIRI, but the address may be publicly available in other databases. If address is copied from KAIRI not for the performance of the duties of the police officer, but for someone who does not have access to the database, then data protection principles are violated. The fact that the address can be obtained from other sources does not wave the non-disclosure obligation of the police officer.

One Supreme Court case tells about the assistant police officer who asked the police officer to provide him with the information about two people. The information included addresses, car registrations, records of misdemeanours and criminal offences. The assistant police officer could not have obtained this information by himself except addresses perhaps. His position did not allow him to access KAIRI, because the assistant police officer is not the member of the police. People who apply to work on voluntary bases together with the police in street patrols become assistant police officers. Rights, obligations and activities of the assistant police officer are regulated in the Assistant Police Officer Act.[28]

In another case the husband of the police officer received an e-mail with the information about his co-workers. The intention of his wife working in the police was to provide him with sensitive information about these two people so that they could be fired if necessary. Again KAIRI was used as the source of information.

The most recent case was about the police officer who used her position in the criminal investigation of theft to give information to victims who wanted to track down and to threaten thieves as a way to force them to pay. The police officer shared the information obtained from the database and the information collected during the investigation with victims.

In general, it is fair to assume that a police officer does not misuse personal data, because he is bound to the regulation prescribed to ensure the protection of privacy. The referred case law shows that the misuse of personal data is argued in the context of complex legal instruments including laws, regulations, directives and job descriptions. The police officer must have the comprehensive understanding that he is the processor of personal data who is under the obligation not to use personal information for any other purposes except for the performance of a public duty. The quality of education and the awareness of the regulation help the police

[27] Register of Economic Activities http://mtr.mkm.ee/default.aspx. Accessed 19 Mar 2014.

[28] Assistant Police Officer Act RT I, 20.12.2010, 1; RT I, 30.12.2011, 58, § 2 (1).

officer to achieve the required understanding. On the other hand, cases of misuse of personal information require the expertise of highly qualified prosecutors and attorneys to argue a case. Evidence has to be collected before that. And, most importantly, there is no case without a victim. A person who has learnt about the misuse of personal data may initiate the case or the violation may be discovered by internal audits. No one knows how many violations have taken place, which victims do not know about, nor have internal audits discovered them.

3 Purpose of Software Agent

Traces to prove the use of information in cases discussed were log files and other evidence left behind. Every enquiry leaves a footprint of a person who made it. Traceability is a feature which helps to enforce the protection of privacy, because the probability exists that a person who made an arbitrary enquiry may be discovered. The problem with such a system is that it has minimal knowledge about the intended use of the information enquired in order to decide whether the person looking for the information should be granted access to it or not. Police officers in different positions have different access rights to the information in KAIRI. Classified surveillance information is available to approximately one third of 4000–5000 officials who can use the system. The system identifies the individual, recognises the level of access and provides the information accordingly, but the subsequent use of the information is not controlled by the system. The possibility that a system would exercise full control over the use of the information is difficult to imagine in the police work. Instead, the more sophisticated approach to the task oriented use of the information should be developed.

The described misuses of personal data in the investigation and the traffic patrol work are the result of intentional or subconscious human error. The traffic patrol may be inclined to make a biased decision, because the full history of past mistakes of the driver can be studied via KAIRI. As a result, a severe punishment may be a subconscious decision as a reaction to recidivist behaviour. The current information system does not address these issues. We suggest to explore the idea of using the agent technology which could stand in between the police officer and databases in order to aid the police officer in the decision-making process, yet, at the same time to achieve the enhanced protection of privacy thro' more sophisticated way of processing personal data.

The primary task is to solve two basic issues: (1) how the agent technology can regulate the flow of information so that it only gives the police officer the right type of information required for the performance of a certain task; (2) and how such technology can enforce legal norms and react to regulatory changes. Consequently, the successful performance of these tasks will decrease the number of intentional or subconscious human errors as it will correct the mistakes resulting from the imperfect knowledge of the police officer about data protection law. Furthermore, the decrease of the number of misuses of personal data shall affect the resources spent for internal audits and court cases. Overall, the fundamental right to privacy is protected better than today.

Two tasks can be accomplished together or separately. The combined implementation of these tasks would require a systemised approach to semantics of law and computer linguistics in order to be able to develop a methodology that enables to build a link between the legal system and a particular task to be performed by a computer programme.[29]

3.1 Legal Software Agent

Agent technologies have been developed over past decades. The notion of "agent" was first used by Hewitt in 1973.[30] The technology has been used for various purposes, for example, to predict the perception of consumers before the launch of new consumer goods.[31] Agents assimilate humans, indicating their consumer preferences and behaviour, and in this way contributing to the making of sales forecasts for manufactures. Another example is the IBM solution called Watson, which beat the best player in the quiz competition in Jeopardy TV show in 2011. Intelligence demonstrated by agent technologies renders remarkable results, which in some aspects are better or comparable to the best of human beings. Artificial intelligence has become possible with agent technologies. The same cannot be stated for the automated decision making applications developed in the field of law. In 1977 Harvard Law Review published the article about legal reasoning and artificial intelligence written by L. Thorne McCarty who explained how tax issues related to corporate reorganisation can be resolved with the help of a computer programme called TAXMAN.[32] Little progress has been made ever since. Tax authorities use algorithms to check the payment of taxes. Systems have been programmed to recognise irregularities or to react to certain predetermined conditions which trigger the automated processing of administrative acts, for instance, issuing the administrative act which informs a person about the start of the tax investigation procedure. Fines sent to drivers who have been caught for over speeding by speed cameras is also an example of automated enforcement of law. Still, most processes are semi-automated, requiring human intervention in a certain stage of a process.

The problem is that computer programmes do not have the capability to adjust themselves automatically to the regulatory changes. For instance, in Estonia the V.A.T. tax was changed from 18 to 20 % in 2009 in order to raise funds for the state budget in the midst of the financial crises. The change in the tax law was announced and implemented in a short notice. The business sector could not adapt to the new regulation without the extra costs that occurred with the implementation of changes into software and the changing of price labels in stores, etc.

---

[29] See e.g., Nyman-Metcalf and Täks 2013, pp. 1–30.

[30] Hewitt et al. 1973, pp. 234–245.

[31] Gowda 2008, pp. 246–251.

[32] McCarty 1977, pp. 837–893.

The Chancellor of Justice argued that the state violated the *vacatio legis* principle by not giving ample time for the business sector to comply with the new regulation, because the notice given was barely a week. In the end, the state agreed to compensate the extra costs. The fact that software had to be programmed to comply with the new tax regulation reiterates the disability of software to adapt itself to the changes in law. In other words, there is no interaction between two environments. The tax law regulates taxes in the living world and a software providing certain functionality replicates this environment. A change of law in the living world does not transform a functionality of software without human intervention. A sequence of activities performed by one or more people may be needed in order to achieve compatibility between two environments:

1. identifying regulatory changes which have to be transformed into software;
2. designating a person who is qualified to plan and implement changes in software so that the compatibility with new legislation is achieved;
3. evaluating the quality of changes;
4. checking for the compliance of changes to the legal system as a whole;
5. monitoring the operation of software as to its compliance to legal changes over time;
6. intercepting if there are inclinations from the result initially planned (beginning the process from the start).

The ability of software to adjust its functions can be described in the following scenario. Police officers have different access rights to KAIRI. The system is programmed to differentiate between police officers who have different responsibilities and tasks in the police work. The data in the system has been categorised into A, B, C, D categories, and the access to data has been determined by these categories. If a police officer who works in a street patrol is promoted to the position of the investigator, then he is given access rights to more categories of data. The person responsible for changing access rights has to adjust it to the new position. The person responsible for employment contracts and other related documents such as job descriptions has to prepare and introduce new documents to the police officer. The change of access rights could be automated by integrating the access functionality of different categories of data with the level of access defined in the employment contract. The job description can be linked to the employment contract as well. If necessary, the change in the employment contract automatically changes the access right and the job description. Furthermore, data protection law can be linked to the employment contract by the definition of the processor of personal data. The police officer being the processor of personal data is bound to several obligations prescribed in law. One could speculate whether a change of the obligation in law could be automatically implemented into the employment contract, the job description and thereby also affecting the access right. This is a theoretical example how software uses information received from legal sources so that it does not have to be reprogrammed, but the changes in law are automatically transformed into certain functionality.

The model of the legal software agent is shown in Fig. 1. The agent derives its legal knowledge from the legislation. The purpose of the agent is to provide the

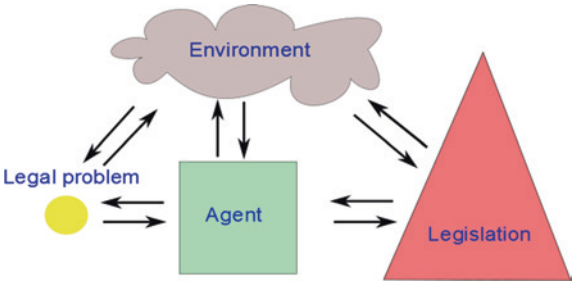

Fig. 1 Legal agent model

functionality for solving a legal issue, for instance, the limiting of access to personal information in order to achieve better privacy protection.

The environment in the model depicts the living world. Agents have growing capabilities to sense the world in a similar way as humans do. Different sensory technologies researched and developed today and in the future can establish and increase the sensory capabilities of an agent, for instance, technologies using smart dust or medical technologies which enable to detect health conditions including mental state of a human. A smart agent could be useful for multiple purposes in the police work. For example, if the agent could detect the over weight of heavy trucks, then the efficiency of the police work would grow considerably. Today the procedure of checking heavy trucks requires a crew of police officers together with the van full of equipment which has to be carried and mounted under the wheels of a vehicle each time the checking is performed. So can the problem of access to information be tackled by a software agent? The capability of the agent to evaluate the health of a police officer may include the ability to sense alcohol or drug consumption and the level of stress. For example, in case the agent diagnoses the depression of the police officer who is working in the traffic patrol and uses KAIRI for obtaining information about drivers stopped, then software agent could limit the access to information and direct the police officer for a medical check. The role of the agent in this scenario is to limit the risk of the making of biased decisions, or to prevent other misuses of personal information. If the agent has detected the alcohol consumption, then it could initiate the disciplinary procedure, which means that the police officer has to be removed from work for the duration of the procedure. The role of the agent is to block the access to databases and to inform the people responsible for the disciplinary procedure. Furthermore, a smart agent may have an ability to adjust its behaviour if the conditions of the disciplinary procedure prescribed in law change. It means that software has to be able to understand civil service law and to adjust its actions accordingly.

It is thrilling to speculate about conceptual ideas and benefits that software agents could deliver in the future. The purpose of these examples and illustrations is to explain possible practical solutions ahead of time. The discussion of the possibilities to establish the link between software agent and legislation is abandoned in the following chapters. The focus is on the basics of the information technologies that are forming the grounds on how the agent technology can regulate the

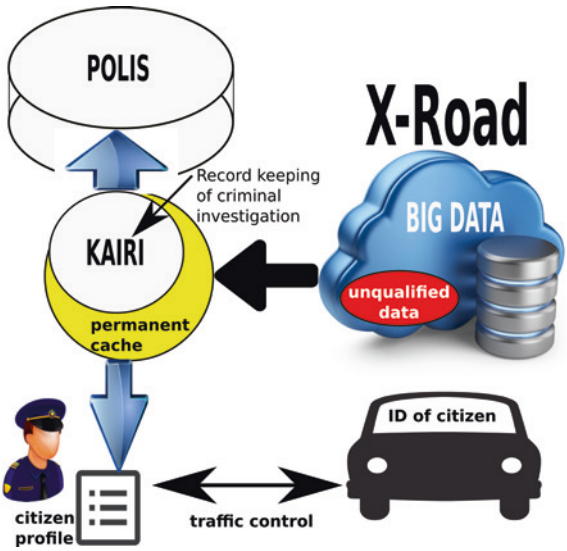

Fig. 2 System landscape supporting a police officer during a traffic control

flow of information so that it only gives the police officer the right type of information required for the performance of a certain task—the first task proposition formulated above.

4 Current Technology Surrounding KAIRI

The previous chapters sum up the legal scenario of privacy violations in Estonia that are specific of the degree of societal digitalization.[33] In Fig. 2, this larger digitalisation aspect also affects the way how traffic controls happen. Most importantly, the so-called X-Road system is the underlying system infrastructure on top of which also the police operate in Estonia. X-Road is a platform that enables secure Internet-based data exchange between the states information systems in a distributed peer-to-peer (P2P) and scalable way.[34] Thus, the X-Road allows organizations and people to securely exchange data from public and private domains.

Pertaining to the privacy-violation problem discussed in this chapter, the X-Road enables public enquiries during traffic controls of Estonian police officers. In order to use the services, the car driver must produce an identification to the police officer the latter uses for searching the personal record from state databases. The advantage of X-Road for officials work is the avoidance of the

[33] http://e-estonia.com. Accessed 27 Mar 2014.

[34] https://www.ria.ee/x-road. Accessed 27 Mar 2014.

labour-consuming processing of paper documents, large-scale data entry and data verification. Communication with other officials is also faster and more accurate, e.g., with other staff from the police force or the boarder patrol unit.

We conceptually depict the system landscape in Fig. 2. We assume the earlier mentioned case of a police officer performing a traffic control on a citizen. The latter produces her identification that comprises of the name together with the ID number. The police officer uses this data to search for citizen-related information on a mobile, wireless IT-device that connects to the database KAIRI. KAIRI is connected to a bigger database system that is part of the police's information system infrastructure called POLIS. The initial purpose of KAIRI is to manage data around criminal investigations and as Fig. 2 shows, it connects to a big data pool around the X-Road system that constitutes a federation of distributed databases.

As the police officer has to perform the citizen check quickly during the traffic job, it is not possible to perform elaborate searches in distributed database systems related to X-Road. The solution is to cache in KAIRI information from the big-data cloud to the right of Fig. 2. Depicted in a contained ellipse we show a subset of data termed *unqualified data*. The latter is a specific collection of rumour that could be important for resolving a criminal investigation at some point of time. However, as the name indicates, the quality of this data is not certified.

The KAIRI database in Fig. 2 comprises two tiers. The inner tier comprises the facts around a criminal investigation which adheres to the original purpose of the KAIRI database. The second tier serves as a cache of data taken from the big-data cloud, including unqualified data. A cache is an extra store of data so that future requests for that data are served faster. Without such a cache, the data must be first recomputed or fetched from the original storage location. Thus, the more requests are served from the cache, the faster the overall system performance while the police officer carries out the traffic control. Additionally, this architecture overcomes the bottleneck of limited IT-skills of the police officer as the KAIRI-system configuration automatically.

The problem of this pragmatic solution to use KAIRI as data cache has multiple disadvantages. First, as the caching procedure from the big-data cloud repeats periodically, the former consequently keeps growing in size. As the big data is from a heterogeneous distributed source, they lack structure and are of questionable quality. Additionally, being in the cache, keeping the data up to date is a challenge in correlation to the big-data source. Finally, a lot of the data may be very sensitive and in condensed combination could give insight about a citizen that a police officer must not be aware of.

More problems occur when the police officer looks at the automatically generated profile about a randomly stopped citizen in a traffic stop. As previous sections discuss, records about a citizen beyond a certain age must not be available to a police officer. However, the current architecture of the system depicted in Fig. 2 grant the police officer full access to all records beyond what he is permitted to see. The lack of provided privacy protection mechanisms during the automatic profile generation is problematic when the police officer must decide on possible punishment degrees during the traffic job. Earlier sections discuss this issue as

the police officer decides more severe punishment in case prior violations of the law exist. Assuming profile data access that reaches beyond the intended level for this decision-making process, it is likely the police officer takes into account, for instance, the traffic violations that are older than one year.

5 Privacy-Ensuring Socio-technical Solution

The current state of KAIRI does not comprise adequate mechanisms to protect the privacy of individuals adequately and consequently, the system infrastructure requires a resolution. However, that solution must be of a socio-technical nature in that the system must adhere to a specific set of principles.

- *Responsible autonomy* addresses a shift towards teams or groups as the primary unit that also conforms to the traffic control case as policemen engage at least in pairs with a citizen and have potential reinforcement on standby. Thus, the privacy-assuring solution must pay particular attention to internal supervision and leadership at the level of the "group" and avoid rigid and inflexible silo thinking.
- *Adaptability* pertains to the way how an organisation responds to the external complexity by reducing the internal control and coordination needs by adopting the strategy of simple organisations and complex jobs. This strategy implies that groups must be relatively empowered to make their own decisions. Mapped to the traffic control case this means the police officer judges herself how the data delivered by KAIRI leads to a possible punishment degree of a law-violating citizen.
- *Whole tasks* that can be assigned on to a single, small, face-to-face group which experiences the entire cycle of operations within the compass of its capabilities and permissions. Thus, a police offer must complete an entire traffic control as a task but the sequence of activities involved changes in a flexible way on a case-by-case basis.
- *Meaningfulness of tasks* is the consequence of the earlier three principles. This task meaningfulness implies for each participant the task has total significance, dynamic closure and requires a set of skills to achieve the desired degree of autonomy. For the traffic-control scenario, it means KAIRI must provide the targeted means with the right level of utility to the police officer for completing a citizen inspection in one place at one time. In other words, in classic organisations the "wholeness" of a task is often diminished by multiple group integration and spatio-temporal disintegration. Thus, KAIRI must perform the right degree of information logistics so that privacy of the citizen remains assured.

The socio-technical solution for restoring privacy assurance rests on two factors. Firstly, the introduction of a detailed definition of role profiles for police officers that specify the permissions, competencies, access rights, and so on, in Sect. 5.1. Secondly, in Sect. 5.2 socio-technical artificial agents use these profiles for creating citizen profiles on the fly that protect a citizen's privacy.

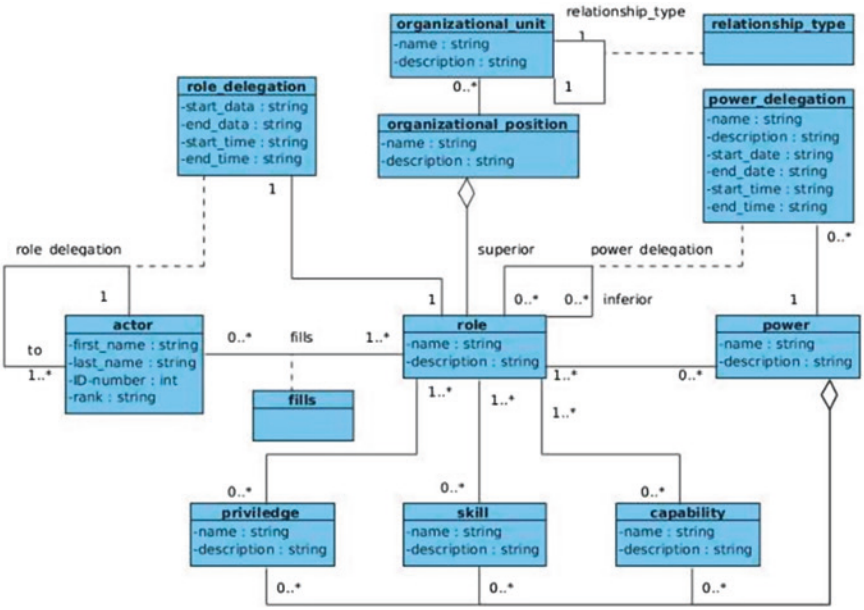

Fig. 3 Role model

5.1 Role Definition

An integral ingredient is the proper capture of details around a role affiliated with a police officer. The concept of a role in a system allows for enhanced flexibility compared to hard person assignment of properties. If the latter seizes to exist, it may cause problems of the functioning of the overall system. Instead functionality assignment to a role such as police officer into which an individual person slips, enhances the resilience of system use.

We use a class diagram for expressing the entities and relationships of the role model. A class diagram is a diagram for describing the structure of a system. The diagram in Fig. 3 shows classes as rectangular boxes and with contained attributes. The relationships between classes are logical connections and comprise several types. An association link is a straight line between classes, e.g., in Fig. 3 between classes actor and role. Numbers on both sides of the association link express the relationship cardinality, e.g., an actor can slip into one or many roles while a role either may remain unpopulated or populated by many actor instances. An association link may also link to one class only, e.g., an actor instance may delegate a role to another actor instance. If cardinalities on association links indicate a many-to-many relationship between classes, we assign a so-called association class to assure it is always clear which class instance relate to each other, e.g., role delegation. Finally, Fig. 3 also comprises a so-called aggregation association that

represents a part-whole or part-of relationship. For example, an instance of power is composed of optional parts of privilege-, skill- and capability instances.

The role model depicted in Fig. 3 is a small part of a larger version that we omit due to space limitation. An individual resource has an actor as a subclass who is a concrete person. Such an actor may be directly assigned to a task such as performing a traffic control. An actor references one or many roles that can be delegated to other actors, e.g., another police offer. Furthermore, an actor has also one or many organizational positions that are related to organizational units that reflect the rank of a police officer. Such an organizational position may mean several privileges are attached that are also related to roles. For example, a police officer is privileged to directly collect money for a fine. A role is a subclass of a resource type and may be filled by several actors.[35] Besides already mentioned, several capabilities may be required to fill a role such as checking unqualified data. Furthermore, a role can give certain power that can also be delegated to other roles for a limited time, e.g., for punishing a citizen who commits a traffic violation. Power that is attached to a role is also related to capabilities and privileges.

5.2 Socio-technical Agents

For privacy assurance during a traffic stop, socio-technical artificial agents are instrumental. In this context, an agent is a software application that supports social behaviour of a computational system. An agent is an intelligent system that perceives its environment and takes actions that maximize its chances of success. Additionally, an agent is an active entity that reasons on behalf of a police officer.

The depiction in Fig. 4a shows the reference architecture of a sociotechnical agent.[36] It comprises four components with different functions. The bottom left component labelled sensor gathers events as input that occur in the context of an agent. Those events are split inside the agent and partially the knowledge base and the controller receive. The knowledge base comprises entities and facts of the agent's context together with ontological repositories for allowing a correct interpretation of the stored data. The second recipient of sensor-processed events the controller receives. The latter component uses in addition the knowledge base for algorithmic processing to perform pseudo anthropomorphic reasoning that copy humans in a machine-learning way. The latter is a branch of artificial intelligence and focuses on the construction and study of systems that learn from data.

- *Belief* in a human-agent sense is a state of mind in which an individual holds an unproven proposition or assumption of something to be true.
- *Responsibility* in a legal sense is the mental capacity to decide if a person can be held accountable for a crime.

[35] See e.g., Norta 2007.

[36] Sterling and Taveter 2009.

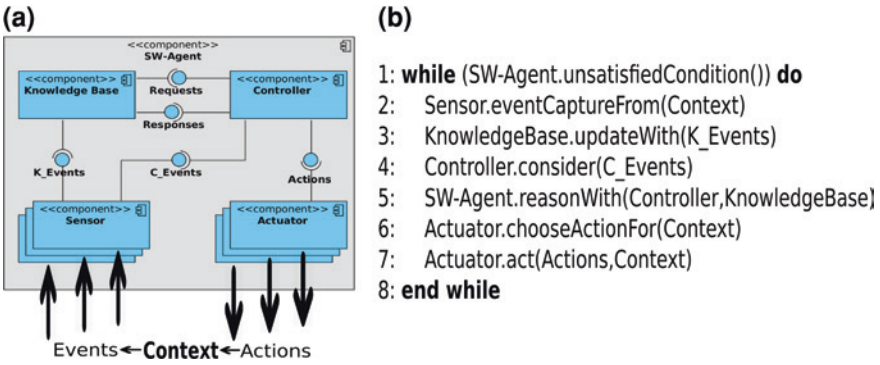

Fig. 4 Conceptual agent architecture in (**a**) and a pseudo-code algorithm for agents in (**b**)

- *Expectation* is a belief centered on the future, with a particular probability to be realistic.
- *Capability* is the ability to perform or achieve certain actions or outcomes through a set of controllable and measurable faculties, features, functions, processes, or services.
- *Goal* is a desired result a person or a system envisions, plans and commits to achieve an individual or socially desired end-point in accordance with a plan and within a deadline.
- *Desire* is a sense of longing for an agent, or object, or hope for an outcome.
- *Intention* is an agent's specific purpose in performing an action, series of actions, or targeted goal.

The pseudo-code algorithm in Fig. 4b shows the abstract structure of this machine-learning algorithm in the controller component of a socio-technical agent. Accordingly, the main encompassing control-flow element is a while-loop that performs as long as the agent is unfulfilled. Inside the while-loop, the agent senses events from the environment and uses that input for updating the knowledge base if needed. These events also serve for the reasoning in the controller in a way that the agent's machine learning algorithm displays the pseudo anthropomorphic properties in an artificial-intelligence sense as discussed above. Consequently, the socio-technical agent projects events through the actuator component onto its contextual environment. The latter reacts to that projection and the loops starts again from the beginning unless a satisfaction occurs of the condition-statement in the while-loop.

6 Resolution Suggestion for Privacy Protection

The proposed approach from the previous section we map on a TO-BE architecture that Fig. 5 depicts. The changes in comparison to the AS-IS architecture in Fig. 2 are as follows. The most important change the introduction of

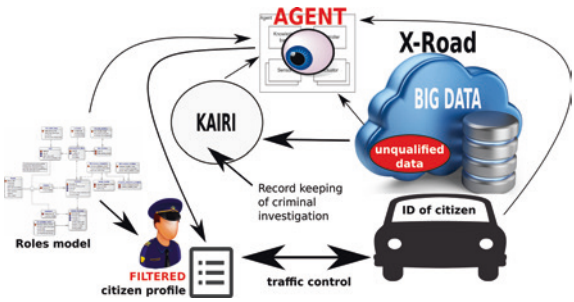

Fig. 5 Privacy-protection resolution proposal using socio-technical agents

a socio-technical agent that a traffic-control case instantiates i.e. each control instance has a dedicated agent instance too which terminates its lifecycle once the control-case ends. The police officer has a proper affiliation with a data-model instance the agent uses on inception. The KAIRI database shrinks back to its original purpose of criminal-investigation record keeping. The problematic cache is now not necessary any longer as the agent creates tailor-made citizen profiles based on the data-model instance assigned to a police officer.

With the cache falling off from KAIRI, the data-exchange protocol shrinks between KAIRI and the big-data cloud affiliated with the Estonian X-Road system. Instead, the agent now has dedicated access to the distributed databases for accumulating profile data. The agent assures not only that data access and processing happens at feasible speed but the resulting citizen profile comprises only the data a respective police officer has permission to see. Note that KAIRI is still part of the larger POLIS system, however, in Fig. 5 we omit a repeated depiction. Finally, the agent also assures a fast relaying and committing of newly created data the police officer creates during the lifecycle of a traffic control, e.g., the citizen drives under the influence of alcohol.

7 Conclusion

With the intense degree of digitalisation of Estonia by using the unique X-Road system for administrational purposes in public but also private domains, novel problems occur with respect to privacy of personal data. We show in this chapter that the pace of technological innovation makes it a challenge for the legal situation to keep up. As the listed cases in the introduction show, several cases of privacy violations have gone to the Estonian Supreme Court. Particularly prevalent among the privacy violations are situations related to police activities such as during regular traffic controls.

While there are general privacy protection laws in place, the high degree of digitalization makes it very challenging for police officers during a traffic control to respect the privacy laws. The situation is simply too complex for the following

reasons. In order to adhere to the complex privacy protection regulations, the police officer must make a continuation expert assessment during a traffic control situation as if s/he would be trained in a comparable way as a professional lawyer. Secondly, the required data for performing a traffic control with a citizen is distributed in many different databases. Thus, the police officer must also act in a comparable way to an ICT-expert and know how to quickly access all data in the distributed technological infrastructure of X-Road. These two factors show the complexity of the situation that results in data privacy violations even without mal intent.

Not only is the police officer overwhelmed with the imperative of respecting citizen data privacy, also the system designers of X-Road play a role in causing this problem to occur. While the initial designing and implementation of the X-Road is initially driven by purely technically considerations such as security and dependability of interoperability, privacy assurance has a socio-technical dimension that requires taking into account the nature of human action during system design. The currently existing system architecture forces the maintenance of a local data cache around a database called KAIRI that merely has the original purpose of maintaining criminal-investigation records. However, as it is the objective to quickly process personal data during a traffic control, it is necessary to copy from the highly distributed X-Road databases permanently into the KAIRI cache to allow for the quick permanent access. The problem is that complete datasets become available that a police officer should not be able to see. The cached data is impossible to keep in an updated state compared to the source in the distributed X-Road databases. Additionally, the cache itself continuously keeps growing in size, making it ever more complex to maintain dataset consistency.

As a remedy to this novel level of complexity that public workers experience in highly digitalized Estonia, we propose two specific solutions that not only restore data privacy on the fly but also correct the original architecture flaw in KAIRI system design. Firstly, we give a role-focused model to capture additional facts that describe the profile of police officers. The model captures facts about the police organization, recording privileges, skills, capabilities. In a flexible way persons may assume specific roles which grant them certain powers such as during a traffic control situation. The delegation of specific powers and roles are possible, making the model flexible to contextual changes.

The second remedy is the use of software agents that take into account the facts recorded in the role model to create on the fly tailor made citizen profiles with exactly the facts an official is permitted to see based on the assumed role without any violation of data privacy. The software agent comes into existence when a traffic control commences and terminates when this control comes to an end. The software agent has privileged access to the distributed X-Road databases so that the creation of personal data happens in real time so that a citizen can be controlled quickly. The side effect of introducing such a software agent is that the need disappears for a cache attached to the KAIRI system.

For future work two directions exist. First, the introduction of software agents only partially resolves all problems related to a traffic inspection. The complexities involved around a traffic control can be reduced even more when the

administrational process is automated too. The police officer can then instantiate an administrational-process template and follow pre-defined steps for traffic controls that software agents support by delivering on the fly targeted data flow from the distributed X-Road database systems. Adopting administrational processes also allows for a design that enforces adherence to public law and regulations.

Another angle of future work focuses on the safeguarded introduction of intelligent software agents. The artificial-intelligence community recognizes the dangers of allowing unchecked introductions of AI systems into society.[37] Specifically in a highly digitalized society such as Estonia, the introduction of badly designed intelligent software agents carries the potential for considerable destruction in the X-Road system and the affiliated distributed databases.

References

Gowda, R. S. (2008). Role of software agents in e-commerce. *International Journal of Computational Engineering, 3*(3), 246–251.

Hewitt, C. et al. (1973). *A universal modular ACTOR formalism for artificial intelligence*. In Proceedings of the 3rd International Joint Conference on Artificial Intelligence (pp. 234–245). San Francisco: Morgan Kaufmann Publishers Inc.

HOMER Report (2013). *Socio-economic impact study*, March 2013, http://homerproject.eu/publications-documents. Accessed 1 April 2014.

Janssen, K., & Dumortier, J. (2003). Towards a European framework for the re-use of public sector information: A long and winding road. *International Journal of Law and Information Technology, Oxford University Press, 11*(2), 184–201.

Männiko, M. (2001). Õigus Privaatusele ja Andmekaitsele. Juura.

McCarty, L. T. (1977). Reflections on TAXMAN: An experiment in artificial intelligence and legal reasoning. *Harvard Law Review, 90*(5), 837–893.

Norta, A. (2007). *Exploring dynamic inter-organizational business process collaboration*. PhD thesis, Technology University Eindhoven, Department of Information Systems.

Nwana, H. S. (1996). Software agents: An overview. *Knowledge Engineering Review, 11*(3), 1–40.

Nyman-Metcalf, K., Täks, E. (2013). Simplifying the law—can ICT help us? *International Journal of Law and Information Technology*, 1–30.

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53*, 1413–1434.

Sterling, L., Taveter, K. (2009). *The art of agent-oriented modeling*. Cambridge: MIT Press.

Westin, A. F. (1970) *Privacy and freedom*. The Boadley Head, 7.

Yampolskiy, R. V. (2012) AI-complete CAPTCHAs as zero knowledge proofs of access to an artificial intelligent system. *ISRN Artificial Intelligence*.

[37] Yampolskiy 2012.

Striking a Fair Balance Between the Protection of Creative Content and the Need to Foster Its Dissemination: The Challenges Posed by Internet Linking and Meta Search Engines

Johan Axhamn

Abstract In recent years, the ability to make available, locate and access copyright protected content over the Internet has increased considerably. Some business models are directly aimed at linking or locating content already made available by other services. Such business models may create value for end users by making it easier to locate and find content on the Internet, but at the same time, they may be deemed to appropriate value from the rightholders or their service providers. In some cases, this has led to tensions and even litigations between the providers of these new business models and the rightholders or their service providers. These tensions are reflections of the underlying policy concerns inherent in the field of copyright law on the necessity to strike a fair balance between the protection of creative content and measures to foster its dissemination. This article will discuss, analyse and draw conclusions from two recent cases from the Court of Justice of the European Union on Internet linking and meta search engines, Svensson and Others and Innoweb, and relate them to the underlying policy concerns in copyright law.

1 Introduction

The Internet and the World Wide Web are some of the most important and profound creations of humankind. Among many Internet applications and services available today, information retrieval is very likely one of the two primary uses of the Internet. The possibility to *link* to and *search* for content on the Internet plays an important role for users to find and locate resources or content for a particular

J. Axhamn (✉)
Faculty of Law, Stockholm University, Stockholm, Sweden
e-mail: johan.axhamn@juridicum.su.se

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_6

need.[1] Linking is intimately bound to the conception of the Internet as a network: it has even been held that linking is the single most important feature that differentiates the Internet from other forms of cultural dissemination.[2]

These technical developments and features could be seen in the light of basic copyright principles. In general, the primary role of the system of copyright norms established in the EU directives on copyright is to foster the production and dissemination of creative works.[3] To a great extent, these norms build on norms established at international level, e.g. in the Berne Convention (BC),[4] the WIPO Copyright Treaty (WCT)[5] and the WIPO Performances and Phonograms Treaty (WPPT).[6] The two latter instruments were adopted in response to the need to ensure that appropriate levels of protection were made available in the "digital environment", at the time referred to as the "digital agenda".[7]

The main or most significant EU directive, which also serves the purpose of implementing the WCT and the WPPT in a harmonised way at EU level, is directive 2001/29 on copyright in the information society.[8] The dual aim to stimulate the production of creative works and at the same time foster their dissemination, *inter alia* in relation to technological developments, is enshrined in several of the recitals in the preamble to that directive.[9] Similar statements are found in the

---

[1] Wu and Li (2004, p. 305), Olivas (2008, p. 537). Cf. de Beer and Burri (2014, p. 103), Strowel and Ide (2001, p. 404) and Ginsburg (2014, p. 147).

[2] See e.g. European Copyright Society (2014) (hereinafter: Opinion by the European Copyright Society on Svensson). Cf. Benkler (2006), Tsoutsanis (2014, p. 1), Udsen and Schovsbo (2006, p. 47) *et seq*. and Westman (2012, p. 800).

[3] In this article, unless otherwise specified, the terms "copyright" or "work" also refer to so-called related or neighbouring rights.

[4] Berne Convention for the Protection of Literary and Artistic Works, last revised in Paris on 24 July 1971, and amended on 28 September 1979.

[5] WIPO Copyright Treaty (WCT), adopted in Geneva on 20 December 1996.

[6] WIPO Performances and Phonograms Treaty (WPPT), adopted in Geneva on 20 December 1996.

[7] See e.g. Ficsor (2002), para 1.45 *et seq*.

[8] Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

[9] Recital 31 of directive 2001/29 holds that "A fair balance of rights and interests between the different categories of right holders, as well as between the different categories of right holders and users of protected subject-matter must be safeguarded." Cf. recital 4 which states that "A harmonised legal framework on copyright and related rights, through increased legal certainty and while providing for a high level of protection of intellectual property, will foster substantial investment in creativity and innovation, including network infrastructure, and lead in turn to growth and increased competitiveness of European industry, both in the area of content provision and information technology and more generally across a wide range of industrial and cultural sectors. This will safeguard employment and encourage new job creation." See also recital 2 which holds that "[c]opyright and related rights play an important role in this context as they protect and stimulate the development and marketing of new products and services and the creation and exploitation of their creative content".

preamble to the WCT[10] and WPPT[11] and article 7 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).[12] Hence, at its very core, the copyright system is concerned with the production and dissemination of creative content for the benefit of society and the need to strike a fair balance between these interests.[13] This has been stressed by the Court of Justice of the European Union (CJEU) on several occasions.[14]

This balance of interests—or dual aim—of the copyright system in relation to linking and certain search engines has been brought to the fore in two judgements recently delivered by the CJEU. Depending on the interpretation of these cases, they will probably have a direct impact on how content is made available, located and accessed on the Internet, the development of new business models and indirectly also on the remuneration provided for authors and other actors in the creative sectors.

The first case, *Innoweb,*[15] concerned the activities of a so-called dedicated meta search engine and its compatibility with the right of re-utilisation in article 7 of EU directive 96/9 on the legal protection of databases.[16] The second case, *Svensson and Others*,[17] dealt with linking to content protected by copyright on the Internet in relation to article 3.1 of EU directive 2001/29 on copyright in the information society. Considering the potential importance of the two cases, it is somewhat surprising that neither of the cases was subject to an opinion by the Advocate General. This is supposed to occur only in cases that do not give rise to a new point of law. At least *Svensson* concerned a topic with considerable differences of opinion, not

[10] The preamble to the WCT includes the following statements: "Recognizing the need to introduce new international rules and clarify the interpretation of certain existing rules in order to provide adequate solutions to the questions raised by new economic, social, cultural and technological developments", "Recognizing the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information, as reflected in the Berne Convention" and "Recognizing the profound impact of the development and convergence of information and communication technologies on the creation and use of literary and artistic works".

[11] The preamble to the WPPT includes the following statements: "Recognizing the need to introduce new international rules in order to provide adequate solutions to the questions raised by economic, social, cultural and technological developments", "Recognizing the profound impact of the development and convergence of information and communication technologies on the production and use of performances and phonograms", and "Recognizing the need to maintain a balance between the rights of performers and producers of phonograms and the larger public interest, particularly education, research and access to information".

[12] Article 7 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) sets out the goal to protect property under the Agreement for "the mutual advantage of producers and users of technological knowledge … in a manner conducive to social and economic welfare".

[13] Axhamn (2013, p. 164).

[14] See e.g. joined cases C-403/08 and C-429/08, FAPL, para. 179.

[15] Case C-202/12, Innoweb BV v Wegener Media BV and Wegener Mediaventions BV.

[16] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ 1996 L 77, p. 20 (hereafter: the database directive).

[17] Case C-466/12, Nils Svensson and Others v Retriever Sverige AB.

only among legal scholars but also between EU Member States; as regards both the issue of linking and general issues related to the interpretation of the notion of "communication to the public" as expressed in recent case law from the CJEU.

This article will describe and analyse the two cases and discuss their potential impact on how content is accessed, reused and made available on the Internet. The analysis and discussion will relate to the underlying need to strike a fair balance between the protection of creative content and its dissemination, inherent in many copyright cases and legislative copyright policy decisions.

2 Innoweb

Innoweb refers to a ruling from the CJEU following a request for a preliminary ruling by the Gerechtshof te's-Gravenhage (The Hague Regional Court, The Netherlands). The decision sheds light on how the *sui generis* database right, which dates back to 1996, applies to modern day meta search engines in the Internet advertising market—a phenomenon barely thought of 18 years ago when the directive was adopted. Thus, when reading the Innoweb case, one should have in mind that the underlying rationale of the *sui generis* right is to safeguard the position of makers of databases against misappropriation of the results of the financial and professional *investment* made in obtaining and collecting the contents of the database,[18] *inter alia* by serving as a means to *secure the remuneration* of the maker of the database.[19] This is reflected in article 7 of the directive, which relates the investment to acts carried out with the contents of the database:

> Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.

In addition, under article 7.5 of the same directive, which serves as a safeguard clause to ensure that the lack of protection of the insubstantial parts does not lead to their being repeatedly and systematically extracted and/or re-utilised,[20] it is not permissible to re-utilise insubstantial parts of the contents of a protected database where that re-utilisation is repeated and systematic, implying acts which conflict with a normal exploitation of that database or which unreasonably harm the

[18] Recital 39 to the database directive.

[19] Recital 48 to the database directive.

[20] See case C-203/02, The British Horseracing Board and Others, para 85 with reference to Common Position (EC) No 20/95 adopted by the Council on 10 July 1995 (OJ 1995 C 288, p. 14), point 14 of the Council's statement of reason.

legitimate interests of the database maker. The objective of the *sui generis* right to protect investment is thus quite different from the objective of copyright, which is to protect subject matter that constitute an author's own intellectual creation.[21]

2.1 Background

Through its AutoTrack website (www.autotrack.nl), the Dutch company Wegener provided access to an online collection of advertisements for cars, together with a list, updated daily, of about 200,000 second-hand cars.[22] The sellers were private individuals, car showrooms or garages. Approximately 40,000 of those advertisements were found only on autotrack.nl, while the other advertisements could be found elsewhere as well. With the help of the AutoTrack website search engine, users could carry out targeted searches for vehicles on the basis of various criteria.[23]

Another company, Innoweb, ran GasPedaal, a dedicated meta search engine via its gaspedaal.nl website, and this too was devoted to car sales.[24] In its reasoning, the CJEU explained that a dedicated meta search engine is "dedicated" in so far as it searches only through specific websites, and it is "meta" in so far as it gets the search engines of those specific websites to do the searching and in this case to supply the results to the GasPedaal search engine.[25] According to the Court, the latter feature differentiates meta search engines from general ("web") search engines such as Google or Yahoo, which are based on algorithms.[26]

---

[21] Cf. Article 3(1) of the database directive which holds that "databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection". Similar statements are found for the copyright protection of photographs in article 6 in directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights, and, as regards computer programs, in article 1.3 of directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version). Via case law from the CJEU, the requirement of "author's own intellectual creation" has been deemed to have general application also for other categories of works than databases, photographs and compute programs. See e.g. case C-5/08, Infopaq International A/S v Danske Dagblades Forening, paras. 30 to 51, case C-393/09, Bezpečnostní softwarová asociace—Svaz softwarové ochrany v Ministerstvo kultury, paras. 43–51, case C-403/08, Football Association Premier League and Others, paras. 96–100, and case C-145/10, Painer, paras. 85–99. For a discussion, see e.g. Rosati (2013).

[22] Innoweb, para. 2. AutoTrack was a venture of Dutch/Belgian publisher De Persgroep.

[23] Innoweb, para. 8.

[24] Gaspedaal was a venture of Dutch publisher De Telegraaf.

[25] Innoweb, paras. 9 and 25.

[26] Innoweb, para. 24.

Although it most probably did not have an impact on the outcome of the case, it should, however, be noted that meta search engines are also based on algorithms. The difference between the algorithms used by ordinary search engines and algorithms used by meta search engines is that in the former case, the algorithms serve the purpose of compiling a physical database or catalogue of the web ("indexing"). Meta search engines do not index web pages; their algorithms serve the purpose of collecting the results from the selected search engines, merging them together and presenting them to the user.[27] Due to the enormous quantity of documents that the Internet contains, it is impossible that a single search engine index links the totality of the web. Therefore, by means of providing a unified interface for consulting a combination of different searchers, meta search engines serve the purpose of improving web search results.[28]

Accordingly, a car search using GasPedaal enabled the user simultaneously to carry out searches of several collections of car advertisements listed on third-party sites, including AutoTrack. When a GasPedaal user searched for a particular type of car, GasPedaal translated the query into the format of the search engines of these websites. GasPedaal then retrieved data directly, i.e. in "real time", from these websites and displayed the combined search results in its own layout to the user. A web page with the list of results showed essential information relating to each car, including the year of manufacture, the price, the mileage, a thumbnail picture and links to all the sources where the car could be found.[29]

The total number of website advertisements searched through GasPedaal was around 300,000. GasPedaal daily carried out around 100,000 searches on the AutoTrack website, subjecting approximately 80 % of the various combinations of makes or models listed on the AutoTrack collection to search daily. In response to each query, however, GasPedaal displayed only a very small part of the contents of that collection, as the displayed data were determined on the basis of the criteria keyed into GasPedaal by the user.[30]

On the view that Innoweb was compromising its *sui generis* right in relation to its database of car advertisements, Wegener brought an action for injunctive relief to protect its database right and, at first instance, succeeded in all essential respects. Innoweb appealed to the Gerechtshof te's-Gravenhage (Regional Court of Appeal, The Hague). The Court held that Wegener's collection of car ads was a database, but did not consider this to be a situation in which the whole or a substantial part of that database was *extracted* in the meaning of article 7.1 of directive 96/9 on the protection of databases. Nor did the Court find the *repeated extraction* of insubstantial parts of the contents of that database to have cumulative effect in the meaning of article 7.5 of the same directive. However, the Court decided to stay the proceedings and to refer a total of nine questions to the CJEU

[27] Wu and Li (2004, p. 305), and Olivas (2008, p. 538). Cf. Innoweb, paras. 24 and 25.

[28] Olivas (2008, p. 537 ff).

[29] Innoweb, paras. 10 and 11.

[30] Innoweb, paras. 12 and 13.

for a preliminary ruling mainly related to the concept of *re-utilisation* in article 7.1 of directive 96/9. The Court of Appeal asked the CJEU whether Innoweb's acts constituted "re-utilisation" of the "whole or of a substantial part" of the contents of Wegener's database.[31]

2.2 The Response of the CJEU with Comments and Analysis

In answering the questions from the referring Court, the CJEU ruled that article 7.1 of directive 96/9 must be interpreted as meaning that an operator who makes available on the Internet a dedicated meta search engine re-utilises the whole or a substantial part of the contents of a database under article 7, where that dedicated meta engine

i. provides the end user with a search form which essentially offers the same range of functionality as the search form on the database site,
ii. "translates" queries from end users into the search engine of the database site "in real time", so that all the information on that database is searched and
iii. presents the results to the end user using the format of its own website, grouping duplications together into a single block item but in an order that reflects criteria comparable to those used by the search engine of the database site concerned for presenting results.[32]

The CJEU reached this conclusion by referring to previous case law, according to which the use, in article 7.2.b of directive 96/9, of the phrase "any form of making available to the public" indicates that the Community legislature attributed a broad meaning to "re-utilisation".[33] That broad construction is lent support by the objective pursued by the Community legislature through the establishment of a *sui generis* right.[34] As held by the CJEU in previous cases, that objective is to stimulate the establishment of data storage and processing systems which contribute to the development of an information market against a background of exponential growth in the amount of information generated and processed annually in all sectors of activity.[35] To that end, the *sui generis* right under directive 96/9 is intended to ensure that the person who has taken the initiative and assumed the risk of making a substantial investment in terms of human, technical and/or financial resources in the setting up and operation of a database receives a return on his

[31] Innoweb, para. 18.

[32] Innoweb, para. 54.

[33] Innoweb, para. 33, with reference to Case C-203/02, The British Horseracing Board and Others, para. 51 and Case C-173/11, Football Dataco and Others, para. 20.

[34] Innoweb, para. 34, with reference to Case C-304/05, Directmedia Publishing, para. 32.

[35] Innoweb, para. 35, with reference to Case C-203/02, The British Horseracing Board and Others, paras. 30 and 31 and Case C-604/10, Football Dataco and Others, para. 34.

investment by protecting him against the unauthorised appropriation of the results of that investment.[36]

According to the Court, GasPedaal was thus depriving AutoTrack of revenue which should have enabled AutoTrack to redeem the cost of its investment.[37] This was the case as GasPedaal was not limited to indicating to the user databases providing information on a particular subject[38] and because it ordered duplications into one item.[39] This, the Court stated, created a risk that the database maker would lose income,[40] a risk that could not be ruled out by force of the argument that it is still necessary, as a rule, to follow the hyperlink to the original page on which the result was displayed.[41] The Court further held:

> As the end user no longer has any need to proceed via the database site's homepage and search form, it is possible that the maker of that database will generate less income from the advertising displayed on that homepage or on the search form, especially to the extent that it might seem more profitable for operators wishing to place advertisements online to do so on the website of the dedicated meta search engine, rather than on one of the database sites covered by that meta engine.
>
> As regards, furthermore, database sites displaying advertising, sellers—aware that, with the dedicated meta search engine, searches will be made simultaneously in several databases and duplications displayed—may start placing their advertisements on only one database at a time, so that the database sites would become less extensive and therefore less attractive.[42]

It is thus important to bear in mind that the ruling concerned the activities made possible by Innoweb which occurred *prior* to the activities carried out by the end users, namely the actual searching of the databases. The actual search undertaken by GasPedaal in response to a query—including the presentation of the results to the end user—took place automatically, in accordance with the way in which the meta search engine had been programmed, without any intervention on the part of GasPedaal at that stage.[43] It was thus Innoweb's *offering* of the whole or a substantial part of Wegener's database that was *made possible* by the creation of Gaspedaal that the Court deemed deprived Wegener of potential advertising revenues which it would have used to recoup its investment.[44] The fact that only part of the entire database was actually consulted was held irrelevant as the entire

---

[36] Innoweb, para. 36, with reference to Case C-203/02, The British Horseracing Board and Others, paras. 32 and 46 and Case C-304/05, Directmedia Publishing, para. 33.

[37] Innoweb, para. 37, with reference to Case C-203/02, The British Horseracing Board and Others, para. 51.

[38] Innoweb, para. 39.

[39] Innoweb, para. 43.

[40] Innoweb, para. 41.

[41] Innoweb, para. 44.

[42] Innoweb, paras. 42 and 43.

[43] Innoweb, paras. 28 and 29.

[44] Innoweb, paras. 29 and 39–54.

database was in fact made available to the end user.[45] According to the Court, this practice by Innoweb came "close to the manufacture of a parasitical competing product"[46] and thus infringed Wegener's right of re-utilisation.[47]

The reasoning by the CJEU in *Innoweb* has been met by both praise and criticism by commentators. Some have held that as Innoweb's service and similar business models are for the benefit of consumers, the law should not discourage it.[48] The decision might outlaw the operation of most socially beneficial websites that help consumers to compare prices or qualities of different goods offered on the Internet. It is thus not obvious that it is beneficial for the innovation policy of the EU to make the operation of such websites dependent on the mere tolerance of the "big players", especially when smaller competitors are possibly the greatest beneficiaries of these comparison websites.[49]

Others have stressed that the ruling in *Innoweb* will be of utmost importance for the digital publishing industry; it has been held to be "a strong incentive to develop quality data products without having to fear that these products will immediately be parasitized."[50] Indeed, one of the reasons for creating the *sui generis* database right in the first place was the desire to increase the EU's rate of producing databases—a desire which has so far not been borne out in practice: a fact that might be reversed by this decision.[51]

The ruling is quite detailed and fact-specific—concerning a dedicated meta search engine that gives the user essentially the same range of functionality as that on the underlying site, does searches in real time, blocks duplicated results and allows the user to rank the output. The tenor of the judgement, however, indicated that other "parasitical" web scraping will also be contrary to the *sui generis* right.[52]

---

[45] Innoweb, paras. 46 and 47.

[46] Innoweb, para. 48.

[47] Innoweb, paras. 53 and 54.

[48] See e.g. Stepping on the GasPedaal (2013).

[49] Cf. Husovec, Does Innoweb hinder innovation on the web? posted on the Kluwer Copyright Blog on 20 Jan 2014. Available at http://kluwercopyrightblog.com/2014/01/20/eu-does-innoweb-hinder-innovation-on-the-web/. Last visited on 14 Apr 2014.

[50] See CJEU takes foot of the GasPedaal, then puts the boot in, posted on The 1709 Blog on 25 Dec 2013. Available at http://the1709blog.blogspot.se/2013/12/cjeu-takes-foot-off-gaspedaal-then-puts.html. Last visited on 14 Apr 2014.

[51] Indeed, even the EU Commission has remarked: "Is sui generis protection therefore necessary for a thriving database industry…the empirical evidence, at this stage, casts doubt on this necessity". See 2005 DG Internal Market and Services Working Paper; First Evaluation of Directive 96/9/EC on the legal protection of databases, 12 December 2005, p. 5.

[52] Cf. Prinsley & Byrt, When is web-scraping of a database unlawful? posted on 7 Jan 2014. Available at http://www.mayerbrown.com/When-is-web-scraping-of-a-database-unlawful-01-07-2014/. Last visited on 20 Apr 2014.

However, anyone seeking to venture into the attractive territory of meta search should study the judgement carefully before deciding to throw in the towel.[53]

In any case, even if there is logic inherent in the *Innoweb* case based on the *sui generis* right, a question that immediately springs to mind is how a similar situation, however, specifically focused on linking, is dealt with from a copyright perspective (See Footnote 49). This issue was subject to the CJEU's ruling in *Svensson* and is dealt with in the next section.

3 Svensson

The treatment of clickable Internet links (hyperlinks) under copyright law is important because they are found everywhere on the web, forming an essential part of the web's infrastructure by enabling access to information. Millions of hyperlinks are created and clicked on around the world on a daily basis, forming an integral component of e-commerce and day-to-day practice for businesses and consumers alike. Thus, the legal status of Internet links has been a widely discussed subject in recent times, pitting those[54] who consider links an act of communication to the public within the meaning of article 3.1 of directive 2001/29 against those[55] who argue that the creation of Internet links does not, strictly speaking, constitute an act of communication to the public. Article 3.1 stipulates:

> Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.

Recitals 23 and 25 to the directive serve as a means for the interpretation of article 3.1. Recital 23 holds that the directive "should harmonise further the author's right of communication to the public. This right should be understood in a broad sense covering all communication to the public not present at the place where the communication originates. This right should cover any such transmission or retransmission of a work to the public by wire or wireless means, including broadcasting. This right should not cover any other acts". Recital 25 holds that all rightholders recognised by directive 2001/29 should have an exclusive right to make available to the public copyright works or any other subject matter by way of interactive

---

[53] Cf. ECJ ruling on meta search engines strengthens position of database right holders available at http://www.debrauw.com/newsletter/ecj-ruling-meta-search-engines-strengthens-position-database-right-holders/#. Last visited on 20 Apr 2014.

[54] Cf. ALAI Report and Opinion on the making available and communication to the public in the internet environment—focus on linking techniques on the Internet. Adopted unanimously by the Executive Committee 16 Sept 2013. Available at http://www.alai.org/assets/files/resolutions/making-available-right-report-opinion.pdf. Last visited on 16 Apr 2014 (hereinafter ALAI Opinion on Svensson).

[55] See e.g. Opinion by the European Copyright Society on Svensson.

on-demand transmissions. Such interactive on-demand transmissions are "characterised by the fact that members of the public may access them from a place and at a time individually chosen by them".

Article 3.1 builds on and serves to implement article 8 of the WCT in the European Union in a harmonised manner.[56] Moreover, article 3.1 of the directive must, so far as possible, be interpreted in a manner that is consistent with the obligations arising from the corresponding provision of WCT.[57]

Whereas the first part of article 3.1 establishes a broad right of communication to the public, the second part ("making available") refers to a specific type of communication to the public: a right to control individualised and interactive (*on demand*) uses of copyrighted works.[58] The introduction of the "making available" right is widely regarded as one of the main achievements of the WCT.[59] The phrase "may access" indicates that actual access to the work by a member of the public may occur at a later time, or not at all: a "transmission" is thus not required for an act of "making available".[60] The right of "making available" thus differs from traditional "communications", such as broadcasting and cable retransmission, in that it explicitly encompasses the mere *offering* to the public of a work.[61] This includes individualised pay-per-view television services or online services providing streaming or downloading of music and films. Hence, the right of communication to the public in article 3.1 of the directive includes the act of making

[56] See recital 15 to directive 2001/29.

[57] See e.g. SGAE, para 35.

[58] Article 3.1 of directive 2001/29 is almost verbatim to article 8 WCT, which holds that "Without prejudice to the provisions of Articles 11(1)(ii), 11bis(1)(i) and (ii), 11ter(1)(ii), 14(1)(ii) and 14bis(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them". The first part of article 8 extends the coverage of the right of communication to the public in the Berne Convention from certain categories of works (see articles 11, 11*bis* and 11*ter* of the Berne Convention) to all categories of works. See von Lewinski (2008, paras. 5.138 and 17.107); Ricketson and Ginsburg (2006, para. 4.25); Goldstein and Hugenholtz (2013, p. 325).

[59] See e.g. Ricketson and Ginsburg (2006, para. 12.57) and von Lewinski (2008, para. 17.72).

[60] Cf. WIPO, Chairman of the Committees of Experts, Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be considered by the Diplomatic Conference, WIPO Doc. CRNR/DC/4, 30 August 1996, para 10.10: "The relevant act is the making available of the work by providing access to it. What counts is the initial act of making the work available…" See also von Lewinski (2008), para. 17.73 and ALAI Opinion on Svensson.

[61] See e.g. Ricketson and Ginsburg (2006), para. 12.58, WIPO Guide to the Copyright and Related Rights Treaties Administered by WIPO, para. CT-86, Walter and von Lewinski (2010), para. 11.3.30, Ginsburg (2014), p. 147 *et seq*.

available online, an activity that presumes an active role on the part of the communicator and also a potential activity on the part of the consumer.[62]

Strangely enough, up until recently, there had been no case before the CJEU on the interpretation of article 3.1 in relation to linking. The first case to reach Court on this matter was *Svensson*. In this case, the CJEU held that a website which redirected Internet users through hyperlinks to protected works which were already freely available online did not infringe copyright in those works. This was the case even if the Internet users who clicked on the link had the impression that the work appeared on the site that contained the link.

3.1 Background

The background to the case was the following. Retriever was a Swedish company that operated a website (Retriever, http://retriever-info.com) through which users were provided with hyperlinks to articles on other websites. Svensson and the other claimants in the main proceedings were all journalists who wrote articles published in the Göteborgs-Posten newspaper and on the newspaper's website, where they were freely accessible. Retriever provided hyperlinks to articles on the Göteborgs-Posten website without the permission of their respective authors.[63]

It is not apparent from the available facts of the case how retriever created these links. i.e. if Retriever acted as an ordinary search engine by indexing the pages on the Göteborgs-Posten website and proved links to these website after an individual search by an end user. If this is the case, Retriever would be more akin to an "ordinary" search engine than a meta search engine.

The claimants brought an action against Retriever Sverige before Stockholms tingsrätt (the Stockholm District Court) in order to obtain compensation on the grounds that that company had made use, without their authorisation, of certain articles by them, by making these articles available to its clients. After losing in first instance, the claimants then brought an appeal against the judgement before Svea hovrätt (the Svea Court of Appeal). The Court of Appeal decided to stay the proceedings and to refer four questions to the CJEU for a preliminary ruling on the

[62] Cf. European Commission, Proposal for a European Parliament and Council Directive on the harmonisation of certain aspects of copyright and related rights in the Information Society, 10 December 1997, COM(97)0628, pp. 25–26: "The second part of Article 3(1) addresses the interactive environment. It follows closely the pattern chosen in Article 8 WCT and implements it at Community level. … As was stressed during the WIPO Diplomatic Conference, the critical act is the 'making available of the work to the public', thus the offering [of] a work on a publicly accessible site, which precedes the stage of its actual 'on-demand transmission'. It is not relevant whether any person actually has retrieved it or not". See also Ricketson and Ginsburg (2006), para. 12.57 *et seq*, Walter and von Lewinski (2010), para. 11.3.30 and ALAI Opinion on Svensson.

[63] Svensson and Others, para. 8.

interpretation of the notions of "communication to the public" and "making available to the public" in article 3.1 of directive 2001/29.[64]

The first three questions posed by the Svea Court of Appeal concerned whether article 3.1 of directive 2001/29 must be interpreted as meaning that the provision, on a website, of clickable links to protected works available on another website constitutes an act of communication to the public as referred to in that provision, where, on that other site, the works concerned were freely accessible.[65] The fourth question concerned the meaning of the last sentence in recital 23; whether article 3.1 must be interpreted as precluding a Member State from giving wider protection to copyright holders by laying down that the concept of communication to the public includes a wider range of activities than those referred to in that provision.[66]

3.2 The Response by the CJEU with Comments and Analysis

In answering the first three questions, the CJEU emphasised that it follows from article 3.1 of directive 2001/29 that *every* act of communication of a work to the public has to be authorised by the copyright holder.[67] However, an act of communication to the public requires both an "act of communication" of a work and the communication of that work to a "public".[68]

As regards the first of those criteria, the Court held that for there to be an "act of communication", it is sufficient that a work is made available to *a public* in such a way that the persons forming *that public* may access it, irrespective of whether they avail themselves of that opportunity.[69] It followed that, in circumstances such as those in the case in the main proceedings, the provision of *clickable links* to protected works must be considered to be "making available" and, therefore, an "act of communication", within the meaning of article 3.1.[70] Thus, it is not relevant whether there the work has been subject to a *transmission* or if it is has been "made available"—i.e. merely offered—*on demand* in such a way that members of the public may access it from a place and at a time individually

[64] Svensson and Others, paras. 9–13.

[65] Svensson and Others, para. 14.

[66] Svensson and Others, para. 33.

[67] Svensson and Others, para. 15.

[68] Svensson and Others, para. 16, with reference to Case C-607/11, ITV Broadcasting and Others, paras. 21 and 31.

[69] Svensson and Others, para. 19, with reference to Case C-306/05, SGAE, para. 43.

[70] Svensson and Others, para. 20.

chosen by them. This is a dead end for the arguments that a communication always presupposes a transmission and that hyperlinking acts as a mere indication of source or reference.[71]

As regards the requirement of "public", the Court held that it follows from article 3.1 that, by the term "public", that provision refers to an *indeterminate number* of *potential* recipients and implies a *fairly large* number of persons.[72] However, with reference to previous case law, the Court noted that "a communication concerning the same works as those covered by the initial communication and made … *by the same technical means*, must also be directed at a *new public*, that is to say, at a public not taken into account by the copyright holders when they authorized the initial communication to the public". [my emphasis][73]

The Court found that the initial communication (carried out by Göteborgs-Posten) targeted *all potential users*, as access to the Göteborgs-Posten website was not subject to any restriction (e.g. paywalls). Accordingly, the links provided by

[71] See Hyperlinks, making available and the "new public"—or just a dead end? posted on the 1709 Blog on 14 Feb 2014. Available at http://the1709blog.blogspot.se/2014/02/hyperlinks-making-available-and-new.html. Last visited on 15 Apr 2014. This interpretation had been put forward in ALAI Opinion on Svensson and Rosén (2012), p. 163 *et seq*. Cf. Bentley and Sherman (2008, p. 151): "Most hyper-linking simply makes it easier to locate (and, if desired, access) works which are already available to the public, and it would be unduly constraining to require all links to be authorized." Similar arguments are put forward by Litman (2001, p. 183) ("Referring to a copyrighted work without authorization has been and should be legal. … Posting a hypertext link should be no different."), de Beer and Burri (2014, p. 104) ("We … stress yet again the critical role of hyperlinking for the working of the internet. In light of the case law, we think in particular that there has been no transmission, which is clearly a prerequisite for the communication to the public."), and Aplin (2005, s. 151) ("It seems misconceived to say that [links] constitute making available … all they have done is referred other users to where the files may be readily found."). See also case law from the German Supreme Court in the Paperboy case, dated 17 July 2003, para. 42 ("A person who sets a hyperlink to a website with a work protected under copyright law which has been made available to the public by the copyright owner, does not commit an act of exploitation under copyright law by doing so but only refers to the work in a manner which facilitates the access already provided."), and case law from the Norwegian Supreme Court in the Napster. no case, dated 27 January 2005, para. 47 ("It cannot be doubted that simply making a website address known by rendering it on the internet is not making a work publicly available.") See further Opinion by the European Copyright Society on Svensson, e.g. at para. 40: "[A] hyperlink is a location tool, allowing a user to find where a work is".

[72] Svensson and Others, para. 21, with reference to Case C-306/05, SGAE, paras. 37 and 38, and ITV Broadcasting and Others, para. 32.

[73] Svensson and Others, para. 24, with reference to Case C-306/05, SGAE, paras. 40 and 42, and ITV Broadcasting and Others, para. 39. In this connection, it is significant that the CJEU does not find direct support for the interpretation the right of communication in relation to authors' works in article 3.1 of directive 2001/29 in its case law concerning the right of communication to the public for certain neighbouring rights in article 8.2 of directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version). This case law includes e.g. case C-135/10, SCF, and case C-162/10, Phonographic Performance.

Retriever did *not* make the articles available to a *new public* and, therefore, there was no requirement for Retriever to obtain the journalists' consent.[74]

By this, the Court thus seem to indicate that there is connection between the requirement of a "new public" in cases where the communication is carried out by the same technical means, whereas this requirement does not seem to be present if the technical means differ. This reasoning seems to be built on the three-tier model of communication to the public as set out in article 11*bis*(1) of the BC. This provision holds that authors have the exclusive right to authorise (i) primary broadcasts of their work, (ii) rebroadcasts by third parties and (iii) presentations of the original broadcast by loudspeakers and the like.[75] A requirement of "new public" in cases where the communication to the public is carried out by the same technical means seems to be present also in previous rulings by the CJEU. In any case, neither the BC nor any other international treaty on copyright defines the term "public". It may, however, not be defined too narrowly; the core potential of the rights must be safeguarded.[76]

> The case *SGAE*[77] involved the dissemination of satellite broadcasts to, inter alia, hotel guests in their rooms. The hotel was held to have carried out a type-(ii) communication to the public, separate from the original broadcasts. It was an independent act through which the broadcast was communicated to a new public (i.e. a different public from the one at which the original broadcast was directed).[78] This case was followed by *Airfield and Canal Digitaal,*[79] which involved the dissemination of encrypted satellite broadcasts to a satellite package provider's customers. The intervention by the satellite package provider was again held to be a separate type-(ii) communication to the public.[80] A type-(iii) communication to the public was considered in *Football Association Premier League and*

[74] Svensson and Others, paras. 25–32.

[75] Article 11*bis*(1) of the Berne Convention for the protection of literary and artistic works states that authors of literary and artistic works shall enjoy the exclusive right of authorizing: (1) the broadcasting of their works or the communication thereof to the public by any other means of wireless diffusion of signs, sounds or images; (2) any communication to the public by wire or by rebroadcasting of the broadcast of the work, when this communication is made by an organisation other than the original one; (3) the public communication by loudspeaker or any other analogous instrument transmitting, by signs, sounds or images, the broadcast of the work.

[76] See also von Lewinski (2008), paras. 5.147 and 17.77 and Ricketson and Ginsburg (2006), paras. 12.02 and 12.41.

[77] Case C-306/05, Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles SA.

[78] SGAE, para 40: "It should also be pointed out that a communication made in circumstances such as those in the main proceedings constitutes, according to Article 11bis(1)(ii) of the Berne Convention, a communication made by a broadcasting organisation other than the original one. Thus, such a transmission is made to a public different from the public at which the original act of communication of the work is directed, that is, to a new public".

[79] Joined cases Airfield NV and Canal Digitaal BV v Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (Sabam) (C-431/09) and Airfield NV v Agicoa Belgium BVBA (C-432/09).

[80] Airfield and Canal Digitaal, para. 82: "[A]ccordingly it must be found that the satellite package provider expands the circle of persons having access to the television programmes and enables a new public to have access to the works and other protected subject-matter".

> *Others*,[81] which involved the showing of satellite broadcasts on a television in a pub. The intervention by the pub owner was held to be a communication to a new public for the works comprised in the broadcasts.[82] In *ITV Broadcasting and Others*,[83] which concerned the redistribution by an intermediary of terrestrial broadcasts on the Internet, the CJEU stated that each transmission or retransmission by a "specific technical means" may give rise to a separate communication to the public. As the communication to the (general) public over the Internet was carried out through a different technical means to the primary broadcast, the CJEU deemed that it was not necessary to consider whether it was a new public or not to find that it was a "communication to the public".[84]

Thus, the Court seems to apply a "new public" test only where the technical means of communication to the public is the same for the "re-communication" as for the original or primary communication (situations which might be referred to as "dependent" acts of communication of the public), whereas this is not necessary in cases where the technical means differ ("independent" acts of communication to the public). This interpretation finds support in the Guide to the BC, an interpretative document drawn up by WIPO which, without being legally binding,

---

[81] Joined cases Football Association Premier League Ltd and Others v QC Leisure and Others (C-403/08) and Karen Murphy v Media Protection Services Ltd (C-429/08).

[82] Football Association Premier League and Others, paras. 192 and 197–199: "[A]s Article 11bis(1)(iii) of the Berne Convention expressly indicates, that concept encompasses communication by loudspeaker or any other instrument transmitting, by signs, sounds or images, covering—in accordance with the explanatory memorandum accompanying the proposal for a copyright directive (COM(97) 628 final)—a means of communication such as display of the works on a screen. … That said, in order for there to be a 'communication to the public' within the meaning of Article 3(1) of the Copyright Directive in circumstances such as those of the main proceedings, it is also necessary for the work broadcast to be transmitted to a new public, that is to say, to a public which was not taken into account by the authors of the protected works when they authorised their use by the communication to the original public. … When those authors authorise a broadcast of their works, they consider, in principle, only the owners of television sets who, either personally or within their own private or family circles, receive the signal and follow the broadcasts. Where a broadcast work is transmitted, in a place accessible to the public, for an additional public which is permitted by the owner of the television set to hear or see the work, an intentional intervention of that kind must be regarded as an act by which the work in question is communicated to a new public. … That is so when the works broadcast are transmitted by the proprietor of a public house to the customers present in that establishment, because those customers constitute an additional public which was not considered by the authors when they authorised the broadcasting of their works".

[83] Case C-607/11, ITV Broadcasting Ltd and Others v TV Catch Up Ltd.

[84] ITV Broadcasting and Others, para. 39: "[T]he main proceedings in the present case concern the transmission of works included in a terrestrial broadcast and the making available of those works over the internet. … [E]ach of those two transmissions must be authorised individually and separately by the authors concerned given that each is made under specific technical conditions, using a different means of transmission for the protected works, and each is intended for a public. In those circumstances, it is no longer necessary to examine below the requirement that there must be a new public, which is relevant only in the situations on which the Court of Justice had to rule in the cases giving rise to the judgments in SGAE, Football Association Premier League and Others and Airfield and Canal Digitaal".

nevertheless assists in interpreting that Convention,[85] the preparatory works to the BC,[86] and in legal scholarship.[87] It also finds support in a panel report settling a dispute between the European Communities and the USA on the compatibility of Sect. 110(5) of the US Copyright Act, with obligations in TRIPS. Section 110(5) in the US Copyright Act permitted, under certain conditions, the playing of radio and television music in public places (bars, shops, restaurants, etc.) without the payment of a royalty fee—i.e. communications to potentially "new publics".[88]

As regards the type of linking in question, the CJEU held that it did not matter if, when Internet users clicked on the link, the work appeared in such a way as to give the impression that it was appearing on the site on which that link was found, whereas in fact that work came from another site.[89] Thus, it would appear to be permissible to "deep-link"[90] or to "frame"[91] to freely accessible content on another

[85] It is held in the Guide that when the author authorises the broadcast of his work, he considers only direct users, that is, the owners of reception equipment who, either personally or within their own private or family circles, receive the programme. According to the Guide, if reception is for a larger audience, possibly for profit, a new section of the receiving public hears or sees the work and the communication of the programme via a loudspeaker or analogous instrument no longer constitutes simple reception of the programme itself but is an independent act through which the broadcast work is communicated to a new public. As the Guide makes clear, such public reception falls within the scope of the author's exclusive authorisation right. See WIPO (1978, pp. 68–69). The CJEU refers to this Guide in connection with the requirement of "new public" in SGAE, para 41.

[86] See Berne Convention Centenary (1986, p. 185) (referring to the discussions at the 1948 Brussels Revision Conference): "According to the explanatory memorandum prepared by the Belgian authorities and the Bureau of the Union, any broadcast aimed at a new circle of listeners or viewers, whether by means of a new emission over the air or by means of a transmission by wire, must be regarded as a new act of broadcasting, and as such subject to the author's specific authorization. … Consequently, the majority (12 votes to six) decided in favour of a Belgian proposal presupposing the intervention of a body other than the original one as a condition for the requirement of a new authorization".

[87] See e.g. Westman (2012, p. 801 ff.), Tsoutsanis (2014, p. 13) and Ricketson and Ginsburg (Ricketson and Ginsburg 2006), para. 12.24 *et seq*. Cf. Kur and Dreier (2013, p. 299), de Beer and Burri (2014, p. 103), Rosén (2012, p. 164) *et seq*.

[88] See panel report, USA—Section 110(5) of US Copyright Act (WT/DS160/R, dated 15 June 2000), paras. 6.19–29, 6.131–134, 6.152, 6.173 with footnote 155, 6.175 and 6.206. This interpretation was also put forward by the European Community during the proceedings, see Communication, from the Permanent Delegation of the European Commission to the Chairman of the Dispute Settlement Body, WT/DS160/5 concerning USA—Section 110(5) of US Copyright Act (WT/DS160/5, dated 15 April 1999), para 44, and the parties respective replies to Q4 on p. 112 and 174.

[89] Svensson and Others, paras. 29.

[90] Deep linking consists of using a hyperlink that links to a specific, generally searchable or indexed, piece of web content on a website, rather than the general home page as such. See e.g. Strowel and Ide (2001, p. 407), and Rosén (2012, p. 163).

[91] At the time of writing (April, 2014), the CJEU is still to provide a preliminary ruling in Case C-273/13, C More Entertainment. C-348/13, a case which concerns, *inter alia*, framing. Framing is the juxtaposition of two separate web pages within the same page, usually with a separate frame with navigational elements. Framing is a method of presentation in a web page that breaks the screen up into multiple non-overlapping windows. Each window contains a display from a separate HTML file, for example, a web page from a different website that is fetched by automatically hyperlinking to it. See e.g. Strowel and Ide (2001, p. 407).

website.[92] However, as the CJEU only gave a response in relation to "clickable" links, it is not clear what line is taken in regard to so-called inline or "embedded linking",[93] as such links do not necessarily concern situations where the end user "clicks" on a link; the content is usually provided to the user without any activity carried out by him or her. As the content is provided to the user, it seems quite probable that such acts are also considered to constitute a "making available".[94] However, a link which does not target a specific work, but merely works as a reference to a source from which it may subsequently be possible to access the work, is most probably not considered to make that work available to the public.[95]

The CJEU went on to explain that if the link allowed users to *bypass restrictions* designed to limit access to a protected work to, for example, a website's subscribers, those non-subscribing users would be a *new public* which was not taken into account by the copyright holders when they authorised the initial communication.[96] It would seem that the type of restriction the CJEU had in mind is a paywall. Paywalls are technological systems aimed at preventing users from accessing some of all contents of a given website without, e.g., paying a subscription fee.[97]

---

[92] This interpretation had been put forward in the ALAI Opinion on Svensson and the Opinion by the European Copyright Society on Svensson, paras 53–55. Cf. Ginsburg (2014, p. 148) and Svensson—it's all about the "new public", posted on the 1709 blog on 13 Feb 2014. Available at http://the1709blog.blogspot.se/2014/02/svensson-its-all-about-new-public.html. Last visited on 20 Apr 2014.

[93] Inline or embedded linking is the use of a linked object, often an image or a video, from one site by a web page belonging to a second site. The second site thereby has an inline link to the first site (where the object is located). See e.g. Strowel and Ide (2001, p. 407).

[94] At the time of writing (April, 2014), the CJEU is still to provide a preliminary ruling in case C-348/13, Bestwater, a case that has been stayed pending the decision in Svensson. The question referred is "Does the embedding, within one's own website, of another person's work made available to the public on a third-party website, in circumstances such as those in the main proceedings, constitute communication to the public within the meaning of Article 3(1) of Directive 2001/29/EC, even where that other person's work is not thereby communicated to a new public and the communication of the work does not use a specific technical means which differs from that of the original communication?"

[95] See e.g. Ginsburg (2014, p. 148): "The latter kind of linking may be compared to pointing a potential bookstore patron to a shelf of books and identifying the requested work; the first kind offers to pull the requested book off the shelf and put it in the patron's hands". Similar arguments are put forward in ALAI Opinion on Svensson. See also Strowel and Ide (2001, p. 407).

[96] Svensson and Others, paras. 31. It is supposed that the CJEU wanted to defer the argumentation to the pending referrals, especially Case C-273/13, C More Entertainment.

[97] See e.g. Strowel and Ide (2001, p. 425): "[A]s the work is already available to the entire Internet community at the linked site's web address, we cannot be dealing with a new act of making it available to the public. The link does not extend the work's audience; surfers who access the work by activating the link can also consult the page directly (as long as they know its URL)". See also Opinion by the European Copyright Society on Svensson, at para. 48(a): "It is well-known that material placed on the Internet without e.g. firewalls can be accessed from anywhere, and can be located using a range of search tools. Consequently, the copyright holder who authorises or permits such making available, must be assumed to contemplate the access to the work from anywhere. The creation of a hyperlink will thus not normally add to the public, as the targeted public is universal".

Mere contractual restrictions seem to fall outside of the kinds of "restrictions" envisioned by the Court.[98]

Although the requirement of "new public" appears to be a subjective criterion, rather than an objective requirement,[99] the CJEU stated affirmatively that the intention is given when the work is put openly on the Internet: a copyright holder who authorised an initial communication on the Internet of his or her content had in mind a "public" composed by "all Internet users [who] could have free access" to it.[100]

One factor that might have led the Court to emphasise the criterion of "new public" in cases concerning dependent acts of communication may be the principle underlying the doctrine of *exhaustion* of rights: a rightholder should not be entitled to additional remuneration once he has realised the full economic value of his content by putting it on the market. Seen from this perspective, the notion of "new public" could be considered as building on similar "economic" considerations as the CJEU put forward in its judgement in *UsedSoft.*[101] That case concerned *inter alia* the application of the principle of exhaustion to digital copies of computer software that had been bought and downloaded by customers of the Internet. The CJEU held that the owner of copyright in software cannot prevent a perpetual licensee who has downloaded the software from the Internet from selling his "used" license. Although the principle on "digital exhaustion" expressed in *UsedSoft* is most probably only relevant for computer software, *inter alia* because directive 2001/29 expressly stipulates that the exhaustion doctrine does not apply to the communication to the public

[98] See e.g. Post-Svensson stress disorder #2: What does "freely available" mean? posted on the IPKat blog on 7 March 2014. Available at http://ipkitten.blogspot.se/2014/03/post-svensson-stress-disorder-2-what.html. Last visited on 20 April 2014.

[99] See Post-Svensson Stress Disorder #1: Does it matter whether linked content is lawful? posted on the IPKat on 21 February 2014. Available at http://ipkitten.blogspot.se/2014/02/post-svensson-stress-disorder-1-does-it.html. Last visited on 14 April 2014. See also hyperlinks, making available and the "new public"—or just a dead end? posted on the 1709 Blog on 14 February 2014. Available at http://the1709blog.blogspot.se/2014/02/hyperlinks-making-available-and-new.html. Last visited on 15 April 2014.

[100] Svensson and Others, para. 26. Cf. ALAI Opinion on Svensson, where it is argued that linking to targeted content infringes the "making available" right if "the availability of the content, even if initially disclosed over the Internet with consent, otherwise clashes with the declared or clearly implied will of the rightholder. Accordingly, Courts should not introduce a general presumption of the rightholder's consent to further communication to the public of what initially has been posted on the Internet with the rightholder's consent, since this would amount to introducing an exception or limitation to the right, while general exceptions to the scope of the 'making available' right require legislative action". Similar arguments are put forward by Rosén (2012, p. 166) *et seq*. Cf. Rognstad (2003, p. 472).

[101] Case C-128/11, UsedSoft. See Riis, "Ophavsrettens fleksibilitet", Nordiskt Immateriellt Rättsskydd, p. 139 *et seq*.

right set out in that directive,[102] its economic rationale has strong similarities with the "restraint" on the exclusive right that has been introduced on the right of communication to the public by the requirement of "new public".

Svensson deals only with links to content that have been authorised to be made available online by the rightholders. A reasoning *e contrario* based on the Court's arguments seems to imply that if the copyright holder has *not* performed or authorised the initial communication, he or she would logically not have taken into account any public (at all). Consequently, if works have initially been made available on the Internet without the consent of the copyright holder, any subsequent act of communication of the infringing work—including hyperlinking to it—makes the work available to a new public. Thus, consent of the copyright holder in relation to content that is linked to on the Internet seems to be material in order to assess whether a link amounts to an act of communication to the public. This reinforces the argument that links are not merely references to a source, but rather constitute acts that are relevant from a copyright perspective.[103] It puts great responsibility on Internet users to make an assessment whether content that they link to has been put on the Internet with initial consent from the rightholders.[104]

Finally, in response to the fourth question, the CJEU held that Member States do not have the right to give wider protection to copyright holders by broadening the concept of "communication to the public". To allow this would lead to legislative differences between Member States, which was precisely what the directive in question

[102] The rights of communication and making available to the public for authors and holders of neighbouring rights are set out in articles 3.1 and 3.2 of directive 2001/29. Article 3.3 holds that "[t]he rights referred to in paragraphs 1 and 2 shall not be exhausted by any act of communication to the public or making available to the public as set out in this Article". Further, recital 29 to the directive states that "The question of exhaustion does not arise in the case of services and on-line services in particular. This also applies with regard to a material copy of a work or other subject-matter made by a user of such a service with the consent of the rightholder. Therefore, the same applies to rental and lending of the original and copies of works or other subject-matter which are services by nature. Unlike CD-ROM or CD-I, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which should be subject to authorisation where the copyright or related right so provides". The CJEU has also confirmed the view that it is apparent from article 3.3 of directive 2001/29 that authorising the inclusion of protected works in a communication to the public does not exhaust the right to authorise or prohibit other communications of those works to the public. See case C-607/11, ITV Broadcasting and Others, para 23.

[103] Tsoutsanis (2014, p. 13). Cf. Litman (2001, p. 183): "Referring to an infringing work is similarly legitimate".

[104] Hyperlinks, making available and the "new public"—or just a dead end? posted on the 1709 Blog on 14 Feb 2014. Available at http://the1709blog.blogspot.se/2014/02/hyperlinks-making-available-and-new.html. Last visited on 15 Apr 2014. See also Post-Svensson stress disorder #2: What does "freely available" mean? posted on the IPKat blog on 7 Mar 2014. Available at http://ipkitten.blogspot.se/2014/03/post-svensson-stress-disorder-2-what.html. Last visited on 20 Apr 2014. See also Svensson—free to link or link at your risk? posted on the Cybereagle blog on 18 Feb 2014. Available at http://cyberleagle.blogspot.se/2014/02/svensson-free-to-link-or-link-at-your.html. Last visited on 20 Apr 2014.

sought to avoid.[105] The scope of this response remains to be seen, *inter alia* in relation to specific legislation introduced in some Member States to supplement copyright protection for certain acts of linking, e.g. in relation to news aggregation services.[106]

4 Discussion and Conclusion

Beginning in the copyright sphere, the legal "novelty" of the concept of "new public" introduces the possibility for economic considerations to be taken into account when evaluating whether a specific act falls within the scope of the right of "communication to the public" in cases where the act of communication is carried out by the same technical means as the original communication. In such cases, it could be argued that the requirement of a "new public" introduces a "restraint" or even a "limitation" on the right of communication to the public, as not every communication to a public is deemed to fall within the scope of the right. However, as indicated, treating the conditions of "communication" and "the public" as separate criteria seems to be compatible with the scheme set out in the BC: and the lack of international harmonisation as regards the notion of "the/a public". Viewed against this backdrop the "novelty" introduced by the CJEU is mainly related to the application of the criteria in other cases (such as the online environment) than the ones envisioned by the drafters of the Convention.

In a converging Internet environment, where more and more uses are carried out "by the same technical means", the notion of "new public" will have a direct impact on the development of services based on content that has been already been made available online. The precise scope of *Svensson*, especially its application in situations where content has previously been made available online without restrictions, remains to be seen. From the reasoning of the CJEU in previous cases, the answer probably lies in an assessment of what the requirements are for a "new" or "subsequent" *communication*, especially whether "the same technical means" has been used as for the original communication. In this regard, *Svensson* and previous case law on the notion of communication to the public may be reflections of the CJEU's view that the right of communication to the public has inherent limitations based on economic considerations similar to the principle of exhaustion. Such economic considerations seem to be a way for the Court to open up for more "nuanced"—one might even refer to them as "balanced"—assessments based on fair remuneration to the authors rather than a strict view that every communication to a public (regardless of whether the same technical means are used and whether it is the same public or not) constitutes a copyright-relevant act. In this way, there seem to be good arguments for holding that the Court has struck a fair balance between the protection of creative content and the

[105] Svensson and Others, paras. 33–41.

[106] Cf. An ancillary right over news to be soon introduced (also) into Spanish law? posted on the IPKat blog on 16 Feb 2014. Available at http://ipkitten.blogspot.se/2014/02/an-ancillary-right-over-news-to-be-soon.html. Last visited on 20 Apr 2014.

need to foster its dissemination. On the other hand, this nuanced approach means that much will be based upon the circumstances of each individual situation; this might not be the legal certainty sought after by Internet users, right holders or providers of online services based on content already made availablee via the Internet.

The "legal innovation" that constitutes the database *sui generis* right provides greater flexibility in *providing protection* against acts that harm underlying investment, and/or the possibility to recoup the investment in the creation of a database. It is noteworthy that the CJEU does not apply the "new public" criterion developed in copyright law to the database re-utilisation right. This is probably due to the fact that we are dealing with different kinds of rights with different subject matter for protection; creative works which are the result of original creativity and databases which are the result of a substantial investment. The potential for the *sui generis* right to protect investments may thus provide a safeguard against situations like the one on *Innoweb*, which could be described as akin to *unfair competition*.

It is clear from *Innoweb* that the Court did not consider the links generated to AutoTrack's website to constitute the infringing acts; rather, it was the making available on the Internet of a dedicated meta search engine for translating queries into the search engines of the databases covered by the service of the meta search engine in question.[107] However, *Innoweb* makes plain that the "additional layer" of protection that was one of the main drivers behind the establishment of the *sui generis* right has been brought to fruition. Ironically, it has done so for a use and in a context (meta search engines) that was most probably not envisioned by the drafters of the database directive. From this perspective, the *sui generis* right—as a right supplementary to copyright—could well serve to cure some of the "unfair" effects of the concept of "new public" within copyright law in relation to certain uses of pre-existing content that is already publicly accessible online with the consent of the rightholder(s). This is not to say that this is the only valid purpose of the *sui generis* right, but rather as an indication that copyright and the *sui generis* right serve different purposes. *Innoweb* elucidates that there might be an important future for the *sui generis* right after all.

References

Articles, Books and Book Chapters

Aplin, T. (2005). *Copyright law in the digital society: the challenges of multimedia*. Oxford: Hart Publishing.

Axhamn, J. (2013). Exceptions, limitations and collective management of rights as vehicles for access to information. In D. Beldiman (Ed.), *Access to information and knowledge 21st century challenges in intellectual property and knowledge governance* (pp. 164–186). Cheltenham: Edward Elgar.

Benkler, Y. (2006). *The wealth of networks: how social production transforms markets and freedom*. New Haven: Yale University Press.

[107] Cf. Innoweb, paras. 23, 39 and 54.

Bently, L., & Sherman, B. (2008). *Intellectual property law* (3rd ed.). Oxford: Oxford University Press.
Berne Convention Centenary (1986). *The Berne Convention for the Protection of Literary and Artistic Works from 1886 to 1986*, published by the International Bureau of Intellectual Property, 1986.
de Beer, J., & Burri, M. (2014). Transatlantic copyright comparisons: Making available via hyperlinks in the European Union and Canada. In: *European intellectual property review* (pp. 95–105). Cheltenham: Edward Elgar
Ginsburg, J. (2014). Hyperlinking and "making available". In *European intellectual property law review* (pp. 147–148).
Ficsor, M. (2002). *The law of copyright and the internet*. Oxford: Oxford University Press.
Kur, A., & Dreier, T. (2013). *European intellectual property law: text cases and materials*. Cheltenham, Edward Elgar (p. 299).
Goldstein, P., & Hugenholtz, P. B. (2013). *International copyright. Principles, law, and practice*. Oxford: Oxford University Press.
Litman, J. (2001). *Digital copyright: Revising copyright law for the information age*. New York: Prometheus Books.
Olivas, J. A. (2008). Fuzzy sets and web meta-search engines. In H. Bustince, et al. (Eds.), *Fuzzy sets and their extensions: Representations, aggregation and models* (pp. 537–552). Berlin: Springer.
Ricketson, S., & Ginsburg, J. (2006). *International copyright and neighbouring rights: The Berne convention and beyond*. Oxford: Oxford University Press.
Riis, T. (2013). *Ophavsrettens fleksibilitet, Nordiskt Immateriellt Rättsskydd*, p. 139 et seq.
Rognstad, O. -A. (2003). Konsumpsjon og digitale overføringer—Et forslag til en alternativ løsningsmodell. In: *Festskrift til Mogens Koktvedgaard* (pp. 447–472).
Rosati, E. (2013). *Originality in EU copyright: Full harmonization through case law*. Northampton: Edward Elgar.
Rosén, J. (2012). Media-och upphovsrätt, Skrifter utgivna av Juridiska fakulteten vid Stockholms universitet nr 78.
Rosén, J. (2012). Länkning till streamade TV-program, in Media-och upphovsrätt (p. 164).
Strowel, A., & Ide, N. (2001). Liability with regard to hyperlinks. *Columbia Journal of Law and the Arts, 24*, 403–448.
Tsoutsanis, A. (2014). Why copyright and linking can tango. *Journal of Intellectual Property Law & Practice* (pp. 1–15).
Udsen, H., & Schovsbo, J. (2006). *Ophavsrettens missing link? Nordiskt Immateriellt Rättsskydd* (pp. 47–65).
von Lewinski, S. (2008). *International copyright law and policy*. Oxford: Oxford University Press.
Walter, M., & von Lewinski, S. (2010). *European copyright law*. Oxford: Oxford University Press.
Westman, D. (2012). *Länkning som upphovsrättslig överföring till allmänheten? Svensk Juristtidning* (pp. 800–823).
WIPO (1978). *Guide to the Berne Convention for the protection of literary and artistic works (Paris Act, 1971)*. Geneva: WIPO.
WIPO Guide to the Copyright and Related Rights Treaties Administered by WIPO and glossary of copyright and related rights terms. Geneva: WIPO.
Wu, S., & Li, J. (2004). Effectiveness evaluation and comparison of web search engines and meta-search engines. In: Advances in web-age information management. *Lecture Notes in Computer Science.* (Vol. 3129, pp. 303–314).

Web resources

ALAI Report and Opinion on the making available and communication to the public in the internet environment—focus on linking techniques on the Internet. Adopted unanimously by the Executive Committee 16 Sept 2013. Available at http://www.alai.org/assets/files/resolutions/making-available-right-report-opinion.pdf. Last visited on 16 Apr 2014.

An ancillary right over news to be soon introduced (also) into Spanish law? posted on the IPKat blog on 16 February 2014. Available at http://ipkitten.blogspot.se/2014/02/an-ancillary-right-over-news-to-be-soon.html. Last visited on 20 Apr 2014.

CJEU takes foot of the GasPedaal, then puts the boot in, posted on The 1709 Blog on 25 December 2013. Available at http://the1709blog.blogspot.se/2013/12/cjeu-takes-foot-off-gaspedaal-then-puts.html. Last visited on 14 Apr 2014.

Does Innoweb hinder innovation on the web? posted on the Kluwer Copyright Blog 20 January 2014. Available at http://kluwercopyrightblog.com/2014/01/20/eu-does-innoweb-hinder-innovation-on-the-web/. Last visited on 14 Apr 2014.

ECJ ruling on meta search engines strengthens position of database right holders available at http://www.debrauw.com/newsletter/ecj-ruling-meta-search-engines-strengthens-position-database-right-holders. Last visited on 20 Apr 2014.

European Copyright Society: Opinion on the reference to the CJEU in Case C-466/12 Svensson, dated 15 Feb 2013. Available at http://www.ivir.nl/news/European_Copyright_Society_Opinion_on_Svensson.pdf. Last visited on 16 Apr 2014.

Hyperlinks, making available and the "new public"—or just a dead end?, posted on the 1709 Blog on 14 Feb 2014. Available at http://the1709blog.blogspot.se/2014/02/hyperlinks-making-available-and-new.html. Last visited on 15 Apr 2014.

Post-Svensson Stress Disorder #1: Does it matter whether linked content is lawful? posted on the IPKat on 21 Feb 2014. Available at http://ipkitten.blogspot.se/2014/02/post-svensson-stress-disorder-1-does-it.html. Last visited on 14 Apr 2014.

Post-Svensson stress disorder #2: What does "freely available" mean? posted on the IPKat blog on 7 March 2014. Available at http://ipkitten.blogspot.se/2014/03/post-svensson-stress-disorder-2-what.html. Last visited on 20 Apr 2014.

Stepping on the GasPedaal: CJEU rules on re-utilisation of car-ad database, posted on The IPKat blog on 24 Dec 2013. Available at http://ipkitten.blogspot.se/2013/12/stepping-on-gaspedaal-cjeu-rules-on-re.html. Last visited on 14 Apr 2014.

Svensson—free to link or link at your risk? posted on the Cybereagle blog on 18 Feb 2014. Available at http://cyberleagle.blogspot.se/2014/02/svensson-free-to-link-or-link-at-your.html. Last visited on 20 Apr 2014.

Svensson—it's all about the "new public", posted on the 1709 blog on 13 Feb 2014. Available at http://the1709blog.blogspot.se/2014/02/svensson-its-all-about-new-public.html. Last visited on 20 Apr 2014.

When is web-scraping of a database unlawful? posted on 7 January 2014. Available at http://www.mayerbrown.com/When-is-web-scraping-of-a-database-unlawful-01-07-2014/. Last visited on 20 Apr 2014.

Intermediary Service Providers' Liability Exemptions: Where Can We Draw the Line?

Mari Männiko

Abstract The role of e-services has rapidly developed in recent years. Within these developments, the role of Internet service provider has changed from substance provider to neutral platform provider. The knowledge and control of the information available has changed from total control to no control at all. In many or we can even say in most of cases, intermediary service providers (ISPs) are not aware of information available on their service platform and therefore cannot be held responsible in the case of the breach of any rights regarding substance of information. This article analyzes the conditions on which a service provider can expect the liability exceptions to be applied. The interpretation of liability exceptions does not differ only in Member States but differ in high courts of Europe, namely in European Court of Justice (ECJ) and European Court of Human Rights (ECHR). Comparative analyses of the court reasoning show that the present legislation is too general and gives too much room for interpretation. Liability exemptions should not be applicable only on grounds of neutrality. The author believes that notice and take down principle should be implemented as a ground for exempting the liability. This article focuses on need for common approach in European level as in present situation neither ISP nor data subjects can find effective remedy to protect their interests.

1 Introduction

1.1 Scope of Analyses

This paper focuses on liability of an ISP of user-generated contents in ISP-managed platforms. The question to be answered is that to what extent is ISP responsible for data protection violations executed by uploading information concerning third parties by service users.

M. Männiko (✉)
Law Firm LEXTAL, Rävala pst 4, 10143 Tallinn, Estonia
e-mail: mari.manniko@lextal.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_7

Analyzing the court practice in Europe, the ISP liability is a question in many conflict relations (copyright and intellectual property). The applicability on liability does not depend on the right or freedom breached, and some of the judgments referred base on breach of some other right (intellectual property for instance); the main focus of this paper is on privacy violations.

Before analyzing the practice, I intend to give an overview of the legal background of the right to privacy that ISPs have to respect while providing individuals with services.

For the comparative analyses, I have chosen two European Courts, ECJ and European ECHR, whose decisions are binding for Member States.

With examples, I intend to prove that liability exceptions do not actually release ISPs from liability only due to the fact that service is listed in liability exception. The services are combined and not to be evaluated only on technical features but rather on the character of ISPs activity. Current situation does not really provide ISP with liability exceptions nor provides an individual with effective remedy in case of privacy breach.

1.2 Development Privacy-Covered Relations

Before going into details on ISP responsibility, it is important to visualize the understanding of privacy that can be violated (by ISP in this paper).

The need for common understanding of universal human rights became unavoidable after World War II. The universal right to privacy was to regulate the relationship between an individual and a state and to set minimum standards in order to prevent the abuse of power.

By the development of democracy, economical well-being and substantial raise of individualism, the privacy transformed from negative right into positive, and the right to privacy applied besides individual-state relation to individual–individual relation as well. Yet the scope was narrow. There was no Internet, and the application of the right to privacy was easy to follow.

The introduction of the Internet to the general public in early 1990s changed the world in many ways. We almost can compare the introducing of the Internet to the inventing of the printing press in terms of innovation and spreading of information.

Internet is a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect. Sometimes referred to as a 'network of networks,' the Internet emerged in the USA in the 1970s but did not become visible to the general public until the early 1990s. By the beginning of the twenty-first century, approximately 360 million people, or roughly 6 % of the world's population, were estimated to have access to the Internet.[1]

In the context of the Internet, three situations should be distinguished that relate to personal data. The first is the publishing of elements of personal data on any Web page on the Internet. The 'Internet' comprises two main services, namely the World Wide Web and the e-mail services. While the Internet, as a network of interconnected

[1] http://www.britannica.com/EBchecked/topic/291494/Internet (last reviewed in January 31, 2014).

computers, has existed in various forms for some time, commencing with the Arpanet (United States), the freely accessible open network with www addresses and common code structure only started in the early 1990s. It seems that the historically correct term would be World Wide Web. However, given the current usage and terminological choices made in Court's case law, the word 'Internet' is primarily used to refer to the World Wide Web part of the network (the 'source Web page'). The second is the case where an Internet search engine provides search results that direct the Internet user to the source Web page. The third, more invisible operation occurs when an Internet user performs a search using an Internet search engine, and some of his personal data, such as the IP address from which the search is made, are automatically transferred to the Internet search engine service provider.[2]

Besides enormous availability of information, different ways of communication became available. New ways of information sharing and communication were introduced. Protecting privacy in the Internet became essential but not so easily achievable. Individuals were to be protected from each other but even more important from themselves. And Internet continued to develop.

While the old Web was about Web sites, clicks and 'eyeballs,' the new Web is about communities, participation and peering.[3]

To put is Simply, the old Internet (or Web) was an environment where users got together, the service provider was the owner of a server, and the control over the content provided by users was easy to handle. New Web is the environment where the contact between users is established by using service of ISP, but communication is carried out between users without ISP, sharing the content and having control over it.

The scope of privacy protected relations transformed once again, and the responsibility of platform provider, i.e., ISP, became relevant.

The dispute of liability rarely comes out when the service provided is not dubious, pure hosting, for example. The question of service provider responsibility hardly rises when one receives an insulting e-mail.

The question is more difficult to answer when the service provider provides with multi-level services, for example, a news portal provides readers with news together with the possibility to comment either anonymously or not.

1.2.1 European Convention on Human Rights Article 8: Common Grounds

The right to privacy was established and codified in European level in 1950 with ECHR of which Article 8 states that everybody has the right for respect his private and family life, his home and his correspondence.

Private life has been furnished by different aspects of privacy ever since. Starting with the question what is privacy and ending with answering where privacy can be enjoyed.

---

[2] Opinion of Attorney General Jääskinen in Case C-131/12 paragraph 3.

[3] See Tapscott and Williams (2008, p. 9).

Section 2 of the Article 8 provides with the conditions[4] under which the breach of privacy is acceptable. It is necessary to note that at the time when ECHR was adopted, the privacy protection was a state–individual relation. It was a negative right of a state not to interfere unless the precondition for interference was met. The wording of Article 8 has remained the same, but the substance has transformed by the court practice besides the individual–state relation to the individual–individual relation, and the contracting state has to provide an individual with an effective remedy for privacy protection.

1.2.2 Charter on Fundamental Rights of European Union

It was a remarkable development regarding the uniform implementation of fundamental rights within European Union. Most importantly, the right to data protection was separated from general protection of privacy. The right to data protection was no longer a part of the right to privacy, but it became an individually protected value. In substance, nothing really changed.

According to Advocate General Jääskinen[5] *this fundamental right, being a restatement of the European Union and Council of Europe acquis in this field, emphasises the importance of protection of personal data, but it does not as such add any significant new elements to the interpretation of the Directive.*[6]

1.2.3 Data Protection Directive 95/46/EC

As mentioned before, Internet became commonly available in early 1990s, and by 1995, European Union introduced the first[7] framework act to unify data protection laws in EU.

Data Protection Directive[8] established several new principles and instruments, but in the present paper, I would like to point out the individuals' right to have

[4] There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[5] In his opinion the the case of European Court of Justice no C-131/12 paragraph 113.

[6] Data Protection Directive 95/46/EC.

[7] The Directive can be called first in European Union but it is surely not the first act that separated data protection from the rest of privacy protection. Outstanding codification has be en done before. In September 23, 1980 OECD adopted Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In 1981 European Council adopted Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. According to this Convention tozens of recommendations have been adopted.

[8] Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred as to Data Protection Directive).

control over his/her personal data to be processed by third persons, and the institute of consent for data processing.

In relations with ISP, it is also important to know how and if the consent for data processing is achieved and if the data subject is informed about the possibility not to give consent knowingly.

ISP services and relations with the users of services are very different. From the perspective of Data Protection Directive, it is important to define if the ISP is a data controller and if activities of an ISP can be defined as data processing. The answer to those questions is the fact if an ISP can influence the data flow and the substance of the data.

1.2.4 E-Commerce Directive 2000/31/EC

E-Commerce Directive[9] gave a definition of ISP as well as limited service providing from other possible activities done in Internet.

Information Society Services (hereinafter ISS) is a service that must meet the following conditions according to E-Commerce Directive Article 2(a).

Article 2 of the E-Commerce Directive uses the definition contained in Article 1(2) of Directive 98/34/EC[10] as amended by Directive 98/48/EC[11]; ISS is a service normally provided for remuneration, at a distance, by electronic means and at the individual request.

Privacy can be affected when an individual uses an information society service, in particular for the purposes of seeking information or making it accessible.

Distinction of the Activities Listed in Liability Exceptions of the E-Commerce Directive

The liability exceptions derive from Section 4 (Articles 12–15) of the E-Commerce Directive.

ISP who provide with intermediary services liability is limited. The keywords for liability limitations are 'mere conduit,' 'caching' and 'hosting.'

Mere conduit means that ISP does not initiate the transmission, does not select the receiver of the transmission and does not select or modify the information contained in the transmission.

---

[9] E-Commerce Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (hereinafter E-Commerce Directive).

[10] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations.

[11] Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. Last reviewed at January 29, 2014.

Caching means that ISP activities are performed exclusively for more efficient onward transmission of the information to other recipients of the service upon such recipients' requests.

Hosting means that ISP is storing information without monitoring the substance of it.

According to the functional character of information society services, they can be distinguished as follows:

- Hosting service provider provides users with the possibility to make the content available using service providers server(s). The server can be used by content providers and third persons. A distinction may be established between caching, where the purpose of hosting is to facilitate the functioning of the network through automatic, intermediate and transient storage of information, and hosting, that is, commercial or other storage that is permanent or more than merely provisional.[12]
- Access service provider connects service users computer to Internet.
- A transit service provider provides service users with possibility to transfer data (*mere conduit*)

The E-Commerce Directive (Article 15) sets general rule that ISP who provides its users with the platform does not have the general obligation to monitor the data shared by service users. The analyses of the case law show that there are certain limitations to that rule.

2 ISP Liability Exceptions According to Law and Practice of ECJ and ECHR

According to several judgments of ECJ in order to benefit from liability exemptions, ISP has to prove the lack of control and knowledge over the information processed on its platform. At the same time, ECJ gives controversial meaning to neutrality and seems that within the court there is no consensus about the substance and applicability of being neutral.

2.1 Google Case

The dispute in Google versus Louis Vuitton and the others[13] concerned the display on the Internet of advertising links on the basis of keywords corresponding to

[12] Gallardo Claudio Ruiz and Gálvez J. Carlos Lara Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America available at http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/02-Liability_Internet_Service_Providers_exercise_freedom_expression_Latin_America_Ruiz_Gallardo_Lara_Galvez.pdf. Last reviewed at January 30, 2014.

[13] Joined Cases C-236/08 to C-238/08.

trademarks and the question taken to the ECJ was if the liability exemptions from E-Commerce Directive Articles 12–14 apply to Google.

Google operates an Internet search engine. When an Internet user performs a search on the basis of one or more words, the search engine will display the sites, which appear best to correspond to those words, in decreasing order of relevance. These are referred to as the 'natural' results of the search.

Besides natural results which Google provides with advertising link that provides the user with commercial announcements. Natural and commercial results are easily distinguished.

The question taken to the ECJ was whether Google is responsible for intellectual property infringements or will liability exceptions applying due to the character of services provided by Google. From perspective of this paper, only the latter is important.

The ECJ had the occasion to give its interpretation in the case; the ECJ interpreted the role of the host service according to recital 42 of the preamble of the E-Commerce Directive. The exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature,' which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored.'[14]

Article 14 of the Directive 2000/31 must be interpreted as meaning that the rule laid down therein applies to an Internet-referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned.[15]

In his opinion, the Advocate General Poiares Maduro pointed out a need for common notice and take down principle adaption for attribution of liability following the taking down of content.

The ECJ found that the services of Google can be interpreted according to the exceptions provided by the E-Commerce Directive and Google cannot be held liable.

2.2 L'Oreal Versus eBay

The dispute in L'Oreal versus eBay[16] the main proceedings was between L'Oréal SA and its subsidiaries ('L'Oréal'), on the one hand, and three subsidiaries of

[14] Viola de Azevedo Cunha, Mario, Martin, Luisa, Sarator, Giovanni EUI Working Paper Law 2011/011. Department of Law, Peer-to-peer privacy violations and ISP Liability: Data protection in the User/Generated WEB p. 6.

[15] Judgement in Joined Cases C-236/08 to C-238/08.

[16] European Court of Justice, Case C-324/09.

eBay Inc. ('eBay'), together with certain natural persons, on the other. It related to offers for sale of goods by these persons on eBay's electronic marketplace. The offers for sale allegedly infringed L'Oréal's intellectual property rights.

eBay, the defendant in the national proceedings, operates a popular and sophisticated electronic marketplace in the Internet. It has built-up a system, which greatly facilitates the selling and buying over the Internet by individuals, with a powerful search engine, a secure payment system and extensive geographical coverage. It has also designed compliance mechanisms to fight sales of counterfeit goods. In order to attract new customers to its Web site, eBay has also bought keywords, such as well-known trademarks, from paid Internet-referencing services (such as Google's AdWords). The use of a selected keyword in the search engine triggers the display of an advertisement and a sponsored link, which leads directly to eBay's electronic marketplace.[17]

eBay has installed a notice and take down system that is intended to assist intellectual property owners in the removing of the infringing listings from the marketplace.

The question to be answered is whether eBay can be held liable for the infringements.

ECJ had to define the scope of the exemption of the information service providers' liability as contained in Article 14 of the Directive 2000/31 ('E-Commerce Directive').

ISP's role in the data processing is the determining factor. Does ISP have knowledge of, or control over, the data stored. If the role can be defined as passive, i.e., no knowledge nor control, the service provider cannot be held liable for the data which it has stored.

In the case of *L'Oreal versus eBay*, the meaning of 'neutrality' was analyzed by Advocate General Jääskinen in his opinion.

Advocate General contended that the liability exceptions should apply, but he had doubts whether neutrality should be the right test under the E-Commerce Directive for applying the exemptions.

When anchoring the limitation of liability criteria of the hosting provider to 'neutrality,' the Court has referred to recital 42 of the Directive 2000/31. I share the doubts expressed by eBay as to whether this recital 42 at all concerns hosting referred to in Article 14.

Even if recital 42 of the directive speaks of 'exemptions' in plural, it would seem to refer to the exemptions discussed in the following recital 43. The exemptions mentioned there concern—expressly—'mere conduit' and 'caching.' When read this way, recital 42 becomes clearer: it speaks of the 'technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient.' In my view, this refers precisely to 'mere conduit' and 'caching,' mentioned in Articles 12 and 13 of the Directive 2000/31.

[17] Ibid, paragraph 2.

Rather, it is recital 46 which concerns hosting providers mentioned in Article 14 of the Directive 2000/31, as that recital refers expressly to the storage of information. Hence, the limitation of liability of a hosting provider should not be conditioned and limited by attaching it to recital 42. It seems that if the conditions set out in Google France and Google for a hosting provider's liability are confirmed in this case to apply also to electronic marketplaces, an essential element in the development of electronic commerce services of the information society, the objectives of the Directive 2000/31 would be seriously endangered and called into question.[18]

Moreover, Jääskinen highlights that he *would find it surreal that if eBay intervenes and guides the contents of listings in its system with various technical means, it would by that fact be deprived of the protection of Article 14 regarding storage of information uploaded by the users.*[19] *The Advocate General suggests that it is possible to sketch out parameters of a business model that would fit perfectly to the hosting exemption. And even if it were, a definition made today would probably not last for long. Instead, we should focus on a type of activity and clearly state that while certain activities by a service provider are exempt from liability, as deemed necessary to attain the objectives of the directive, all others are not and remain in the 'normal' liability regimes of the Member States, such as damages liability and criminal law liability.*[20]

Therefore, when it is accepted that certain activities by a service provider are exempted that means conversely that activities not covered by an exemption may lead to liability under national law.

Thus, for eBay, the hosting of the information provided by a client may well benefit from an exemption if the conditions of Article 14 of Directive 2000/31 are satisfied. Yet the hosting exception does not exempt eBay from any potential liability, it may incur in the context of its use of a paid Internet-referencing service.[21]

Mario Viola De Azevedo Cunha and other authors believe that the interpretation of the provider's exemption given by Advocate General Jääskinen could fall under neutrality broadly understood, which applies to an activity which is meant to enable or facilitate the activities in which the user autonomously engages in his or her own behalf. The Advocate General urges us to rethink the foundations of the liability exemption. We should consider the specific activity performed by an ISP and understand neutrality as appropriateness with regard to the purpose of that activity.[22]

According to Mario Viola de Azevedo Cunha, the neutral activity of the providers should be exempted from the liability also with regard to national data protection rules.

---

[18] Paragraphs 130–165.

[19] Paragraph 146.

[20] Paragraph 149.

[21] Paragraphs 150–151.

[22] Viola de Azevedo Cunha, Mario, Martin, Luisa, Sarator, Giovanni, EUI Working Paper Law 2011/011. Department of Law, Peer-to-peer privacy violations and ISP Liability: Data protection in the User/Generated WEB p. 7–8.

Attorney General Jääskinen gave his view on the notion of notice and take down as following.

It should be recalled that Article 14(1)(b) of the Directive 2000/31[23] reflects the principle of *notice and take down*. Accordingly, the hosting provider has to act expeditiously to remove or to disable access to the illegal information upon obtaining actual knowledge of the illegal activity or illegal information or awareness of facts or circumstances from which the illegal activity or information is apparent.

In the application of the principle of *notice and take down*', recital 46 of the Directive 2000/31 must be taken into account. According to it, the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level. Moreover, the directive does not affect Member States' possibility of establishing specific requirements, which must be fulfilled expeditiously prior to the removal or disabling of information.[24]

The Court took a different approach on neutrality in case of eBay and found that Article 14(1) of the E-Commerce Directive is to be interpreted as applying to the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored. The operator plays such a role when it provides assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting them.[25]

ECJ found that the operator has provided assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer–seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of the Directive 2000/31.[26]

2.3 Scarlet Extended SA

Scarlet Extended SA[27] is an Internet service provider, which provides its customers with access to the Internet without offering other services such as downloading or file sharing.

SABAM is a management company that represents authors. SABAM concluded that Internet users using Scarlet's services were downloading works in SABAM's catalogue from the Internet, without authorization and without paying

[23] E-Commerce Directive.

[24] Opinion of Attorney General Jääskinen in Case C-324/09.

[25] European Court of Justice, Case C-324/09: paragraph 123 of the judgment.

[26] Ibid, paragraph 116.

[27] Judgement of the Court, In Case C-70/10.

royalties, by means of peer-to-peer networks, which constitute a transparent method of file sharing which is independent, decentralized and features advanced search and download functions.

SABAM claimed that Scarlet had infringed copyrights and sought an order requiring Scarlet to bring such infringements to an end by blocking, or making it impossible for its customers to send or receive in any way, files containing a musical work using peer-to-peer software.

At the same time, the filtering and blocking system required by SABAM for the protection of intellectual property rights would be in conflict with E-Commerce Directive principle that the service provider cannot be obliged to monitor the substance of data.

Scarlet claimed that such an injunction was contrary to Article 21 of the Law of 11 March 2003 on certain legal aspects of information society services, which transposes Article 15 of Directive 2000/31 into national law, because it would impose on Scarlet, de facto, a general obligation to monitor communications on its network, inasmuch as any system for blocking or filtering peer-to-peer traffic would necessarily require general surveillance of all the communications passing through its network. Scarlet considered that the installation of a filtering system would be in breach of the provisions of European Union law on the protection of personal data and the secrecy of communications, since such filtering involves the processing of IP addresses, which are personal data.

The question put to the court were, whether the E-Commerce Directive and the Data Protection Directive among other directives (2001/29, 2004/48 and 2002/58), read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction imposed on an Internet service provider to introduce a system for filtering all electronic communications passing via its services, in particular those involving the use of peer-to-peer software, which applies indiscriminately to all its customers, as a preventive measure, exclusively at its expense and for an unlimited period which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audiovisual work in respect of which the applicant claims to hold intellectual property rights, with a view to blocking the transfer of files the sharing of which infringes copyright ('the contested filtering system').[28]

The ECJ found that all rules must respect Article 15(1) of the E-Commerce Directive, which prohibits national authorities from adopting measures, which would require an Internet service provider to carry out general monitoring of the information that it transmits on its network.

The Court has already ruled that that prohibition applies in particular to national measures which would require an intermediary provider, such as an ISP, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual property rights. Furthermore, such a general

[28] Ibid, paragraph 29.

monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly.

Firstly, the filtering system would require the ISP to identify, within all of the electronic communications of all its customers, the files relating to peer-to-peer traffic, secondly, to identify, within that traffic, the files containing works in respect of which holders of intellectual property rights claim to hold rights, thirdly, to determine which of those files are being shared unlawfully, and fourthly, to block file sharing that it considers to be unlawful.

ECJ found that the abovementioned must be interpreted as an obligation to monitor such activities according to the Article 15 of the E-Commerce Directive.

As for the data protection rights, ECJ found that it is the common ground that the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content, and the collection and identification of users' IP addresses from which unlawful content on the network are sent. Addresses are personal data because they allow those users to be identified.

The answer to the questions submitted is that the E-Commerce Directive, the Data Protection Directive and Directives 2001/29, 2004/48 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an ISP, which requires it to install the contested filtering system.

The ECJ found that ISP must not be held liable for the infringement of rights on its platform.[29]

2.4 Google Spain SL, Google Inc. Versus Agencia Española de Protección de Datos and Mario Costeja Gonzáles

The proceedings concerned the application of the Data Protection Directive to an Internet search engine that Google operates as service provider. In the national proceedings, it is undisputed that some personal data regarding the data subject have been published by a Spanish newspaper, in two of its printed issues in 1998, both of which were republished at a later date in its electronic version made available on the Internet. The data subject thought that this information should no longer be displayed in the search results presented by the Internet search engine operated by Google, when a search is made of his name and surnames.[30]

The questions referred to the Court fell into three categories. The first group of questions related to the territorial scope of the application of EU data protection rules. The second group addressed the issues relating to the legal position of an Internet search engine service provider. Finally, the third question concerned the

[29] The ECJ came to the same conclusion as in the case C-360/10.

[30] Opinion of Advocate General Jääskinen delivered on 25 June 2013 (1) Case C-131/12.

so-called right to be forgotten, and the issue of whether data subjects can request that some or all search results concerning them are no longer accessible. All of these questions were new to the Court.

It is useful to review the opinion of ECJ about the liability of ISP for not providing data subject with the right to be forgotten.

It is necessary to analyze their position vis-à-vis the legal principles underpinning the limitations on the liability of Internet service providers. In other words, to what extent are activities performed by an Internet search engine service provider, from the point of view of liability principles, analogous to the services enumerated in the E-Commerce Directive 2000/31 (transfer, mere caching, hosting) or transmission service mentioned in recital 47 in the preamble to the Directive, and to what extent does the Internet search engine service provider act as content provider in its own right.[31]

Here is no doubt that the newspaper who is keeping the old articles about data subject available is a data processor in the meaning of Data Protection Directive. The question to be answered is whether and to what extent Google is liable or is the liability to be excluded by exceptions.

It is important to examine the liability of Internet search engine service providers in respect of personal data published on third-party source Web pages, which are accessible through their search engines. In other words, the Court is here faced with the issue of 'secondary liability' of this category of information society service providers analogous to that it has dealt with in its case law on trademarks and electronic marketplaces.[32]

The Internet search engine service provider merely supplying an information location tool does not exercise control over personal data included on third-party Web pages. The service provider is not 'aware' of the existence of personal data in any other sense than as a statistical fact Web pages are likely to include personal data. In the course of processing of the source Web pages for the purposes of crawling, analyzing and indexing, personal data do not manifest itself as such in any particular way.[33]

Attorney General Jääskinen is of the opinion that ISP cannot be held a data controller due to the technical character of its services, and it meets all the essential requirements of the liability exemption. Besides the E-Commerce Directive, the liability for personal data processing is excluded by the recital 47 in the preamble of the Data Protection Directive.[34]

---

[31] Ibid, paragraph 38.

[32] Ibid, paragraph 46.

[33] Ibid, paragraph 84.

[34] Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services.

If a data subject finds that his rights are breached by continuous availability of his personal data, he must find a legal ground for stopping the processing at the original data processor (newspaper in this case); as ISP is not responsible neither for the fact that data has been processed nor for the substance of the data.

In this case, ECJ gave opinion on notice and take down concept and found that a national data protection authority cannot require an Internet search engine service provider to withdraw information from its index except for the cases where this service provider has not complied with the exclusion codes or where a request emanating from the Web site regarding update of cache memory has not been complied with. A possible *notice and take down* procedure concerning links to source Web pages with illegal or inappropriate contents is a matter of national law civil liability based on grounds other than the protection of personal data.

ECJ refers to Article 29 Data Protection Working party Opinion 1/2008 on data protection issues related to search engines according to which the formal, legal and practical control the search engine has over the personal data involved is usually limited to the possibility of removing data from its servers. With regard to the removal of personal data from their index and search results, search engines have sufficient control to consider them as controllers (either alone or jointly with others) in those cases, but the extent to which an obligation to remove or block personal data exists may depend on the general tort law and liability regulations of the particular Member State. In some EU Member States, data protection authorities have specifically regulated the responsibility of search engine providers to remove content data from the search index, based on the right of objection enshrined in Article 14 of the Data Protection Directive and on the E-Commerce Directive. According to such national legislation, search engines are obliged to follow a notice and take down policy similar to hosting providers in order to prevent liability.

2.5 Conclusion on ECJ Judgments

According to the rule that is generally adopted by ECJ, an ISP is not liable if it has neutral and technical role. Neutral means not having influence on data or on conditions on which data are available at ISP's platform. ISP is not liable in case it is not a data controller.

The substance of neutrality is subjective, and ECJ has not reached the consensus on the question if neutrality should be unconditional.

Either in judgments or opinions of attorney General the ECJ has pointed out the need for common approach for adapting notice and take down principle and its effect to liability.

As the First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal

Market (Directive on electronic commerce)[35] noted the notice and take down principle was to be adopted on self-regulatory principles on the discretion of Member States.

The time has shown that self-regulation is not sufficient and the principle should be adopted in Member States' national legislation in order for it to become an effective remedy in case of violations and for balancing the liability.

2.6 Delfi Versus Estonia

The applicant company owned one of the largest Internet news portals in Estonia. On its Web site, readers could anonymously and without prior registration post comments below the published articles. Although the applicant company could not edit or moderate such comments, it could remove them using a prior automatic word filtering system or on being alerted by readers.

There was a system of notify-and-take-down in place: Any reader could mark a comment as appropriate and the comment was removed expeditiously. Furthermore, there was a system of automatic deletion of comments that included obscene words. In addition, a victim of a defamatory comment could directly notify the applicant company, in which case the comment was removed immediately.

In 2006, the applicant published an article stating that a ferry company had changed its routes thereby causing the breakup of ice at potential locations of ice roads. As a result, the opening of the roads—which were a cheaper and faster connection to the Estonian islands compared to the company's ferry services—had to be postponed for several weeks. A number of comments containing personal threats and offensive language directed against the ferry company owner were posted below the article. The applicant company removed them some 6 weeks later at the insistence of the ferry company. The owner of the ferry company instituted defamation proceedings against the applicant company, which was ultimately ordered to pay EUR 320 in damages.

The Information Services Act[36] (adopted under E-Commerce Directive) limits ISP responsibility on the same grounds as E-Commerce Directive, i.e., ISP will not be held responsible for the content in case the service consists of mere conduit, caching or hosting. The same as in E-Directive there is no obligation to monitor.

The Supreme Court approved the lower courts' interpretation of the Information Society Services Act and reiterated that an ISP, falling under that Act and the Directive on Electronic Commerce, had neither knowledge of nor control

[35] First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[36] https://www.riigiteataja.ee/akt/106012011012.

over information, which was transmitted or stored. By contrast, a provider of content services governed the content of information that was being stored. In the present case, the Delfi had integrated the comment environment into its news portal and invited users to post comments. The number of comments had an effect on the number of visits to the portal and on the applicant company's revenue from advertisements published on the portal. Thus, the applicant company had an economic interest in the comments. The fact that the applicant company did not write the comments itself did not imply that it had no control over the environment. It enacted the rules of commenting and removed comments if the rules were breached. The users, on the contrary, could not change or delete the comments they had posted; they could merely report obscene comments. Thus, the applicant company could determine which comments were published and which not. The fact that it made no use of this possibility did not mean that it had no control over the publishing of the comments.

The Court found that the services of Delfi do not fall under scope of exemptions of E-Commerce Directive and relevant local act and Delfi was held responsible on general principles of tort law.

ECHR noted that the interpretation of local law is the task of local courts and as Estonian Courts ruled that Delfi's activities do not fall under exceptions provided by E-Commerce Directive and relevant local law the ECHR will not take the task of local courts and will not start re-interpretation.

The ECHR reviewed the case law (analyzed above) and found that the neutrality principle that was essential in findings of ECJ was of no relevance in this case as ECHR relied on interpretation of Estonian courts regarding applicability of neutrality.

ECHR found that there was infringement with Article 10[37] of European Convention on Human Rights (hereinafter the Convention), but the exercise of this freedom was restricted by the law with sufficient amount of foreseeability.

The parties' views differed as to whether the applicant company's civil liability for the defamatory comments amounted to a disproportionate interference with its freedom of expression. In other words, the question is whether the applicant company's obligation, as established by the domestic judicial authorities, to ensure that comments posted on its Internet portal did not infringe the personality rights of third persons was in accordance with the guarantees set out in Article 10 of the Convention.[38]

[37] Article 10. Freedom of expression. 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[38] Paragraph 84.

As regards the measures applied by the applicant company, the Court notes that, in addition to the disclaimer stating that the writers of the comments—and not the applicant company—were accountable for them and that it was prohibited to post comments that were contrary to good practice or contained threats, insults, obscene expressions or vulgarities, the applicant company had two general mechanisms in operation. Firstly, it had an automatic system of deletion of comments based on stems of certain vulgar words. Secondly, it had a notice and take down system in place according to which anyone could notify it of an inappropriate comment by simply clicking on a button designated for that purpose, to bring it to the attention of the portal administrators. In addition, on some occasions, the administrators of the portal removed inappropriate comments on their own initiative. Thus, the Court considered that the applicant company could not be said to have wholly neglected its duty to avoid causing harm to third parties' reputations. Nevertheless, it was discovered that the automatic word-based filter used by the applicant company was relatively easy to circumvent. Although it may have prevented some of the insults or threats, it failed to do so in respect of a number of others. Thus, while there is no reason to doubt its usefulness, the Court considers that the word-based filter as such was insufficient for preventing harm being caused to third persons.[39]

The ECHR considered that the applicant company exercised a substantial degree of control over the comments published on its portal even if it did not make as much use as it could have done of the full extent of the control at its disposal.

The author believes that as the ECHR found that Delfi had a control over the comments and monitored the comments to some extent, it could not be held neutral and the liability exemptions from the E-Commerce Directive could not apply.

The ECHR found that Article 10 of the Convention was not violated.

2.7 Case of Yildirim Versus Turkey

The applicant owns and runs a Web site on which he publishes material including his academic work. It was set up using the Google Sites Web site creation and hosting service. On June 23, 2009, the Criminal Court of First Instance ordered the blocking of another Internet site under the Law on regulating publications on the Internet and combating Internet offences. The order was issued as a preventive measure in the context of criminal proceedings. Later that day, under the same Law, a copy of the blocking order was sent to the Telecommunications Directorate for execution. On June 24, 2009, further to a request by the Telecommunications Directorate, the Criminal Court of First Instance varied its decision and ordered the blocking of all access to Google Sites. As a result, the applicant was unable to access his own site. On July 1, 2009, he applied to have the blocking order set

[39] Ibid, paragraph 87.

aside in respect of his own site, which had no connection with the site that had been blocked because of its illegal content. On July 13, 2009, the Criminal Court dismissed the applicant's application. In April 2012, he was still unable to access his own Web site even though, as far as he understood, the criminal proceedings against the owner of the offending site had been discontinued in March 2011.[40]

Following the blocking of another Web site as a preventive measure, the court had subsequently, further to a request by the Telecommunications Directorate, ordered the blocking of all access to Google Sites, which also hosted the applicant's site. This had entailed a restriction amounting to interference with the applicant's right to freedom of expression.

The blocking of the offending site had a basis in law, but it was clear that neither the applicant's site nor Google Sites fell within the scope of the relevant law since there was insufficient reason to suspect that their content might be illegal. No judicial proceedings had been brought against either of them. Furthermore, although Google Sites were held responsible for the content of a site it hosted, the law made no provision for the wholesale blocking of access to the service. Nor was there any indication that Google Sites had been informed that it was hosting illegal content or that it had refused to comply with an interim measure concerning a site that was the subject of pending criminal proceedings. Furthermore, the law had conferred extensive powers on an administrative body, the Telecommunications Directorate, in implementing a blocking order since it had been able to request an extension of the scope of the order even though no proceedings had been brought in respect of the site or domain concerned and no real need for wholesale blocking had been established.[41]

ECHR referred to a decision of ECJ (see Section 2.1.4 of the article) which found that imposing ISP with an obligation to filter the content provided on its platform is to be interpreted as an obligation to monitor that is in contrary with E-Commerce Directive and breaches fair balance between the rights.

Besides that ECHR analyzed practices in Council of Europe Member States and finalized that freedom of expression protected by Article 10 of the Convention implied freedom of access to Internet.

Although Google was not a part of the proceeding and it was not a subject matter if ISPs rights have been violated by Turkish Court order, the ECHR took approach on ISP liability as well. The ECHR noted that neither Google Sites nor the applicant's Web site was the subject of judicial proceedings for the purposes of relevant national laws. It appears from national court decision that Google Sites were held to be liable for the content of a Web site which it hosted. However, the national law, which deals with the liability of content providers, hosting service providers and access providers make no provision for a wholesale blocking of access such as that ordered in the present case.

[40] Information Note on the Court's case-law No. 158.

[41] Ibid.

Nor has it been maintained that the law authorized the blocking of an entire Internet domain-like Google Sites, which allows the exchange of ideas and information. Moreover, there is nothing in the case file to indicate that Google Sites were notified under that it was hosting illegal content, or that it refused to comply with an interim measure concerning a site that was the subject of pending criminal proceedings.

ECHR found that there has been a breach of Article 10 of the Convention.

3 Conclusion

Neutrality in the meaning of the E-commerce Directive liability exemptions means passive role and not knowing or adapting conditions to the data processed at the platform.

Liability exemptions should not be applicable only on grounds of neutrality. Implementing sole neutrality clause may bring along unwillingness of ISP to interfere, and it affects the protection of personal rights on the ISPs platform.

Liability exceptions should be applied in case an ISP acts promptly after being informed about a breach of law (notice and take down principle).

The conditions under which a hosting provider is exempted from liability, as set out at Article 14(1)(b) constitute the basis for the development of notice and take down procedures for illegal and harmful information by stakeholders. Article 14 applies horizontally to all types of information.

In the year 2000, when the Directive was adopted, it was believed that notice and take down procedures do not have to be regulated in the E-Commerce Directive as it was hoped that the self-regulation is sufficient as Article 16 and Recital 40 of the E-Commerce Directive expressly encourage it.

This approach was followed by the Member States in their national laws. Out of those Member States which have transposed the Directive, only Finland has included a legal provision setting out a notice and take down procedure concerning copyright infringements only. All the other Member States have left this issue to self-regulation.[42]

Cases analyzed above prove that self-regulation has failed in the case of protection of privacy[43] in ISP platforms. The E-Commerce Directive should implement regulation for notice and take down procedure in order to have an effective remedy for the protection of rights on ISP platforms.

---

[42] First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF. Last reviewed at January 29, 2014.

[43] The same as protecting copyright, intellectual property etc.

References

Book, Multiple Authors/Editors

Tapscott, D., & Williams, A. D. (2008) *Wikinomics: How mass collaboration changes everything* (p. 19). New York: Portfolio.

Journal Articles

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations.

Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.

E-Commerce Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

Gallardo Claudio Ruiz, & Gálvez J. Carlos Lara, Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America available at http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/02-Liability_Internet_Service_Providers_exercise_freedom_expression_Latin_America_Ruiz_Gallardo_Lara_Galvez.pdf.

Viola de Azevedo Cunha, Mario, Martin, Luisa, Sarator, Giovanni, EUI Working Paper Law 2011/011. Department of Law, Peer-to-peer privacy violations and ISP Liability: Data protection in the User.

Online Documents

Article 10: Right to freedom of expression.

Information Note on the Court's case-law No. 158.

Internet—http://www.britannica.com/EBchecked/topic/291494/Internet.

First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF.

https://www.riigiteataja.ee/akt/106012011012.

Court Decisions

European Court of Justice no. C-131/12 paragraph 113.

European Court of Justice, Case C-324/09.

European Court of Justice, Case C-324/09: paragraph 123 of the judgment.
Judgement in Joined Cases C-236/08 to C-238/08.
Judgement of the Court In Case C-70/10.
Opinion of Attorney General Jääskinen in Case C-131/12 paragraph 3.
Opinion of Attorney General Jääskinen in Case C-324/09.

Civil Status Registration–More than Data Collection: EU Digital Development in Promoting the Free Movement of Civil Status Document

Kristi Joamets

Abstract Digital technologies have changed the relationship between the citizen and the state. Online options facilitate/make more comfortable, expedite, secure and accessible the exchange of data and information. Digitalization has had the same positive effect in the field of civil status registration. In the European Union (EU), the civil registration systems of member states are improving their management of cross-border cases. At this level, the tendency is towards a common digital environment. Estonia has a considerable e-government practice; from 2002, data collection is made in digital form, and from 2010, the administrative procedure of registering the family events and civil status data is electronic. This chapter introduces the Estonian model of digital civil status registration. It can be defined as an example of person-centred, transparent and effectively operating e-government function.

1 Introduction

Information and communication technology has substantially changed the environment we live in. With the ever-increasing communication options via the technological solutions and an enormous amount of information in the Internet, most people can have access to this regardless of their geographical location[1]—acting in this digital environment is not influenced by state borders. Also, digital technologies have fundamentally changed the relationship between citizens and their governments.[2] Europe is an online continent—over half of all EU citizens use Internet every day, and three quarters of households have Internet access.[3]

[1] Infoühiskonna arengukava aastani (2013), p. 2.

[2] Duvivier (2013, p. 14).

[3] Living Online.

K. Joamets (✉)
Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia
e-mail: kristi.joamets@ttu.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_8

The Estonian information society policy states: “Information society is a society’s way of life, where most values created by the society are put in information and most of the collected information is stored, transformed and transmitted in an universal digital form”.[4] The digital society is dynamic, it develops continuously. The State must notice new developments in this area and not to hesitate using new solutions that the information society may offer as a result of those developments. Civil status registration is a field in which continuous progress is marked by digital technologies, in Estonia and in the EU. Inner-state solutions are gradually shaping to handle cross-border cases adequately, and at the supranational level, the trend is towards one common digital environment, which would facilitate the exchange of the civil status data between the member states. A more ambitious aim is one common civil status register of EU.

However, the civil status registration has much wider scope than Europe, it is a global question. The United Nations have considered the family events registration through the human rights perspective. Silveira states that of all the rights recognized by the European Convention of Human Rights, including the right to private and family life, established in article 8, is the right that is the most directly and strikingly applicable to civil status under several forms.[5] He explains that from birth, a child is truly entitled to registration in the civil status registers. The right to private life implies, beyond its strictly biological content, the right for a person to be an integral part of society or political institutions, and this right to assert one’s individual personality before others and before societies.[6]

As mentioned above, in the policy of the EU, the civil status registration plays an important role, especially related to the developments of family law. Baarsma points out that as after Lisbon Treaty, the right of free movement together with an emerging European citizenship has gradually gained more significance in the discussion on the unification of private international law in family matters as well as on the harmonization of substantive family law; then, the Treaty of the Functioning of the EU specifies that the union “shall offer its citizens an area of freedom, security and justice without internal borders”, playing an important part in the process of European integration.[7] The Stockholm Programme[8] indicates that an important priority for the coming years will be the focus on the interests and the needs of citizens.[9] Main importance in this is the cooperation between the member states in family matters, including the recognition of civil status documents and exchange of civil status data.[10] These developments have changed the

[4] Ibid, p. 5.

[5] Silveira (2009).

[6] See ibid.

[7] Baarsma (2011, p. 103).

[8] OJ C 115/8 04/05/2010.

[9] See Baarsma (2011, p. 105).

[10] See also the European Commission (2010).

attitudes of the member states to the digital Population Registers—those states who have been sceptical in new developments since, have also worked out similar policies that the "leaders in e-government" already have. However, unity in the Europeanization cannot take place if the civil registries are isolated and their data out of the reach of other member states. This diminishes also the freedom of people in interacting with different institution and can be considered to restrict the right to free movement.

Estonia has already a considerable experience on e-government. For the country, the electronic system of dealing with family events is not merely a collection of vital statistics, but a whole administrative procedure of registering births, deaths, marriages and divorces electronically. The electronic registration of family events is in use from 2010, but already from 2002 an electronic data, including family events data collection for the Population Register.

The nature of civil status registration in the context of e-government is discussed in this chapter. The Estonian model shows one possible application to the use of electronic resources in delivering governmental services: the civil status registration. EU future trends are explained on the basis of an assessment of recent developments of civil status registration. These analyses explain the links between a functioning and integrated EU register and the right to free movement of people.

2 The Nature of Civil Status Registration

In most countries, a civil registration system is used to record statistics on "vital events" such as births, deaths, marriages, divorces and fatal deaths. This administrative system creates a permanent record of each.[11] "Vital statistics" are used to derive the fundamental demographic and epidemiological measures that are needed in national planning across multiple sectors, such as education, labour and health. They are also critical for a wide range of government activities (e.g. "population registers" and other registers) and commercial enterprises (e.g. life insurance and marketing of products).[12, 13]

Too often the demographic role of civil status has been emphasized, but it is important to notice that the civil status has a fundamentally legal basis besides it is the demographic use. The records derived from the civil registration systems have the following main uses: They are personal legal documents, required by citizens as proof of facts (e.g. age and identity) surrounding events; such documents are used, for example, to establish family relationships and inheritance rights; provide proof of age; establish the rights based on age (e.g. school entry, driving privileges); provide proof of marriage or divorce and the right to marry;

[11] World Health Organization (2010, p. 1).

[12] Ibid, p. 1.

[13] See Farooq (1981).

provide evidence of death.[14] In general, they are the scope of competences of human beings as it is explained by the civil laws and the laws of personality. It measures the legal competences and relevance of a person and defines the links between persons and the state. Everyone needs to know who they are dealing with, and the state relates to its population depending on the records it keeps. These records shape the individuals competences, their capacity and their entitlements. In that respect, the civil status data serves both, the private and public interests.[15]

The United Nations has defined civil registration as a continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population as provides through decree or regulation in accordance with the legal requirements of each country.[16] It provides a safeguard for the human right to social status and individual benefits.[17] For the individual, the main benefits of a civil registration system are the provision of legal status and the official documentation of important life events.[18]

A system of civil registration includes all institutional, legal and technical settings needed to perform the civil registration functions in a technically sound, coordinated and standardized manner throughout the country, taking into account the cultural and social circumstances particular to the country.[19] Correct civil status data are a ground for legitimate administrative deed and protect the rights of the person being a subject in a certain legal relations as well as the rights of third persons.

Civil registration as such has a very long tradition. Already 2000 years ago, household registration existed in ancient China (Sia Dynasty; 21st century BC), as early as 701, a household law was passed in Japan, institutionalizing Japan's first household registration.[20] De Groot explains vividly that if the population registration had not taken place, Jesus—very likely—would have not been born in a stable in Bethlehem, but in a very normal house in Nazareth.[21]

In Europe during the Middle Ages until the French Revolution, the registration of personal data was often undertaken by churches, as the first is mentioned Cardinal Xiemenes, the archbishop of Toledo (in 15th century), who provided for the introduction of registers which were to be maintained regularly by the parish priests.[22] The French Revolution introduced the registers of civil status carried by

---

[14] Ibid, p. 1.

[15] See Bidaud-Garon (2009).

[16] United Nations (2002, p. 5).

[17] Ibid, p. 5.

[18] World Health Organization (2010, p. 4).

[19] Ibid, p. 5.

[20] Szép (2000).

[21] See De Groot (2009).

[22] Statistical Office of United Nations (1991, p. 3).

the local governments.[23] This new French system of registration of persons (Napoleon's Civil Code) was introduced in many other countries during the nineteenth century.[24] However, while Finnish and Swedish parish registers go back to the seventeenth century, the local registers in Belgium, Germany, Italy, Luxembourg and Spain are only of twentieth-century origin.[25]

Historically, the registration itself developed differently in different states—the data collected varied, the systems transformed and the administrative organs dealing with registering had different ranks of authority. This led to the current situation where today, when Europe dreams of unified civil status certificates, it faces a problem of having over the forty different details given in the EU member states' birth certificates.[26, 27]

Besides the divergence of family laws and the differences mentioned above, every member state has been using their own digital solutions that are not necessarily interoperable. Furthermore, those technical solutions have different level of sophistication, some are contemporary while others could be considered outdated. Anyway, local family books in certain region on a paper or digital form do not satisfy the needs of citizens any more for the reason of raised cross-border family events and spread mobility of people. Often citizens raise the obligation to bring the document certifying their civil status as a limitations of their rights and freedoms, especially when travelling from one state to another.[28]

This shows that civil registration is not a local but global question demanding the knowledge of registration systems of other states as well as the cooperation between the states. EU policy emphasizes the cooperation between the registrars of member states of EU in this context to promote the free movement of citizens and plans to use the one common information system[29] to deliver the information about civil status or control the authenticity of the document, including in a process of entering the data into the Population Register.

EU member states had agreed to make all major services of the administration available on the Internet by the end of 2005.[30] Implementation is based upon national strategies and subject to on-going benchmarking by the European Commission. A key factor in the development of e-government is a simple design of the services offered, so that the users can transact business with public authorities rapidly and conveniently via the Internet. Applications have to pay

---

[23] See De Groot (2009).

[24] Ibid.

[25] Redfern (1989, p. 2).

[26] See European Commission Green Paper to Promote Free Movement of Public Documents and Recognition of the Effects of Civil Status Records. COM (2010, p. 9).

[27] About the differences in family documents see Joamets and Kerikmäe (2013).

[28] See also Zadravets (2012).

[29] Internal Market Information System.

[30] See ECRN (2008, p. 8).

added attention to the mobility of society and offer appropriate services, making it possible to use specific services of the administration via mobile terminal equipment.[31]

The EU Commission communication calls for interoperability among all national and regional administrations in the EU. E-government at a pan-European level will remove administrative barriers and facilitate the free movement of businesses and citizens within the internal market. A modern public administration has to be built upon digital services together with streamlined e-government process.[32] This means a considerable development of the information and communication technology. In Estonia, such development has received and will continue to receive great attention; this includes the Population Register and issues of civil status registration.

Civil registration as a recording of vital statistic data means, in principle, inserting information into a register—the Population Register. However, civil status data are only one section of the many in a register; register consists also of other data related to the person, which is not considered as civil status data.

Registration systems can be local[33] (e.g. Germany); or central[34] (e.g. Sweden, Finland, Latvia, Lithuania, Poland, Netherland, Belgium, Austria, Czech Republic, Slovakia, Hungary, Slovenia, Rumania and Bulgaria). Population Register can get its data from local register, or be as one electronic environment, which is accessed by the local officials to enter the data directly into the Population Register with no need to keep it in the local register for some time and send then the data to the central register. Although member states are responsible for the interoperability of their own systems, interoperability at European level is needed in order to implement common EU policies related to Population Registers as well.

The issue of such interoperability on electronic services of public interest remained therefore high on the EU Agenda, notably as a part of the new strategic framework "i2010[35]—A European Information Society for growth and employment" and the various related initiatives and programmes. i2010 explicitly addressed interoperability as one of the four main challenges for the creation of a single European information space.[36] The new policy was planned by the Green Paper to Promote Free Movement of Public Documents and Recognition of the Effects of Civil Status Records[37] related to the civil status data.

---

[31] Ibid, p. 8.

[32] See ibid, p. 9.

[33] Data collected into the different local registers stored in different administrative regions. Problems arise because, e.g. birth and marriage can be registered in different local units.

[34] As one electronic environment, which is accessed by the local officials to enter the data directly to the Population Register.

[35] COM (2005).

[36] See ECRN (2008, p. 12).

[37] COM (2008) 747 final, 14 December 2010.

3 Estonian Population Register

Civil registration in Estonia began in the 19th century; until 1926, there was no uniform system of registration provided by clergyman in special books with different form, data and language.[38] Since 1925, the ecclesiastic system was replaced by the "bourgeois system"[39] similar to other European states. "Family letters" were kept by the commune administration of the living place of the person, family event acts were made in two copies on paper, the first of them was stored in the archive of the Ministry of Interior and another in the family archive of certain county government in which the registration took place. Despite the German and Russian occupation, the system remained rather similar except the data collected and the forms of vital statistics acts which were changed.

After the restoration of independence in 1991 a strong need for population data was emerged. This was caused by elections, the exchange of Rouble into Estonian Crone, issuing the new identification documents, etc. Because a central database was missing, different separate registries were established by the different authorities to collect the data. The first population database was established in Statistical Office in 1992 by the cashing list. From this database, the Population Register was created.[40]

With the entry into force of the Population Register Act in 2002, civil status data began being recorded into the electronic Population Register. In 2010, there was an important development related to the civil registration and this register—by the Vital Statistics Registration Act[41] the complete electronic registration of family events was created, now the procedure of registering a family event was fully electronic, from the application citizen presents up to the certificate issued after the entering the data into the register.

Population Register[42] is a base register for the national public administration. Data contain the basic data of individuals (citizens and residents) which is updated continuously. Population Register is one of the most important registers in Estonia, next to the civil status data it consists also many other data used by the public and private sector. Main importance of the register is serving the public sector in executing the state functions by facilitating the access to the needed information.

The Population Register plays a central role in the Estonian information society policy. One aim of developing e-government and information society is to increase the availability of existing solutions and promote the genesis of new e-services;

---

[38] In different periods the different languages were used—Estonian, German, Old-Russian.

[39] Teder (1939, p. 3).

[40] Kontrolliaruanne (2002).

[41] Entered into force in 01.07.2010.

[42] In Estonia, the Ministry of Internal Affairs exercises the rights of the chief processor of the Population Register and authorized processor is AS Andmevara which is a limited company belonging to the state, which ensures technical operation of Population Register (Population Register Act par 10 and 12).

one course of action in developing the person-centred, transparent and an effectively operating public sector is reshaping the administrative deeds and procedural logic according to the availabilities of information and communication technology.[43] The Estonian civil status registration model can be a good example.

4 Estonian Model of Digital Civil Registration

In Estonia, a civil register as a digital environment for the procedure of registering the family event is a section of Population Register. This means that a civil registrar enters the data and makes all the administrative deed procedures directly into the Population Register in registering the family event.

Civil status data can reach to the register by many ways, e.g. by the registration of certain family event (birth, death, marriage, divorce), by entering the civil status data from the (foreign) family event document into the Population Register, by entering the data from the Estonian "paper family event certificate", etc. In terms of digital environment, these procedures are built up and regulated differently.

The entire administrative deed is electronic from the state side. Instead of *vital statistics act on paper,* there is a *digital vital statistic entry* being an administrative decision of a registrar on the one hand and the collection of data entered into the Population Register on the other. Vital statistics entry enters into force upon storage in the Population Register. Enforcement is important as they have legal meaning—when vital statistics are entered into the Population Register by the civil registrars, other public officials, anywhere in the world can use them in their deeds immediately after.

Every public authority (judges, court officials, administrative organs, consuls, police, notaries and local governments, etc.) must use the vital statistics data from the Population Register. They have access to the data and are not allowed to ask any certificate (in paper or digital) proving a family event, status or other relevant facts, when this information is available as registered.[44] Whereas in the beginning, officials dismissed this obligation, still asking people for paper certificates to prove civil status, a year or more after the law entered into force, today it seems natural that information is all available from the "desktop" of an official. Furthermore, if a public official outside the civil registrar's office notices that the data of certain citizen is not entered into the Population Register, it is solved with a request on an e-mail. Vital statistics acts on paper are digitalized, civil registrar can take the document from the digital archive and enter its data immediately into the Population Register, and there is no need to send a citizen to the registrars

[43] Ülevaade avaliku sektori toimimisest digitaalse dokumenditöö tõhustamiseks. Uuringu lõpparuanne. Tallinn (2011), p. 3.

[44] Also private persons have the possibility to receive an access to the Population Register data they need in their services. This need will be assessed by the state and state provides the control over the use of Population Register data.

office to correct the data by him/herself. Such solution is comfortable and practical, saving time and money, being clearly a good example of an effective e-government.

As a person knows best his/her data, it is important to give him/her a possibility to control his/her data and there are comfortable means to inform about the wrong data found. In Estonia, it is possible to do it through the Gateway to eEstonia.[45]

On the other hand, the *object*[46] of a Population Register is a person, that is someone whose civil status data must be entered into the register according to the legal acts, has an obligation to present a state the data about the family event taken place abroad. Such obligation, though not sanctioned, helps the updating of the data in a register.

There is an ongoing process of entering the *paper vital statistics acts data* into the Population Register. This process will take years. Undoubtedly, it is also a difficult task—the Second World War and different practices in the different eras make it difficult or sometimes even impossible to read and understand the data on a document, some family books and vital statistics act books are burned or lost in during the war.[47] Reading and understanding the data need the knowledge of legal acts of certain periods regulating the meaning of vital statistic acts and the skill to read different handwritings, including in German and Russian as in different periods, the acts were performed by those languages. However, a lot has already been done, and the entered data facilitates the use of civil status information considerably.

The electronic administrative process is very practical. Unfortunately not all the applications of family events can yet be presented online; however, the move is towards such solution. Although the use of digital signature is widely used, family events registration like birth and death, marriage and divorce needs still an applicant to come to the registrar's office. Today, the only full online deed is a birth registration in case parents of the child are married. An application can be sent electronically digitally signed by both parent, civil registrar registers the birth and sends electronic certificate to the parent(s) in case they want a certificate. There is also in a process the working out of the full online death registration by the data sent by the medical facility.

However, a citizen does not have to fulfil any application but informs the registrar about the needed data and the registrar adds it into the pre-fulfilled electronic application form[48] and then prints it out for signing by the applicant. After the signing, the application gets a digital form and is entered into the civil register. Every "paper document" presented in a civil registration procedure is also stored in a civil register after they get a digital form; similarly, all the documents (letters,

---

[45] www.eesti.ee.

[46] Population Register Act par 4.

[47] Possible nature disasters, wars and cyber attacks are the main enemies of the Population Register.

[48] This form is "pre-filled" taking the existing data from the Population Register.

e-mails, etc.) related to the procedure are stored in a civil register allowing to control the facts that the data in a Population Register are based on and facilitate the state supervision over the administrative body as well as over the legality of the administrative deed.

As mentioned above in the relationship with a state, a citizen does not need a certificate of civil status at all because an Estonian official has an obligation to take the needed data from the Population Register, only in relation with private person there could be a need for a vital statistic certificate.[49] Such certificate can be issued in a paper or in a digital form.

The main need for paper certificate is for their use abroad. Vital statistic certificates are issued in Estonian, English, German and French, for the convenience of the citizen as it does not require translation.

The digital civil register allows Estonian Embassies abroad to fulfil the certain civil status procedures as well. However, this capacity is limited—Embassies do not register births and deaths, do not contract marriages or divorces, but only enter the appropriate data from the foreign documents into the Population Register and issue the certificates needed. By this, they use the digital civil status environment of Population Register.

As a citizen has an obligation to present the data of family event taken place abroad to the Estonian Population Register, it is more comfortable for him/her to present a document to the Embassy in his/her state of residence.

An obstacle for online family events registration is the obligation of a civil registrar to explain the legal consequences of the declaration of intention to the person concerned, e.g. in case of birth registration the acknowledgement of paternity, deciding the custody, choosing the matrimonial property in marriage and divorce. However, in analysing the single deeds and the content of the explanation, there could be found no reason to require the (physical) personal presence of the citizen in front of the civil registrar. A legal explanation can be given also in written form in the same way we have become accustomed to "accept" the legal conditions of many contracts online, which also bring along legal obligations. By the digital signature, the state of event and acceptance get the legal meaning. This is a challenge for the future developments of civil status registration.

5 Future Developments

Civil status registration is dynamic; it depends on the developments of the quickly changing needs of the society and greater opportunities facilitated by digital tools. In practice, there is a rotation of front-office perspective as the perspective of service user and back-office perspective as the perspective of the provider of

[49] See footnote 44.

service.[50] In the developments of the civil status registration, both aspects have a continuous attention in Estonia. Development projects are directed to make the register stronger, faster and more secure.

The trend towards the connection of all the public registers so that all the registers take some of their data (especially civil status data) from the Population Register ensures the similar data in every register and gives possibility to correct the data as person communicates to different registers in different periods.[51] As Redfern states "The greater the number of administrative functions served by a Population Register the more accurate and up to date it is likely to be, because opportunities for updating and correction are frequent and the citizen becomes used to quoting his personal number. Conversely a register serving only one or two functions is likely to be inaccurate: though the citizen may be obliged by law to notify changes, there are infrequent references to the register and the citizen may have little incentive—or indeed disincentive—to have it updated".[52] In Estonia, not all the registers are yet connected. One of the reasons here is the different technical structure which does not work in the case of connection as is needed. The registers are, however, developed considered the need to attach them to each other. This means that a citizen presents his/her valid civil status document/data only once to the state[53] and all the administrative organs who need the data can/must use it from the Population Register or take it as the basic data for its own register.

The Estonian National Audit Office has stated that the Population Register must follow including the following principles: collected data must be available for all; only the one main personal data is correct and they must be in a Population Register; it is efficient to collect the data in the process they are formed; data are collected only once, they are kept actual and are used when needed; it is forbidden to have the registers with the same content and collect data from people for such registers.[54] All these principles are considered in developing the digital registers in Estonia.

It is evident that the e-government does not mean digitalization of the civil registration blindly and in force. Every single development needs an analysis of the expenditures. In an economic sense, the costs and benefits must be considered, for example if there is a real need for keeping next to the digital service also a traditional service,[55] then one has to prognose how much they both would be used. It is normal that every new form of service needs some time to diffuse and apply correctly. Digital changes as a change in one small part of the register can bring along

[50] See Ülevaade avaliku sektori toimimisest digitaalse dokumenditöö tõhustamiseks. Uuringu lõpparuanne. Tallinn (2011).

[51] According to the Estonian Communication Society development plan 2013 public power must organize its activity to ensure that the same information is asked from the citizen, enterpreuners and organizations only once (Eesti infoühiskonna arengukava 2013, p. 7).

[52] Redfern (1989, p. 2).

[53] Data is entered into the Population Register.

[54] Kontrolliaruanne (2002).

[55] Administrative deed in a state or local government office.

bigger problems in other parts of this database. This is especially important in regards to the connection of registers. This means that every single change must be tested correctly. A new Population Register in 2010 by which all the data from the old one was transferred into the new environment was a big challenge for Estonia.

Developing the Population Register and civil status registration there cannot forget the trends and expectations of EU. The spread of cross-border family relations needs the revaluation of the content of the collected civil status data. Convergence of the data collected and entered into the Population Register can lead to the promotion of free movement by simplifying the recognition of certain data.

However, also in Estonia despite a notable and quick development of a digital society some problems can be identified. The National Audit Office of Estonia has criticized that sometimes, it is not clear what profit one or another information system gives in reality. Most of the development projects are started without the assessment of their technical and economic implementability. Also, in many cases, there has not been involved to the projects all needed stakeholders, which has lead to the situation where information system does not conform to the expectations and needs of the users of those systems. The National Audit Office also refers to the need to consider more of interaction of information systems. Uniform structure of communication limits possible fraud in delivering public benefits and goods and avoids evasion of obligations.[56] From the view of Population Register, this is not a critic towards this register, but to other registers which have not yet linked themselves to the Population Register to take the basic data from it but continue to collect their own data instead of using one unite central database.

In improving the state governance, the following must be considered: the whole conduct in public sector is electronic; state information system is service-based and works according to the needs of users instead of the needs of departmental structures of government; applications of identification used in Estonia correspond to the best practices of the world and are applicable in Estonia as well as internationally; other people, especially the citizens of EU living in Estonia, have an access to the e-services.[57]

EU policies impact the development of Population Registers and civil status registration considerably. Popiołek states that if EU wants to be competitive in the international market, it must keep up with technological development, for that reason the development of the information society structures is not only a choice but a necessity.[58] Population Register is one of the components.

The principle of mutual recognition and convergence of family laws are some of the main goals of the EU policy in this area. One example here is a Green Paper—Less Bureaucracy for Citizens: Promoting Free Movement of Public

---

[56] Mattson (2010).

[57] See Infoühiskonna arengukava aastani (2013). Available at: http://www.riso.ee/et/infopoliitika/arengukava, p 3.

[58] See Popiołek (2013, p. 399).

Documents and Recognition of the Effects of Civil Status Records—to work out measures within the framework of Stockholm Programme to guarantee full exercise of the right of freedom of movement[59, 60] Related to one common pan-European civil status certificate and the cooperation between the civil registrars of different member states—the exchange of information which allows the civil registrar of the member state of origin of a person to be informed of the fact that a record concerning that a person has been made in another member state, allowing to update the civil status data should be fulfilled through the digital channels.[61] Popiołek explains the e-government in EU and United Nations as the transformation and new perception of administration caused by popularization of e-government in which the new way of governing is admittedly designed to facilitate the process of dealing with any official matters, to save time and money, to enable citizens to cope with every case without leaving home.[62]

In its future developments, EU has put the idea also into the proposal[63] of the Regulation of the European Parliament and of the Council on promoting the free movement of citizens and businesses by simplifying the acceptance of certain public documents in the European Union and amending Regulation (EU) No 1024/2012,[64] in which the document authenticity should be verified through the Internal Market Information System (IMI) established by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012.[65] The Market Information System includes also a functionality to maintain a repository of model templates of public documents used within the Single Market that can serve as first checking point of unfamiliar documents.[66]

This EU policy related to family law is a move to converge the family laws of member states. Stockholm Programme and aforementioned Green Paper provide bottom-up regulatory means to abolish the obstacles for the free movement of person. Undoubtedly the civil status data act an important role in this. Though in practice the trust for the civil status data on the documents of the later joined member states has been increased, there have still remained the questions about the authenticity of the civil status certificates in practice.

---

[59] See Joamets and Kerikmäe (2013).

[60] See also EU Citizenship Report (2010) and EU citizenship Report (2013), footnote 9.

[61] Ibid, p. 38.

[62] Popiołek (2013, p. 399).

[63] Related also to the Digital Agenda for Europe (COM(2012).

[64] Brussels, 24.4.2013 COM(2013) 228 final 2013/0119 (COD).

[65] OJ L 316, 14.11.2013, p. 1.

[66] See proposal of the Regulation of the European Parliament and of the Council on promoting the free movement of citizens and businesses by simplifying the acceptance of certain public documents in the European Union and amending Regulation (EU) No 1024/2012, COM (2013) 228 final 2013/0119 (COD).

One important question in delivering the data in the area of EU is data protection. As the legal regulations of data protection of member states differ, there should be solved first the "regulatory complexity in practice". In EU, the trend in policy of this field is "one continent, one law".[67]

The IMI is a software application accessible via the Internet, developed by the Commission in cooperation with the member states, in order to assist member states with the practical implementation of information exchange requirements laid down in EU. It operates by providing a centralized communication mechanism to facilitate cross-border exchange of information and mutual assistance. In particular, IMI helps competent authorities to identify their counterpart in another member state, to manage the exchange of information, including personal data, on the basis of simple and unified procedures and to overcome language barriers on the basis of pre-defined and pre-translated workflows. Where available, the Commission should provide IMI users with any existing additional translation functionality that meets their needs, is compatible with the security and confidentiality requirements for the exchange of information in IMI and can be offered at a reasonable cost. The purpose of IMI should be to improve the functioning of the internal market by providing an effective, user-friendly tool for the implementation of administrative cooperation between member states and between member states and the Commission.[68]

IMI should be seen primarily as a tool used for the exchange of information, including personal data, which would otherwise take place via other means, including regular mail, fax or electronic mail on the basis of a legal obligation imposed on member states' authorities and bodies in EU acts. Personal data exchanged via IMI should only be collected, processed and used for purposes in line with those for which it was originally collected and should be subject to all relevant safeguards.[69]

6 Conclusion

Civil status registration is a function of the state which has been in use from the ancient times. It has evolved with the changes of society and performing to satisfy the specific needs for a certain era. Besides a demographic role, civil status has also an important legal role protecting the rights of an individual. Civil status registration has been strongly related to state borders carrying the different cultural and traditional values, also in the EU.

The free movement and the spread of the cross-border family relations have revealed the needs to converge the civil status registration systems. Developments of the digital and information society have established the need for speed and

[67] European Commission—Speech (2013).

[68] Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC OJ L 316/1.

[69] Ibid.

convenience in dealing with "data", directing the member states to replace the local Population Registers by the central ones.

It is evident that in the context of free movement of persons there is a need to converge the civil status data member states collect and issue. In EU, there is a trend towards digital exchange of data as an additional mean for pan-European Population Register. It serves also the harmonization of the family laws of member states, but as a bottom-up policy means.

Estonia is a state which has a considerably long practice in digital solutions related to the civil status registration. Today, the whole administrative procedure is digital and the developments on this area are to leave aside the paper documents at all. From Estonian practice, there could be taken over many applicable solutions in digitalizing the civil status registration in other member states of the EU.

References

Baarsma, N. A. (2011). *The Europeanisation of international family law*. Berlin: T.M.C. Asser Press/Springer.

Bidaud-Garon, C. (2009). *The probative value of civil-status records: infringement of state sovereignty or protection of the state*. CIEC. Colloquy organised in Strasbourg on 13 and 14 March 2009 to mark the 60 years of existence of the ICCS : "Civil status in the XXIst century: Dusk or dawn?". Available at: http://ciec1.org/Etudes/ColloqueCIEC/Colloque60ans/PageAccueilColloque60ans.htm.

Data protection reform: restoring trust and building the digital single market. European Commission—speech/13/720, Sept 17, 2013. Available at: http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm.

De Groot, R. (2009). *Civil-status registers and population registers: battling brothers or siamese twins?* Colloquy organised in Strasbourg on 13 and 14 March 2009 to mark the 60 years of existence of the ICCS: "Civil status in the XXIst century: dusk or dawn?" Available at: http://www.ciec1.org/Etudes/ColloqueCIEC/Colloque60ans/PageAccueilColloque60ans.htm.

Digital Agenda for Europe (COM(2012) 784 final) and the proposed legislation on electronic identification andeSignatures (COM(2012) 238 final).

Duvivier, K. K. (2013). E-legislating. *Oregon Law Review, 92*, 9–76.

ECRN. (2008). *Situation and regulation of the civil status administration in Europe.*

Farooq, G. M. (1981). Population, human resources and development planning: towards an integrated approach. *International Labour Review, 120*(3), 335–350.

Joamets, K., & Kerikmäe, T. (2013). The new developments in EU family law—its applicability to Estonian law. *Korea University Law Review, 13*, 25–42. (The Korea University Legal Research Institute).

Mattson, T. (2010). *Sageli ei ole riigi infosüsteemide arendamine tulemuslik*. Available at: http://www.riigikontroll.ee/Suhtedavalikkusega/Pressiteated/tabid/168/557GetPage/1/557Year/2010/ItemId/474/amid/557/language/et-EE/Default.aspx.

Popiołek, M. (2013). E-government in popland—selected issues. *Journal of Education Culture and Society, 2*, 397–403.

Redfern, P. (1989). Population registers: some administrative and statistical pros and cons. *Journal of the royal Statistical Society, Series A, 152*(1), 1–41.

Silveira L (2009) *Civil status and the protection of the individual under the European convention on human rights*. CIEC. Colloquy organised in Strasbourg on 13 and 14 March 2009 to mark the 60 years of existence of the ICCS: "Civil status in the XXIst Century : dusk or dawn?". Available at: http://ciec1.org/Etudes/ColloqueCIEC/Colloque60ans/PageAccueilColloque60ans.htm.

Szép, J. (2000). *Population Registration Overview of some Eastern Countries*. Available at: http://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&ved=0CHAQFjAHOAo&url=http%3A%2F%2Fwww.riserid.eu%2Ffileadmin%2Fuser_upload%2FDatei%2F5_konferenz%2FS6_17_Population_Registration_in_Asia_Jeno_Szep.pdf&ei=P7eVUqbvBqXuygPms4CYDw&usg=AFQjCNFDGOuBjqFCpA2Ig6Gtn9uPOcOKzw&sig2=el5bmQ90bOuRzxQs1fY0Fw&bvm=bv.57155469,d.bGQ.

Teder T (1939) *Perekonnaseisuametniku käsiraamat*. Siseministeeriumi Administratiivala Kirjastuse väljaanne.

Books and Articles

Official Materials

EU Citizenship Report. (2010). Available at: http://ec.europa.eu/commission_2010-2014/reding/factsheets/index_en.htm, 2010 EU citizenship report—24 key actions Available at: http://ec.europa.eu/geninfo/query/resultaction.jsp?query_source=REDING&QueryText=civil+status+registration&swlang=en&x=0&y=0.

EU Citizenship Report. (2013). Available at: http://ec.europa.eu/commission_2010-2014/reding/factsheets/citizenship-report/index.html.

European Commission Green Paper to Promote Free Movement of Public Documents and Recognition of the Effects of Civil Status Records. COM(2010). 747 final, Dec 14, 2010.

United Nations. (2002). *Handbook on training in civil registration and vital statistics system*. New York. (pdf) Available at: http://unstats.un.org/unsd/demographic/standmeth/handbooks/default.htm.

Statistical Office of United Nations. (1991). *Handbook of vital statistics systems and methods,* Vol. I. Legal, organisational and technical aspects. Series F, No 7. . Department of Economic and Social Affairs. New York. Available at: http://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCwQFjAB&url=http%3A%2F%2Funstats.un.org%2Funsd%2Fpublication%2FSeriesF%2FSeriesF_35v1E.pdf&ei=e-H4UvfAEvHb7AbnkoG4BQ&usg=AFQjCNFihLAjG6bpsQX58LXS8NyrmI8FFw&sig2=0uBkv89_vs0GHv5ewBJo-w&bvm=bv.60983673,d.ZGU.

Infoühiskonna arengukava aastani. (2013). Available at: http://www.riso.ee/et/infopoliitika/arengukava.

i2010—A European Information Society for growth and employment. COM (2005). 229 final of 1 June. http://europa.eu/legislation_summaries/information_society/strategies/c11328_en.htm.

Kontrolliaruanne. (2002) *nr 058/2001 Rahvastikuandmed riigi registrites*. Tallinn, Dec 17, 2002.

Living Online. Digital Agenda for Europe. A Europe 2020 Initiative. Available at: http://ec.europa.eu/digital-agenda/living-online.

Proposal of the Regulation of the European Parliament and of the Council on promoting the free movement of citizens and businesses by simplifying the acceptance of certain public documents in the European Union and amending Regulation (EU) No 1024/2012, COM(2013) 228 final 2013/0119 (COD).

Regulation (EU). (2012). No 1024/2012 of the European Parliament and of the council of 25 Oct 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC OJ L 316/1.

Stockholm Programm OJ C 115/8 04/05/2010.

Ülevaade avaliku sektori toimimisest digitaalse dokumenditöö tõhustamiseks. Uuringu lõpparuanne. Tallinn (ordered by RISO & RIA). (2011). https://www.google.ee/search?q=%C39Clevaade+avaliku+sektori+toimimisest+digitaalse+dokumendit%C3%B6C3%B6+t%C3%B5hustamiseks.&ie=utf-8&oe=utf-8&rls=org.mozilla:en-US:official&client=firefox-a&channel=fflb&gws_rd=cr&ei=jOj4UqHPNsmP7Aa0pYGYBg.

World Health Organisation. (2010). *Improving the quality and use of births, deaths and cause-of-death information: Guidance for a standards-based review of country practices*. WHO Press, Geneva.

Zadravets, B. (2012). European Parliament. Directoral General for Internal Policies. Policy Department C. Legal Affairs Citizen's Rights and Constitutional Affairs. Civil status documents—challenges for civil registrars to circumvent problems stemming from the legal void. Note. http://www.europarl.europa.eu/studies.

The Fragmented Securitization of Cyber Threats

Agnes Kasper

Abstract Cybersecurity is one of the most pressing national security issues nowadays. Cyber threats reached truly global scales, cyber attacks that potentially or actually cause physical damage are on the rise, and securing critical infrastructures against cyber incidents is seen as a priority by many. Virtually every national cybersecurity strategy points out the importance of the international cooperation in this field, and there have been initiatives for a global cybersecurity treaty as well. Although a number of national and regional policy and legal instruments exist in this field, the conclusion of a truly international treaty remains a highly controversial topic. The aim of this chapter is to identify the factors that make such a global cybersecurity treaty (un)viable. It will begin with an overview of the history of cybersecurity and its early securitization process by the USA and Russia, and then, the focus will shift to the present strategic approaches and responses.

1 Introduction

Cyber space with its opportunities and threats is a dynamically changing environment characterized by increasing the complexity of IT products, entangled public and private interest, consistently emerging new vulnerabilities, sophistication and availability of tools and attacks in the underground markets, and networks enabling transfer of knowledge and resources to the masses. Impacts of cyber threats on the economic, political integrity and physical security of states, organizations, and individuals are discussed widely.

A. Kasper (✉)
Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia
e-mail: agnes.karpati@mail.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_9

Nations have started to take a number of steps to fight computer fraud and misuse already in the mid-1980s and the 1986 in USA. Computer Fraud and Abuse Act (18 USC 1030) was the first piece of specific legislation to address cyber crime and criminalize illegal access to computers. The issue of cybersecurity has arrived to the international discussion forums in the 1990s, and despite that the borderless and transnational nature of cyber threats was understood, there are few truly global legal answers in this field. Although already significant amount of legislation exists in national and regional level that deals with some aspects of the cyber space, there is little evidence that the world became more secure than 15 years ago. One Internet security company, Symantec reported that it blocked an average of 247,350 Web attacks per day in 2013[1]—each is a potential attempted crime—while the UN Cyber crime Study suggests that only 1 % of the victims of cyber crimes turn to the law enforcement authorities.[2]

There already exist over hundred legal instruments related to cybersecurity and tackling a narrower slice from the broad cyber spectrum, including the most prominent ones such as the Cyber crime Convention,[3] Shanghai Cooperation Organization's agreement,[4] and the EU Directive on attacks against information systems. Several international regimes are somewhat helpful in addressing cybersecurity, but they tend to remain regional and none of them alone offer a comprehensive framework for regulating all of its aspects. There have been numerous initiatives and suggestions for global instruments addressing aspects of cybersecurity or creating entire frameworks, but there is a disparity between the concepts and assumptions between the Western and Russian views and states do not seem to agree on some basic principles and definitions.[5]

The fragmentation in policies tackling cybersecurity, the uncertainties in determining jurisdiction, and the scarcity of law enforcement capabilities to combat cyber crime and the asymmetry between the offensive and defensive sides in cyber space keep offering new opportunities for criminal activities. This chapter will discuss the increasing concern of states about cyber threats and how they became issues of national security and look for the differences that prevent states from agreeing on the basic principles of tackling cyber threats globally.

---

[1] See at http://www.symantec.com/security_response/publications/threatreport.jsp (Accessed 15 Mar 2014).

[2] United Nations Office on Drugs and Crime (2013), p. 118.

[3] Council of Europe Convention on Cyber crime of 23. November 2001, CETS No.: 185.

[4] Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, signed in Yekaterinburg on 15th June 2009.

[5] Russia's Draft Convention on Information Security—A Commentary, Conflict Studies Research Centre and Institute of Information Security Issues, Moscow State University 2012. Available at http://www.conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf (Accessed 15 Mar 2014).

2 History of the Internet and Cyber Threats

The predecessor of the Internet is US Department of Defense project that got out of the governments hands. ARPANET was a response to the 1960s threat of total war and aimed to provide a robust communication network without a central hub.[6] The adoption of the technology by the private sector, business, and consumers brought about the most significant changes in how information is produced, made available, used, and consumed. ARPANET and the early networks were not meant to be the underlying technology and the backbone of our global economy, and they were not built with security considerations in mind. As a result, the decentralized architecture of the Internet and the lack of built-in security together with the societies' ever-growing dependence on information and communication technologies seriously challenge our legal concepts and mechanisms.

On October 29, 1969, the first transmission was made, while the first public demonstration of ARPANET took place in 1972.[7] The first virus appeared already in 1971, and it was dubbed the "Creeper worm," a self-replicating program, which jumped from machine to machine, demonstrating how programs propagate through the Internet, but it did not do any malicious activity.[8]

While in the 1973, first transmission between the USA and Europe foresaw that this technology will become a global platform, in the initial period, several parallel networks were running, serving mainly academia and research communities and only the universal adoption of the TCP/IP protocol[9] transformed the independent systems into an a real Internetwork—the Internet.[10] The first spam e-mail is believed to have been sent on May 1, 1978, by Gary Thuerk, and reached 400 users over ARPANET.[11] It was also in the 1970s that the first mobile phones were built by Motorola, the first 1G wireless network emerged in Japan, and smaller computer designs led to a paradigm shift in computing.

---

[6] See Cridland (2008), p. 2.

[7] Ibid.

[8] Melissa Hathaway, Keynote address on 17 June 2010, Conference on Cyber Conflict 2010, 15–18 June 2010, Tallinn.

[9] According to the Institute of Electrical and Electronics Engineers, the TCP/IP (transmission control protocol and Internet protocol) is a standard that deals with packets and enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

[10] Barry M. Leiner, Brief History of the Internet, Internet Society. Available at: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (accessed 15 Mar 2014).

[11] Gina Smith, *Unsung Innovators: Gary Thuerk the father of spam*, Computerworld, Security 2007, available at http://www.computerworld.com/s/article/9046419/Unsung_innovators_Gary_Thuerk_the_father_of_spam (accessed 15 Mar 2014).

The 1983 DNS[12] registry test opened the door for the logical organization of data as we know it today, and private use of the Internet started soon to grow at an increasing rate.[13] In 1984, the breakup of the AT&T monopoly in the USA despite the Defense Secretary's concern that divestiture would jeopardize national security interest leads to intense competition and innovation in telecommunication—leaving the government with decreasing influence over the sector.[14] While the number of networks in the beginning of the 1980s was around 60 and they were serving the closed communities of researchers and developers, from the mid-1980s, services begun to target the wider audiences, prompting the need for compatibility between the networks and infrastructure investment (See Footnote 10). As the US Department of Defense was an early adopter of the technology, concerns were raised that the civil and military interests became entangled on the core infrastructure (See Footnote 8).

In 1988, the first Internet worm, the Morris worm was created, and the author, a PhD student in information technology, simply wanted to expose a security hole in the target system, but the worm turned out to propagate much faster than expected and caused serious harm to federal computer systems, leading to the first conviction under the Computer Fraud and Abuse Act of 1984. The industry learned the lesson from the Morris case and started to take security more seriously and started to build security features into software, intrusion detection systems, antivirus software, and firewalls emerged,[15] and the first CERT was established for the coordination of network emergencies at the Software Engineering Institute in Carnegie Mellon University.[16]

In 1990, Microsoft released a graphical user interface (GUI) operation system, Windows 3.0, that provoked a staggering market response and wide adoption both by home and by work users.[17] By 1993, the year of the development of graphical browsing[18] and the real starting point for what became known as the World Wide Web, there were approximately 50,000 operational networks on the Internet.[19] The

[12] The domain name system (DNS) helps users orient over the Internet. Every device on the network has a unique identification number (IP address), which is hard to remember. The DNS allows the use of a string of letters—a domain name—and the association of it with an IP address. When the user is surfing the Internet, the domain names are "resolved" to corresponding IP addresses, and the user's device can make the connection with the host. So instead of typing 193.40.254.28 into the browser's address line, it is possible to type www.ttu.ee.

[13] See Cridland (2008), p. 2.

[14] Kate Ballen, Labics Kenneth, *Was Breaking Up AT&T a Good Idea?* CNN Money, Fortune, 1989. Available at http://money.cnn.com/magazines/fortune/fortune_archive/1989/01/02/71446/ (accessed 15 Mar 2014).

[15] Ibid.

[16] See at www.cert.org.

[17] See at http://windows.microsoft.com/en-us/windows/history#T1=era3 (accessed 15 Mar 2014).

[18] The first graphical browser, Mosaic, had a distinctive feature that it used small icons for navigation, which made the surfing on the Internet easy for non-expert users as well.

[19] See Cridland (2008), p. 2 and Footnote 10.

World Wide Web was invented in 1989 at European Organization for Nuclear Research (CERN) answering the demand for automated sharing of scientific information.[20] CERN put this technology, which is independent of hardware, software platform, and physical location, into the public domain on April 30, 1993,[21] laying the foundations for a free and open Internet.[22]

Having in place the foundations of a technology that could be migrated to commercial use without much technical modifications, concrete and strong commercial interest in the Internet started to develop in the early 1990s and the primary open questions were concerning business models of service and profitability of providing Internet access outside the academic community.[23] In 1994, Nokia demonstrated that data transfer is possible through Wi-fi that forestalled the mobility revolution and the mobile payment systems (See Footnote 8). In 1994, Citibank was penetrated by Russian hackers and managed to steel around $10 million.[24] This is believed to be the first online bank robbery, and it is used to publicize the vulnerability of financial institutions. A technological response followed, and the secure socket layer (SSL) protocol was developed[25] to provide security and reliability between two communication applications.[26] In 1995, phishing started targeting America online (AOL) users and the scammers tricked out credit card numbers, passwords, other sensitive information, etc., which are subsequently used to compromise identities and/or gain some monetary benefit.[27]

Hotmail, the very first free Web-based e-mail service, was born in 1996,[28] followed by another prominent player, Google, in 1997. In 1998, complete hardware virtualization became possible with the VMware software that was one of the milestones toward cloud computing. In 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was set up to encourage interoperability and stability of the Internet (See Footnote 8). In 1997, the "Eligible Receiver" live exercise in the Pacific showed grave vulnerabilities using commercial off-the-shelf capabilities to penetrate the US defense computer networks.[29]

The end of the 1990s brought about the increase in processing and storage capacities that also made mass violations on the Internet possible. Napster was

---

[20] See at http://home.web.cern.ch/topics/birth-web (accessed 15 Mar 2014).

[21] Declaration is available at http://cds.cern.ch/record/1164399 (accessed 15 Mar 2014).

[22] The first Web site and the technology description are available at info.cern.ch (accessed 15 Mar 2014).

[23] See Greenstein (2001), pp. 151–186.

[24] Ibid.

[25] SSL was developed by Netscape, but only the SSL version 3.0 was successful.

[26] IETF RFC 6101.

[27] See at www.phishing.org (accessed 10 Mar 2014).

[28] Dick Craddock, The short history of Hotmail. Inside Windows Live (2010), available at http://blogs.windows.com/windows_live/b/windowslive/archive/2010/01/06/a-short-history-of-hotmail.aspx (accessed 10 Mar 2014).

[29] Ibid.

operating a peer-to-peer network for sharing audio and video files between users, which ended up shot down in 2001, and the court found that since Napster had the ability to regulate what its users distribute over its network, they had the responsibility to prevent infringement of copyright from taking place.[30] At the same time, a more vicious than ever malware appeared. The Melissa macrovirus exploiting vulnerability in MS Outlook on the other hand was the first fast propagating malware, infecting over 100,000 individual hosts.[31] In the year 2000, CNET reported that a massive distributed denial-of-service attack was conducted against major companies, such as Amazon, Yahoo, CNN, and eBay, rendering the services inaccessible[32] and that resulted in 1.2 billion USD in damage. The perpetrator turned out to be a 15-year-old Canadian teenager alias "Mafiaboy" who used online available hacking tools and was caught only because of his ego, and he bragged about what he had done.[33]

In the year 2001, the first 3G network was offered in Japan for commercial use that signifies a landmark in the history of mobile revolution by enabling innovative applications and services with fast connection.[34] In 2002, social networking started with the launch of the Friendster Web site, followed by the way more influential Facebook in 2004 that provides an environment ripe for identity theft, scams, cyber bullying, stalking, and other malicious activities, but also used by law enforcement and other government agencies for collection of intelligence.

As the Internet became the backbone and nervous system of the global economy and societies began to depend on information and communication technologies, it was also becoming a tool to undermine the dominance of the USA in a series of coordinated and precise attacks targeted against defense contractors, known as "Titan Rain," which is associated with the advanced persistent threat from China.[35] Cyber corporate espionage started to emerge as a national security problem, and Business Week reported a series of NASA network breaches.[36]

---

[30] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (2001).

[31] Software Engineering Institute Carnegie Mellon University CERT Division (1999) Frequently Asked Questions about the Melissa Virus, available at http://www.cert.org/historical/tech_tips/Melissa_FAQ.cfm (accessed 10 Mar 2014).

[32] Greg Sandoval and Troy Wolverton, Leading Web sites under attack, CNET News (2000), available at http://news.cnet.com/2100-1017-236683.html (accessed 10 Mar 2014).

[33] Justin Stephen, The Changing Face of Distributed Denial of Service Mitigation, SANS Institute Information Security Reading Room, 2001, available at http://www.sans.org/reading-room/whitepapers/threats/changing-face-distributed-denial-service-mitigation-462 (accessed 10 Mar 2014).

[34] See at ITU, 3 g: All about the technology, available at http://www.itu.int/osg/spuold/ni/3g/technology/index.html (accessed 10 Mar 2014).

[35] See The lesson of Titan Rain: Articulate the dangers of cyber attack to upper management, Homeland Security News Wire, 14 Dec 2005. Available at http://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management (accessed 15 Mar 2014).

[36] See at http://www.businessweek.com/stories/2008-11-19/network-security-breaches-plague-nasa (accessed 10 Mar 2014).

In 2006, a new business model is introduced in computing, and the first widely accessible cloud services were launched by Amazon Web Services and the Elastic Compute Cloud infrastructure as a service.[37] Soon after storage, software and platform were commoditized by the industry and began being offered as a service upon demand. Cloud computing magnifies some of the legal challenges related to the borderless nature of the Internet.

In the meanwhile, there were profound changes happening in the other end as well, cyber crime became increasingly organized, and due to the asymmetry in cyber space, the lack of real deterrence, and high return on investment, highly sophisticated tools appeared in the underground markets, such as the first banking Trojan "Zeus" in 2007. A trend can be observed that form of cyber crime targeting all users of the Internet shifts to forms that focus power on specific targets.[38] Zeus, a crimeware toolkit, included features like keylogging in order to steel banking credentials of customer, while the SpyEye toolkit version 1.0.7 exhibited an interesting new feature of "killing" the competitor (Zeus) first on an infected host.[39] This coding is also a clear implications that a strong competition between criminal networks emerged by the year 2010 in the underground market.

In addition to the mere economic importance, another facet of the Internet was exposed in 2007 in the Estonian cyber space and the first politically motivated wave of attacks was launched against a nation-state as a whole demonstrated the level of dependency and vulnerabilities of entire societies.

The year 2008 brought another landmark case, the international cooperation against the "Conficker" worm. Conficker built an unprecedented botnet of an estimated 10–12 million hosts; however, it was not used for any attack.[40] Significance lays in the fact that during the cleanup of the botnet, industry organizations', individuals', and government's efforts were united to respond to a global threat.

During the 2008 invasion of Georgia by Russia, the computer networks of Georgia were also attacked by unknown foreign intruders defacing and launching distributed denial-of-service attacks and other attacks against governmental, financial, and media Web sites.[41] Discussions were sparked about whether these events were cyber warfare, but soon another incident shocked the international community. Ghostnet, a cyber espionage network allegedly created by China, was discovered in computer networks of foreign ministries, diplomatic missions, media, and businesses in 103 countries. The malware's purpose was to collect information on high-profile

---

[37] Mohamed Arif, *A History of Cloud Computing*, Computerweekly.com available at http://www.computerweekly.com/feature/A-history-of-cloud-computing (accessed 10 Mar 2014).

[38] See Wilson (2009), p. 417.

[39] See Symantec blog available at http://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot (accessed 10 Mar 2014).

[40] See Conficker Working group: Lessons Learned (2011) available at http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf (accessed 14 Mar 2014).

[41] See Tikk et al. (2010), pp. 69–76.

politicians, businessmen, journalists, and other important persons, which caused an outrage. Investigation disclosed that the attackers potentially obtained unprecedented sensitive information, but it remains unclear whether it was exploited for commercial or intelligence purposes.[42]

In 2010, the Norton cyber crime report revealed the shocking fact that over 65 % of adults have been victim of cyber crime and 79 % do not expect cyber criminals to be brought to justice.[43]

Stuxnet in 2011 exhibited a new and more dangerous potential of cyber attacks: The myth about a malware causing physical damages became reality. The Stuxnet worm was probably developed a few years earlier, and it was targeting SCADA systems of industrial plants. Stuxnet manipulated the processes controlling centrifuges, and it is believed that this caused the malfunctions of parts in Iranian nuclear facilities.[44] Another similarly concerning incident took place in 2012, when the computer network of the Saudi Aramco was infected by the self-replicating Shamoon virus, causing significant disruption to the world's largest oil producer.[45]

In 2013, security firm McAfee compiled a report and stated that "cyber crime and cyber espionage global costs are estimated $300 billion annually."[46] Loss of intellectual property through cyber espionage is a serious concern for the society, and with the emergence and mass adoption of new technologies, the number of vulnerabilities will increase, so as the losses from cyber attacks and the sophistication of attacks.

Internet economy is growing, which creates new opportunities itself; however, it is worth to mention the risky practices (weak passwords, providing personal information in social networks), and unawareness of users also seriously contributes to the success of attacks. Societies are becoming increasingly dependent on the use of information and communication technologies in every aspect of life, while 80 % of cyber crime originates from organized activity and significant portion of attacks are directed against the confidentiality, integrity, and availability of information systems, illegal access amounting to 30 % of all acts.[47] Effective outsourcing models emerged in the underground markets offering crime as a service and other "products,"[48] and there is even a malware "copyright" system that is enforced by the criminals themselves.

---

[42] Information Warfare Monitor, Tracking Ghostnet: Investigating a Cyber Espionage Network (2009), available at http://www.tracking-ghost.net (accessed 12 Mar 2014).

[43] Norton Cyber crime Report: Human Impact, available at http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_UK-Human%20Impact-A4_Aug4.pdf (accessed 12 Mar 2014).

[44] See Ziolkowski (2011), pp. 3–4.

[45] See Bronc and Tikk-Ringas (2013).

[46] See at http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf (accessed 20 Jan 2014).

[47] See at http://resources.infosecinstitute.com/2013-impact-cybercrime/ (accessed 20 Jan 2014).

[48] See at http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf (accessed 20 Jan 2014).

In February 2014, the biggest DDOS attack of 400Gbps hit the service Namecheap hosting millions of Web sites.[49] This is the largest ever-recorded attack, and it affected the Internet connection internationally, but probably, the next record will come around soon.

Cybersecurity concerns have come to the center of attention in the recent years, and issues of potential impacts, need for resilience, investment, and international cooperation are debated by private and public sectors. The following sections will examine how such concerns have emerged through securitization processes and address the diverging perceptions and intertwined interests of stakeholders and the various international legal responses.

3 The Securitization of Cyber Threats and Fragmentation of International Responses

3.1 Securitization Theory and Threat Framework

States have decided that national security has a cybersecurity component.[50] Cybersecurity concerns arrived to the level of national security through the securitization process, by a conscious policy to emphasize the increasing seriousness of cyber threats, while using it as a ground for introducing extraordinary measures.

The concept of "securitization" started to emerge in the beginning of the 1990s, and it crystallized in the work of Buzan, Waever, and de Wilde by expanding the concept of security horizontally, from the material military focus to five political sectors as well (political, military, economic, society, and environmental).[51] Securitization refers to a process of moving a political agenda into the forefront of security, presenting issues as a significant or existential threat that warrants taking extraordinary measures, including the use of force.[52] Securitization theory examines the role of speech in framing the threats for explaining how issues become securitized.

Buzan's framework is often criticized for its state-centric approach, and it can take into account only a few years of post-cold war experience. The ending of the bipolar international system was a starting point for the Internet as in its current form, and the use of applications available on the Internet grew exponentially.[53] Appearance of new market-led economies and technological innovation drove the capacity of societies to process information with more efficiency that was imaginable before. Information and communication technologies, such as the Internet,

[49] See at http://news.cnet.com/8301-1009_3-57619235-83/namecheap-targeted-in-monumental-ddos-attack/ (accessed 20 Jan 2014).

[50] See Hare (2010), p. 214.

[51] See Buzan et. al (1998).

[52] See Buzan (1991), pp. 432–433.

[53] See Cridland (2008), p. 2.

became essential part of the newly emerged information societies. Although it has been proposed that cyber space constitutes an international commons,[54] because it shares characteristics with air, sea, and space, and therefore, it does not fall under the jurisdiction of a single state, neo-realist approach takes the position that states remain the actors in addressing cyber threats, because they have power and authority and they have capacity to improve the defenses against most existential cyber threats,[55] but more importantly because the infrastructures comprising cyber space are located within a territory of a state.

Existential threat is understood by Buzan only in relation to the particular referent object in question.[56] In the military sector, the referent object is usually the state, but in the political sector, existential threat is defined in terms of the constituting principle of the state. Anything that existentially threatens sovereignty or perceived to do so, such as non-recognition, questioning of legitimacy, or governing authority, can be invoked to warrant extraordinary measures.[57] Such measures include means that break the normal political rules of the game, such as forms of secrecy, levying taxes or conscription, limiting otherwise inviolable rights, or focusing society's energy and resource on a specific task.[58] In addition, the audience must accept the securitizing move, and securitization therefore has three elements: existential threat, emergency action, and legitimizing the breaking of the rules.[59] Securitization is recognizable from rhetoric and statements such as "if we do not solve this problem, everything else will be irrelevant."[60] Consequently, "security…ultimately rests neither with the object nor with the subjects but among the subjects"[61] and therefore implies that security is an agreement and securitization is a negotiated process.

However, it is usually not clear how different societies construct or securitize threats in cyber space, and there is a dispute whether the threat emanates from military, political, economic, or societal fields. To put it simply, military threats can affect all components of the state, political threats weaken the state as a political entity, economic threats are seen as destabilizing, for example, an economic sector, and societal threats relate to identity and culture of people.[62]

Based on the factors of relative military power and sociopolitical cohesion, Buzan has created a model for determining the typical types and importance of threats states are facing. He asserted that countries with weak military power, in order to

[54] See Kramer (2009), p. 12.

[55] See Hare (2010), p. 215.

[56] See Buzan et al. (1998), pp. 21–26.

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] Ibid. p. 24.

[61] Ibid. p. 31.

[62] Stone (2009).

Table 1 Traditional and cyber vulnerabilities and types of states combined[a]

		Sociopolitical cohesion	
		Weak	Strong
Power	Weak	Highly vulnerable to most types of threats/de-stabilizing political action in cyber space, attacks on Internet infrastructure, and criminal activities	Particularly vulnerable to military threats/DDOS and other major attacks on critical infrastructure
	Strong	Particularly vulnerable to political threats/de-stabilizing political actions in cyber space	Relatively invulnerable to most types of threats (less inclined to characterize issues as military)/ criminal activities in cyber space

aIbid

reduce their vulnerabilities, should specialize on their economies, while countries that display weak sociopolitical cohesion are interested in suppressing the threats to the idea of the state, its institutions, and territorial integrity (Table 1).[63]

Forrest Hare has applied the Buzan framework to cybersecurity and provided four basic models for categorizing states according to aspects of power and sociopolitical cohesion. These two factors are the indicators of the types of cyber vulnerabilities a state may face.[64] Military threats' equivalent could be, for example, a distributed denial-of-service attack against critical infrastructure, which has the characteristics of an invasion, taking over targets vital to population welfare, such as communication centers and financial institutions. In addition, economically developed countries that have relatively strong sociopolitical cohesion tend to rely on Internet infrastructures for financial transactions and intellectual property; therefore, they are vulnerable to stealing information assets (cyber corporate espionage and cyber crime). Politically destabilizing cyber threats appear in Internet forums and Web media, and they would target Web sites of political and state institutions (e.g., defacement).

Securitization of domains, regardless of whether threats are perceived or real, has public policy implications and determines the approach states take in responding to threats, including the legislative process relating to cybersecurity, both on national level and on international level. Hare explains that the P-S/SC-S states and P-W/SC-S states are the most likely to form alliances, while the P-W/SC-S and P-S/SC-W states policies are expected to be the most divergent. If the above application of Buzan's framework to cybersecurity is correct, then corresponding state policies should be identifiable to a certain extent in legal and strategic instruments as well, since sources of law are the results of compromise between states and the state policies should be manifested therein (or in negotiations, travaux preparatoire, etc.). It follows that if cyber threats securitized on a different basis by states, the core concepts relating to cybersecurity must vary as well, potentially

63 See Hare (2010), p. 215.

64 Ibid. p. 218.

leading to a deadlock in the negotiation of any meaningful global instruments between states and ending up with several regional agreements and divergent approaches. Therefore, Buzan's explanation of securitization and his framework appears to be promising in explaining the lack of global cybersecurity treaty, the emergence of regional instruments, and the modest results of the more than a decade-long process in the UN to propose a treaty.

It was demonstrated previously by the historical data that concern about the threats posed by the misuse of IT arose first from the IT sector, but it has been taken seriously by other disciplines with delay.[65] The potential misuse of Internet, unauthorized accessing of sensitive or confidential information, the alteration of data critical for the operation of infrastructure facilities, etc. have been considered as national security threats from the mid-1990s; therefore, it is possible to talk about the securitization of cyber space and cyber attacks can be perceived as an existential threat from that period. Understanding the underlying assumption and agenda of actors for securitization can assist to design informed responses to proposals and challenges, and they can either reduce their own vulnerabilities to a particular threat or take steps to mitigate the threat itself.[66]

3.2 Evidences of National, International, and Regional Securitization Processes

States have been securitizing cyber threats in their rhetoric and demonstrated corresponding action. Just to bring a few prominent examples: President Obama has devoted a 20-min speech on May 29, 2009, to the issue of securing the nations' cyber infrastructure,[67] and Estonian President Ilves has openly attributed the 2007 cyber attacks to Russia, despite the reported lack of conclusive evidence on that matter,[68] and the European Commission has brought forward a package of new initiatives dealing with cybersecurity.

All these moves of stakeholders can be analyzed to understand the underlying interests and reasons for invoking the corresponding issues and presenting them as supreme priority. The following section will look for some of the first evidences of securitization of cyber threats by the USA and Russia in the early period of the emergence of international cyber security problems and will compare the initial approaches to the present developments.

---

65 See Sect. 2.

66 See Hare (2010), pp. 221–222.

67 Remarks by the President on Securing Our Nation's Cyber Infrastructure, 29 May 2010. Available at: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed on 29 Sept 2010).

68 Opening speech by president Mr Toomas Hendrik Ilves at the Conference on Cyber Conflict 2010, Tallinn, 16 June 2010.

3.2.1 The United States

In the middle of the 1990s, the US military recognized its dependence on the privately owned critical infrastructure of the nation, where great vulnerabilities were discovered.[69] The Joint Vision 2010 strategic document issued by the chairman of the Joint Chiefs of Staff in 1995 states that "[a]ccelerating rate of change will make the future environment more unpredictable and less stable… How we respond to dynamic changes concerning potential adversaries, technological advances and their implications, and the emerging importance for information superiority will dramatically impact how well our Armed Forces can perform its duties in 2010. … Information superiority requires both offensive and defensive information warfare."[70] This document sets the stage for both organizational and operational changes in the US military, and the exploration of vulnerabilities to cyber warfare in DoD information systems was followed by the emergence of information warfare doctrines and establishment of special institutions to deal with this new threat.[71] In 1998 Joint Publication 3–13, Joint Doctrine for Information Operations was released and the doctrine comes to include both defensive and offensive elements to conduct computer network operations.[72]

The quality of staging the importance of information superiority as one of the main conditions for the armed forces to be able to operate effectively is indicative of securitization of cyber threats. It also suggests that the discovery of dependence of the defense on the private-held critical infrastructure that triggered the chain of changes in the US military is less important than the process of constructing the shared understanding that information superiority needed to be achieved in order to defend the nation. The language that the document uses implies that the present state is unpredictable and unstable, and it is not possible to determine the development with any certainty. The nation is exposed to dynamic changes and factors independent of the will of the state, and the survival of the nation is at stake in 25-year perspective unless the defense forces obtain information superiority to counter the threats that emanate from the adversaries who collect, process, and exploit information about the USA. The document iterates that offensive capabilities are needed as a response to this threat, which includes therefore the possibility of aggression and use of coercive measures, and it can be regarded as extraordinary. Since the information warfare doctrine was worked out so that it included the offensive capacity and structural entities dedicated to computer network operations were established, the process of securitization was successful.

---

69 See Kilroy (2009), pp. 439–440.

70 Shalikasvili, J., Joint Vision 2010. Washington DC: U.S. Government Printing Office and Department of Defense, Office of the Joint Chiefs of Staff. 1995. Available at http://www.dtic.mil/jv2010/jvpub.htm (accessed 14 Mar 2014).

71 See Kilroy (2009), pp. 440–444.

72 Ibid. p. 443; Joint Pub 3–13, Joint Doctrine for Information Operations, available http://www.c4i.org/jp3_13.pdf (accessed 13 Mar 2014).

Looking at the newest developments in the USA and analyzing the recent International Strategy for Cyber space, the results of further successful securitization processes can be observed in the US politics. The strategy opens emphasizing that the "[d]igital infrastructure is….the backbone of prosperous economies,…strong militaries, transparent governments and free societies."[73] The USA is recognizing the importance of cyber space for military, economy, politics, and social fields; however, as opposed to the Russian concerns about criticism to and influence on the state and its people, diversity in both political opinion and cultural diversity is highly valued. Open, interoperable, secure, and reliable cyber space is seen as a vehicle for the economic development, which theme is reiterated repeatedly throughout the document. The strategy is centered on two basic themes: the economic and technological priorities, and regulation and governance (both domestic and international). Both the structure and the content of the strategy suggest the elevation of cyber threats as posing existential threats to the economy. This view is confirmed by dramatized statements by state persons regarding what is became to known as advanced persistent threat (APT) and believed to be a large-scale Chinese computer network operation (mainly) against the USA.[74] One prominent testimony originates from General Alexander, who called the ongoing cyber espionage and cyber theft of information assets from private and public organizations the "greatest transfer of wealth in human history."[75] The strategy is clear on the point that immense effort and resources are directed in ensuring security of cyber space, and this theme is taken into consideration in several other policy fields related to information society. The fact that cybersecurity is above the normal political process has been definitely proven by the enactment of the failed CyberSecurity Bill by executive order issued on February 12, 2013, by US President Barack Obama.[76] Critical infrastructure protection from cyber threats, information sharing, and introduction of baseline framework of cybersecurity risk management were main issues that warranted this extraordinary action. It is not far-fetched to conclude that cyber threats became

[73] International Strategy for Cyber space—Prosperity, Security, and Openness in a Networked World (2011), available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/international_strategy_for_cyberspace_US.pdf (accessed 10 Mar 2014).

[74] In 2012, Mandiant Intelligence Center released a report exposing one of China's cyber espionage units. Available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed 11 Mar 2014).

[75] US Army General, Commander Cyber Command, Director, NSA/Chief CSS Keith B. Aletxander, An introduction by General Alexander. The Next Wave, Vol 19. No 4. 2012, available at http://www.nsa.gov/research/tnw/tnw194/article2.shtml (accessed 15 Mar 2014).

[76] Executive order—Improving Critical Infrastructure Cybersecurity, 12 Feb 2013. The White House, Office of the Press Secretary, available at http://m.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed 14 Mar 2014).

existential threats in the USA emanating from the military and economic fields, but at the same time, it is worth to note that there are no significant indications that political or societal security of the USA would be seriously threatened by this issue.[77]

3.2.2 Russia

In 2000, Russia's President Vladimir Putin signed an "Information Security Doctrine," which stated that "[t]he information sphere as a system-forming factor of societal life actively influences the state of the political, economic, defense, and other components of Russian Federation security. The national security of the Russian Federation substantially depends on the level of information security, and with technical progress this dependence is bound to increase."[78] The Doctrine consists of eleven sections and covers the national interests of the Russian Federation, lists the types of threats to the information security, identifies the external and internal sources of threats, and frames the state and objectives of information security in Russia, considering limitations on freedom of expression.

Threats to the Russian information security are subdivided into four types according to their directionality: threats to the constitutional rights and freedoms of man and the citizen in the area of spiritual life and information activities, to individual, group, and public consciousness, and to Russia's spiritual revival; threats to information support to Russian Federation state policy; threats to Russian information industry (including informatization, telecommunication, and communication facilities) development, to the satisfaction of domestic market requirements with its products and their entry into the world market, and to the accumulation, storage reliability, and effective utilization of national information resources; and threats to the security of information and telecommunication systems and facilities whether already deployed or being set up on the territory of Russia.[79]

Furthermore, the Doctrine proclaimed that the greatest danger is, among others, the informational influence that foreign political, economic, military, and information entities may have on the elaboration and implementation of the foreign policy strategy of the Russian Federation; attempts at unsanctioned access to information or attack attempts against information resources and the information infrastructure of the federal executive bodies implementing Russian Federation foreign policy, of

---

[77] Earlier the Comprehensive National Cybersecurity Initiative stated that the cybersecurity "is one of the most serious economic and national security challenges we face as a nation." Office of the President of the United States, Comprehensive National Cybersecurity Initiative, Washington, D.C.: The White House (2009), p. 1. Available at http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (accessed 14 Mar 2014).

[78] Information Security Doctrine of the Russian Federation, Approved by President of the Russian Federation Vladimir Putin on 9 Sept 2000, available at http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument (accessed 15 Mar 2014).

[79] Ibid.

Russian representations and organizations abroad and the representations of the Russian Federation at international organizations; violation of established information gathering, processing, storage, and transmission procedures in the federal executive bodies implementing Russian Federation foreign policy and their subordinate enterprises, institutions, and organizations; and the information and propaganda activities of political forces, public associations, media, and individuals distorting the strategy and tactics in the foreign policy activity of the Russian Federation.[80]

Doctrine's language expresses that the national identity, freedom, and culture of Russian people; the governing and strategy setting authority of the state; and the Russian economy, markets, and resources are at stake, and this rhetoric is indicative of securitization of these areas. The fact that the document is signed by the Russian president and it claims to focus considerable attention and resources to ensure information security in the country is evidence of successful securitization of cyber threats in Russian politics, but here, the existential cyber threats seem to emanate from military, political, economic, and social fields. Russia clearly perceives content as a threat.[81]

3.2.3 International Cooperation

In 1998, the USA and Russia have signed the joint statement on Common Security Challenges at the Threshold of the Twenty-First Century, where the two powers "recognize the importance of promoting the positive aspects and mitigating the negative aspects of the information technology revolution now taking place, which is a serious challenge to ensuring the future strategic security interests of…[the] two countries."[82] The joint statement calls the technological development a revolution that is dramatization of the process and suggested that present challenges may have disastrous consequences for either one or both country's ability to survive (strategic security interest). Since the cooperation of the two states is reserved to specific issues and their security interests are often considered as conflicting, the proposed cooperation can be construed as extraordinary. The US–Russian joint statement was signed by both powers, which is a requisite act to consider a document as legitimate and accepted in the international forum; therefore, the agreement is indicative of the securitization of cyber threats internationally. The document incorporates significantly less on information security than Russia desired, and it is considered as a failed attempt to agree on anything substantial with the USA.[83] Following this, Russia instead pushed for the adoption of a UN resolution on cybersecurity, which became the first international information-security-related legal instrument as such.[84]

---

[80] Ibid.

[81] See Giles (2012), p. 64.

[82] Available at http://www.gpo.gov/fdsys/pkg/WCPD-1998-09-07/pdf/WCPD-1998-09-07-Pg1696.pdf (accessed 15 Mar 2014).

[83] See Tikk-Ringas (2012), p. 3.

[84] A/RES/53/70.

3.2.4 The European Union

When considering the securitization and militarization level of cyber space, it cannot escape attention that the European Union has became rather active in stepping up against cyber crime, composed a comprehensive cybersecurity strategy, and engaged closely in several international cooperations as well as with the private sector. It is worth therefore to take a closer look at the cybersecurity policy of the EU.

Securitization processes have been examined in national contexts, where we can talk about conventional military powers and sociopolitical cohesion in straightforward terms. It can be disputed whether the EU can be treated as a single entity similar to a state when assessing its military powers and sociopolitical cohesion for the sake of analysis within the Buzan framework or whether these aspects were elevated to and reconstructed in the level of European information society and digital single market reflecting the transformations in the concepts of power and European identity. The European Union, although was created as an essentially economic cooperation, now has broader competences reaching a deeper, political level of integration that was gained through the "spillover" effect.[85]

The European Union policies on different aspects of cybersecurity have been widely criticized in the past for the lack of clear sense of direction, blurring priorities, and fragmented and overlapping competences between institutions.[86] In 2013, the EU has adopted the cybersecurity strategy of European Union, which essentially is a compilation of different measures planned by the Commission.[87] The strategy defines principles for cybersecurity and lays out a holistic approach to cybersecurity. The strategy sets forth policies regarding cyber threats deriving from economic and defense spheres and focuses on regulation, governance, and international cooperation.[88] The emphasis of economic aspects and the importance of cybersecurity for the functioning of the single market should not surprise the audience, but the inclusion of defense aspects does deserve a closer discussion.

The strategy invokes the crucial importance of cybersecurity, because cyber threats have the potential to endanger the physical survival of people and they pose a significant peril to the vital services for the welfare of population.[89] It states that "[c]ybersecurity incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins—including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes." It is clear from this

---

[85] The spillover effect of integration of individual sectors to further integration was described by neofunctionalist political scientist Ernst B. Haas.

[86] See Bigo et al. (2012), p. 8.

[87] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber space, JOIN (2013) final, Brussels, 7 Feb 2013.

[88] Ibid.

[89] Ibid.

formulation that cyber threats have been elevated to the level of and presented as an existential threat, whereas the referent object, that is, the population of the European Union, must be protected from different forms of cyber terrorism and from effects of cyber attacks targeting critical infrastructures. Without question, these threats are emanating from the military and national security spheres. The measures proposed by the Commission are rather modest and do not require spectacular and outstanding moves outside the usual political process (assessments, promoting dialogue between civil and military actors and leaves offensive capabilities alone and focuses exclusively on defensive actions),[90] but could be significant enough to cause another "spillover" onto the political sphere, thereby moving the issue as a special kind of politics beyond the established rules.

The securitization of cyber threats with the referent object being the (digital) single market is manifest in the strategy, which states, for example, that "[t]he EU economy is already affected by cyber crime activities against the private sector and individuals. Cyber criminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyber space poses a new category of threats for EU governments and companies." However, stepping up against economic crime, cyber or conventional, has already been in the agenda for a while; therefore, in this perspective, the rhetoric is not new.

Significant cybersecurity-related legislative proposals by the Commission have been adopted, and other planned measures were carried out since the adoption of the strategy in 2013,[91] and this is indicative of the shared understanding that cyber threats represent existential threats to the [digital] single market and these threats emanate to some extent from military, but more significantly from the economic fields. It is important to note for the purpose of the later analysis in this chapter that there was no indication or evidence that the EU as a whole would perceive cyber treats originating from the political or social sphere as existential threats, the cyber threats that challenge to recognition of the EU institutions, and governing authority of the EU is not perceived as serious or endangering the political stability of the EU, nor the different forms of critique in cyber space that challenge the European identity and cultural values are considered as particularly disruptive.

---

[90] In Sect. 2.3, developing cyber defense policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP) the strategy states that "[t]o increase the resilience of the communication and information systems supporting Member States' defense and national security interests, cyber defense capability development should concentrate on detection, response and recovery from sophisticated cyber threats. Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, private sector and academia in the EU."

[91] For example, the Directive on attacks against information systems was adopted by the European Council on July 22, 2013, and another piece of important legislation, the Network and Information Security Directive, has been voted through by the European Parliament on the March 13, 2014. See http://europa.eu/rapid/press-release_STATEMENT-14-68_en.htm (accessed 15 Mar 2014).

3.3 Fragmentation of Policies: Main Fault Lines

Major difference between the Western and Russian positions is the territorially based nation-state approach of Russia to cybersecurity, which should not strike as a surprise, considering the above analysis of cyber threat securitization. The divergence in perspectives can be analyzed by investigating the negotiation process of the UN instruments and comparing the language of the Shanghai Cooperation Organization's approach to the one expressed by states who signed up for the Cyber crime Convention.

Following the signature of the joint statement on "Common Security Challenges at the Threshold of the Twenty-First Century" by the US and Russian presidents, in a letter sent to the UN secretary-general, the Russian Foreign Minister proposed a resolution dealing with military aspects of information technologies.[92] The divergence of interest of the two big powers in the security of information and communication technologies became apparent already during the negotiations of the joint statement, where the Russian party wanted to deal with the issue more in length.[93] The rejection of this proposal by the USA foreshadowed the split of the international community into two blocks when it comes to cybersecurity. The main fault lines lie between the Western and Eastern blocks of states, where their Eastern block's states have lower level of sociopolitical cohesion, and therefore, their governments are more sensitive to political threats, whether perceived or real. Consequently, and according to the Buzan framework, it should be predictable that the Russian views focus on the political nature of cyber threats, which is reflected in the definition of basic concepts—which view is not shared by the West, but rather qualifies cyber threats as economic in nature.

The Russian Information Security Doctrine asserts that the greatest dangers to Russian information security in the foreign policy sphere, *inter alia*, are "the information and propaganda activities of political forces, public associations, media and individuals distorting the strategy and tactics in the foreign policy activity of the Russian Federation" and "informational influence that foreign political, economic, military and information entities may have on the elaboration and implementation of the foreign policy strategy of the Russian Federation."[94] Another crucial theme throughout the doctrine is the security of physical information infrastructure of the Russian Federation.

In 1999, Russia proposed the creation of a legal regime that the "international community should consider and adopt …as a package, that is, bearing in mind threats of a military, terrorist or criminal nature and with a view to applying those

---

[92] See Tikk-Ringas (2012), pp. 3–4.

[93] Ibid.

[94] Information Security Doctrine of the Russian Federation, Approved by President of the Russian Federation Vladimir Putin on 9 Sept 2000, available at http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument (accessed 13 Mar 2014).

principles to both the military and civilian spheres."[95] One of the basic criticisms is concerning the definition of information area, "[t]he sphere of activity involving the creation, transformation or use of information, including individual and social consciousness, the information and telecommunications infrastructure and information itself." The information area according to the definition includes information itself, which is in harmony with the Russian policy to achieve security and promote stability by removing the threats to the information and communication infrastructure, as well as the information itself.[96] This approach was rejected by liberal democracies invoking the principle of freedom of expression, forming a group focusing exclusively on the security of infrastructure and networks.[97]

Russia was not able to seriously engage the USA and the EU in discussion about subsequent initiatives dealing with cyber disarmament, information weapons, and cyber warfare, and the USA opined that the law of armed conflict and its basic principles provide all the necessary rules with respect to military use of information technologies.[98] The Western countries' focus remained on non-state, criminal, and terrorist activities in cyber space, and the Council of Europe Cyber crime Convention was signed on September 23, 2001, in Budapest.[99] The Cyber crime Convention created a Western block signing up for liberal democratic values, respect of individual rights and freedoms, and combating crime in the global cyber space.

Not only the sovereignty considerations concerning the views trying to impose a "global" nature on cyber space can be found in the use of language and definition of concepts in the Russian Information Security Doctrine, which refers to, for example, "infrastructure of the unified information space of the Russian Federation," but also it can be observed and derived from the Russian Federation's refusal to sign the Council of Europe Cyber crime Convention.

Russia has adopted a view that it is not in its interest to sign the Council of Europe Cyber crime Convention, which is addressing a number of core and computer-related crimes committed via the Internet or other computer networks, because it considers that Article 32 of the Convention allows for transborder access to stored computer data and it threatens its sovereignty.[100] Russia emphasized the need for a new international treaty, which is more in line with its views, cures its perceived inferiority in information and communication technologies, and prevents an arms race by imposing bans or constrains the development and use of a wide range of technologies.[101] There have been suggestions that instead, Russia

[95] UN GA Resolution A/54/213.

[96] See Tikk-Ringas (2012), pp. 3–4.

[97] Ibid.

[98] Ibid. p. 6.

[99] Council of Europe Convention on Cyber crime, ETS No. 185.

[100] Gady and Austin 2010, pp. 12–13.

[101] Ibid, p. 6.

should focus on cracking down on cyber crime domestically and not further fuel views that Russia is encouraging, using, or at least tolerating cyber attacks that are in its political interest.[102]

It was not until 2007 that the cyber incidents in Estonia, Georgia, and Lithuania[103] raised the relevance of cyber threats as a matter of national security in the Western democracies and NATO, and the Shanghai Cooperation Organization was beginning to consider cyber threats from military perspective.[104] In 2011, Russia, China, Tajikistan, and Uzbekistan proposed the adoption an International Code of Conduct for Information Security in the UN General Assembly, thereby relaxing their approach toward the type of legislative measure.

The preference for governance (although occasionally it is forced) in the domestic policy toward cybersecurity in the USA is reflected in the international level also. The USA's reluctance to sign a binding treaty can be explained by its technological and economic dominance that allows achieving its desired goals by exerting influence and projecting its powers by these means, whereas international law has no prohibitions on state behavior in the cyber space, whereas the opposite interest of Russia is to curve the US dominance by adopting clear limitations on actions, such as a cyber space treaty, and being concerned about the principle that what is not prohibited is allowed.

The Russian Concept of a Convention on International Information Security sets forth provisions preserving the sovereignty of a state over its information space, and it lists the main threats international information security: the use of information technology and means of storing and transferring information to engage in hostile activity and acts of aggression; purposefully destructive behavior in the information space aimed against critically important structures of the government of another State; the illegal use of the information resources of another government without the permission of that government, in the information space where those resources are located; actions in the information space aimed at undermining the political, economic, and social systems of another government and psychological campaigns carried out against the population of a State with the intent of destabilizing society; the use of the international information space by governmental and non-governmental structures, organizations, groups, and individuals for terrorist, extremist, or other criminal purposes; the dissemination of information across national borders, in a manner counter to the principles and norms of international law, as well as the national legislation of the government involved; the use of an information infrastructure to disseminate information intended to inflame national, ethnic, or religious conflict, racist and xenophobic written materials, images or any other types of presenting ideas or theories that promote, enable, or incite hatred, discrimination, or violence against any individual or group, if the supporting reasons are based on race, skin color, national or ethnic origin, or religion; the manipulation of the flow

[102] Orji Uchenna Jerome 2012, 18(1), pp. 16–17.

[103] Tikk et al. 2010.

[104] Eneken and Tikk-Ringas 2012, pp. 7–8.

of information in the information space of other governments, disinformation or the concealment of information with the goal of adversely affecting the psychological or spiritual state of society or eroding traditional cultural, moral, ethical, and aesthetic values; the use, carried out in the information space, of information and communication technology and means to the detriment of fundamental human rights and freedoms; the denial of access to new information and communication technologies and the creation of a state of technological dependence in the sphere of informatization, to the detriment of another State; and information expansion and gaining control over the national information resources of another State.

However, according to the US International Strategy for Cyber space, the challenges come in a variety of forms: Natural disasters, accidents, or sabotage can disrupt cables, servers, and wireless networks on US soil and beyond. Technical challenges can be equally disruptive, as one country's method for blocking a Web site can cascade into a much larger, international network disruption. Extortion, fraud, identity theft, and child exploitation can threaten users' confidence in online commerce, social networks, and even their personal safety. The theft of intellectual property threatens national competitiveness and the innovation that drives it. Cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyber space."[105]

According to the Draft UN Resolution of October 18, 2013, on developments in the field of information and telecommunications in the context of international security, the fourth Group of Governmental Experts (GGE) will be set up to examine the potential threats, possible cooperative measures to address them, including norms, rules and principles of conduct, confidence-building measures, issues of use of information and communication technologies, and application of international law thereof.[106] The setup of the next GGE can be explained with recent controversial events (Snowden revelations, Stuxnet case) that could serve as grounds for accusing the USA with application of double standards. It should also be noted that the circle of supporters of the Russian approach is growing and it includes CIS countries, China, and African and Latin American countries. Since the Russian stance has been since 1998 to create hard law and define the prohibited acts and the discovery of the NSA surveillance of high-profile politicians outraged European and other countries, there is a political opportunity for Russia to lead a shift in strategy, though it implies compromises from both sides and the emergence of a third position—perhaps by a non-state actor—cannot be excluded either. It is now difficult to conceptualize what a third position may entail due to the fragmented state of cybersecurity.

---

[105] International Strategy for Cyber space—Prosperity, Security, and Openness in a Networked World, 2011. Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/international_strategy_for_cyberspace_US.pdf (accessed 15 Mar 2014).

[106] A/C.1/68/L.37.

3.4 Fragmentation of Cybersecurity in National Strategies

Comprehensiveness is one of the shared characteristics of national cybersecurity strategies, which in this context means the trend of the last decade that countries increasingly adopt national cybersecurity approaches, taking into account the wider context of the cyber space, such as social, diplomatic, legal, economic, intelligence, and military aspects of cybersecurity. Strategies often address all prevention, detection, response, and recovery phases of cybersecurity incident management and combine expertise and competencies in many levels.[107]

The OECD carried out a study in 2012 that identified the common themes in strategic national cybersecurity documents.[108] The report found that states agree that cybersecurity has become a national security priority and governments generally find that the Internet and ICTs are essential for economic and social development and form a vital infrastructure; cyber threats are evolving and increasing at a faster pace. Majority of the strategies embrace concepts such as enhanced governmental coordination at policy and operational levels; public–private cooperation; international cooperation; and respect for fundamental values. Emerging trend in national cybersecurity strategies is to list sovereignty considerations, such as defense or intelligence aspects, or to emphasize the need for a flexible approach.

However, the level of technological and economic development, dependency on information and communication technologies, political regime, sociocultural traditions, and several other factors influence what aspects of cybersecurity a nation holds more important than others. A plausible consequence of the comprehensive and holistic approach is that national understandings and strategies will be diverse in the absence of effective coordination. Fragmentation is manifest in the national cybersecurity strategies with respect to definitions, objectives, and measures.

The Russian Information Security Doctrine defines information security of Russia as "the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state,"[109] and it focuses on managing the flow of information to its citizens and on securing its information infrastructure.[110] Russia is more conscious of the cognitive aspect of cyber threats than other nations, which is in line with the Buzan framework for a state that is concerned about political and societal threats. However, the new Russian CyberSecurity Strategy is being drafted and it will probably include a definition of both cybersecurity and information security, as well as information space (that includes both infrastructure

---

[107] Tikk 2011.

[108] Cybersecurity Policy Making at a Turning Point—Analyzing a New Generation of Cybersecurity Strategies for the Internet Economy, OECD Report, 2012.

[109] See at http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument (accessed 13 Mar 2014).

[110] Thomas (2009), p. 465.

and information itself) and cyber space. It is clear that the Russian position on that cybersecurity is extended to the elimination of certain undesired information that will remain the same.

Another state that used similar terminology "information security," but in different context, was Japan until the issue of the new, ambitious cybersecurity strategy in 2013. Japan defines cyber space as global virtual spaces such as the Internet, composed of information systems, information communication networks, and similar systems which circulate large quantities of a large variety of information and which have expanded and begun permeating real space.[111] In addition, Japan signs up for the view that cyber space is a digital commons, thereby rejecting the nation-state-based territorial approach.[112]

At the same time, for example, the German cybersecurity strategy does not include within its scope the virtual space that is not connected to the Internet: "Cyber space includes all information infrastructures accessible via the Internet beyond all territorial boundaries." This approach may have profound consequences in certain critical infrastructure networks, which are isolated from external connections due to security concerns. The German strategy does not define cybersecurity, but it refers to it as a condition determined by its properties: "the level of cybersecurity reached is the sum of all national and international measures taken to protect the availability of information and communications technology and the integrity, authenticity and confidentiality of data in cyber space."[113]

The Dutch strategy defines cybersecurity as it "refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred."

The Estonian Cybersecurity Strategy from the year 2008 states that "[n]ational cybersecurity is a broad term encompassing many aspects of electronic information, data, and media services that affect a country's interests and wellbeing."[114] Meanwhile, the new strategy is under way, and the drafters seem to be serious about moving all facilities necessary for the functioning of the state into the "cloud" claiming to be essentially creating "cloud-Estonia."[115] This project is not

[111] Cybersecurity Strategy—Towards a word-leading, resilient and vigorous cyber space, June 10, 2013. Information Security Policy Council, Japan. Available at http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf (accessed 14 Mar 2014).

[112] Ibid.

[113] CyberSecurity Strategy For Germany, Federal Ministry of the Interior. Available at http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf;jsessionid=227F71D24AD8151E4C4412D0C3B42A4C.2_cid334?__blob=publicationFile (accessed 13 Mar 2014).

[114] CyberSecurity Strategy, Ministry of Defense, Estonia, Tallinn (2008). Available at http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (accessed 13 Mar 2014).

[115] Tänavsuu 2014, pp. 12–13.

without legal twists, since according to Estonian legislation, all critical data must remain within the territory of Estonia. This was not an obstacle for a minute, and the drafters invented the concept of "data embassy," which is essentially a data storage facility in friendly foreign states.[116]

Cybersecurity strategies of some countries[117] recognize the need to adapt policies to the dynamically changing environment, and they promote flexibility and agile implementation. The Japanese cybersecurity strategy states that "conventional information security measures have tended to remain as symptomatic treatment that addresses individual risks whenever they arise, and often fail to address the actual cause." Japan is looking for a fundamental solution and at the same time proposes to utilize dynamic tools and shift toward active attitude.

German choice of measures includes the use of reliable and trustworthy information technology and emphasizes the need for diversity in technology and standardization (See Footnote 117), the French[118] and British strategy[119] reveals preference of government-ruled approach, while the Dutch strategy's focus is on public–private participation, networks, and capacity building.[120]

Cybersecurity strategies remain heterogeneous, and they include different definitions and approaches to cybersecurity, which makes cooperation a difficult undertaking.[121] ENISA, the European Network and Information Security Agency in a study concerning the cybersecurity strategies of Member States, made several observations of gaps between these documents.[122] The first step toward a strong international cooperation in order to tackle cyber threats is to *have* a national strategy dealing with this issue and to define the subject matter of cybersecurity and their related interests and objectives. However, the Western national strategies may exhibit diverging features in definitions and approaches, no Western strategy is concerned about the cyber threats emerging from the political field, and the respect for freedom of expression is repeatedly emphasized.

---

116 Ibid.

117 UK, Japan, The Netherlands, and Canada.

118 Information systems defence and security—France's Strategy. Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf (accessed 13 Mar 2014).

119 The UK CyberSecurity Strategy—Protecting and promoting the UK in a digital world. 2011. Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/UK_NCSS.pdf (accessed 13 Mar 2014).

120 National CyberSecurity Strategy 2—From awareness to capability, The Netherlands. Available at https://www.enisa.europa.eu/ac8activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf (accessed 13 Mar 2014).

121 ENISA (2012), p. 9.

122 Ibid, p. 12.

4 Categorizing Legal Responses to Cyber Threats

The previous sections demonstrated that world powers have diverging interests (perceived or real) and views on the origins of cyber threats. Placing the cybersecurity issue within the framework of traditional security studies reveals that the securitization of cyber space has different motives in Western countries and Russia. US rhetoric can be interpreted as securitizing cyber threats in military and economic context, but rigorously insist on respecting the individual freedoms, such as free speech and privacy, in cyber space. Since the USA is considered as one with strong military power as well as sociopolitical cohesion, the theory predicted that its problems will emanate from the exploitation of its prospering economy. This was confirmed above.

Meanwhile, Russia seems to be advocating to strike a balance between the individual rights and the interest of the state in the information space, but which balance is different from the one accepted in Western countries. In addition, Russia is clearly concerned about the political-, military-, and economy-related cyber threats, and ones that it construes as endangering the physical survival of the state itself undermine the government's authority or the prosperity of the economy. The theory and Buzan framework indeed predicted that a state having strong military power, but struggling with certain areas in sociopolitical cohesion, will be inclined to be sensitive about and sanction actions that advocate to further weaken or give up its authority (e.g., separatist ideas).

Once it has been assessed what is the underlying reason for bringing a certain issue into the "emergency sphere," a more informed decision can be made on the most adequate measure to address that insecurity. For example, if country A's corporations are facing problems of corporate espionage by country B's, and the issue is elevated to the level of emergency, it needs to be assessed whether the issue is presented as a question of physical survival of the nation, political, economic, or societal threats. However, another difficulty lies in how to choose strategies to counter threats and what is the most appropriate and effective means in the corresponding context that could be considered to decrease insecurity of the reference object. Understanding the underlying reasons and origins of the threat can not only provide help to devise solutions, but also help to identify and assess the arising legal problems.

Staying with the concrete case invoked by General Keith Alexander (that the ongoing corporate espionage and theft of intellectual property are the greatest transfer of wealth in history),[123] we can see that this is a securitization attempt of a threat that emerges from the economic field. The General addresses the loss of profit and damage the threat is causing to businesses, and he could be saying that

[123] US Army General, Commander Cyber Command, Director, NSA/Chief CSS Keith B. Alexander, An introduction by General Alexander. The Next Wave, Vol 19. No 4. 2012. Available at http://www.nsa.gov/research/tnw/tnw194/article2.shtml (accessed 13 Mar 2014).

"we are losing the income that we could have had if the intellectual property was licensed to country B." However, it is possible to securitize this issue differently as well, depending on the military strength and socioeconomic cohesion attributes of the country in question. In a different context, it could be explained that "state B's intention is likely to be the use of the stolen information assets to develop weapons against our people," thereby emphasizing the physical security and military aspect. The responses to such threats should take into account the nature of the field where the threat is arising from, and the application of well-targeted measures should be considered accordingly.

Sun Tzu in his famous piece, the Art of War, suggested four basic strategies to counter a threat:

> Thus the highest form of generalship is to balk the enemy's plans; the next best is to prevent the junction of the enemy's forces; the next in order is to attack the enemy's army in the field; and the worst policy of all is to besiege walled cities.[124]

Threats can be countered essentially either by decreasing the threat or by lessening the vulnerability.[125] Therefore, these two vectors combined with Sun Tzu's four methods yield eight principal ways to decrease insecurity and they are presented below. Some solutions may seem extreme or absurd; however, they remain theoretical choices. Decreasing a treat can therefore take four distinct forms:

"Balking the enemy's plans" or plan elimination at threat source: The corresponding policy measures are incentives applying active cyber defense measures by the corporations. Active cyber defense is understood as the collection and use of intelligence, application of deception, and potentially offensive techniques with defensive purpose,[126] in order to predict, prevent, or postpone indefinitely acts of cyber espionage.[127] This is essentially a technical method and carries no political implications itself and therefore may be suitable measure in countries where the referent object is not vulnerable to political threats. However, the question of active cyber defense is not without legal twists, since there is a fine line between offensive measures and that can be understood as taken in "cyber self-defense." Legal problems associated with this solution are to clarify the extent of allowed proactive measures taken by the private sector both in national legislation and agreeing on the definitions internationally.

"Prevent junction of enemy's forces" or capability mitigation at threat source: This strategy corresponds to measures that entail entering into a treaty combating international cyber espionage by providing universal jurisdiction over cyber spies or fostering the adoption of laws criminalizing the conduct of cyber espionage. The aim is to have the source country to deal with those threats at their source. Such a step is also essentially a political solution, and entering into alliances to

---

124 Tzu (2013).

125 See Hare (2010), pp. 221–222.

126 See at http://www.military-dictionary.org/active_defense.

127 Elazari (2013). www.gigaom.com. (Accessed 05 Jan 2014).

tackle a shared threat can be preferable when the reference object is vulnerable to political threats.

"Attack enemy's army in the field" or mitigating the threat in process: It refers to, for example, the conclusion of bilateral cooperation agreements on issues such as mutual legal assistance in investigation, rules on electronic evidence, forensics and prosecution of cases of cyber espionage, and technology export control measures and is perhaps more technical than political solution, but this could be certainly disputed depending on the actual issue at hand. In any case, these measures focus on the victim's efforts to directly deal with the threat, weaken the enemy or prevent it from becoming stronger, and probably could be preferred option when referent object is not vulnerable to political threats.

"Besiege walled cities" or eliminate full threat vector by force: Adoption of this policy entails suppressing, and openly confronting the threat by the application of offensive measures (or tolerating such conduct from the corporations) may seem suitable in cases when the reference object is vulnerable to military and information warfare threats. Such steps could be interpreted by the international community as "cyber aggression," conducting "cyber warfare" or "cyber attack"; therefore, state responsibility could be invoked according to international legal norms. However, the applicability and interpretation of norms of public international law and different branches of international law to cyber operations are still widely discussed, and there are only a few settled questions.[128]

Decreasing own vulnerability could entail the following four main options:

"Balking the enemy's plans" or eliminating vulnerability at reference object, transformation: Eliminating the risk is a case for application of alternative intellectual property protection regimes and transparency. Disclosing the contents of information assets and applying open source licensing simply eliminate the need for corporate espionage. This solution would necessitate deep structural changes in international regimes and organizations for the protection of intellectual property.

"Prevent junction of enemy forces" or mitigating threat capability at target: Such direction means applying incentives to use distributed methods in data storage and processing, such as cloud computing. Adopting good practices, working out and prescribing minimum security standards, investing in cloud R&D, etc., are the measures that belong to this type of response. This clearly technical solutions imply neutrality and suitable for cases where reference object is not vulnerable to political threats.

"Attack enemy's army in the field" or mitigating threat in process: There are a great number of options to engage in the vulnerability mitigation openly, and there are a variety of legal measures that could be involved. Secure software and system design, malware detection and removal techniques and other similar technological measures can be applied, as well as legal deterrence, which can be translated into such legal terms as standardization, manufacturer's liability, strengthening of data protection, and imposing grave criminal and civil sanctions. Such solutions imply neutrality in the international forums, since they are primarily directed at

[128] On these questions, see, for example, Ziolkowsky (2013).

the potential victim and prevention of victimization. They are therefore suitable to decrease insecurity when the referent object is not vulnerable to political threats.

"Besiege walled cities" or isolation: Information assets are isolated by the severance of connection, restriction, or limitation on communications. This essentially entails local or global of censorship, in the meaning of prescribing the use of some passive security measures, such as packet filtering at ISP or company level or the introduction of technical solutions such as the great firewall. This strategy can have both political and technical implications, and the legal issues can be assessed on a case-by-case basis; however, it appears that the main questions focus on the limitations of individual freedoms—freedom of speech (expression) and privacy.

It can be observed in each policy choice that the identity of response agent makes a difference how the opponent may perceive the move and that the "wrong" choice could lead to securitization of the matter at the opponent side fueling a conflict between opposing parties. The chance of this happening is multiplied due to the intertwined interests of public and private sectors in cyber space; therefore, this problem calls for coordination between multiple stakeholders.

5 Conclusion

We are in an era of cyber military confrontation—or at least clashes—in a domain where there is almost no regulation internationally. The traditional domains of land, sea, and air, and even outer space have far more rules for safe "international navigation" than does cyber space.[129] Discussions about the scope of international action and measures have been going on for more than a decade, leading to no agreement. What is not prohibited is allowed in international law, and the Western approach has been to avoid enacting formal legislation in respect to international cybersecurity.

Cybersecurity concepts lack shared understanding and common terminology in all levels. Responses to cybersecurity became fragmented not only along the lines between the traditionally strongest powers, but also on regional levels, and states have developed several unique and sometimes exotic approaches to tackle problems that essentially need global solutions.

There is need for layered coordination according to a framework that reflects and reconciles the different interests and objectives into a common denominator, which can be the foundation of a truly international regime in the future. A number of measures exist for decreasing real or perceived insecurity; however, several of them may lead to intensification of conflict. For this reason, the responses to threats needed to be coordinated through new institutions, power sharing, and de-securitization, having a bottom-up approach and beginning with to focus on engaging multiple stakeholders from fields where there is an overlap in interest over the main fault lines.

[129] Gady and Austin (2010). www.ewi.info.

References

Buzan, B. (1991) New patterns of global security in the twenty-first century. *International Affairs 67*(3).

Buzan, B., Weaver, O., & de Wilde, Jaap. (1998). *Security: A new framework for analysis*. London: Lynne Rienner Publisher.

Bigo, D., Boulet, G., Bowden, C., Carrera, S., Jeandesboz, J., & Scherrer, A. (2012). *Fighting cybercrime and protecting privacy in the cloud, directorate general for internal policies, policy department c: Citizens' rights and constitutional affairs*. Brussels: European Parliament.

Bronc, C., & Tikk-Ringas, E. (2013) The cyber attack on Saudi Aramco. *Survival: Global Politics and Strategy 55*(2).

Cridland, C. (2008) The history of the internet: The interwoven domain of enabling technologies and cultural interaction. In *Responses to cyber terrorism.* Ankara: Centre of Excellence Defence Against Terrorism.

Elazari, K. (2013) Proactive security: Integrating active defense in cybersecurity. *Gigaom Research.* www.gigaom.com. Accessed January 5, 2014.

ENISA (2012) National cyber security strategies, Setting the course for national efforts to strengthen cyber security. *Report*.

Gady, F. S., & Austin, G. (2010) *Russia, the United States, and cyber diplomacy: Opening the doors*. New York: EastWest Institute.

Giles, K. (2012). Russia's public stance on cyberspace issues. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *4th International Conference on Cyber Conflict, Proceedings*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

Greenstein, S. (2001) Commercialization of the internet: The interaction of public policy and private choices or why introducing the market worked so well. In Jaffle, A. B., et. al. (eds.) *Innovation policy and the economy*. Cambridge: MIT Press.

Hare, F. (2010) *The cyber threat to national security: Why can't we agree?* In C. Czosseck & K. Podins (Eds.) *Conference on Cyber Conflict Proceedings 2010*. Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia.

Kilroy, R. J. (2009) The U.S. military response to cyber warfare. In L. J. Janczewski, & A. M. Colarik (Eds.) *Cyber warfare and cyber terrorism* (Information Science Reference).

Kramer, F. D. (2009). Cyberpower and national security: Policy recommendations for a strategic framework. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security*. Washington, D.C.: National Defense University Press.

OECD (2012) Cybersecurity policy making at a turning point—analyzing a new generation of cybersecurity strategies for the internet economy. *OECD Report*.

Orji, U. J. (2012). Russia and the council of Europe convention on cybercrime. *Computer and Telecommunications Law Review, 18*(1), 16–17.

Stone, M. (2009) Security according to Buzan: A comprehensive security analysis. *Security Discussion Papers Serie 1. Groupe d'Etudes et d'Expertise, Sécurité et Technologies* (*GEEST*).

Tikk, E. (2011) A comprehensive legal approach to cyber security. *PhD Thesis*, Tartu University.

Tikk-Ringas, E., Kaska, K., & Vihul, L. (2010). *International cyber incident: Legal considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence.

Tikk-Ringas, E. (2012) *Developments in the field of information and telecommunication in the context of international security*: Work of the UN First Committee 1998–2012. Geneva: ICT4Peace Publishing.

Thomas, L. T. (2009). Nation–state cyber strategies: Examples from China and Russia. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security*. Washington, D.C.: National Defense University Press.

Tänavsuu, T. (2014) Pealegi oleme kogu täiega pilves. *Eesti Ekspress 9* (1264), 12–13.

Tzu, S. (2013) *The art of war*. Colorado: Orange Publishing.

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime, Report*. New York: United Nations.

Wilson, C. (2009) Cyber crime. In F. D. Kramer, et. al *Cyberpower and national security*. Dulles: Potomac Books.

Ziolkowski, K. (2011). *Stuxnet—legal considerations*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

Ziolkowsky, K. (Ed.). (2013). *Peacetime regime for state activities in cyberspace—international law, international relations and diplomacy*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

Legal Aspects of CyberSecurity in Emerging Technologies: Smart Grids and Big Data

European Answers to Security Breaches and "Common" Cyber crime

Agnes Kasper

The clever combatant looks to the effect of combined energy, and does not require too much from individuals. Hence his ability to pick out the right men and utilize combined energy.

Sun Tzu

Abstract This article will discuss some of the legal challenges in the emerging cyber threat landscape in the private sector. After introduction and description of some key technical terms, I will analyze the (mis)use and security challenges related to some emerging information technologies and methods from legal perspective. The basic themes include critical information infrastructure protection, smart grids, and big data, but the use of cloud computing will also be touched upon. The results of the analysis will point out the strengths and weaknesses of the relevant legislations. Recommendations and conclusion will be offered at the end.

1 Introduction

Emerging technologies may represent incubating environments for new threats, while they also reflect the latest trends in social interaction and expectations of the consumers in information societies due to their low technical maturity and low adoption rate. Innovation is driven by market demand (real or perceived), and new entrant technologies may have vulnerabilities that offer entirely new ways of exploitation.

A. Kasper (✉)
Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia
e-mail: agnes.karpati@mail.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_10

The architecture, design, and practice of the Internet underline its openness and access-centered purpose, whereas security was never considered as a primary factor.[1] The Internet grew out of a project to devise a new instrument for communication, to connect people.[2] The growing number of social networks is satisfying the natural need to communicate and interact with other human beings, and there are technologies that make our lives more convenient, save us time, money, and resources. However, when Facebook was created, it was hard to foresee that "likes" will be sold in order to manipulate market and create a "buzz" for some product or company or that the digital meters will be collecting sufficient information to analyze any aspect of our habits—that could be misused in turn.

On the one hand, the examination of emerging technologies can serve as a test for the robustness of existing legislation, so whether regulation of a certain area is sufficiently technology independent. On the other hand, since law is assumed to be responding to emerging challenges with delay, analysis of emerging technologies and detection of gaps and opportunities in legislation may produce more up-to-date solutions.

After a short glance at the distant future, the present legal challenges will be discussed related to security of technology areas of critical infrastructure, in particular smart grids and big data, while the role of cloud computing will also be mentioned.[3]

2 Trends in Cybersecurity: A Glance at the Future

Project2020 of European Cyber Crime Center at Europol and the International CyberSecurity Protection Alliance anticipates the future of cyber crime for individuals, businesses, and government in the year 2020, and it distinguishes two different types of regulatory regimes—risk-based and control-based cybersecurity models. The control-based model is associated with strict control mechanisms both technical and legal, absolute protection for intellectual property, and it also implies heavy surveillance of communications for prevention. While the control-based model probably inhibits interoperability, the risk-based model leads to truly converged networks through open and generative Internet and conditional intellectual property protection.[4] The Project2020 makes its predictions using the risk-based model, but it notes that probably, a combination of the two models is what we will see in the future.

On the one hand, in liberal democracies where the individual rights and freedoms of persons are respected, it may be presumed that limitations and controls imposed on communications and data exchanges are (at least in theory) very cautious and well grounded, subject to critique, challenge, and revision if necessary. On the other hand,

[1] See Goodman 2008, p. 25.

[2] See Cridland 2008, p. 2.

[3] ENISA 2013, p. 42.

[4] International CyberSecurity Protection Alliance 2013 Project2020, European Cyber Crime Center at Europol. Available https://www.icspa.org/activities/work-programmes/project-2020/.

there are a number of events that confirm the increasing reliance of governments on control-based cybersecurity models, such as the disclosure about the large surveillance schemes or the growing support for the Russian cybersecurity proposals in the UN.

The authors of Project2020 make a number of bold suggestions about the implications of new and reinvented cyber threats, including that authorities will need to develop creative and flexible approaches to criminality.[5] The increasing complexity of cyber-related activities is apparent from a few examples, such as use of botclouds,[6] distributed bulletproof processing,[7] biohacks,[8] attacks on critical infrastructure, use of big data principles for criminal purposes, and hacks against devices with direct physical impact (Internet of things).[9] Rules are bent more easily in cyber space than in real life, Internet is becoming truly ubiquitous, and the mass violations turn criminal laws into a mere recommendation about conduct in the absence of effective deterrence and enforcement.

According to the study, it will be increasingly difficult to distinguish between data misuse and legitimate use, which can have profound implications on detection techniques, privacy, and data protection.

Effective cybersecurity will require involvement of multiple stakeholders both from public and from private spheres, including users, organizations, and governments, and it is highly questionable who is going to have the capacity to combat cyber crime.[10] Since the telecommunication, financial and Internet security companies are already engaged in investigations, they seem to be best placed to get further involved.

The UN-commissioned cyber crime study concluded that "[r]eliance on traditional means of formal international cooperation in cyber crime matters is not currently able to offer the timely response needed for obtaining volatile electronic evidence. As an increasing number of crimes involve geo-distributed electronic evidence, this will become an issue not only for cyber crime, but all crimes in general."[11] It is safe to say that the face of crime is taking a 180° turn, and in the future, virtually all crime will have something to do with communication and information technologies, since the adoption and use of emerging and new technologies by malicious actors is a global trend and has consequences on global scales.

---

[5] Ibid.

[6] Cloud-based botnets using distributed processing power.

[7] Bulletproof processing is the offering of processing services from jurisdictions with weak or no cyber crime legislation with the aim to evade law enforcement. Distributed bulletproof processing would use shared resources from several jurisdiction, making any law enforcement actions practically ineffective and meaningless.

[8] For example, compromising the communication between a medical diagnostic device and an implant, such as a peacemaker. Such devices often communicate through (insecure) Wi-fi connections.

[9] Ibid. The study identified these threats by horizon scanning of the technology field. Most of these technologies are being developed currently, and their adoption on large scale depends on the market and users.

[10] Ibid.

[11] United Nations Office on Drugs and Crime 2013, p. xi.

ENISA, the European Network and Information Security Agency, has identified major emerging technologies that begin to shape as our everyday lives as businesses. In the next sections of this paper, I will identify a few gaps and opportunities for future change by looking at some of the legal problems related to the (mis)use and security challenges of emerging technologies.

3 Fundamental Concepts: Cyber threats, Threat Agents, Cyber Kill Chain, and Security Management Models

There are a number of views on how to categorize cyber threats and perspectives that vary according to the purpose of use and sector. David S. Wall identified three main types of cyber crimes: computer-assisted crime, computer content crime, and computer integrity crime.[12] The Council of Europe Cyber crime Convention primarily distinguishes between offenses against availability, integrity, and confidentiality of computer data and systems (or "core" crimes); computer-related offenses; content-related offenses; and offenses related to infringements of copyrights and related rights.[13] Directive 2013/40/EU on the attacks against information systems (Botnet Directive) follows the logic of the Cyber crime Convention and prescribes sanctions for the core computer crimes: illegal access to information systems; illegal system interference; illegal data interference; and illegal interception and prohibits the intentional production, sale, procurement for use, import, and distribution or otherwise making available of certain computer programs and computer passwords, access codes, and other similar data.[14]

However, not all cyber threats are criminalized, and when we are addressing cyber threats, a broader perspective is needed. There are a range of security breaches in different levels that could escalate to an incident in user, organization, national, or even international level, triggering responses according to competences of corresponding institutions.[15] Major cyber incidents have happened for reasons of negligence, carelessness, lack of awareness, and other similar reasons. Two clear examples for such escalation are the spread of Conficker worm and the Spamhouse DDoS[16] attacks. The Conficker worm has exploited vulnerability in

[12] See Wall 2007.

[13] Council of Europe Convention on Cyber crime of 23. November 2001, CETS No.: 185.

[14] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[15] See Tikk 2011.

[16] "A denial-of-service attack (DoS) occurs when large number of requests are directed to a target URL. The requests occur so quickly that the Web server cannot respond and the site becomes inaccessible. A distributed denial-of-service attack (DDoS) occurs when hundreds or thousands of compromised computers are enlisted." See in Eneken Tikk, Kadri Kaska, Liis Vihul, International Cyber Incident: Legal Considerations, Cooperative Cyber Defence Centre of Excellence, Tallinn 2010.

the Windows operating system and infected hundreds of thousands of hosts *after* the (automatic) security update was issued by Microsoft.[17] Also, one record is set after the other in the viciousness of DDoS attacks. In 2013, Spamhouse attack the DoS bandwidth reached 300 Gbps,[18] which was "beaten" in 2014 in the attack against CloudFlare services with 400 Gbps.[19] Both attacks are reported to have used the so-called DNS reflection method, which target poorly configured DNS servers. These cases are illustrative of the process how, for example, breach of internal rules, company policies, disregard to good practices and standards, if taken place in large numbers, creates vulnerabilities that can lead to increasingly serious cyber incidents.

The ENISA study grouped main cyber threats into fifteen categories: drive-by-exploits, worms/trojans, code injection, exploit kits, botnets, physical damage/theft/loss, identity theft/fraud, denial of service, phishing, spam, rogueware/ransomware/scareware, data breaches, information leakage, targeted attacks, and watering hole.[20] These threats have various roles in the attack process, and some of them are deployed with a very limited purpose. Three threats will be discussed in detail in this chapter: denial of service, data breaches, and information leakage.

Threat agents are identified according to their objectives, affiliation, and/or skill in studies and publications. For example, the United Nations Interregional Crime and Justice Research Institute lists nine groups of hackers (threat agents) ranging from low-skill "wannabes," through cyber-warrior mercenaries to highly skilled industrial spies, government agent hackers, and military hackers.[21] ENISA approaches the question from a slightly different angle and focuses more on affiliation: Threat agents are corporations, nation-states, hacktivists, cyber terrorists, cyber criminals (providers/developers/operators of malware), cyber fighters, script kiddies, online social hackers, and employees.[22] It appears that there are two basic motivations for intentional criminal violations: One group is clearly profit driven, and there is a group of threat agents with some agenda, be it political, personal, or other. In addition, the main attributes of information security are confidentiality, integrity, and availability of data and/or systems,[23] while cybersecurity can add two more properties of non-repudiation and authenticity.[24] Malicious actors' objectives are typically aimed to compromise these attributes.

---

[17] See Kaska 2012.

[18] ENISA 2013, p. 24.

[19] Steven Musil 2014.

[20] For detailed explanation, see ENISA 2013, pp. 16–33.

[21] Raoul Chiesa, Hacker Profiling 2010.

[22] ENISA 2013, pp. 36–39.

[23] Confidentiality refers to protection of data and/or system from unauthorized disclosure; integrity means information or system is protected from unauthorized modification, and it is accurate and complete; availability requirement refers to timely access to data and/or system.

[24] Non-repudiation attribute refers to the state when data transfer cannot be denied, and authenticity means genuinity of data.

Sun Tzu said that success in warfare is gained by carefully accommodating ourselves to the enemy's purpose.[25] It is for the legal policy to deal with strategic challenges and overall motivations of the threat agent. But in order to identify the suitable mitigating or eliminative measures, responses must take into account the operational aims of the threat agent.

The security industry has developed models for both the offensive and the defensive workflows. The cyber kill chain[26] and the NATO "Cyber Defense Capability Breakdown" models capture the operative intents of offensive and defensive measures, respectively.

The cyber kill chain is a set of generic steps characterizing an attack: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.[27] The coverage of steps by a particular threat represents the width of intent for that threat. It is possible to cover just a few steps of the cyber kill chain, for example, code injection is relevant for the exploitation and installation phase, while some other threats may cover all the phases. This paper will rely on such assessments done by ENISA.[28]

As for the responses to threats, the information security management uses a few models that are built in a similar manner. The most well-known ones are the PDRR model,[29] the PDCA cycle,[30] and OODA loop.[31] The above models appear to serve as an inspiration to the cyber defense capabilities breakdown developed

[25] Sun Tzu 2013.

[26] Eric M. Hutchins et al. 2011.

[27] Ibid. p. 4. See also the more general description by ENISA in the Threat Landscape 2013 Report. "Reconnaissance: is the action of researching and analysing information about the target and the environment within which the attack will be deployed. In this phase, assumptions for the number and kind of vulnerabilities to be exploited are being made. Weaponization: is the phase where the malicious payload to be used has been selected and "loaded", that is, made ready for use for the target environment. Delivery: is the action of transmission of the malicious payload to the target environment. Exploitation: is the act of letting the delivered payload make his job by exploiting vulnerabilities that are available in the target environment. Usually these are technical vulnerabilities but in some attacks these may well also be systemic or organisational vulnerabilities including humans. Installation: is the phase where the delivered payload has successfully exploited vulnerability and has been installed in the target environment. Command and Control (C2): in this step the installed payload establishes outbound connection to the controller environment in order to enable interaction with the adversary who launched the attack. Action on Objectives: this is the final phase of a successful attack where the threat agent is in the position to take over the targeted asset. Depending on the kind of target, this activity may include information retrieval, information manipulation, application misuse, etc."

[28] ENISA 2013.

[29] This model consists of protection/prevention, detection, response, and recovery functions, forming a dynamic security period.

[30] Plan-do-check-act cycle is forming a dynamic management period.

[31] Observe, orient, decide, and act concept is developed for military operations.

Table 1 Intent widths and security management phases

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C&C	Actions on objectives
Time →						
Detect	Detect	Detect	Detect	Detect	Detect	Detect
Prevent/ respond	Prevent/ respond	Prevent/ respond	Prevent/ respond	Prevent/ respond	Prevent/ respond	Prevent/ respond
Assess	Assess	Assess	Assess	Assess	Assess	Assess
Recover	Recover	Recover	Recover	Recover	Recover	Recover
Communicate	Communicate	Communicate	Communicate	Communicate	Communicate	Communicate

by NATO,[32] and it includes incident detection,[33] prevention/response,[34] assessment,[35] recovery,[36] and communication.[37] In addition, the model takes into account the timely decision-making factor.[38] This model takes a broader view on cyber defense, one that accommodates the policy dimension better, since it includes steps such as information sharing, and while it focuses on technical responses, it must be kept in mind that technical, legal, and policy measures are complimentary in combating cyber threats. For this reason, the model can be used to assess where the technical and policy measures are insufficient and legal framework should/could be improved. Since the NATO model was developed having in mind military and national security aspects of cybersecurity, it could be suitable also for use in critical infrastructure protection, because although the defense tactics may differ in military and civil context, the overall objectives remain the same.

These models in combination could serve as a framework for assessing whether the threats in emerging technologies are covered by existing legal, technical, or policy measures and indicate gaps in regulation. For each threat phase, there could be a full cycle of security measures applied, but whether that measure is legal or technological, risk based or control based, or a combination of these remains subject of discussion (Table 1).

[32] See Hallingstad and Dandurand 2011.

[33] Detection includes activities such as data collection, entity assessment, and situation assessment.

[34] Prevention/response includes activities, such as topology/policy reconfiguration, traffic flow termination/throttling/redirection/interference, deception, active defense, external response coordination.

[35] Assessment includes risk, damage assessments, and attack assessment.

[36] Recovery comprises of activities such as system integration restoration, information integrity restoration, service availability restoration, and registration of compromised information.

[37] Information collection, sharing, vetting, quality assurance, collection, and exploitation of historical data.

[38] The time factor refers to, but not limited to activities such as swift identification of options, impact, decision-makers, decision coordination, and dissemination.

Reconnaissance and weaponization are the most problematic from defense angle, since they are difficult to spot. While the delivery, exploitation, installation, C&C, and actions on objective steps are within the so-called cyber engagement zone and they are therefore more clearly actionable.[39] These characteristics of the different phases of attacks have profound implications on the legislative possibilities. The following sections will concentrate on some of the legal challenges related to cybersecurity of emerging technologies, but it is not intended to provide a comprehensive legal analysis. The purpose is to merely indicate some questions and point out where is some room for discussion.

4 Legal Challenges in Security Aspects of Emerging Technologies

4.1 Critical Infrastructure: Smart Grids

Smart grids are upgraded electricity networks depending on two-way digital communications between the consumer and the supplier.[40] Smart metering and monitoring are significant part of smart grid technology; therefore, information and communication technologies are the underlying platform for the grid.[41] Smart grid is composed of connected and interacting systems on component, communication, information, function, and business layers.[42]

The "smart" part of the new grids consists of the ICT solution that uses digital technology to transmit, distribute, and deliver power to end consumers. Smart meters enable remote reading of meter data in real time, and they communicate the recorded data about energy consumption to a power distributor.[43] The customer end of smart grids generally includes both end users and producers of electricity in industrial, commercial, and home facilities, such as chemical plants, harbors, shopping centers, and homes. These premises can host generation of electricity in forms of photovoltaic generation, electrical vehicle storage, batteries, micro-turbines, etc.[44] In homes, smart meters can communicate with other smart appliances, such as refrigerators, television sets, and washing machines collecting real-time information about their electric use, potentially enabling the utility to switch appliances off or on remotely.[45] While entities involved in smart grid operation (e.g., distribution system operators or transmission system operators) are usually

[39] Irwing Lachow 2013.

[40] ENISA, Smart Grid Security, European Network and Information Security Agency, 2012, p. 8.

[41] ENISA, Smart Grid Security, European Network and Information Security Agency, 2012, p. 8.

[42] CEN-CENELEC-ETSI Smart Grid Coordination Group 2012.

[43] Daniela Havlíková 2011.

[44] CEN-CENELEC-ETSI Smart Grid Coordination Group 2012, p. 6.

[45] See Daniela Havlíková 2011, pp. 8–12.

required to adhere to some security standards, the customer end is probably considered as a high-risk area, since it is more difficult to monitor and control.

Smart grids are often good candidates as critical infrastructure and/or critical information infrastructure and their main components (industrial control systems) are considered as main potential targets by terrorist groups and nation-states.

Council Directive 2008/14/EC concerns the critical infrastructure protection, and Communication COM(2009)149 gave some thoughts to critical information infrastructure protection in EU member states. The main applicable piece of the EU's cybersecurity framework is the Directive 2013/40/EU (Botnet Directive).

Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (Energy Internal Market Directive (EIMD)) is together with the Directive 2004/22/EC on measuring instruments (Measuring Instruments Directive (MID)), the main legal framework for smart grids. Furthermore, Directive 95/46/EC (Data Protection Directive), Directive 2006/24/EC (Data Retention Directive), Directive 2002/58/ EC (as amended by Directive 2009/136/EC, E-Privacy Directive), and Commission Regulation No 611/2013 may apply to smart grids from privacy and data protection perspective, which will be discussed in relation to big data.

In addition, there are a number of new initiatives, such as the proposal for Network and Information Security Directive or the proposal for General Data Protection Regulation, and non-legislative measures focus on research and development and international cooperation. Application of the Cyber crime Convention is also meaningful where the EU legislation does not cover some malicious or defensive activity.

4.1.1 Critical Infrastructure Protection

The European Union has addressed the information security aspects of European critical infrastructures[46] to some extent; however, the critical infrastructure and cybersecurity are separate policies with overlaps. The Digital Agenda for Europe[47] and the CIIP Action plan[48] are assessing the information security challenges for vital infrastructures in Europe.

Council Directive 2008/14/EC on critical infrastructure protection establishes rules for identification and designation of European critical infrastructures and provides some basic guidelines for carrying out risk assessment if such has not been done. In order to

[46] Commission of the European communities. Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection 2008.

[47] Commission of the European Communities. Communication from the Commission: A Digital Agenda for Europe, COM(2010) 245 2010.

[48] Commission of the European Communities. Communication from the Commission: Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience, COM(2009) 149 2009.

qualify as European critical infrastructure, the impact of disruption or destruction of the infrastructure would have to have serious impact on at least two Member States. The directive provides important definitions of "critical infrastructure,"[49] "risk analysis,"[50] "protection,"[51] and others, all of which are indispensable for the establishment of a common European vocabulary not only in respect to critical infrastructure protection, but for the entire security industry. Annex I of the directive lists the European critical infrastructure sectors, where the smart grids may fall within the category of "[i]nfrastructures and facilities for generation and transmission of electricity in respect of supply electricity." The directive does not provide specific rules for cybersecurity of European (or other) critical infrastructures, although Article 9 makes an attempt to deal with the problem of "insider information misuse" at its roots.[52] As a non-legislative measure, the European Reference Network for Critical Infrastructure Protection has a thematic group addressing industrial automation and control systems and smart grids, focusing on the human vulnerabilities and testing and certification of technology components.

4.1.2 Critical Information Infrastructure Protection

Critical Information Infrastructures include for instance industrial control systems, which are designed to monitor, control, and operate industrial processes such as gas and electricity distribution, water treatment, oil refining, or railway transportation. These systems are strategic assets, and their vulnerabilities to cyber attacks were exposed by a number of incidents; however, real concerns were raised later by the Stuxnet and Aramco incidents.

Stuxnet demonstrated that malware is capable of doing physical harm in critical infrastructures,[53] and the attack against the world's largest oil producer Aramco showed that the indiscriminate destruction of data from company hard drives can cause serious disruption not only locally, but globally as well, since due to the potential impact of oil supply and prices.[54]

---

[49] Article 2(a) provides that 'critical infrastructure' means an asset, system, or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

[50] According to Article 2(c) 'risk analysis' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure.

[51] Article 2(e) sets forth that the 'protection' means all activities aimed at ensuring the functionality, continuity, and integrity of critical infrastructures in order to deter, mitigate, and neutralize a threat, risk, or vulnerability.

[52] Article 9 concerns the handling of sensitive information related to European critical infrastructure protection.

[53] See Ziolkowski 2011.

[54] See Bronc and Tikk-Ringas 2013.

Commission Communication on Critical Information Infrastructure Protection introduced an action plan for the protection of the information and communication systems underlying critical infrastructures.[55] It proposed five pillars to tackle network and information security challenges: (1) preparedness and prevention; (2) detection and response; (3) mitigation and recovery; (4) international cooperation; and (5) criteria for the ICT sector. Concrete action is focused on establishing and strengthening the role of national CERTs,[56] engages and defines the contributions of private stakeholders,[57] cooperation between Member States, establishment of early warning networks,[58] development of national contingency plans, and carrying out exercises, and reinforces cooperation between CERTs. The Commission's next Communication on Critical Information Infrastructure Protection nr COM(2011) 163 lists the achievements and sets forth an evolved action plan along the same lines as the previous one.[59]

The R&D activities, with focus on technical and organizational solutions, make up a significant part of the EU's actions to address critical information infrastructure protection, and some projects are dedicated specifically to smart grids. Some examples are brought below. The cybersecurity strategy[60] states that the Joint Research Centre in close cooperation with the Member States and critical infrastructure owners and operators carries out research for identifying the network and information security vulnerabilities of the European critical infrastructures and encourages the development of resilient systems. In this document, the Commission also directed ENISA to assist the Member States to develop strong national cyber resilience capabilities, in particular by building expertise on security and resilience of industrial control systems, transport, and energy infrastructures.

4.1.3 Cybersecurity Requirements for Smart Grids

ENISA recommendations for industrial control systems (ICS) were delivered prior to the issue of the cybersecurity strategy, and in 2013, ENISA has also prepared the Smart Grid Security Recommendations: Improve the regulatory and policy framework; foster the creation of a Public–Private Partnership entity to coordinate

[55] Commission Communication nr COM(2009) 149 on Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" 30.03.2009.

[56] Computer Emergency Response Team.

[57] European Public Private Partnership for Resilience (EP3R).

[58] European Information Sharing and Alert Systems (EISAS).

[59] Commission Communication nr COM(2011) nr 163 on Critical Information Infrastructure Protection: 'Achievements and next Steps: towards global cybersecurity.'Brussels, 31.3.2011.

[60] Joint Communication to the European Parliament, the Council, the European Economic and Social Committe and the Commitee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber space, JOIN(2013) 1 final, 7.2.2013.

smart grid cybersecurity initiatives; foster awareness-raising initiatives; foster dissemination and knowledge-sharing initiatives; develop minimum set of reference standards and guidelines; promote the development of security certification schemes for products and organizational security; foster the creation of test beds and security assessments; refine strategies to coordinate large-scale pan-European cyber incidents affecting power grids; involve CERTs to play an advisory role in dealing with cybersecurity issues affecting power grids; and foster research in smart grid cybersecurity leveraging existing research programmes.[61]

Although state-of-art security management encompasses risk management,[62] there is no mandatory risk assessment requirement for smart grids, nor assessment methodology. Risk assessment is voluntary, and examples exist such as the IS1 methodology from the UK.[63] However, the Measuring Instruments Directive sets forth rules that can be interpreted in the cybersecurity context regarding smart meters. Annex 1 of the MID requires a measuring instrument to provide security for measurement data; in particular, protection against corruption must be ensured by applying security measures that provide for evidence of intervention. This provision does not specify the format of the data or the security measure; therefore, it can be understood from the context as digital measurement data must also be secured appropriately against intentional or unintentional, unauthorized modification. This requirement can be satisfied as regards smart meters perhaps by a combination of physical and cybersecurity measures designed to prevent alteration of data, metering system, or the smart meter itself physically. Therefore, this rule settles some of the problems concerning data integrity, non-repudiation, and authenticity requirements regarding smart meters. In other words, the end user has hard time denying the amount of energy consumption corresponding to the smart meter data, since any breach or hijacking must have evidence either in the logical or in the physical layer of the smart meter, which in itself contributes to the protection of data from unauthorized modification.

The Energy Internal Market Directive states that "[t]he security of energy supply is essential element of public security and is therefore inherently connected to the efficient functioning of the internal market in energy," it does not expressly deal with cybersecurity issues, and it refers to "security" in general categories, such as security of supply and provision of electricity, rather than meaning special security measures and thereby inherently addressing the system availability requirement of cybersecurity.[64]

4.1.4 The Challenges to Critical Infrastructure Protection

Regardless of the repeatedly emphasized importance of the critical infrastructures and demonstrated need for harmonization as regards the cybersecurity of industrial control and other information systems underpinning the critical infrastructures, the European

[61] ENISA, Smart Grid Security 2012.

[62] See ISO 27,000 series security standards.

[63] ENISA, Smart Grid Security 2012, p. 13.

[64] Article 2(28) includes technical safety in the meaning of security.

Union keeps on relying on soft law and technical measures to address critical information infrastructure protection and there is no obligation for the operators to adhere to common standards or requirements. There are no established rules on the EU level to apply risk assessment and cybersecurity measures in critical infrastructures and critical information infrastructures, including smart grids. Accordingly, the national requirements are not harmonized and the designation of facilities as critical may also vary country by country. One infrastructure that is considered as critical in one Member State does not necessarily have the same status in another. Moreover, it is not clear what parts of facilities/services/organizations are considered as critical, what is the status of entities involved in providing merely ancillary, non-essential services to critical infrastructures, whether they fall under the same regulation, and whether they have to comply with the same requirements. This has a number of consequences as regards the assessment of the seriousness of potential and ongoing attacks, cooperation between the Member State authorities in addressing trans-border cyber crimes against critical infrastructures, and financing of the facilities' operation. Critical infrastructures and critical information infrastructures are often privately owned, and the private sector does not have the sufficient incentives and motivation to have national security concerns to the same extent as a government and the market-oriented approach also implies that cybersecurity risks and losses due to cyber attack would be quantified and calculated in the company overall losses, perhaps balancing it with an increase in prices. According to experts, the smart grid projects focus on testing essential functionalities and do not concern cybersecurity or privacy until mass deployment.[65] This runs contrary to the "privacy by design"[66] and "security by design" principles represented by the Commission's Smart Grid Information Security working group.[67] Therefore, the problem calls for regulator's intervention in bridging the gaps in identification and designation of national critical infrastructures and critical information infrastructures, providing clear guidance on mandates and roles of organizations, Member States, and the EU, establishing rules for mandatory risk assessments and providing alternative methodologies and standards for application of cybersecurity measures in critical infrastructures.

4.2 Top Threats to Smart Grids

According to ENISA, the most frequent threats appearing in critical infrastructure in particular in smart grids are worms and Trojans, followed by code injection and drive-by-downloads; however, the most concern is raised about DDoS attacks.[68]

---

[65] ENISA, Smart Grid Security 2012, p. 18.

[66] 139 Article 29 WP, Opinion 168, The Future of Privacy—Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf in Art. 29 WP Opinion 183.

[67] CEN-CENELEC-ETSI Smart Grid Coordination Group 2012, p. 3.

[68] ENISA 2013, p. 32.

Fig. 1 Position of denial-of-service attack in the attack workflow. ENISA (2013), p. 32

These are clearly Web-based threats that focus on technological solutions rather than human factors.

DoS and DDoS attacks aim to compromise the availability of information systems, while availability is an essential requirement for electricity transportation. However, depending on the smart grid, stakeholder activity requirements of confidentiality and/or integrity may be prioritized.[69] The intent width of denial-of-service attack is depicted in Fig. 1. Distributed denial-of-service attacks comprise of four main steps: research and identification/selection of target; making the malicious payload ready by, for example, purchasing or renting a botnet and/or some other tool; establishment of connection between the bots and the controller environment; and carrying out the DDoS attack.

4.2.1 Reconnaissance

Reconnaissance activities (target research/identification/selection) for DDoS, phishing, or other malicious activity are technically difficult to be detected or limited when they are carried out in the open Internet. Reconnaissance detection entails action that distinguishes between legitimate Web-based research and adversary gathering information in preparation of an attack.[70] In the reconnaissance phase of the DoS attacks, there is little direct action the defending side can take against the attacker(s). Since rendering a system unavailable is the aim and characteristic of DoS attacks, the identification of vulnerabilities tends to focus on resource-intensive activities, such as large-size images on Web sites.[71] Often crawling Web sites, exploiting search engine vulnerabilities methods are used and which does not necessarily involve illegal access. Reconnaissance can compromise system or data confidentiality, and in this case, it is covered by the Botnet Directive and the Cyber crime Convention.

The Smart Grid Coordination Group has provided basic scenarios for cybersecurity risk assessment in smart grids. They consider confidentiality, availability, and integrity breaches.

Confidentiality of data is breached when internal, but unauthorized people or outsiders (such as competitors, other customers, and providers) gain access and

---

[69] CEN-CENELEC-ETSI Smart Grid Coordination Group 2012, p. 5.

[70] Irwing Lachow 2013.

[71] Randware, Pre-attack planning http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/Attack_Planning_ERT_Research_Brief.pdf.

disclose information to outsiders. Typical issues are legitimacy and authenticity of access of all actors and roles, the lack of encryption and authentication when transmitting control information to smart grid devices, and the existence of pathways from outside to smart grid energy transport control systems.[72]

Article 2 of the Council of Europe Cyber crime Convention applies to illegal access.[73] The explanatory report to the Convention states that the mere unauthorized intrusion should be illegal in itself and access comprises of entering of the whole or any part of a computer system, regardless of what kind of communication method is used. This provision therefore covers Wi-fi, Bluetooth, infrared, RFID, and other technical solutions. Access to any restricted system or device, such as a smart meter, or data store therein, therefore constitutes an illegal access.

Without right means, that access by authorized users should not be covered by the provision. This raises the question whether, for example, in case of breach of contract that leads to automatic termination between two parties can result in situation that the *right* of access was withdrawn, but the access itself is not restricted. Another interesting issue could be the automatic access by other devices to a system or a device, when such kind of configuration is applied and connection is made to a restricted system without a person taking any direct action.[74]

Similar questions are raised by the possibility to apply qualifying elements, such as the "infringing security measures." This is the case with Article 3 of Directive 2013/40/EU on attacks against information systems (Botnet Directive) which states that "Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor." The directive differentiates between information systems of critical infrastructures and other information systems, prescribing harsher criminal penalties for attacks on information systems of critical infrastructure. However, there are certain active defense measures—which may not per se be regarded as security measures—to prevent and detect reconnaissance for attacks, such as traffic flow redirection into "honeypots"[75] or deception techniques to feed false information to potential attackers. It is not clear whether in such cases, active cyber defense measures can be understood as security measures within the meaning of the Botnet Directive. At the time

---

[72] CEN-CENELEC-ETSI Smart Grid Coordination Group 2012, p. 30.

[73] "Article 2—Illegal access: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

[74] However, practice of "bring your own device" or allowing smartphones and other devices in networks is often limited or prohibited by company security policies.

[75] "Honeypots" are information systems set up with the purpose to attract malicious actors in order to study their methods and tools or to feed them bogus data.

of its proposal, the directive did not contain such a language and "infringing a security measure" requirement was included on the proposal of the European Parliament. The explanatory report of the Cyber crime Convention does not provide much guidance on this question either. It should be noted though that defense usually does not rely on a single measure, but rather they are used in combination.

As to the issue of DDoS attack infringing the confidentiality requirement and illegal access, the Cyber crime Convention Committee found that DoS and DDoS attacks can be covered by Article 2—Illegal access, depending on what the attack actually does.[76] While DoS attacks may not always require illegal access to the target or other information systems (e.g., attacks can abuse different flaws in networking protocols, such as one of the basic technique, the "SYN flood attack"), DDoS attacks typically rely on botnets, the creation and operation of which requires illegal access to computer systems.

4.2.2 Command and Control

Command and control step of DDoS workflow is directly linked to the integrity attribute and alteration of computer data. Integrity scenarios provided by the Smart Grid Coordination Group include both a customer-end and a provider-end hypothetical case: altering consumptions' data to reduce bills or causing incorrect decisions for the generation and distribution of energy. Data manipulation (that is by authorized actors) and authenticity (concern about unauthorized users or agents) are the two main concerns as regards to malicious actors.[77] Article 4 of the Cyber crime Convention[78] and Article 5 of the Botnet Directive[79] address data integrity breaches. These provisions aim to protect the proper functioning of computer systems.[80] As regards DDoS attacks, they typically involve compromising the integrity of computer data of bots used for carrying out the attack, since the control over the bots is taken over by the "bot herder" through C&C (command and control) servers. Consequently, data in the bot's computer systems are suppressed or altered, which view is confirmed by the Cyber crime Convention Commission.[81]

---

[76] Cyber crime Convention Committee, T-CY Guidance notes, T-CY (2013)29, Strasbourg, 8.10.2013, p. 9.

[77] CEN-CENELEC-ETSI Smart Grid Coordination Group 2012, p. 3.

[78] Article 4 of the Cyber crime Convention criminalizes the intentional damaging, deletion, deterioration, alteration, or suppression of computer data without right.

[79] Aricle 5 of the Botnet Directive provides that deleting, damaging, deteriorating, altering, or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, should be punishable as a criminal offense.

[80] Explanatory Report to the Cyber crime Convention.

[81] Cyber crime Convention Committee, T-CY Guidance notes, T-CY (2013)29, Strasbourg, 8.10.2013, p. 9.

4.2.3 Action on Objectives

At last, the availability scenarios of the Smart Grid Coordination Group refer to unavailability of required information for particular services due to information security incidents against any component supporting the analyzed information asset or even directly to the asset (i.e., distributed denial-of-service Attacks). Carrying out DDoS attack is penalized by Article 5 of the Cyber crime Convention[82] and Article 4 of the Botnet Directive.[83] The objective of DoS and DDoS attacks is precisely to hinder the availability of the target computer systems, which is to have a significant effect on the owner or operator to use the system or to communicate with other systems.[84]

4.2.4 Weaponization

Finally, the weaponization step of DDoS attacks is regulated by misuse of device/tool provisions in the Cyber crime Convention and in the Botnet Directive.[85] It is forbidden to purchase for use or produce computer programs, passwords, access codes, etc. (devices/tools) that are designed or adapted primarily for committing the crimes listed in the respective instruments. The content misuse of device/tool articles is the most controversial one discussed in this chapter, since here it is not enough to show that a certain device could be used to commit the above crimes (dual-use devices are therefore excluded), but the design and primary intention of the device must objectively indicate its use for illegal purposes.[86] In practice, this can prove a rather difficult task due to the use of obfuscation techniques or by providing evidence to the contrary stating in the attached license contracts that the device is meant for research or training purposes, etc.

4.2.5 Gaps and Legislative Opportunities

We have seen that all steps of DDoS attacks against smart grids have the potential to fall within the scope of Botnet Directive and/or Cyber crime Convention, which provides deterrence and sanctions for this threat. These answers are either

[82] Article 5 of the Cyber crime Convention prescribes that intentional and serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data should be a criminal offense in domestic laws.

[83] Article 4 of the Botnet Directive requires that seriously hindering or interrupting the functioning of an information system by inputting computer data; by transmitting, damaging, deleting, deteriorating, altering, or suppressing such data; or by rendering such data inaccessible, intentionally and without right, should be punishable as a criminal offense.

[84] Explanatory Report to the Cyber crime Convention.

[85] Article 6 of the Cyber crime Convention and Article 7 of the Botnet Directive.

[86] Explanatory Report to the Cyber crime Convention.

preventive or responsive as regards their purpose. The detection, recovery, assessment, and communication phases of cyber incident management are covered only partially or not at all by European legislation. In particular, assessment is tackled by policy and technical measures that appear to be insufficient, although carrying out security risk assessment and being aware of the strengths, weaknesses, and vulnerabilities of the smart grid is a precondition for building appropriate defenses. Sun Tzu said that:

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

It is clear that without adequate preparation, even the best security measures could not be effective and systems will be certainly compromised and information assets will be lost.

Recovery from incidents and collection and analysis of data are non-existent in legislative level; however, these phases are mandatory and essential parts of standards regarding security incident management. Communication, however, will be addressed by the proposed Network and Information Security Directive.[87]

Regulation of detection of malicious actors/activity in smart grids also relies on policy and technical measures, although there are other critical infrastructures, where supportive and complementary legal measures exist (in banking, e.g., the money laundering and terrorist financing prevention regulation require to perform certain due diligence steps).[88] The Smart Grid Coordination Group gave guidance on how standards can be used to secure smart grids, and it included the use of active cyber defense measures in its analysis (e.g., the use of honeypots,[89] which is a technique to gather information about the opponent); the assessment represents merely an expert opinion. The use of active defense, information gathering, and assessment activities could be motivated, of course respecting individual rights and freedoms at the same time, since the sophistication level of threats is increasing and the Stuxnet and Aramco cases demonstrated that malicious actors and agents bypass passive defense lines with ease.

4.3 Big Data

The term big data refers to the massive amount of digital information that is collected about individuals and our environment, and it is characterized by high volume, velocity, and variety.[90] The novelty relating to big data lays not in the

[87] Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final. 7.2.2013. Brussels.

[88] Third Anti-Money Laundering Directive 2005/60/EC.

[89] See 77.

[90] Sreeranga Rajan et al. 2013.

creation of large databases, and this has been done by governments and large companies, but in that, it is now available for use to all sizes of organizations and they also have the means to employ it.[91] Big data are/can be used in marketing analytics, healthcare research, national security, law enforcement, environmental protection, achieving better economic efficiency, optimization of energy supply, and use of renewable sources, etc.[92] Several computational techniques related to data mining[93] tasks can be of help to discover new knowledge in big data, such as association rule mining, cluster analysis to discover hidden patterns, anomaly detection, predictive modeling, and visual data mining.[94]

Smart grids and other networked critical infrastructures generate large amounts of data and store personal data. The bidirectional flow of information and the design of the smart grid allow customers, suppliers, and other third parties to monitor and control the consumption of electricity.[95] This could threaten privacy since smart meters collect personal data from each place of installation. Article 29 Data Protection Working Party identified that smart meters process a number of different types of data, such as unique smart meter ID number and/or unique property reference number; metadata referring to the configuration of the smart meter; description of a message being transmitted[96]; data and time stamp; and message content. Smart meters process personal data since the use of unique identifiers in smart devices enables us to single out individuals, and the information collected relates to a consumer's energy profile and behavior.[97] The Smart Grid Cooperation Group proposed two classes for information assets: personal information (within the broad meaning of information related to persons, identified, identifiable, or otherwise) and system information. The class of personal information therefore includes sensitive personal information; personal information within the meaning of the Data Protection Directive; de-personalized, anonym zed, and pseudonym zed personal information; and no personal information, while the class of system information consists of system data, configuration data, customer credentials, etc.;

---

[91] Ibid.

[92] Omer Tene and Jules Polonetsky, Privacy in the Age of Big Data: A Time for Big Decisions, 64 Stanford Law Review Online 63, February 2 2012.

[93] According to the European Data Protection Supervisor, data mining is the process of analysing data from different perspectives and summarizing it into useful new information. Data mining software is one of a number of tools for interrogating data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection, and scientific discovery. Obviously, for data mining to be effective, it is necessary to analyze large amounts of previously collected data. See at https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/74.

[94] Mark Last 2008.

[95] Tene and Polonetsky 2012, p. 64.

[96] For example, whether it is a meter reading or a tampering altert.

[97] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering, WP 183, April 4, 2011.

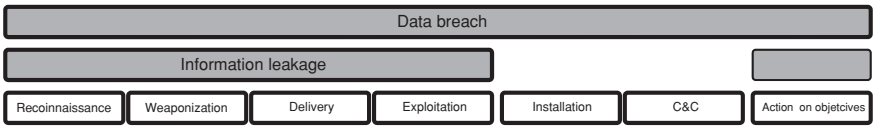

Fig. 2 Position of data breach attack and information leakage in the attack workflow. ENISA (2013), pp. 29–30

governance and reporting information, logging, and audit information; information to administrate remotely; information to operate remotely (control signals); business information; and measurement data.[98]

From the above, it is not hard to see that there can be some overlaps and a piece of data may be considered as personal data and system data at the same time. Also, data can be final target or tool of attacks. A number of EU legal instruments address data privacy issues and regulate the security requirements to process personal data. Less attention is paid to security of data, that is, not personal data. However, it is not only the security of personal information that we should be concerned about.

4.4 Top Threats for Big Data

The ENISA Threat Landscape study distinguishes at least two data-related threats: data breaches and information leakage. Data breaches concern compromising confidential information, where the final objective of the attacker is to get access to or steel certain valuable data (examples are financial fraud and corporate industrial espionage),[99] whereas information leakage covers revelation of information security-related technical or organizational data (e.g., user credentials, information on network structure) that could be used to deliver attacks.[100] These two are the top threats related to big data.[101] The intent widths are shown below in Fig. 2.

The legal aspects of reconnaissance and weaponization steps for data breaches and information leakage are to a certain extent similar to those of DDoS attacks discussed in the previous section of this chapter. Reconnaissance and weaponization activities are difficult to spot, but they may fall under the scope of the Botnet Directive and/or the Cyber crime Convention. Information leakage and data breach attacks may use tools such as drive-by-downloads, Trojans, exploit kits, botnets, phishing, and identity theft to achieve the phase intents in the attack workflow.[102]

[98] CEN-CENELEC-ETSI Smart Grid Coordination Group 2012, p. 9.

[99] See more in Verizon 2013.

[100] ENISA 2013, pp. 35–37.

[101] ENISA 2013, pp. 53–55.

[102] Ibid.

For example, malicious payload can be delivered of by using drive-by-download, e-mail, or other tools. However, the transmission step as such is not covered by separate substantial provisions in the Botnet Directive nor in the Cyber crime Convention. Transmission may not result in successful exploitation and installation of malware to the target system, and in such case, therefore, the mere sending of an e-mail or file to the target is not considered "entering" the system.[103] However, such transmissions may be caught by provisions concerning attempt to commit cyber crimes. Exploitation, installation, and C&C steps typically encompass illegal access and data (and/or system) interference. Exploitation is the exact correspondent to "hacking," "cracking," or "computer trespass,"[104] since it entails the abuse of an identified vulnerability in order to get access to the target system; therefore, it may qualify as illegal access under the above two cyber crime instruments. Installation of malicious payload and C&C causes changes in computer system by adding, modifying, deleting, and suppressing data in the computer system and as such is caught by the provisions concerning data and system integrity breaches.[105]

4.5 Role of Big Data in Detection, Prevention, and Response

Detection of malicious intelligence gathering, attacker profiling, and attack detection should be discussed from legal viewpoint in relation to big data more in depth, since it is a trend to focus on the security applications of mining, analyzing large data sets and use of big security data is emerging as well.

In relation to smart grid security, ENISA noted that anomaly detection seems to be a very promising method to data manipulation, fraud, and targeted attacks.[106] Big data are increasingly used for anomaly detection, intelligence gathering, and analysis by both the private and the public sector.[107] Since smart grid big data contain personal and other data, it is necessary to assess the use of big data from data privacy perspective.

4.5.1 Privacy Concerns

As to the EU-level regulation of personal data processing in the public sector, the adoption of a directive is being discussed by the legislative bodies. The directive would relate to the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation,

[103] Explanatory Report of the Cyber crime Convention, 46.

[104] Ibid, 44.

[105] Ibid, 61 and 66.

[106] ENISA 2013, p. 45.

[107] ENISA 2013, p. 55.

detection, or prosecution of criminal offenses or the execution of criminal penalties and the free movement of such data.[108] Currently, the processing operations concerning public security, defense, state security, and activities of the state in areas of criminal law are not covered by community legislation. The Data Protection Directive is the main regulating instrument regarding processing of personal data in other cases.[109]

The use of personal data for the other purposes than the smart grid distribution system operator's legal obligations requires specific and informed consent from the data subject, or processing needs to be necessary in the interest of the data subject or another person that overrides the data subject's fundamental right to privacy with respect to the processing of personal data.[110] The Smart Grid Task Force Expert Group 2 provided a non-exhaustive list of activities when personal data are processed: network management, metering activity, supply of energy, essential energy services, and provision of value-added services to customers with specific consent.[111] Furthermore, it can be argued that smart grid operators may process customer's personal data when performing certain computational activities for security purposes, since the security of the grid is in the public interest. Being a critical infrastructure, it is conceivable that smart grid operators may exercise some official authority, if such task is delegated according to national laws.[112]

"[T]he uses of big data can be transformative and the possible uses of data can be difficult to anticipate at the time of initial collection,"[113] which may turn out to be contradicting the principle that personal data processing may not be excessive in relation to the purposes for which they are collected.[114] Indeed, smart meters collect more data that are strictly necessary for the performance of the contract between the customer and energy supplier, since one of the smart metering technology's purpose is to increase energy efficiency and that can be achieved by increasing energy efficiency of individual customers.[115] The potential uses and benefits of big data are endless, as well as the potential for its misuse and big data-based surveillance that became subject of worldwide discussion recently.

---

[108] European Commission, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties and the free movement of such data COM(2012) 10.

[109] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[110] See Article 7(a), (b), (d), (f) of the Data Protection Directive.

[111] Task Force Smart Grids Expert Group 2 2011.

[112] See Article 7(e) of the Data Protection Directive.

[113] See Tene and Polonetsky 2012, p. 64.

[114] See Article 6(c) of the Data protection Directive.

[115] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering, WP 183, April 4, 2011.

4.5.2 Personal Data Security

A popular way to mitigate privacy threats arising from improper internal access or external data breach is to de-identify data,[116] which is the process through which organizations remove or obscure links between the data subject and the personal data.[117] Indeed, de-identification has become an essential element of numerous business models, such as online behavioral advertising and health data regarding clinical trials.[118] According to the Data Protection Directive, anonymization should be done such way that the data subject is no longer identifiable.[119] De-identification, therefore, also removes data from the protected status of personal data and allows data processing without fulfilling the strict requirements of the Data Protection Directive.

However, recent research has shown that our reliance on de-identification methods to protect data privacy is undermined by the development of technology that enables the increasingly robust uses of data.[120] Cloud computing, pooled processing power, and storage coupled with data mining and analytics make data re-identification and attribution to specific individuals possible; however, some uncertainty will remain in the equation.[121] The Data Protection Directive was drafted in the middle of the 1990s, when the present re-identification techniques were simply not possible. In the last few years, anonym zed data suddenly became object of interest and new re-identification techniques potentially render previous anonymization ineffective, thereby placing organization in breach of the Data Protection Directive.

Considering the challenges around the processing of personal data or de-identified data for cybersecurity purposes, an alternative approach that relies on data minimization could be discussed. The Smart Grid Task Force Expert Group report contains a recommendation on data privacy: "The Expert Group's recommendation is to distinguish between personal and non-personal data to minimize the exposure of personal data. Personal data is considered as specific data and can be traced back to the individual consumer whereas non personal data could be aggregated data."[122] Although the exact meaning of aggregated data is not defined by the expert group, it is implied that aggregated data are based on individual pieces of personal data. If we consider using aggregated data instead of anonym zed or even personal data for security activities, we can ask ourselves what happens to the precision of anomaly detection and other computational techniques in the detection of malicious cyber

[116] The legal obligation to do so may arise also from Article 6(e) of the Data Protection Directive.

[117] See Lagos and Polonetsky 2013, pp. 103–104.

[118] See Tene and Polonetsky 2012, p. 65.

[119] Recital 27 of the Data Protection Directive.

[120] See Tene and Polonetsky 2012, pp. 68–69.

[121] See Tene and Polonetsky 2012, pp. 64–66.

[122] Task Force Smart Grids, Expert Group 2 2011.

activity and cyber attacks. Such data minimization may not always be a practical and desirable approach if we take into account the societal value of cybersecurity and economic efficiency that analysis of big data brings. Big data and big security data are a gold mine for active cyber defense techniques, which rely on intelligence analysis to identify potential attackers and their methods, preempt data breaches, and reverse the asymmetry in cybersecurity by making it harder to achieve attack objectives.[123] Active cyber defense techniques represent a paradigm shift in cybersecurity: instead of relying on passive and reactive security measures (that waits for the malicious activity occurring) and proactive measures "go after" the (potential) attackers and putting more faith in the deterrent effect of such operations.

4.5.3 System Data Security

After considering some questions about personal, anonymous, and aggregated data processing, it is worth to take a look whether any legal provision exists that provides either intentionally or accidentally protection to system information (such as system data, configuration data, and customer credentials; governance and reporting information, logging, and audit information; information to administrate remotely; information to operate remotely (control signals); business information; and measurement data). For this, the Data Protection Directive, the e-Privacy Directive, and the Data Retention Directive will be analyzed.

The Data Protection Directive lays down obligations to apply appropriate technical and organizational measures both at the design and at the operation of processing systems in order to maintain security and thereby prevent unauthorized processing of personal data.[124] This provision relates solely to personal data security; however, it may provide incidental protection to system information in case of unstructured or semistructured big data sets.

Data Retention Directive arguably applies to smart grids since they involve publicly available electronic communications as the underlying element of the grid; however, smart grids cover a much wider area than electronic communication. The Data Retention Directive concerns location data, traffic data, and related data that are necessary to identify a customer, but since it is aimed primarily at telecommunication sector, it disregards system information. Article 29 Working Party admitted that smart metering environments present new challenges, and due to the amount of data generated by smart grids, retention policies needed to be revised and adjusted to the purposes of processing.[125] In any case, whatever data types a future regulation may encompass, the present discussion mainly focuses on personal data and Article 7 of the Data Retention Directive prescribes security measures only for location, traffic, and related data that are necessary to identify a

[123] See Elazari 2013.

[124] Recital 46 of the Data Protection Directive 95/46/EC.

[125] Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering, WP 183, 4 April 2011.

customer, which may have some accidental overlaps, but does not intend to cover system, configuration, remote administration, logging, or audit data and other similar data, nor business information or measurement data.

The e-Privacy Directive imposes an express obligation on providers of publicly available electronic communication service to take appropriate technical and organizational measures to safeguard security of its services. Although the electronic communication services are essential part of the smart grid, Article 1 of the e-Privacy Directive can be interpreted as smart grids are not covered by its scope and aim, since smart grids' primary activity is not within the electronic communication sector, but energy sector. Moreover, there is a general understanding expressed in different EU documents that the current regulatory framework requires only telecommunication companies to adopt risk management steps and to report serious network and information security incidents.[126]

4.6 Need for a New Perspective in Data Regulation

It can be concluded that the two main threats of smart grid big data are not addressed adequately by possible levels in European legislation. Smart grids collect more personal data than it is necessary in order to perform their tasks related to delivering energy. However, the collection of additional personal data creates a social value of reducing energy consumption, and therefore, its benefits can be felt in environmental protection as well. Smart grids also collect and create a lot of other data, besides personal data, which puts them into the focus of malicious actors. On the other hand, there is no clear obligation on operators to retain data for purposes of later criminal investigations, which will certainly lead to problems in law enforcement, and it has a national security implication as well considering potential terrorist acts against critical infrastructures.

While defining what type of data smart grids should retain and for how long, legislators must also take into account the quantity of such data and need to store it. For storage of such vast amount of data, cloud computing and distributed storage can offer solutions. However, this indicates the next problem in data retention, namely that cloud technologies present serious practical challenges to evidentiary rules and procedures.[127] As an illustration let us just imagine a situation where a virtual machine using distributed storage and processing in the cloud needs to be accessed by the law enforcement authorities for producing digital evidence in an investigation. A database or a file system that makes one whole in the virtual space could comprise of units that are physically located in different places, potentially even in different countries. Producing digital evidence in such environments could require speedy cooperation between numerous law enforcement authorities, and cloud computing

[126] See, for example, the Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final. 7.2.2013. Brussels, p. 4.

[127] United Nations Office on Drugs and Crime 2013.

has multijurisdiction characteristics. Furthermore, new security risks arise in connection to using cloud technology for storing and processing big data and/or retained data, more precisely that *data at rest* become vulnerable,[128] thereby prompting the need for more security measures appropriate to mitigate such threats. Of course, there is a choice between private and public clouds; however, building and maintaining a private cloud have substantial financial implications.

It should be noted here that the main threats to cloud computing in 2013 were information leakage, same as to big data.[129] Information security data are a top target for it is a tool to gain access to confidential information assets and computer systems. To illustrate the importance and value of information security data, for example, zero-day exploits[130] can sell for as much as 250.000 USD, depending on the use and software.[131] However, no protection is provided to such data, if it does not qualify as personal data. Misuse of devices, and even the mere possession without the right of tools such as passwords, access codes, and other similar data, is sanctioned by the Botnet Directive and the Cyber crime Convention (if committed intentionally and with the intent to be used to commit cyber crimes),[132] but this provision builds on deterrence and it is reactive to offenses. The role and importance of information security data clearly calls for a new perspective of data protection, and a more general and preventive protection regime could be considered that (of course) in conjunction with technical and policy measures, it would aim to tackle information leakage threats, more precisely information security data leaks.

And finally, de-identified, anonym zed data are removed from the scope of personal data protection and it can be used, published, and processed without restrictions. Personal data anonymization 15 years ago could not foresee that technological development might provide ways to re-identify natural persons within that same data set. Similarly, data de-identification might be overturned in a few years. There are a number of potential policies that could be considered in relation to this problem, such as the use of sunset clauses in order to prevent today's measures from threatening fundamental rights tomorrow, or alternatively, a minimal level of protection could be kept for de-identified data.

5 Conclusion

Information and communication technologies are everywhere, and they literally surround us. They are increasingly complex, but so is the misuse of them. Yet regulation of cybersecurity even in critical infrastructures relies on general

128 See Bigo et al. 2012.

129 ENISA 2013, p. 55.

130 Zero-day exploits are new discovered security holes in software.

131 See at http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

132 See Botnet Directive Article 7 and Cyber crime Convention Article 6.

coordination, technical measures, volunteer action, and market forces to a great extent, and the EU lacks a comprehensive overview of the field. Cyber incidents range from breach of internal company policy to serious cyber crimes with national security implications, and the responses must apply a combination of policy, technical, and legal measures. In order to balance these properly, a systematic analysis of the threats is necessary.

The above assessment revealed some gaps, where the need for new legal measures or the reconsideration of the existing ones might be discussed. However, it was also discovered that dealing with one gap could have wide impacts on future enforcement and raise new security concerns. This suggests that the rather pessimistic vision of the Project2020 could be true and a major revision of basic legal concepts and principles will eventually be necessary.

References

Bigo, Didier, Boulet, Gertjan, Bowden, Caspar, Carrera, Sergio, Jeandesboz, Julien, & Scherrer, Amandine. (2012). *Fighting cybercrime and protecting privacy in the cloud, directorate general for internal policies, policy department c: citizens' rights and constitutional affairs*. Brussels: European Parliament.

Bronc, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. *Survival: Global Politics and Strategy*, *55*(2).

CEN-CENELEC-ETSI Smart Grid Coordination Group. (2012). *Smart grid information security*. European Commission grid mandate.

Chiesa, R. (2014). *Hacker Profiling: Who are the attacking us?*. United Nations Interregional Crime and Justice Research Institute, 2010. Available at http://www.unicri.it/special_topics/cyber_threats/hackers_profiling/. Accessed 16.03.2014.

Cridland, C. (2008). The history of the internet: the interwoven domain of enabling technologies and cultural interaction. In: *Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism, Ankara, Turkey* (pp. 1–7).

Elazari, R. (2013). *Proactive security: Integrating active defense in cybersecurity, Gigaom Research*, Report. Available at www.gigaom.com. Accessed 05.01.2014.

Eneken Tikk, A. (2011). *Comprehensive legal approach to cyber security*. Ph.D Thesis, Tartu University.

ENISA, ENISA Threat Landscape 2013. (2013) *Overview of current and emerging cyber-threats*. European Union Agency for network and information security.

ENISA, Smart Grid Security (2012) *Recommendations for Europe and Member States*. European network and information security agency. 01.07.2012.

Goodman, S. E. (2008). Critical information infrastructure protection. In: *Responses to cyber terrorism, centre of excellence defense against terrorism, Ankara, Turkey*. Amsterdam: IOS Press.

Hallingstad, G., & Dandurand, L. (2011, November). *NATO consultation, command and control agency reference document RD-3060. CIS Security* (*including cyber defense*) *Capability breakdown,* NC3A. Netherlands: The Hague. (NATO Unclassified).

Havlíková, D. (2011). *Smart Grids in the European data protection legal framework: Smart metering implications for the EU data protection*. MA thesis, University of Oslo.

Hutchins, E. M. et al. (2011, March 17–18). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Paper presented at the 6th Annual International Conference on Information Warfare and Security, Washington. Available at http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed 16.03.2014.

Kaska, Kadri. (2012). *Conficker: Considerations in law and legal policy*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

Lachow, I. (2013). *Active cyber defense, a framework for policy makers—policy brief*. Center for New American Security. www.cnas.org.

Lagos, Y., & Polonetsky, J. (2013). *Public versus nonpublic data: The benefits of administrative controls*. 66 stanfords law review online 103, Sept 3.

Mark Last, & Data Mining, (2008). In Lech J. Janczewski & Andrew M. Colarik (Eds.), *Cyber warfare and cyber terrorism*. New York: Information Science Reference.

Musil, S. (2014). *Record-breaking DDoS attack in Europe hits 400Gbps*, CNET, 11.02.2014. Available at http://news.cnet.com/8301-1009_3-57618762-83/record-breaking-ddos-attack-in-europe-hits-400gbps/. Accessed 16.03.2014.

Rajan, S., van Ginkel, W., & Sundaresa, N. (2013). *expanded top ten big data security and privacy challenges, cloud security alliance, big data working group,* Report. Available at https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf, April 2013

Sun Tzu. (2013). *The Art of War*. Colorado: Orange Publishing

Task Force Smart Grids, Expert Group 2. (2011). *Regulatory recommendations for data safety, data handling and data protection.* Report, issued 16.2.2011.

Tene, O., & Polonetsky, J. (2012). *Privacy in the age of big data: A time for big decisions*. 64 Stanford Law Review Online 63, Feb 2.

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime*. Report, United Nations, New York

Verizon. (2013). *Data breach investigations report.* Available at http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Wall, D. S. (2007). *The transformation of crime in the information age, polity*. Cambridge

Ziolkowski, Katarina. (2011). *Stuxnet—legal considerations*. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.

Investigating Cybercrimes: Theoretical and Practical Issues

Edita Gruodytė and Mindaugas Bilius

Abstract Communication technologies play an important role in society. Global cybercrime is one of the biggest underworld industries, much of this crime is unreported, new forms of crimes occur. In the light of the new EU Directive (2013/40/EU of the European Parliament and of The Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA), the authors of the Article discuss if and how the new instrument helps to solve some of the aforementioned problems. The first part of the Article presents systemic and historic evaluation of the EU cybercrime policy in comparison with the Convention on Cybercrime. The second and third parts of the Article focus on two specific issues related to cybercrimes. The second part evaluates changes in the material criminal law introduced by the new Directive and their effectiveness in resolving the issue of harmonization. The last part of the paper is answering if introduced procedural changes are successful in providing framework of law enforcement cooperation and capacity to investigate.

1 Introduction

Today, information and communication technologies are the impetus of economy and society as they "*have infiltrated virtually every sector of social life to such an extent as to redefine both State and individual activities*".[1] Without a doubt, wide use of modern technologies is endangered by the new threats, such as mass-scale

[1] Kaiafa-Gbandi (2012), p. 59.

E. Gruodytė (✉) · M. Bilius
Law Faculty, Vytautas Magnus University, E.Ožeškienės St. 18, 44254 Kaunas, Lithuania
e-mail: e.gruodyte@tf.vdu.lt

M. Bilius
e-mail: m.bilius@tf.vdu.lt

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_11

commitments ("botnets").[2] "*These threats are global in nature and are constantly proliferating, shifting in focus and exploiting opportunities presented by technology*".[3] The rising number[4] of cybercrime demonstrates that communities in the global sense show not enough efforts or have not sufficient power for fighting with this phenomenon. Norton Cybercrime Report states that "*cybercrime is bigger than the global black market in marijuana, cocaine and heroin combined ($288bn) and approaching the value of all global drug trafficking ($411bn)*".[5] Global cybercrime is arguably the biggest underworld industry of our times and annual worldwide loss to cybercrime is US$1 trillion.[6] Much of the cybercrime is unreported[7] and the numbers of prosecutions on cybercrime are not increasing[8]—in the FBI opinion, there is less than a 1:20,000 chance of a cyber-criminal being caught.[9] Businesses are afraid that negative publicity about failure to protect their information and servers could lead not only to the damage of their reputation, but also to the loss of their customers.[10] According to the Eurobarometer data on cybersecurity, two biggest concerns in the EU are the misuse of personal data (mentioned by 40 % of respondents) and security of online payments (mentioned by 38 %).[11] Twenty-nine percentages of Internet users across the EU are not confident about their ability to use the Internet for online banking and buying.[12]

The fight against cybercrimes can only be successful if approached holistically, i.e. based on five criteria: legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation.[13] "For

---

[2] Typical "bot-herders" control tens of thousands and even millions of "zombie" computers. More statistics and data on cyberthreats could be found in Nir Kshetri. See Kshetri (2010).

[3] European Union Agency for Network and Information Security, p. 4. https://www.enisa.europa.eu/media/key-documents/cybersecurity-cooperation-defending-the-digital-frontline.

[4] The survey done by Ponemon institute indicates that both the cost and frequency of cybercrime have continued to rise for the fourth straight year. According to this study of a benchmark sample of organizations in the USA, the occurrence of cyberattacks has more than doubled during this period, while the financial impact has increased by nearly 78 %. See Ponemon Institute, http://www.hpenterprisesecurity.com/ponemon-study-2013.

[5] See Norton Cybercrime Report 2012, http://us.norton.com/cybercrimereport.

[6] See Kshetri (2013).

[7] *One global private sector survey suggests that 80 % of individual victims of core cybercrime do not report the crime to the police*. See Expert Group to Conduct a Comprehensive Study on Cybercrime, p. 6. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf.

[8] Communication from the Commission to the European Parliament, (COM 2007) 267 final, Sect. 1.2.1.

[9] Gabrys (2002), p. 21.

[10] See Storm (2013). http://edepot.wur.nl/252016.

[11] European Commission (2012), p. 25. http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

[12] Ibid at p. 22.

[13] Vasiu and Vasiu (2013), p. 44.

successful interdiction of cross-national organized cybercrime, three factors are essential, namely (1) legislative harmony, (2) a framework of law enforcement cooperation, and (3) the capacity to investigate and, if necessary, to prosecute".[14] The first important steps joining all these factors together were taken by the Council of Europe, enacting the Convention on Cybercrime[15] (Convention) followed by a Framework decision[16] (Framework decision) and a Directive[17] (Directive) at the EU level. However, criminal law enforcement is a sensitive area as it infringes national sovereignty, so even when adequate legal provisions are enacted, there may be problems of their effective enforcement and political decisions play an important role.[18] The cooperation of law enforcement agencies could be more complicated, because they can face the principle of dual criminality,[19] which could allow one country to refuse assisting in cybercrime investigation. Refusal of assistance could be based on the ground that the act in relation to which the request is made is not an offence in the territory of the requested State.[20] The harmonization of substantive law facilitates the extradition of alleged or fugitive offenders, facilitates mutual legal assistance, that is, the use of legally controlled investigatory powers, such as search and seizure, examination of witnesses,

[14] Choo and Grabosky (2013), p. 15.

[15] Convention on Cybercrime et al. 2001, Budapest, 23.11.2001.

[16] Council Framework Decision 2005 2005/222/JHA on attacks against information systems.

[17] Directive 2013/40/EU of the European Parliament and of The Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[18] Sommer and Brown (2011), p. 73. http://www.oecd.org/gov/risk/46889922.pdf.

[19] The *dual criminality requirement continues to be important—but not for the purpose of isolating nation states and not because criminal law should be associated with one fixed cultural environment and for this purpose kept separate from other cultures. Rather, the requirement is significant because it helps to put into practice the rule-of-law concept that each legal system must have for its criminal offenses a kaleidoscope clearly defined by the legislature—and can only provide legal assistance for this defined kaleidoscope of offenses. The rapprochement of the states and the corresponding approximation of their common efforts to carry out law enforcement transnationally, therefore, require substantive scrutiny of existing differences among the various systems of criminal law. It is the dual criminality requirement that demands this examination, and it is the dual criminality requirement that by so doing fosters true harmonization*. Capus (2007–2009). http://www.mpicc.de/ww/en/pub/forschung/forschungsarbeit/strafrecht/rechtshilfe.htm.

[20] *Even if the dual criminality rule is not an aspect of all incidents of mutual assistance, it is often a requirement in cases of search and seizure, which is a particularly important means of assistance where data are concerned. Double criminality, furthermore, is basic to other common cooperation modes, such as extradition, or other schemes for solving jurisdictional conflicts as discussed above. Unless domestic criminal legislation, as it develops, moves beyond expressions of sovereignty to espousing common principles as agreed among nations, conflicts will not be avoided. Efforts by States to harmonize their domestic laws will prevent conflicts of jurisdiction and, at minimum, will lay the basic groundwork for cooperation*. See United Nations Manual on the prevention and control of computer-related crime (1990). http://www.uncjin.org/Documents/EighthCongress.html.

electronic surveillance, by one country for the benefit of another country; therefore, harmonization of the concept and even the definition of crime can be crucial to the ability to extradite.[21]

Steps in the EU for successful interdiction of cybercrime were made mostly in the area of legislative harmony, but there must also be a framework of law enforcement cooperation, the capacity to investigate and, if necessary, to prosecute. The last two are closely related with evidences.[22] The split of the computer technologies determines that the computer becomes a part of not only illegal activity, but also a tool and a means when committing a crime. For these reasons, the need to investigate evidence in the cyberspace becomes very relevant.

In the light of the new EU Directive,[23] the authors of the Article discuss if and how the new instrument helps to solve some of the aforementioned problems. The first part of the Article presents systemic and historic evaluation of the EU cybercrime policy in comparison with the Convention on Cybercrime. The second and third parts of the Article focus on two specific issues related to cybercrimes. The second part evaluates changes in the material criminal law introduced by the new Directive and their effectiveness in resolving the issue of harmonization. The last part of the paper is answering if introduced procedural changes are successful in providing framework of law enforcement cooperation and capacity to investigate.

2 EU Policy and Its Sustainability in the Light of the New Directive

Worldwide the Convention on Cybercrime[24] (in force from 2004[25]) is treated as the most important international instrument on cybercrime issues *since it provides a comprehensive and coherent framework embracing the various aspects relating*

[21] Ibid.

[22] *For tracing and identifying suspects, investigators often need access to data that may be deleted shortly after transfer. A very short response time by the investigative authorities is often vital for a successful investigation*. See Gercke (2011), p. 139.

[23] Directive 2013/40/EU of the European Parliament and of The Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[24] Convention on Cybercrime, Budapest, 23.11.2001.

[25] As on 22/1/2014, the Convention on Cybercrime was ratified by 41 State (36 members of European Council) and 11 States who signed convention were not following it by ratifications. Among them are also five EU countries: Greece, Ireland, Luxemburg, Poland, and Sweden. However, five countries, including USA, which are not members of the European Council also ratified this Convention. See Convention on Cybercrime. Explanatory report. ETS 185. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

to cybercrime,[26] especially valued for procedural matters[27] including judicial cooperation.[28] However, the Convention is criticized for being of rather limited application, as such global powers like China and Russia[29] opposed that Convention[30] fearing the possible infringement of powers vested in national authorities.[31] It is treated as the instrument providing inadequate respect for such basic principles of human rights as necessity, proportionality and appropriateness.[32] Also, the rules of dual criminality established in the Convention make it less attractive for international cooperation.[33] Notwithstanding the provided critical remarks, the sphere of regulation in the Convention is wider than the one in the EU instruments as it requires criminalizing not only computer crimes *strictosensu* (mainly Articles 2–6 of the Convention), but also crimes where a computer is used as a means of crime (computer fraud, forgery, child pornography, copyright infringements)[34] and is an instrument encouraging international cooperation.[35]

Specific attention has been given to various cyberspace issues at the EU level-for at least 20 years, but till the Amsterdam Treaty (1999), the criminal law and especially cybercrime was not the priority of the European Union[36] and was viewed mostly from the internal market perspective. For example, the need to address various issues of cyberspace—computer security, privacy rights, or intellectual property as some obstacles to successful development of a common e-market was stressed in the White Paper in Growth (1993)[37] and in Recommendations (1994).[38] With the introduction of the common area of freedom, security, and

---

[26] Proposal for a Directive of the European Parliament and of the Councilon attacks against information systems and repealing Council Framework Decision 2005/222/JHA (2010). http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf.

[27] Especially for the norms taking into account such procedural aspects of cybercrime as *the volatility and vulnerability of electronic evidence.* Procedda (2011), p. 43. http://ec.europa.eu/idabc/en/document/70.html.

[28] Kaiafa-Gbandi (2012), p. 61.

[29] Which are either indicated as world leaders in cybercrime. See Jagadeeswara Rao (2011), p. 113.

[30] Procedda (2011), p. 43. http://ec.europa.eu/idabc/en/document/70.html.

[31] That police might acquire powers to cross national boundaries without consent from the local authorities. Sommer and Brown (2011), p. 71. http://www.oecd.org/gov/risk/46889922.pdf.

[32] The author fears that *states usually will not refuse to cooperate with other countries in which lower standards for safeguard are applied which means that the data could be transferred without required respect for human rights.* Procedda (2011), p. 44. http://ec.europa.eu/idabc/en/document/70.html.

[33] By Article 42, states are empowered to make reservations, including dual criminality. Convention on Cybercrime, Budapest, 23.11.2001.

[34] Kaiafa-Gbandi (2012), p. 61.

[35] Sommer and Brown (2011), p. 71. http://www.oecd.org/gov/risk/46889922.pdf.

[36] Naziris (2014), p. 327.

[37] Commission of the European Communities, (COM(93) 700, 5 Dec 1993).

[38] European Council (1994).

justice in the Amsterdam Treaty, the European Union has become more active in the area of cyberspace, but still mostly from the successful common market perspective, even though the importance of cybersecurity and the need to fight cybercrime in various EU documents is already stressed.[39] When implementing European policy, various legal instruments addressing different aspects of cyberspace were adopted (on child pornography,[40] electronic commerce,[41] data protection[42], etc.).[43] However, the first law designed directly in connection to cybercrimes is the Council Framework decision enacted in 2005,[44] where certain cybercrimes (illegal access to information, illegal systems, and data interference) are explicitly introduced and a minimum level of approximation of Member States' legislation on certain issues is expected. Its value could not be overestimated as all the EU members are parties to the Convention on Cybercrime[45] and the content of the Framework decision[46] comparing with the Convention is not extended. However, the greatest added value was probably expected because of its legal power—the Convention works at a pure intergovernmental level, leaving a lot of discretion to the national legislator, while at the EU level Member States,

[39] Example in eEurope initiative and eEurope Action Plan (1999)—the importance of network security and the fight against cybercrime where already highlighted. Available on Internet http://ec.europa.eu/idabc/en/document/70.html. In Communication of 2000 aimed at *Creating a safer information society by improving the security of information infrastructures and combating computer related crime,* the Commission established the EU priorities and future steps in both prevention and combating cyber crime naming the basic challenges and peculiarities of these crimes. See Communication from the Commission to the European Parliament, the Council and the Economic and Social Committee and the Committee of the Regions, Creating a safer information society by improving the security of information infrastructures and combating computer-related crime, (COM 2000) 890 final, 26.1.2001). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF.

[40] Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography. (Official Journal L.13, 20.1.2004).

[41] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. (Official Journal L 178,17.7.2000).

[42] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. (Official Journal L 201/37, 31.7.2002); Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC. (Official Journal L 105, 13.4.2006).

[43] Procedda (2011), p. 42. http://ec.europa.eu/idabc/en/document/70.html.

[44] Council Framework Decision 2005/222/JHA on attacks against information systems.

[45] Five EU countries—Ireland, Greece, Luxembourg, Poland, and Sweden—have not ratified the document even though they also signed the treaty. See Convention on Cybercrime Chart of signatures and ratifications. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

[46] Council Framework Decision 2005/222/JHA on attacks against information systems.

especially evaluating jurisprudence of the European Court of Justice,[47] have various obligations—for example, to provide information to Commission if and how the Framework decision was implemented, in case national law contradicts the EU legislation, to evaluate a possibility of applying EU law,[48] etc. However, the Commission report on the implementation of this instrument in MS indicates that EU had very limited powers to force states to implement the instrument—at least up to 2008, the seven Member States (out of 27) provided no information to the Commission on how and if they implemented the Framework decision. The second concern expressed by the Commission that Member States use very diverse practice is also well grounded. The commission found out that the legal concepts and expressions used by Member State, while implementing the Framework decision "are not easily comparable",[49] which indicates that even the EU Member States "do not speak" the same language. For example, three Member States (the Czech Republic, Estonia, and Latvia) criminalizing illegal data interference[50] measures used the option (established in the Article 4 of the Framework decision) to criminalize such conduct only "for cases which are not minor". However, Latvian regulation was evaluated as not implementing the Framework decision because criminal liability was dependent upon the fact that "*protective systems are damaged or destroyed or large-scale loss is caused*". Even the laws of the other two countries are also diverse: the Czech law does not require consequences (just the intent to cause harm is sufficient), while the Estonian law requires actual damage to be caused.[51]http://itlaw.wikia.com/wiki/Report_from_the_Commission_to_the_Council_based_on_Article_12_of_the_Council_Framework_Decision_of_24_February_2005_on_attacks_against_information_systems. The example shows that the implementation of the Framework decision is a concern of the Member State and the EU institutions had no instruments to make real influence to national authorities (except may be the good will of Member State) at least until the Lisbon Treaty and the end of the transitional period at the end of 2014.[52] The need for a new instrument was induced by two reasons: legal (such as very limited number of criminal offences in the Framework decision, not adequate gravity of sanctions

[47] Judgement of the Court (2005).

[48] Order of the Court (2008).

[49] COM (2008), p. 3, Sect. 2.1. http://itlaw.wikia.com/wiki/Report_from_the_Commission_to_the_Council_based_on_Article_12_of_the_Council_Framework_Decision_of_24_February_2005_on_attacks_against_information_systems.

[50] Done in accordance with Article 4 of the Framework decision.

[51] Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems (COM (2008)448 final, 14.7.2008), p. 6, Sect. 2.5.

[52] Protocol (No. 36) On Transitional Provisions, Article 10, establishes that Commission's enforcement powers and the powers of the Court of Justice are in force in 5 years after entry into force of the Lisbon Treaty, i.e. from 1 December, 2014. Craig (2010), p. 341.

established in the document, the diverse implementation of Framework decision by the Member States, etc.) and technical (new threats in cyberspace large-scale attacks and increased use of "botnets"[53] for criminal attacks) developments.[54]

The EU gained new opportunities and powers in criminal cases by the Lisbon Treaty, where a new Article 83 of the treaty on the Functioning of the EU declares that "*the European Parliament and the Council may, by means of Directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis*",[55] which allows the EU to base competence on cybercrime as a crime having cross-border dimension and when it is of a "particularly serious" nature which was established in the case of cybercrime.[56]

In 2013, the EU strategy on cybersecurity[57] was established for the first time where five strategic EU priorities[58] were declared, making cyberspace issues one of the targets of Common Foreign and Security policy, especially getting into closer cooperation with key international partners and organizations.

The new powers including the right to include minimum elements describing the *actus rea* and *mens rea* of each criminal offence[59] are reflected in the newly enacted Directive on attacks against information systems.[60]

The fight against cybercrime becomes one of the priorities of the EU policy, while the Lisbon Treaty supplies the European Union with new legal powers in criminal matters. In the following sections, we evaluate how and what material changes are introduced and how they should be treated from the national perspective. However, before going into details, it is important to find out if the new

---

[53] *The biggest botnets witnessed have been estimated to have between 40,000 and 100,000 infected computers per period of* 24 h. See Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM (2010) 517 final, 30.9.2010), p. 3. http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf.

[54] Ibid.

[55] The Lisbon Treaty (2010).

[56] COM (2013. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf.

[57] Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace, (JOIN(2013) 1 final, 7.2.2013).

[58] Such as achieving cyber resilience; drastically reducing cybercrime; developing cyberdefence policy and capabilities related to the common security and defence policy; develop the industrial and technological resources for cybersecurity; establish a coherent international cyberspace policy for the European Union and promote core EU values. Ibid.

[59] Naziris (2014), p. 340.

[60] Directive 2013/40/EU of the European Parliament and of The Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

instrument provides some additional clarity regarding the term "cybercrime" in comparison with the Convention on Cybercrime and Framework decision as the term is crucial for the harmonization of national laws.

3 The Concept of Cybercrime

In a broad sense, cybercrime could be described as a "criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks".[61] The cybercrime "in the context of national security may involve activism, traditional espionage, or information warfare and related activities".[62] In a narrow sense, the cybercrime could be described as "any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them".[63] "Cybercrime can also be regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks".[64] Some definitions could cause difficulties: traditional offences could be covered by them[65] or some crimes which are considered as cybercrime under international treaties could be excluded from them.[66]

"Definitions" of cybercrime mostly depend upon the purpose of using the term. A limited number of acts against the confidentiality, integrity, and availability of computer data or systems represent the core of cybercrime. Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of

---

[61] Gandhi (2012), p. 1.

[62] Ibid.

[63] The challenge of borderless cyber-crime 2000. http://legal.un.org/ola/media/info_from_lc/cybercrime.pdf.

[64] Hale (2002) Cybercrime: Facts and Figures Concerning this Global Dilemma, Crime & Justice International 18 (65). http://www.cjimagazine.com/archives/cji4411.html?id=37.

[65] *The terms "cybercrime," "computer crime", "Information Technology crime," and "high-tech crime" are often used inter-changeably to refer to two major categories of offenses: in the first, the computer is the target of the offense; attacks on network confidentiality, integrity and/or availability—i.e. unauthorized access to and illicit tampering with systems, programs or data—all fall into this category; the other category consists of traditional offenses—such as theft, fraud, and forgery—that are committed with the assistance of or by means of computers, computer networks and related information and communications technology*. See Goodman and Brenner (2002), p. 9. http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf.

[66] *For example, a person who produces USB devices containing malicious software that destroys data on computers when the device is connected commits a crime as defined by Article 4 of the Convention on Cybercrime. However, since the act of deleting data using a physical device to copy malicious code has not been committed through global electronic networks, it would not qualify as cybercrime under the one of the definitions presented*. Gercke (2011), p. 28.

identity-related crime and computer content-related acts (all of which fall within a wider meaning of the term "cybercrime") do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term.[67]

Neither Convention, nor the Framework decision or the Directive provides a definition of the cybercrime as such. However, some presumptions could be made while applying systematic approach and assuming that cybercrime covers crimes enumerated in the aforementioned documents. For example, in the Convention on Cybercrime, four types of offences are distinguished:

- Offences against the confidentiality, integrity, and availability of computer data and systems[68];
- Computer-related offences[69];
- Content-related offences[70]; and
- Offences related to infringements of copyright and related rights.[71]

It should be stated that such differentiation is not consistent because new forms of crimes, which appeared after the announcement of the Convention, could fit into several categories: for example, phishing or cyberterrorism.[72] Also, the Convention does not intend to regulate cyber security which could be described as cyberthreats to national security: economic espionage, crime, cyberwar, and cyber-terrorism.[73] The Directive says even less regarding the definition of cybercrime as it provides just one category of offences, the ones against confidentiality, integrity and availability of computer data and systems and confirms the narrow concept of the cybercrime.

Probably, it is not possible and even worth to make a complete list of crimes which falls into the cybercrime category, because what is suitable today may be very old in the nearest future, or the definition could be so universal that it is too broad and vague to apply in practice. However, "if the multijurisdictional nature of cybercrime prevents us from even defining it, how can we expect to effectively prosecute it?"[74]

---

[67] Expert Group to Conduct a Comprehensive Study on Cybercrime, p. 6. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf.

[68] Article 2—Illegal Access, Article 3—Illegal interception, Article 4—Data interference, Article 5—System interference, Article 6—Misuse of devices. See The Convention on Cybercrime, Budapest, 23.11.2001.

[69] Article 7—Computer-related forgery, Article 8—Computer-related fraud. See The Convention on Cybercrime, Budapest, 23.11.2001.

[70] Article 9—Offences related to child pornography. See The Convention on Cybercrime, Budapest, 23.11.2001.

[71] Article 10—Offences related to infringements of copyright and related rights. See The Convention on Cybercrime, Budapest, 23.11.2001.

[72] Gercke (2011), p. 30.

[73] Nye (2010), p. 16. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

[74] Shinder and Cross (2008), p. 11.

Some scientists[75] suggest solving the problem while implementing the principles of equivalence[76] and technological neutrality.[77] These principles could be applied both at the national and international level and are proposed as a way of escaping from new non-regulated crimes. Applying the principle of equivalence, the usage of the same legal norms which regulate activity in the natural space could be applied in order to evaluate person's behaviour in the cyberspace.[78] In such situations, the priority is given to the interpretation of the law instead of the creation of the new legal norm. This could fill all the gaps which appear if new methods of cybercrime are invented. However, the principle of equivalence could not be used in all situations. There could be crimes which could not fit into any traditional crime definition.[79] Where the consequences of taking an activity online are qualitatively different from its offline equivalent, it seems likely that an attempt to achieve equivalence by applying the existing offline principles is doomed to failure.[80] "Equivalence is likely to be achievable only by conducting a review of the interests involved, both on- and offline, with

[75] The scientific research regarding these principles was done by the Marcinauskaite (2013), van der Haar (2007), Reed (2010).

[76] The principle of equivalence means that *general legal frameworks should be applied on-line as they are off-line*. Actuality of this principle in the criminal law means that it stops people from thinking that the cyberspace is different than the natural space and there are different law standards in it. *In the view of the speed at which new technologies are developing, they will strive to frame regulations which are technology-neutral, whilst bearing in mind the need to avoid unnecessary regulation*. See Declaration of the European Union Ministers, Global Information Networks: Realising the Potential (July 6–8, 1997, Bonn). http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm#Heading01.

[77] The principle of technological neutrality means that the law *neither imposes nor discriminates the use of a particular type of technology*. See Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=EN&type_doc=COMfinal&an_doc=2013&nu_doc=627. The principle of technological neutrality was also used in various Europe legal documents. For example: *The requirement for Member States to ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology*. See Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services. (7 Mar 2002). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:en:NOT.

[78] In a Memorandum entitled 'Legislation on the Electronic Highway' (1998), the Dutch government stated that the same norms have to be applied on-line as are applied offline. See Schellekens (2006), p. 3.

[79] For example, DDoS Attack (distributed denial of service attack–is an attempt to make a machine or network resource unavailable to its intended users) does not fit into any of the traditional crimes categories—it is not theft, burglary, or extortion.

[80] Reed (2010), p. 264.

the aim of developing new rules which can be applied in both situations".[81] The need for the new legal norms should be determined only after the examination of the existing laws.[82]

The importance of the principle of technological neutrality is mentioned in various international documents.[83] The term "technological neutrality" is used for description of a "legislative aim that the rules should not discriminate between technologies and should continue to be applied effectively even if new technologies are developed".[84] Such principle is especially relevant in defining the crimes as cybercrimes which are based on rapid development of technologies. The elements of crime should be described using neutral words and avoiding dependence on changing information and communication technologies, their features if such dependence is not a will of the legislator,[85] but sometimes could be difficult to establish in practice. While using the principle in practice also conformity with the principles of legality (nullumcrimen, nullapoene sine lege) and legal certainty should be ensured,[86] which means that "lawmakers should adhere to a more functional definition, solely relying on functional concepts, thereby leaving out all

[81] Ibid.

[82] Such position is upheld in the Explanatory Report of the Convention on Cybercrime. For example, it is stated: *Articles 7–10 relate to ordinary crimes that are frequently committed through the use of a computer system. Most States already have criminalized these ordinary crimes, and their existing laws may or may not be sufficiently broad to extend to situations involving computer networks (for example, existing child pornography laws of some States may not extend to electronic images). Therefore, in the course of implementing these Articles, States must examine their existing laws to determine whether they apply to situations in which computer systems or networks are involved. If existing offences already cover such conduct, there is no requirement to amend existing offences or enact new ones*. See Convention on Cybercrime, Explanatory Report, p. 79. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[83] Although the substantive law provisions relate to offences using information technology, the Convention uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved. Convention on Cybercrime, Explanatory Report, p. 36. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[84] *Such a rule might be devised only for online activities and is therefore not necessarily aiming at equivalence online and offline*. See Reed (2010), p. 249.

[85] It could be stated that criminal laws should avoid references to the concrete crime methods in the cyberspace (e.g. how the connection was made or in what method the damage to the information system was made), but the attention should be made to the result, which originates from such illegal activity (e.g. the activity caused a breach of the confidentiality of the information system or such system became unavailable to the users). See Marcinauskaite (2013), p. 28.

[86] *The principle of legality is a core value, a human right but also a fundamental defence in criminal law prosecution according to which no crime or punishment can exist without a legal ground. The principle is often associated with the attempts to constrain states, governments, judicial, and legislative bodies from enacting on retroactive legislation, or ex post facto clauses and ensuring that all criminal behaviour is criminalized and all punishments established before the commencement of any criminal prosecution*. See Crisan (2010), p. 2.

references to technologies".[87] Also, the extent of the technological principle is narrowed by other principles of criminal law which suggest avoidance of too broad and baseless criminalization of various activities.[88] It is evidentiary that principles of equality and neutrality even though give some valuable ideas are not the ideal solution.

4 Changes in Substantial Criminal Law: Comparative Analysis of the EU Directive

The main changes introduced by the Directive in comparison with the Framework decision and/or the Convention could be classified into several groups: (1) definitions; (2) substantial criminal law (both general and special part); (3) procedural matters (jurisdiction and exchange of information).

The approximation of national criminal law in the sphere of cybercrime could be evaluated as the first step in further harmonization of approaches in the procedural law and judicial cooperation.[89] The EU Directive makes substantial changes related to substantial criminal law issues. The main changes could be classified into several categories: (1) introduction of new crimes, criminalization of illegal interception (art. 6) and of tools used for committing offences (art. 7); (2) extension of aggravating circumstances (art. 9 Sect. 4); (3) changes related to accomplice liability, aiding, and abetting of crime (art. 8); (4) more binding requirements for sanctions (art. 9). All the enumerated changes could be classified into two big groups: the ones influencing special part of criminal law and those requiring changes in the general part of criminal law. In order to better understand the peculiarities of criminal law, the definitions provided in the Directive should be evaluated first.

4.1 Definitions

The Directive brings no substantial changes in comparison with the Framework decision as we could see from the table below. If compared with the Framework decision, the biggest change is that the legislator while defining information system is more precise indicating one device as sufficient (use both singular and plural forms in the definition of information system). The term "information system" used

[87] *A definition based on functional concepts implies that a definition is drafted in such a way that it describes the use or function of a technology, rather than referring to the technology itself. This way, a definition can "incorporate" the development of new technologies that can be used as substitutes for earlier ones*. See van der Haar (2007), p. 23.

[88] Marcinauskaite (2013), p. 35.

[89] Kaiafa-Gbandi (2012), p. 60.

Table 1 Definitions in convention versus EU instruments

Convention	Framework decision	Directive
Computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data	**Information system** means *any* device or group of inter-connected or related devices, one or more of which, pursuant to a programme, performs automatic processing of computer data, *as well as computer data stored, processed, retrieved, or transmitted by them for the purposes of their operation, use, protection, and maintenance*	**Information system** means *a* device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, *as well as computer data stored, processed, retrieved, or transmitted by that device or group of devices for the purposes* **of its or their** *operation, use, protection, and maintenance*
Computer data means any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function	**Computer data** means a representation of facts, information, or concepts in a form suitable for processing in an information system, including a programme suitable for causing information system to perform a function	**Computer data** means a representation of facts, information, or concepts in a form suitable for processing in an information system, including a programme suitable for causing information system to perform a function

Table 2 Definition "without right"

Framework decision	Directive
"**Without right**" means access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under the national legislation	"**Without right**" *means conduct referred to in this Directive*, including access, interference, *or interception*, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law

in the EU instruments as if indicates that its content should be broader than the term "computer system"; however, no such extension is provided in the definition itself. The definition remains vague as no explanation regarding the term device is provided. However, the EU terminology is broader, as the information system like the one in the Convention includes a device or group of devices, but differently from the Convention, it either includes computer data for the purposes of operation, use, protection, and maintenance of a device or group of devices. Probably, it should be evaluated as done for clarification reasons but not as significant changes because computer system becomes the threat for global community not because an offender has just some types of devices, but because of dangerous materials in these devices—various viruses, spam, programs, etc. (Table 1).

The Directive goes further than the Convention or Framework decision as it provides some guidelines regarding contents of the term "interception", expressly providing that it includes such activities as "*the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means*",[90] but the list is not exhaustive and there is space for a national legislator to interpret the concept.

There are minor discrepancies traceable in the definition of the term "without right" in comparison with the Framework decision which is not provided in the Convention (Table 2).

The Directive includes additional possible offence "Illegal interference" which should be treated as some technical novelty as this offence is introduced into the Directive and specifies that the term "without right" includes conduct referred in the Directive. In scientific literature, some fear from rule of law perspective is expressed that such a definition as if gives too much power to the owner and may impose some unfounded limits in the flow of information and infringe democracy,[91] however, almost identical definition was already provided in the Framework decision and no real infringements were established, especially that the Directive does not provide any regulations or interfere into the relations between service provider and the owner. These issues are regulated separately.

[90] Directive 2013/40/EU of the European Parliament and of The Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, par. 9.

[91] Kaiafa-Gbandi (2012), p. 69.

Table 3 Illegal interception

Convention (art. 3. illegal interception)	Directive (art. 6. illegal interception)
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. *A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system*	Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from, or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor

4.2 Novelties Introduced into a Special Part of the Criminal Law

The first novelty is Article 6 of the Directive, introducing a new offence-Illegal interception of computer data which resembles Article 3 of the Convention on Cybercrime, however, goes further as it does not provide discretion for a Party to base criminalization on *dishonest intent*, or *in relation to a computer system that is connected to another computer system* as was established in the Convention (Table 3).[92]

There is an opinion that convention "only proscribed 'illegal interception' committed 'with dishonest intent' or in relation to computer systems that are part of a network".[93] However, it is obvious from the wording of Article 2 of the Convention that such an exception is just one alternative offered by the Convention, but States have discretion to make such an exception or not, i.e. to exclude offences when they are committed without such an intent or to narrow criminal liability by requiring elements of *mens rea* (dishonest intent).[94]

The main difference in cited documents—allowed reservations to the parties. The main question arises how we should treat expression "which are not minor", i.e. should it be understood as a dishonest intent and/or that only such illegal interceptions should be punished which are done to computer systems ("botnets"). Obviously, the wording of Article 6 is very broad as it is not directly related with "mens rea", infringement of security measure or damages. Simple interception of computer data (e.g. just for curiosity reasons) may suffice. However, the right to

[92] The Convention on Cybercrime, Article 3.

[93] Naziris (2014), p. 340.

[94] Kaiafa-Gbandi (2012), p. 65.

decide which crimes should be treated as minor cases is left for the Member States. This issue may also raise some problems in future as different Member States may criminalize different actions. For example, Lithuania decided not to use minor cases exception as Article 198 of the Lithuanian criminal code establishes criminal liability (fine, or even maximum imprisonment for 4 years) just for illegal observation, recording, interception, acquiring, storing, appropriating, distributing, or otherwise using non-public electronic data, without requiring any consequences or some other factors. In case if such data are the ones having strategic importance for the state possible sanction- imprisonment up to 6 years.[95] Such a decision of the Lithuanian legislator may be questioned on the basis of the *ultima ratio* doctrine principle.

Introduction of criminal liability for tools used for committing offences defined in the Directive is treated as the most controversial norm and "less cautious" than the respective norm in the Convention (Table 4).[96]

The hacking tools are very similar in both documents and include computer programs for criminal purposes and the data, related to illegal access of computer such as computer password, access code, or similar data. However, the final text of the Directive excluding the phrase "devices"[97] (which is used in the Convention) may be evaluated as more limited taking into account rapid technological development. Linguistically, the term "device" is defined as a machine or piece of equipment that does a particular thing[98]; however, the term is not defined or commented in the explanatory note of the Convention, but some guidelines could be guessed from the explanation of a computer system and may include such means as processor, central processing unit, and peripherals such as printer, video screen, CD reader/writer, and storage device.[99] The guidelines for device reveal that probably the term computer program is more correct than a device as it is more narrow and precise. However, it leaves hardware devices out of the scope of the Article.

In the initial stage, mere possession of tools used for committing cyberattacks was treated as a criminal offence in the Directive as well as in the Convention, but after discussions in the working groups, the idea was rejected.[100] The research confirms the conclusion that criminalization and interpretation of the offence is based on *subjective criteria* which is rather difficult to establish.[101]

---

[95] The Criminal Code of the Republic of Lithuania, Art. 198.

[96] Naziris (2014), p. 341.

[97] Such a term was in the initial proposal but was not accepted by parties. See Note from Presidency to Council 8795/11. DROIPEN 27- TELECOM 43- CODEC 609, (8 Apr 2011) p. 6. http://db.eurocrim.org/db/en/doc/1512.pdf.

[98] See Macmillian dictionary. http://www.macmillandictionary.com/thesaurus/british/device#device_4.

[99] Convention on Cybercrime, Explanatory Report, p. 23. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[100] Note from Presidency to Council 8795/11. DROIPEN 27- TELECOM 43- CODEC 609, (8 April 2011) p. 2–3. http://db.eurocrim.org/db/en/doc/1512.pdf.

[101] Naziris (2014), p. 341; Kaiafa-Gbandi (2012), p. 68.

Table 4 Tools for committing offences

Convention (art. 6. misuse of devices)	Directive (art. 7. tools used for committing offences)
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: (a) the production, sale, procurement for use, import, distribution, or otherwise making available of: (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; (ii) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and (b) *The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches*	Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution, or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3–6, is punishable as a criminal offence, at least for cases which are not minor: (a) a computer program designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3–6; (b) A computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed
2. *This Article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution, or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system*	
3. *Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this Article*	

Table 5 Illegal access to information

Convention (art. 2. illegal access)	Directive (art. 3. illegal access to information systems)
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system	Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor

Some discrepancies are traceable regarding illegal access to information systems. The wording of Article 3 in the Directive is more binding as it does not include alternative discretionary factors (such as *infringing security measures, intent of obtaining computer data, other dishonest intent, or in relation to a computer system that is connected to another computer system*) provided both in the Convention and the Framework decision (Table 5).

But the Directive also provides some safeguards—in order to be treated as a criminal offence, it should at least infringe a security measure, i.e. cases where the information system (e.g. smart mobile phone, computer is not protected by password) is accessed, without infringement of such measures the Member State is not required to criminalize such an act. There is also discretion for a Member State to decide which offences are not minor. As there are no suggestions regarding the contents of "minor", Member States have at least some flexibility.

Introducing aggravating circumstances, the EU Commission aimed at tackling two new threats: large-scale cyberattacks and misuse of personal data[102] and these issues are not covered by previous instruments. However, the Article 9 of the Directive enumerates five aggravating circumstances: (1) use of botnets or similar tools; (2) crimes done by criminal organization; (3) causing serious damage; (4) committed against a critical infrastructure information system, or (5) identity theft. The enumerated circumstances are provided different weight as in cases when a perpetrator makes illegal system or data interference (art. 4–5 of the Directive) affecting a significant number of information systems using tools enumerated in Article 7 of the Directive, Member States are required to establish at least 3 years of imprisonment as a maximum sentence. The Directive is most flexible in the case of misusing the personal data of another person—it does not suggest concrete penalties and just offers to treat the fact as an aggravating circumstance in case it

[102] Note from Presidency to Council 8795/11. DROIPEN 27- TELECOM 43- CODEC 609, (8 April 2011) p. 4. http://db.eurocrim.org/db/en/doc/1512.pdf.

is not covered by other offences. For example, in Lithuania, such cases may be covered by fraud if they cause material damages (art. 182). Some flexibility was left intentionally allowing Member States not to cover cases which they consider not harmful to the protected legal interest. First of all, these are cases protecting young people trying to prove their experience in new technologies.[103]

For remaining three aggravating circumstances, the imprisonment of 5 years is required. But it may be a case that the use of botnets may be also punished by higher imprisonment sentence if any of the aggravating circumstances are established (e.g. was done by a criminal organization). The provision of aggravating circumstances and maximum sanctions is one step forward into harmonization of national laws; however, actual contents of every provided factor (such as *significant number of information systems, serious damages, critical infrastructure information system*) is rather subjective and their actual contents is dependent from a national legislator. For example, in one case, Lithuanian Court decided that a person is guilty for unlawful influence on electronic data (art. 196), incurring major damage and convicted the offender for four months of community service. The perpetrator intentionally destroyed a web page of a secondary school. The monetary damage was just 3,000 litas (869 euros) but the court argued that damages may also be moral, social, etc. The court based the decision on facts that the crime was done against an education and training institution, the web page was destroyed just before beginning of a new school year and it caused certain disadvantages to the school community and parents.[104]

4.3 Novelties Influencing General Part of Substantial Criminal Law

The Directive introduces several changes or supplements regarding general part of the substantial criminal law, such as changes in the regulation of complicity and strict provisions regarding criminal penalties.[105]

The institute of complicity in the Directive is rather unusual and very broad—the Directive requires establishing criminal liability even for preparatory acts such as the ones established in Article 7. Some argue that Article 8 of the Directive covers ordinary commercial activity in procurement of hacking tools.[106] However,

[103] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM (2010) 517 final, 30.9.2010), pp. 7–8. http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf.

[104] Ruling of Kaunas district court in Case No. 1A-94-175/2012, enacted on 22 Oct 2012.

[105] The question of jurisdiction, even though traditionally assigned to the general part of a substantial criminal law is not discussed as this issue is also closely connected with procedural issues.

[106] Naziris (2014), p. 341.

Article 8 requires "mens rea", i.e. that such commercial procurement is done with the intention that it will be used to commit any of the offences established in the respective Articles of the Directive, so the ordinary commercial activity could not be punished as lacking that element—intentional fault. Also, the principle of *non bis in idem* should be observed, which means that in order to hold some company or person liable the fault should be proved by state authorities (Table 6).

Criminal liability for the attempt, established in the Directive (art. 8, par. 2) is narrower than the one established in the Framework decision, but coincides with the requirements of the Convention as it requires punishing just for attempts to commit crimes described in Articles 4–5 (illegal system and data interference), while the Framework decision also requires to criminalize attempts to illegally access information system (art. 5), even though such a requirement is discretionary as could be ignored in accordance with the Article 5, part 3 of the Framework decision. But the Directive, in contrast to the Convention, does not establish criminal liability for attempt of illegal system interference (art. 3). It is difficult to evaluate unilaterally if such a provision makes any notable changes for national legislator. For example, in Lithuania, criminal liability for an attempt to commit any criminal offence is established in the general part of criminal law without any exceptions[107] and such a provision in the Directive would be an excessive one.

The establishment of guidelines regarding sanctions was one of the controversial issues, debated by Member States (Table 7).[108]

The Directive (art. 9) goes further than the Convention (art. 13) in specifying what sentences should be imposed for the criminal activities described in the document except Article 7 which is excluded from the requirement to provide a specific level of penalty established in the initial stage.[109] While Convention gives basic principles that penalties should be effective, proportionate, and dissuasive and including deprivation of liberty, the Directive provides suggested maximum term of imprisonment. The regulation in the Directive also differs from the one in the Framework decision, as penalties just for two crimes (illegal system and data interference) are suggested there and it leaves more discretion to the Member States as it provides some interval of suggested maximum penalty (from 1 up to

[107] Article 22 of the Criminal code of Lithuania states that an attempt to commit a criminal act shall be an intentional act or omission which marks the direct commencement of a crime or misdemeanour where the act has not been completed by reason of the circumstances beyond the control the offender. A person shall be held liable for an attempt to commit a criminal act according to paragraph 1 or 2 of this Article and an Article of this Code providing for an appropriate completed crime. A penalty imposed upon such a person may be commuted under Article 62 of this Code. See The Criminal Code of the Republic of Lithuania.

[108] States required to lower penalty up to 1 year or to establish alternative, provided in the Framework decision (from 1 up to 3 years of imprisonment). Note from Presidency to Council 8795/11. DROIPEN 27-TELECOM 43-CODEC 609, (8 Apr 2011) p. 3. http://db.eurocrim.org/db/en/doc/1512.pdf.

[109] Note from Presidency to Council 8795/11. DROIPEN 27- TELECOM 43- CODEC 609, (8 April 2011) pp. 2–3. http://db.eurocrim.org/db/en/doc/1512.pdf.

Table 6 Complicity and attempt

Convention (art. 11. Attempt or aiding and abetting)	Framework decision (art. 5 Instigation, aiding and abetting and attempt)	Directive (art. 8 Incitement, aiding and abetting and attempt)
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding, or abetting the commission of any of the offences established in accordance with Articles 2–10 of the present Convention with intent that such offence be committed Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3–5, 7, 8, and 9.1.a and c. of this Convention Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this Article	1. Each Member State shall ensure that the instigation of aiding and abetting an offence referred to in Articles 2–4 is punishable as a criminal offence 2. Each Member State shall ensure that the attempt to commit the offences referred to in Articles 2–4 is punishable as a criminal offence 3. Each Member State may decide not to apply paragraph 2 for the offences referred to in Article 2	1. Member States shall ensure that the incitement, or aiding and abetting, to commit an offence referred to in Articles 3–7 is punishable as a criminal offence 2. Member States shall ensure that the attempt to commit an offence referred to in Articles 4 and 5 is punishable as a criminal offence

Table 7 Criminal sanctions

Convention (art. 13 sanctions and measures)	Framework decision (art. 6 penalties)	Directive (art. 9 penalties)
1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2–11 are punishable by effective, proportionate, and dissuasive sanctions, which include deprivation of liberty 2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate, and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions	1. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 2–5 are punishable by effective, proportional, and dissuasive criminal penalties 2. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 3 and 4 are punishable by criminal penalties of a maximum of at least between one and 3 years of imprisonment	1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3–8 are punishable by effective, proportionate, and dissuasive criminal penalties 2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3–7 are punishable by a maximum term of imprisonment of at least 2 years, at least for cases which are not minor 3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 and 5, when committed intentionally, are punishable by a maximum term of imprisonment of at least 3 years where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, design adapted primarily for that purpose

3 years of imprisonment).[110] Such provisions of the Directive are being criticized as undermining the principle of proportionality and the inclination of the EU towards inflexible sentences.[111] But it is not the first time the EU provides such guidance regarding penalties. For example, in the Directive combating trafficking in human beings,[112] the same style for sanctions is used. Only the required maximum imprisonment penalty is higher—5 years and in the case of aggravating circumstances, it can reach even 10 years.[113] The principle of proportionality is better served providing the wider margin of discretion for Member States,[114] but still a lot of discretion is left as it is up to a Member State to decide what additional penalties and their limits to provide in addition to the required maximum penalty of imprisonment. For example, in Lithuania, the criminal code states that a person committing illegal system interference against information system of strategic importance for national security or of major importance for state government, the economy or the financial system shall be punished by a fine or by arrest or by imprisonment for a term of up to 6 years,[115] which means that the court has a wide range of sanctions and ability to provide a concrete sentence to the corresponding gravity of the committed offence.

The argument that issues regarding penalties "*show disregard of the ultima ratio and the proportionality principles*"[116] could not be accepted for the reasons described above.

As cybercrimes are modern crimes and almost impossible to fight at a national level, the efforts from the EU to harmonize national laws at least to some extent and help to fight such crimes should be evaluated positive as much as they respect the main principles of human rights.

It is concluded that the EU Directive is a positive instrument, reflecting the biggest threats related to cybercrime and should lead to better harmonization of national laws of the Member States, especially taking into account that Member States are not allowed to introduce additional constitutive elements of offences beyond the ones already included in the Directive and should refrain from adding additional constitutive elements to the basic offences.[117] However, its practical value could be estimated only in future, especially when there would be some

---

[110] Council Framework Decision 2005/222/JHA on attacks against information systems, Art. 6.

[111] Kaiafa-Gbandi (2012), p. 69; Naziris (2014), p. 343.

[112] Directive 2011/36/Eu Of The European Parliament And Of The Council On preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA. (OJ L 101/1, 15.4.2011).

[113] Ibid., Art. 4.

[114] Kaiafa-Gbandi (2012), p. 69.

[115] The Criminal Code of the Republic of Lithuania, Art. 197.

[116] Kaiafa-Gbandi (2012), p. 71.

[117] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM (2010) 517 final, 30.9.2010), p. 7–8. http://ec.europa.eu/dgs/home-affairs/policies/crime/1_en_act_part1_v101.pdf.

jurisprudence regarding the issue from the Court of Justice. The biggest drawback of the existing document—very limited geographical area—would be enforceable just among the Member States while most cybercrimes start in the third world countries and the Directive is not of much help.

5 Law Enforcement Cooperation and Capacity to Investigate in the Light of the New Directive

Main "forms of international cooperation include extradition, mutual legal assistance, mutual recognition of foreign judgments, and informal police-to-police cooperation".[118] However, the study done by the expert group of UN office on drugs and crime in 2013 revealed that for obtaining extraterritorial evidence in cybercrime cases still dominates traditional forms of cooperation—formal requests for mutual assistance and bilateral but not multilateral agreements which are slow and ineffective.[119] Such data, keeping in mind that evidence in cybercrimes could be moved or deleted in seconds, show the need for the improvement of international cooperation.

Gathering of evidence as one of the challenges when fighting with cybercrime was pointed out in the Explanatory Report of the Convention on Cybercrime: "*One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is the subject of a criminal investigation, thereby destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation*".[120] Strangely enough, the question of evidence collection was not given serious attention either

---

[118] *The use of traditional forms of cooperation predominates for obtaining extra-territorial evidence in cybercrime cases, with over 70 % of countries reporting using formal mutual legal assistance requests for this purpose. Within such formal cooperation, almost 60 % of requests use bilateral instruments as the legal basis. Multilateral instruments are used in 20 % of cases. Response times for formal mechanisms were reported to be of the order of months, for both extradition and mutual legal assistance requests, a timescale which presents challenges to the collection of volatile electronic evidence. … Modes of informal cooperation are possible for around two-thirds of reporting countries, although few countries have a policy for the use of such mechanisms.* It was also stated that *due to the volatile nature of electronic evidence, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialized investigative actions, such as preservation of computer data*. See Expert Group to Conduct a Comprehensive Study on Cybercrime, p. 10. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf.

[119] Ibid.

[120] Convention on Cybercrime, Explanatory Report, p. 133. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

in the Convention on Cybercrime, or in any of the discussed EU instruments.[121] The main focus is provided for describing methods of collecting such evidence, while much less attention is given to the collecting of evidence outside a state territory as it is the question of a state sovereignty. The existing procedural EU instruments do not solve this problem. For example, European evidence warrant[122] is only applicable to evidence which already exists and covers therefore a limited spectrum of judicial cooperation in criminal matters with respect to the evidence.[123] Due to the trans-border (manner) character of cybercrime, the new forms of cooperation between the states have to be invented. The first real steps were made in 2013 when the EU "Cybercrime Centre" based within Europol was officially launched.[124] In 2014, similar centre will be launched by Interpol.[125] The Convention, the Framework decision, and the Directive strengthen the importance of networks, of points of contact available on a 24 h, 7-day-a-week basis. But these network units cannot collect evidence—their main function is the assistance and facilitation of the exchange of the relevant information. Such process is an important step, but it is not a substitute for formal procedures.

The trans-border access to stored computer data is mentioned in the Convention of Cybercrime[126] and not in the Framework Decision or the Directive. In order to access such data, it must be publicly available or there must be consent from the person who has authority to disclose such data.[127] Other way to reach such data could be only by the request of mutual legal assistance. Such requirement is based on the rules of international law, which means that the national

[121] Council Framework Decision 2005/222/JHA on attacks against information systems; Directive 2013/40/EU of the European Parliament and of The Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[122] Council Framework Decision 2008/978/JHA on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (OJ L 350, 30.12.2008).

[123] Klimek (2012), p. 277.

[124] The main task of the European Cybercrime Centre is to disrupt the operations of organised crime networks that commit serious and organised cybercrime. Concretely, the EC3 supports and coordinates operations and investigations conducted by Member States' authorities in several areas. See European Cybercrime Centre. http://europa.eu/rapid/press-release_IP-14-129_en.htm.

[125] Media release: International cooperation key to fighting cybercrime, INTERPOL Global Complex for Innovation Director tells security meeting, 03 Apr 2013. http://www.interpol.int/News-and-media/News/2013/PR039.

[126] Article 32—Trans-border access to stored computer data with consent or where publicly available. A. Party may, without the authorisation of another Party: (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. See The Convention on Cybercrime, Budapest, 23.11.2001.

[127] The Convention on Cybercrime, Art. 32.

sovereignty[128] must be respected when carrying out investigations. Having in mind that most of the committed cybercrimes cross national boundaries of the states, the successful investigation of the cybercrime depends on the capability of other state to which the request is made. Europol or Interpol cybercrime centres could provide help, but knowing the amount of cybercrime such way seems unsatisfactory when fighting against cybercrime.

The requirement for the person's consent expressed in the Convention when performing trans-border access to stored computer data[129] shows that states who signed the Convention limited their national sovereignty, allowing foreign investigation officers carry out investigation in their state. The Convention does not require the involvement of official state institutions in such cases. A similar example allowing trans-border investigation could be used when investigating cybercrimes not in the territory of one state, but where cloud computing[130] is used. In the past, investigators were able to focus on the suspects' premises when searching for computer data.[131] Today, they need to take into consideration that digital information might be stored abroad and can only be accessed remotely, if necessary.[132] "*Data 'location', while technically knowable, is becoming increasingly artificial, to the extent that even traditional mutual legal assistance requests will often be addressed to the country that is the seat of the service provider, rather than the country where the data centre is physically located*".[133] For such reason, the laws dealing with the evidence in cloud centres should be reviewed, allowing direct access to such data for law enforcement authorities.

The tendencies in the legal area for successful fighting against cybercrime show that it is impossible to fight this phenomenon without successful cooperation between the states. The EU legislative initiatives are moving towards broadening

---

[128] The principle of national sovereignty does not generally permit a country to carry out investigations within the territory of another country, without permission from local authorities. *Sovereignty is the legal expression of the territorial political community's presumptive monopoly of the last word on internal public order. This entails more than merely the authority to give or withhold the consent to international legal obligations. Although the point is often misunderstood, sovereign authority continues to exist alongside legal obligation with respect to the very same subject matter*. See Roth (2005). http://www.law.uga.edu/intl/roth.pdf.

[129] The Convention on Cybercrime, Article 32.

[130] *Cloud computing and multi-jurisdictional crimes may challenge the traditional way of investigation and prosecution. Data in the "clouds" are data that are constantly being shifted from one server to the another, moving within or access different countries at any time. Also, data in the "clouds" may be mirrored for security and availability reasons, and could therefore be found in multiple locations within a single country or in several countries. Consequently, not even the cloud computing provider may know exactly where the requested data is located*. INTERPOL European Working Party on Information Technology Crime (EWPITC)—Project on cloud computing, 2011 *in* Schjolberg (2012). http://www.cybercrimelaw.net/documents/ICTC.pdf,p.10.

[131] Gercke (2012), p. 84. http://www.scribd.com/doc/206172213/18/Legal-challenges#page=9.

[132] Ibid.

[133] Expert Group to Conduct a Comprehensive Study on Cybercrime, p. 10. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf.

states jurisdiction in cybercrime matters.[134] Another proposal for the improvement of fight against cybercrime is European Investigation Order in Criminal Matters.[135] The Permanent Representatives Committee (COREPER II) on 3 December 2013 in Brussels confirmed the compromise text of the Initiative for a Directive on the European Investigation Order in Criminal Matters. It is assumed that European Investigation Order, which is based on mutual recognition principle, the cornerstone of judicial cooperation, would contribute to simplifying and facilitating the evidence gathering procedures in criminal matters.[136] The goal of the Directive is to set up a unified comprehensive system for obtaining evidence in criminal cases with a cross-border dimension.[137] The criticism of such initiative is based on the assumption that Directive would constitute a reduction in human rights protection and even (due to the abolition of the traditional "territoriality" exception) an attack on the national sovereignty of Member States.[138]

The initiatives for improving battle against cybercrime are also proposed not only at the European level. The Norwegian judge Stein Schjolberg, who is also the Chairman of the global High-Level Experts Group on Cybersecurity, thinks that without an international court or tribunal for dealing with the most serious cybercrimes of global concern, many serious cyberattacks will go unpunished.[139] The Cybercrime Convention "lacks an authoritative international body that could enforce the laws in the realm of international criminal law".[140] The draft of

[134] For example, in the Cybercrime Convention, the States had to establish jurisdiction over the crimes which were made in the state territory or by one of its nationals (Art. 22). See The Convention on Cybercrime. The Council Framework decision broadened jurisdiction including situations where the offence was committed for the benefit of a legal person that has its head office in the territory of the State (Art. 10). See Council Framework Decision 2005/222/JHA on attacks against information systems. The Directive corrected the cited Council Framework rule, establishing jurisdiction outside state territory where (a) the offender has his or her habitual residence in its territory; or (b) the offence is committed for the benefit of a legal person established in its territory. (Art. 12). See Directive 2013/40/EU of the European Parliament and of The Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[135] The European Investigation Order (EIO) shall be a judicial decision issued by a competent authority of a Member State ('the issuing State') in order to have one or several specific investigative measure(s) carried out in another Member State ('the executing State') with a view to gathering evidence within the framework of the proceedings referred to in Article 4. Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia, and the Kingdom of Sweden for a Directive of the European Parliament and of the Council of … regarding the European Investigation Order in criminal matters, Official Journal of the European Union, 2010/C 165/02.

[136] Permanent Representatives Committee Confirms Agreement on European Investigation Order in Criminal Matters, 03 Dec 2013. http://www.eu2013.lt/en/news/permanent-representatives-committee-confirms-agreement-on-european-investigation-order-in-criminal-matters.

[137] Ibid.

[138] Peers (2010). http://www.statewatch.org/analyses/no-96-european-investigation-order.pdf.

[139] Schjolberg (2012). http://www.cybercrimelaw.net/documents/ICTC.pdf.

[140] Wakefield (2012).http://hrbrief.org/2012/12/international-criminal-tribunal-for-cybercrime-and-human-rights/.

International Criminal Tribunal for Cyberspace (ICTC) Statute places it within the International Criminal Court, as stated in the Rome Statute establishing the Court, the "most serious crimes of concern to the international community".[141] But on the other hand, it is not clear how the defined cybercrimes meet the ICTC's jurisdiction, which generally covers the gravest breaches of human rights and the risk of additional restrictions to human rights increases.[142]

6 Conclusions

The fight against cybercrimes is becoming one of the priorities of the EU policy, while the treaty of the Lisbon equips the European Union with new legal tools/instruments in criminal matters including the right to provide minimum elements describing *actus rea and mens rea* of defined criminal offences which are reflected in the newly enacted Directive on attacks against information system.

The scientific analysis revealed that the new Directive continues the EU policy basically reflected in the Framework decision 2005/222/JHA and is compatible with the Convention on Cybercrime but is one step forward towards legislative harmony and is more stringent than the previous EU instrument—the Framework decision.

Introducing aggravating circumstances, the Directive tackles two new threats—use of botnets and identity theft which are not reflected either in the Convention or in the Framework decision. Two new offences, Illegal interference (art. 6) and Tools used for committing offences (art. 7), are either introduced into the Directive, and the last one is evaluated as the most controversial norm and less cautious than the respective norm in the Convention. Notwithstanding the fact that the Directive provides rather concrete and specific obligations, it also provides some flexibility for national legislator as a discretionary term "which are not minor" is used.

The institute of complicity in the Directive could be evaluated as very broad and requiring establishment of criminal liability even for preparatory acts such as the ones established in Article 7 of the Directive. Provisions, regarding sanctions, are one of the mostly discussed issues as they go further than the Convention or the Framework decision and require establishment of maximum term of imprisonment for certain offences which are criticized as undermining the principle of proportionality and the inclination of the EU towards inflexible sentences.

Successful fight against cybercrime requires good cooperation among states, especially gathering extraterritorial evidence. The Directive strengthens the importance of networks, of points available on a 24-h, 7-day-a-week basis, but does not solve the problem of evidence; however, the EU legislative initiatives are moving towards broadening states' jurisdiction in cybercrime matters.

---

[141] Schjolberg (2012). http://www.cybercrimelaw.net/documents/ICTC.pdf.

[142] Wakefield (2012). http://hrbrief.org/2012/12/international-criminal-tribunal-for-cybercrime-and-human-rights/.

Generally, the EU Directive is a positive instrument reflecting the biggest threats related with cybercrime and should lead to more successful harmonization of national laws of the Member States; however, the practical value could be estimated only in the future especially when some jurisprudence from the Court of Justice appears.

References

Books and Articles

Capus, N. (2007–2009). (Head of the research Project), *Sovereignty and criminal law: the dual criminality requirement in international mutual legal assistance in criminal matters*. Munich: Max Planck institute.

Choo, K.-K. R., & Grabosky, P. (2013). Cyber crime. In L. Paoli (Ed.), *Oxford handbook of organized crime* (pp. 1–31). Oxford: Oxford University Press.

Craig, P. (2010). *The Lisbon treaty. Law, Politics and treaty reform*. Oxford: Oxford University Press.

Crisan, I. (2010). The principles of legality "nullum crimen, nulla poena sine lege" and their role. *Effectius Newsletter, 5*, 1–3.

Gabrys, E. (2002). The international dimension of cyber crime. Part 1. Special issue coverage: Information warfare/cyber crime. *Information Systems Security, 11*(4), 21–32.

Gercke, M. (2011). *Understanding cybercrime*: *A guide for developing countries*. Geneva: International telecommunication union (Draft).

Gercke, M. (2012). *Understanding cybercrime: phenomena, challenges and legal response*. Geneva: International telecommunications union.

Gandhi, K. (2012). An overview study on cyber crimes in internet. *Journal of Information Engineering and Applications, 2*(1), 1–5.

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *UCLA Journal of Law and Technology, 6*(1), 1–153.

Hale, C. (2002). Cybercrime: facts and figures concerning this global dilemma. *Crime and Justice International*.18(65).

Rao I. J. (2011). Cyber crimes: issues and concerns. *Indian Stream Research Journal*, 1(X), 111–115.

Kaiafa-Gbandi, M. (2012). Criminal attacks against information systems in the EU: The anticipated impact of the European legal instruments on the Greek legal order. *European Journal of Crime, Criminal Law and Criminal Justice, 20*(1), 59–79.

Klimek, L. (2012). Free movement of evidence in criminal matters in the EU. *The Lawyer Quarterly, 4*, 250–290.

Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly, 31*(7), 1057–1079.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. UK: Palgrave Macmillan.

Marcinauskaite, R. (2013). Criminal offences against the confidentiality of electronic data and information systems (Criminal Code of the Republic of Lithuania articles 198 and 198(1)). *Doctoral Dissertation*, Vilnius.

Naziris, Y. (2014). 'A Tale of Two Cities' in three themes—A critique of the European Union's approach to cybercrime from a "power" versus "rights" perspective. *European Criminal Law Review, 3*(3), 319–354.

Nye J. S., Jr. (2010). *Cyber power, belfer center for science and international affairs*, Harvard Kennedy School.

Peers, S. (2010). *The proposed European investigation order: Assault on human rights and national sovereignty*. Statewatch analysis.
Procedda, M. G. (2011). Transatlantic approaches to cybersecurity and cybercrime. In P. Pawlak (Ed.) *The EU–US Security and Justice Agenda in Action*. Chaillot Papers.
Reed, C. (2010). Online and offline equivalence: Aspiration and achievement. *International Journal of Law and Information Technology, 18*(3), 248–273.
Roth, B. R. (2005). *State sovereignty, international legality, and moral disagreement*, Updated Version of Paper Presented at the Panel on "Questioning the Aspiration to Global Justice" Annual Meeting of the American Political Science Association.
Schellekens, M. (2006). What holds off-line, also holds on-line? *Starting Points for ICT Regulation, Deconstructing Prevalent Policy One-liners*, *IT and Law Series*, 9, 51–75 (T.M.C. Asser Press: The Hague).
Schjolberg, S. (2012). *An International Criminal Tribunal for Cyberspace (ICTC), Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes*. A paper for the East West Institute (EWI) Cybercrime Legal Working Group.
Shinder, D. L., & Cross, M. (2008). *Scene of the cybercrime* (2nd ed.). USA: Syngress Publishing Inc.
Sommer, P., & Brown, J. (2011). Reducing systemic cybersecurity risk, OECD/IFP Project on *Future Global Shocks*, Oxford: Oxford University.
Storm, P. (2013). *The effect of negative publicity on consumer loyalty*. Wageningen: Wageningen University and Research Centre.
Van der Haar, I. M. (2007). Technological neutrality; What does it entail? Tilburg Law and Economics Center (TILEC). *Discussion Paper No. 2007-009*, pp. 1–28.
Vasiu, I., & Vasiu, L. (2013). The cybercrime challenge: Does the Romanian legislation answer adequately? *Law Review III, 2*, 42–51.
Wakefield, M. (2012). *International criminal tribunal for cybercrime and human rights, human rights brief: The center for human rights and humanitarian law*.

Official Material

Commission of the European Communities, Growth, Competitiveness, Employment. (1993). The Challenges and Ways forward into the 21st Century. White Paper, (COM(93) 700, December 5 1993).
Communication from the Commission to the European Parliament, the Council and the Economic and Social Committee and the Committee of the Regions, Creating a safer information society by improving the security of information infrastructures and combating computer related crime, (COM(2000) 890 final, January 26 2001).
Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, Towards a general policy on the fight against cybercrime, (COM (2007) 267 final, May 22 2007).
Convention on Cybercrime, Budapest, November 23 2001.
Convention on Cybercrime. Explanatory report. ETS 185, November 8 2001.
Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography. (Official Journal L.13, January 20 2004).
Council Framework Decision 2005/222/JHA on attacks against information systems, (OJ L69, February 24 2005).
Council Framework Decision 2008/978/JHA on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (OJ L 350, December 30 2008).
Declaration of the European Union Ministers, Global Information Networks: Realising the Potential (July 6–8 1997, Bonn).

Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. (Official Journal L 178, July 17 2000).

Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services. (March 7 2002).

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. (Official Journal L 201/37, July 31 2002).

Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC. (Official Journal L 105, April 13 2006).

Directive 2011/36/Eu Of The European Parliament And Of The Council On preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA. (OJ L 101/1, April 15 2011).

Directive 2013/40/EU of the European Parliament and of The Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, (OJ L 218, August 12 2013).

eEurope initiative and eEurope Action Plan (1999).

European Commission, Special Eurobarometer 390, Cyber security Report, (July 2012).

Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council of … regarding the European Investigation Order in criminal matters, (Official Journal of the European Union, 2010/C 165/02).

Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, (JOIN(2013) 1 final, February 7 2013).

Norton Cybercrime Report 2012.

Note from Presidency to Council 8795/11. DROIPEN 27- TELECOM 43- CODEC 609, (April 8 2011).

Ponemon Institute, 2013 Fourth Annual Cost of Cyber Crime Study: Global Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM (2010) 517 final, September 30 2010).

Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. (COM(2013) 48 final, February 7 2013).

Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No. 1211/2009 and (EU) No. 531/2012.

Recommendations to the European Council, Europe and the global information society, The Bangemann Report (May 26 1994).

Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems (COM (2008)448 final, July 14 2008).

Symposium on the occasion of the signing of the United Nations convention against transnational organized crime, panel on “The challenge of borderless cyber-crime”, Palermo, Italy (December 14 2000).

The Lisbon Treaty, (Official Journal C 83, March 30 2010).

United Nations Manual on the prevention and control of computer-related crime (1990), International review of criminal policy.

Case Law: European Court of Justice

Case C-105/03 Criminal proceedings against Maria Pupino. Judgement of the Court (Grand Chamber) (16 June 2005).

Case Law: Kaunas District Court

Ruling of Kaunas district court in Case No. 1A-94-175/2012, enacted on October 22 2012.

Reflections on the Concrete Application of Principles of Internet Governance and the Networked Information Society in the European Union Institutionalization Process of Alternative Dispute Resolution Methods

Maria Claudia Solarte-Vasquez

Abstract This chapter represents an effort to link concepts that appear to be and are commonly placed in distant theoretical areas but belong much closer together in practical terms: the principles of internet governance, and the networked information society converging in rules on one hand; and self-regulation competences required for collaborative and alternative conflict management on the other. They condense the public and the private roles in compatible regulatory models that could match sociability, economics and technologies of the times. It is an essay on competences, public policies that are not preceded by standards and principles that do not seem to have been captured by the laws. The institutionalization strategy on Alternative Dispute Resolution (ADR) and Online Dispute Resolution (ODR) for cross-border consumer redress in the European Union will be the reference to assess regulatory impact and argue for consistency. Legislating ADR and ODR aims at supporting electronic commerce as an essential component of the digital agenda; the flagship initiative that establishes the digital single market according to the European 2020 Strategy. Questions must be raised considering the marked emphasis placed on promoting social changes merely by passing new laws. The importance of understanding that the European Union is not capable of supplanting its members in turning institutional formulas into operational strategies is underlined, as well as a reflection on the need to support the social and economic transformations that have followed the remarkable developments in telecommunications and other digital technologies. Conceiving a European dispute resolution culture, enabled and mediatized by technological solutions is a viable solution to prevent more of the perceived shortcomings of public actions, and a truly innovative ODR systems design, could support the transition. This text invites the integration of concepts, disciplines and practices, respect for principles

M.C. Solarte-Vasquez (✉)
Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia
e-mail: mcsolartev@gmail.com

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_12

and their consistent application to solutions that could improve human transactions for a sustainable digital economy where empowered private actors can efficiently contribute to the ongoing collective transformations of the global governance.

1 Introduction

The internet is a mature technology, not the only one in the information and telecommunication technologies catalogue, but the first reference that led to the configuration of a global communication network.[1] Few nowadays are interested in answering more questions about whether it has to be ruled or not, and who could do it; the focus has shifted towards resolving issues on the how, to which effect and on whose behalf? Traditional formulations are being redefined with the adoption of new technologies by the networked information society, while others, and new ones are created to protect emerging structures and institutions. This describes a pragmatic revolution on values. Information, for instance, is at the top of both lists.[2] This section of the book departs from the premise that information is a right that ranks at the level of life, freedom and property, featuring strong in the hierarchy among other fundamental rights.

Information and Communication technologies (ICTs) and cybernetics are components of an "assembly" process between products and intelligent life that associate human capacity and people's identity with technology. Some could argue that this represents the beginning of a symbiotic relationship between humans and machines, starting with the handling of rights traditionally defined by personality laws being transferred and delegated to networks, recorded in virtual storage databases and administered by cluster managers.[3] Put in a less dramatic way, not a sector of the society is immune to the impact of the internet and other Telecommunication Technologies; in as long as "connected." ICTs have demonstrated power to transform societies, communities, groups and people in their most intimate affairs; they link the world efficiently and distribute data in massive quantities at a negligible cost, resolving many important institutional governance

[1] Mobile technologies are leading the expansion of the digital economy and interconnectivity in the world; their use continues to raise, and its platforms replace rapidly some of the services that the personal computers used to provide. The figures that the International Telecommunications Union publishes on its webpage speak by themselves: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[2] The value of information is not as disputed as it has been theorizing about it in the human rights context. Information could be also seen as externality to fundamental rights such as dignity and equality or an indispensable mean to achieve the exercise of rights that are affected by the internet and other telecommunication technologies. For an instance on how this discussion is proposed see: Tiilikka (2013).

[3] The rights of the personality (as defined by the civil law tradition) that are being compromised include the following among others: honour, reputation, identity, authorship, intimacy, privacy, etc. Electronic databases and registries, especially when handling sensitive information are not neutral containers exempt of worth, as the section written by Kristi Joamets explains.

difficulties (responsiveness and transparency), but not all; and most logistic problems that the world faced allocating resources in a not so distant past: the cost of innovation diffusion and spreading (copying), distribution, reach, and delivery. It is in this light that ICTs are drivers of development and at the same time the cause of great concern. These technologies are at the service of the networked information society and constitute the promise for a sustainable economic growth sourced on knowledge and information. The digital economy represents an expectation of continuous innovation and generation of immaterial resources that are available to all willing and competent innovators and entrepreneurs, to be exchanged and commercialized at large scales. At the same time, institutional arrangements of the past are challenged through a newly established dialog that has intensified in recent years around topics on global governance, laws and technology, digital rights, and cyber security and defence, mainly. Traditional roles of states and governments have shifted, governance processes became reflexive and at all levels interaction and collaboration have intensified.[4] Academics and technical experts, activists and institutional representatives, have been advocating in favour of institutional capacity building and the development of responsive and effective regulatory structure for the cyberspace.[5]

While awareness is raised, strategies that could effectively reduce the struggles focused on hierarchy and control are still missing. Technology management is problematic at best, especially for legislators that regulate to attain and sustain policy goals by laws that address human problems with technical solutions; technologies enhance people's capacities but do not deliver on their own. Nonetheless, they provide us with numerous supporting affordances, some of which remain undetected or unexplored. Part of the difficulties are caused by the restrictive conceptualization of the ICTs governance. Unlike most of the literature in the field, the study of their structural governance here is not viewed as orthogonal to the field of applications, content, users and interfaces, but integrated to it. It follows that private regulatory capacities and responsibilities of all private actors are acknowledged. Viewed this way, ICTs governance would be an extended notion, including the activities of private entities that are not associated to the technological sector, and all ICTs users.

It could be said that there is an adequate amount of technical digital wisdom to move on and proceed with innovation in governance and regulation for sustainable growth and human development. Many of the disputes about internet governance patterns are already settled and its most general principles have crystalized. The same applies to the Information and internet society. A combination of institutional formulations compete for a position in legal and political doctrine but few classifications capture the deeper sociological and political features that characterize human organizations of the networked information age. The European scholarly

[4] Look into: http://www.intgovforum.org/cms/2012-calendar.

[5] Some of the panels of the Global INET 2012 are recorded and available online at: http://www.livestream.com/inet2 One of them discusses the rule of law and Internet.

environment is enriched by the experience of its own integration process and the economic experiment that has translated in numerous political, social and cultural innovative adjustments. This so to say "experiential regulatory process" (formal and informal), could also turn into a paradigm for association, collaboration and co-regulation (multi-layered governance and subsidiarity principle). Most importantly, Europe has become a forum of great consensus, commitment and political responsibility and at the same time the only fully functional regional organization in the world. However, with the addition of the digital layer as critical resource, enabler, medium and environment, the European action has met considerable challenges.

In this book, the digital agenda, one of the flagships initiatives of the agenda 2020 for Europe, is on focus, and this chapter looks deep into one specific aspect of its e-commerce strategy: Alternative Dispute Resolution (ADR).[6] Conflict management and dispute resolution are not the core of any policy but merely instrumental to some, despite of how revealing they are known to be in diagnosing society tensions and the interplay between informal institutions and the legal system. On the other hand, it is a field that has enjoyed independence, where its actors could find the space to thrive and develop at the personal and organizational levels. Hence, the importance of attending these micro-spheres where institutional influences could effectively unleash a manifold of constructive interactions that multiply as people act at the upper organizational levels. In the aggregate this genuine development could be considered more stable and reliable than one based on statistics and compliance with external prescriptive controls. These reflections draw from self-regulation theories that also emphasize the importance of autonomy (freedom) and confidence.

Below, an expanded view of the current European ADR rules will be proposed, arguing that the global economy of the networked information society, packed as is with opportunities for interaction and gain for those who possess the appropriate skills, is incompatible with formalism, rigour and constraints. Transactional models based on the evolution of the ITCs should favour integrative gains, understanding, collaborative global action and dynamic institutional structures.[7] Implementing a new conflict resolution culture the world wide is too ambitious, but considering the EU success in other fields, a regional initiative could be successful. The most

[6] See for more information: http://europa.eu/rapid/press-release_MEMO-14-194_en.htm and http://ec.europa.eu/justice/effective-justice/files/cepj_study_scoreboard_2014_en.pdf with facts and figures about the Study of the functioning of judicial systems in the EU Member States. ADR has been closely linked to the justice system function and could be relevant for its improvement. Indicators on this respect are included in the Digital Agenda Scoreboard (2014), addressing the training of judges, evaluation of court activities and availability of special resources such as Information and Communication Technologies and ADR methodologies.

[7] Dynamic rules that could be adjusted according to further and faster technological advancements and the differing capabilities of the many possible actors would represent a step forward in the disentanglement of the socio-political labels of the times. Such flexibility is not compatible with regulatory systems affected by the constraints of the rule of law doctrine. On this respects, consult: Baldwin et al. (2011) and Levi-Faur (2011) on regulations and regulatory governance in general; Gibbons (1996) on different types of regulations depending on their agents; and Trubek (2007) reflecting on the transformations of the legal rules and new patterns of governance.

recent regulations on ADR and ODR have a signalling value. They must be coupled with efforts on the non-normative consolidation of values, practices and traditions of collaborative dispute prevention and resolution, and conflict management. It should also be made extensive to all fields relevant. Otherwise, expectations on their economic and social impact will continue to be unmet.

In sum, the present qualitative and interdisciplinary assessment of doctrine is combined with a critical assessment of the European regulatory policy and its legal developments in the field of dispute resolution. It considers sociological, political, legal and economic aspects that link the preventive legal approach, conflict management and ADR methodologies. It starts describing the wider context were this discussion begins to shape: the networks. Then, the information society that has evolved with ITC technologies and also participates in the formulation of rules, attending to its needs, interests and emerging principles. Next, self-regulation and other conflict management competences are connected to ADR methodologies to continue with a summarized review of the European legal and policy frameworks on redress and ADR applicable to cross border disputes. An assessment of the continuous institutionalization process and its direction towards the use of electronic solutions and Online Dispute Resolution methods (ODR) is left for last. The chapter ends with implicit proposals, to replace overregulation with informal institutionalization; and the trends of exaggerated protection/control with support for the empowerment of human self-determination. Parsing these issues could contribute to the formulation of a -*collaborative*- European dispute resolution culture, where issues of system design linked to the increasing mediatisation of communication could be the next range of topics to be highlighted by research.

2 The Greater Context of the Digital Economy: Internet Governance

Responsible regional governance and the comprehensive integration process in Europe are not estranged from the global governance evolution. These arrangements develop with the internet and other telecommunication technologies. The two are part of the networked information society, where every player has a stake and becomes an actor of differing capacities, and according to their own interests, priorities and responsibilities. The European Union is but one more of the global stakeholders and the leading agents of the reflexive governance prevailing at the regional level.[8] In an interconnected world mediatized by technology expansion and resonance take place; the concerns of some become the worries of all. Every "node" of the network has the capacity to influence all others.

[8] Reflexive governance is a recent concept that refers to a self-critical and iterative form of inclusive and participative administration of affairs. It questions static and rigorous roles and goals and implies that the institutions that apply it are constantly transforming through learning. This represents a concrete strategy in the field of laws and government for the creation of better rules. Consult Hendriks and Grin (2007) and Voss et al. (2006).

Internet governance is concerned with a diversity of objects, corresponding to its layers, the technical composed by its infrastructure or architecture (including all critical internet resources)[9]; and its applications and the social and organizational that relates to its content and management. The architectural layer is not immune to policies and regulations, but relate very little to the aspects of social interaction that this text aims to highlight. Internet governance can be studied from the institutional point of view,[10] and its social impact, particularly in the fields mediatized human development, intercultural interaction and communication.[11] The information society concept relates to these last aspects in particular and deal with priorities that the World Summit of the Information Society (WSIS) establishes.[12] Technology, applications and content together compose a broad view of interrelated and fundamental issues that call for regulatory attention, in the same way the laws and politics of the analogous words penetrate practically all aspects of human interaction. Internet governance could be seen as the background policy making and regulatory development of the information society, which implies interconnectivity via any of the ICTs available technologies.[13]

In earlier stages of scholarly debate, discussions differentiated the layers that compose ITCs little, Nowadays much more sophisticated reflections are available, allowing for more precision and insight on the capacity of the actors and effectiveness of evolving regulatory systems regarding each. Furthermore, extreme positions in regard to ruling and governance are now rare; Mueller explained well the polarization between cyber-libertarianism and cyber-conservativism of those days.[14] On one hand, it is recognised that the early success of the nascent ITCs technologies was possible because of their "unregulated" or rather "non-intervened" nature. On the other, the internet, one of the two most popular ICTs, organized from its beginning oblivious but not entirely detached of structure and regulations. These are still progressing towards a complex and dynamic regulatory framework. In other words, regulations have always applied to the networks even if, as in any innovation cycle, specific institutions did not exist and its evolution was informal and independent.[15] This could have been the first agreement on inter-

[9] Electronic resources including to level domains, IP addresses and the Internet root zone. On Internet layering and its regulatory implications see Solum and Chung (2003). Solum was one of the first authors conceptualizing in a cross-disciplinary way on the ICTs engineering aspects affecting regulatory systems.

[10] Institutions is used in this context in its organic meaning, referring to entities with different degree of involvement and power influence and control the networks, including the Internet Corporation for Assigned Names and Numbers (ICANN) and its supporting organizations.

[11] By mediatized it is meant the use of tools, mainly ICTs as mediums in human interaction.

[12] See details on the WSIS 2014 online at: http://www.itu.int/wsis/implementation/2014/forum/.

[13] See Sect. 2. According to Marta Poblet (2011), mobile technologies are critical enhancers of this participation, scoring first in the range of solutions to bridge the digital divide. This could be the reason why the public sector focuses so heavily in the engineering part of these processes.

[14] See Mueller (2002). See also DeNardis (2010) on the controversies and issues that were the most controversial at the time.

[15] Taking place in all innovation cycles according to Utterback's (1996) reference work: *Mastering the dynamics of innovation.*

net principles ever settled. The issue now is not whether regulation is necessary or desirable, but on its qualitative effects: What type of rules are needed and how should they be created? All other matters with relevance for the global and international policies related to Internet governance, are redundant or rapidly changing, but could eventually become additional principles.[16] For the purposes of this chapter, the following simplified classification would suffice:

The *first general principle* of internet governance is regulability; it operates based on normative and other regulatory capacities, and has become in fact one of the most organized components of the global digital environment.[17] More *specifically*, *on its architecture, important principles* that could be identified *are interoperability and internationalization*. The first implies that technologies are compatible and support each other's components and services into one integrated system that rather differentiates at the level of applications, but also has to do with standardization. The second means that the design of specifications, applications and content should ensure usability or adaptability regardless of cultural or regional contingencies. *On other layers* principles manifest on the networked information society interaction, but the most important are *cooperation and increasing self-regulation*.

The *second general principle is transparent and democratic –inclusive-multi-stakeholderism*, summarizing all existing ranges of participation and views on the distribution of power, control and action,[18] attending principally to the challenges

[16] Other so-called principles have been issued in declarations by multilateral organizations and other independent entities interested in raising awareness about their goals and interests. Among them for example, The Internet Engineering Task Force (IETF) that oversees internet standards development processes; The International Telecommunications Union (ITU), a United Nations agency involved with internet governance functions that include developing of standards, quantitative assessments (statistical) and research (Internet Governance Project, 2004); the Internet Systems Consortium; the United Nations Educational, Scientific and Cultural Organization (UNESCO); etc. The list of public, private and mixed organizations that work on this area and perform functions of Internet governance at the national, regional, and international levels continuously grow. For a detailed overview, see Internet Governance Project, 2004; see also Mueller (2004).

[17] The Internet is a partial approximation to the digital world as a whole. It refers only to some of the Information and telecommunications technologies, but also invokes the presence of the Information Society. ICTs and the Information Society cover areas outside of the strict domains of the internet and its protocols but the expression "internet governance" will continue being the reference to all activities resembling but not equivalent to governing the network of networks. The internet protocol (IP) is the most important of the communication technical standards. Mobile technologies compete with it, and expand rapidly, but have not yet displaced the importance of the Internet. On figures concerning these issues consult documents and publications online at: http://www.internetsociety.org/igf?gclid=CNTdguL-lr0CFcuWtAodjgEAAA and statistical databases in the ITU website.

[18] The requirement that internet governance should be conducted according to multi-stakeholder principles was first stated at the WSIS summit of 2003; despite its wide acceptance it is not clear to what extent it shoudl constitute by now a norm of customary international law. See for a current publication on its development: http://www.internetsociety.org/sites/default/files/bp-msfinal-report-20132010-en.pdf. See also *Infra* note, 22.

in regulatory practice identified by abundant academic literature.[19] A formula of success should resemble a compromise between traditional normative systems and cyberspace rules; centralization and decentralization; protection of old values and consideration of the new[20]; geographical and virtual jurisdictional options; and formal and informal institutionalization processes, including the capacities and competences of actors that may become most useful.[21] Multistakeholderism should continue to speak of participants and their entitlements, but also include reflections on their commitment and skills, for functional accountability. Ample documentation describes the ways in which scholars and other private actors were the initiators of dialog, validating the importance of self-organizing operational patterns for the early networks and their establishment. Only after the commercialization of the internet, its exponential expansion, and growing interests vested in the potential of a global digital economy, governments and intergovernmental international entities claimed a voice.[22] The extent of the role of the public sector in deliberative internet governance still attracts controversy. Governments as "newcomers" have operational difficulties in adapting to their position in the global scenery where regulation by laws, the most prevailing tool of governing functions, is of limited capacity, legitimacy, validity and effectiveness.[23] Stakeholders in IG are the civil society with action at community levels, the private sector committed to the economic and technical maintenance of the networks (ICANN belongs here), International Governmental Organizations (IGO) in charge of coordination of policy, International Organizations (IO) that propose technical standards and their policy support, and states, that retain mandate on

[19] The formulation of dynamic rules, and innovative normative solutions that could combine adaptability, flexibility and openness is preferable to attempting to force regulatory uniformity, and even coherence of rules in a context so complex, polycentric and changing.

[20] For instance information pairing life, freedom, and property in the catalogue of human rights doctrines or/and the construction of a social order of the networks with their own description of public goods, etc. These reflections are owed to a multitude of authors from an interdisciplinary background on laws, politics, sociology and economics. From classic texts such as Mill (1859) on liberty; to very recent essays such as Misztal's (2013) about trust and social order.

[21] In here, the references to formal institutions regard laws, statutes and all normative options that follow the rule of law doctrine. Informal institutions in contrast, are all other regulatory systems that condition, affect and influence human behaviour. This approach is presented using expressions that resemble sociological, organizational and managerial terminology, with a purpose. Their use is explained in detail by Solarte-Vasquez (2013) in *Regulatory patterns of the internet development: Expanding the role of private Stakeholders through Mediatized "Self-regulation"*.

[22] A summarized primer on the history of internet was also proposed by Solarte-Vasquez (2013). *Supra* note, 20. But many more are available in popular and academic literature.

[23] The rule of law in democratic systems operates through legislative development, controlled public policy and laws as equalizers of legal systems (to comply with the material requirement of legal integrity, that laws must be general and abstract, and prevent fuzzy, arbitrary rule). See for a recent publication on the rule of law: Barnett (2014).

policy making and legal authority.[24] This global partnership began shaping with the WSIS and the creation of the United Nations (UN) Working Group on Information Society (WGIS) and the Internet governance Forum (IGF) for policy dialogue. These groups engage on an ongoing formulation and revision of the most important issues in internet governance.[25] New topics and principles could emerge, as was the case with the critical internet resources that in 2007 became a category on its own.[26]

Multistakeholderism had to be recognized for a system of interconnected networks of global proportions that promised the advantages of development, growth and knowledge dissemination. It still has a widespread impact in the sphere of the information society, placing extraordinary strain on traditional human organizational patterns, transactional models based on competition and exclusion, and cultures. *The information society* follows a logic premised on a *fundamental principle* that interdisciplinary research admits "must distance from the concepts of efficiency, operational effectiveness, and Pareto-optimal allocation applicable to hierarchical systems and markets[27]:" that is, *collaboration*.[28]

The third consolidated principle of internet governance is *neutrality*. Its discussion escalated as it evolved and subdivided in derivative institutional developments connected to open access and security, debates on human rights protection, inclusion, etc. In the European Union, adherence to this cornerstone principle is fundamental in all it purports in regard to all technical and political components of ICT governance. It involves transparency, non-discrimination in traffic management of information and content. In 2011, The Netherlands pioneered, enacting the first law ever establishing net neutrality, followed by Slovenia. At present the Commission is taking bold steps to legislate in the same direction, with the promise to set up net neutrality rules by July of 2014.[29] Keeping accord with an understanding of these technologies as critical and indispensable for human development, their protection from ideology, politics, economics, and other unaccountable influences compares to some of the components of the rule of law. Academic research could explore this analogies much further.

Other so-called internet governance principles have been issued in declarations by multilateral organizations and other independent bodies interested in raising

---

[24] The text of the Tunis agenda for the Information society is available online at: http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

[25] In Gelbstein and Kurbalija (2005). Issues of internet governance used from the late nineties are like clusters that infrastructure and standardization, legal aspects, economy, and developmental and socio cultural.

[26] *Supra* note, 14.

[27] On Sørensen et al. (2012). Where the authors assess in detail meta-governance tools for institutional design, strategic planning, methodologies and process management, and direct participation.

[28] Consult the social theory for the information age by Christian Fuchs.

[29] EU open Internet Action: http://ec.europa.eu/digital-agenda/en/eu-actions.

awareness about their goals and interests.[30] But for the most part efforts are comparable, forming a rather consistent global system of governance, this is why the UN-sponsored IGF provides adequate context for any analysis. European Organizations and the European Union endorse the same principles, running parallel processes.[31] To keep raising the levels of mutual recognition by all actors in the global regulatory process is necessary for validation. This stages a productive dialog and becomes a precondition for effective associations and cooperation as it occurs to all human relations, no matter how complex might be.[32]

Parsing the problems of internet governance could go through a regression towards theoretical discussions on normative, economic or social choice, but the pragmatic perspective that has prevailed on the web 2.0 would be lost; anyway, most participation models that coexist share and mix conceptual justifications. Progress could better be achieved if keeping general postulates simple and focus on functional matters. The ICT issues that differ most from those in other policy contexts are unique; most of them this approach will claim, are more deeply connected to human capacities and development than to political ideology or legal science.

3 Principles of the Networked Information Society and the Vital Role of Private Stakeholder's Activities in Institutionalization Processes

Internet and ICTs governance is not only a political economy topic, and although is rooted in longstanding public policy discussions it is intimately related to society. Objective considerations such as its global scope and factual observations on the predominant character of its management are not enough assessment tools to justify formal institutional initiatives or explain informal institutional changes.[33] Enough has also been said about reviewing a simplistic conception of technological determinism. Instead, a perspective that offers the most generous analytical

[30] See from the Council of Europe the "*Declaration by the Committee of Ministers on Internet governance principles* (Adopted by the Committee of Ministers on 21 September 2011"available online at: https://wcd.coe.int/ViewDoc.jsp?id=1835773 for an example of engagement of other bodies concerned with the same interests.

[31] In the international aspect of the digital agenda for Europe, the commission explains its endorsement of the multistakeholders principle. Read on Action 97 online at: http://ec.europa.eu/digital-agenda/en/international/action-97-promote-internationalisation-internet-governance. See also Da Silva (2007) on what the future of ICTs was envisioned like according to the EU public policy of the time.

[32] Conflict management theory is extensively referenced in ADR literature, for instance by publications of the Harvard Negotiation Project and associated scholars. Visit their webpage for further information at: http://www.pon.harvard.edu/category/research_projects/harvard-negotiation-project/. Also see: Ramsbotham et al. (2011) and Deutsch et al. (2011).

[33] Laws and social development of practices, habits, etc. See also *supra* note, 19.

possibilities departs from the social theory.[34] This section explains a choice of viewpoint that is themed on the skills revolutions that transcend information and knowledge, based on some of the postulates of critical theories and calls nowadays' society the information and/or networks society.[35] Presented this way, it is possible to reach further towards the individual levels where the interplay between technology, and the possibilities of engagement unfold an enormous range of opportunities. What could be missing to enter an age of the person, so to say, seems to be authentic empowerment.[36]

The raise of the information society resulted from a quantitative rapid and exponential increase in circulating information, and qualitative transformation of social practices and human interaction affected by the apparent chaos of a dispersed authority model.[37] The information society could be seen as an umbrella term containing more specific definitions such as the internet society. Both apply to interconnected human organizations that experience a pervasive technological mediatisation and participants in the digital economy. Manuel Castells has defined it in terms of network society rather than information society, placing the most emphasis on the fact that the construct appeals to interdependence and performance flow, without excluding economic aspects of production and consumption of information, but referring to the historical record on that all societies function on the basis of information and knowledge of their corresponding time, and that these determine wealth and power according to the given system of distribution. Consequently, the human capacity enhancement that contributes to the networks truly depends on their operational –*distribution*-capacity, much in the same way electricity made the expansion of the industrial society possible, that is, information technologies empower and enable; but people develop. "A network society is—a society—whose social structure is made of networks powered by microelectronics-base ICTs."[38] Castells extensively

[34] Ideas about how societies change, ways to explain social evolutionary development, about methods of explaining social and behaviour, power and other deep structures. In contemporary social theory, some themes are of primary concern: socialization, social interaction, social institutions and the self, the possibilities and paths of social transformation. Look into the theory in Giddens work on *Social theory and modern sociology*, published in 2013. A prominent author is Jürgen Habermas (1987) who theorizes on modernity and contemporary problems (very interestingly assessing the doctrine of the rule of law in a critical "social-evolutionary context," and current politics, particularly in the German context). Habermas's theoretical approach emphasizes in the possibilities of reason and emancipation as human capacities.

[35] No strict and universal definition of society has been universally accepted. In literature and doctrine. Information or network society is a choice that suits the theories justifying the present analysis and the conclusions that it draws. The two are used interchangeably throughout this text merely for convenience, without negating the differences that some scholars like Castells have conceptualized on the matter.

[36] See Sect. 3.

[37] *Supra* note, 33. A marked degree of involvement, more regulatory diversity, co-regulation, consensus building, regulatory innovation and implementation, new partnerships, withdrawal of public intervention from some areas, self regulation, etc. These all require freedom, and discipline (self-reliance).

[38] Castells (2004).

discusses the matter in the context of globalization and social movements related to individual identity."[39] Christian Fuchs contributes with arguments about a dynamic theory of society that like every human system, he claims, is self-organizing in the sense that a new arrangement emerges from the old. This, in turn implying that the capacity and agency of its members are essential components of a permanent grass-roots movement of cooperation.[40] For contrast on the validity of a single notion on information society, Webster argues that the most popular definitions of the society affected by the ICTs portray unwarranted social discontinuities, and that they are too vague and copious in the use of references to aspects so different that escape a minimal sense of precision: He elaborates on the way it has been explained by proponents from the occupational, technical, spatial, economic and cultural perspectives, arguing that this last is the most popular approach while in the case of authors who deny its independent features explain society features as continuities of traditional theories such as in the cases of reflexive modernization (Giddens), Neo-Marxism (H.Schiller), or regulation theory (Aglietta).[41]

Besides the many theoretical models available, important institutional references are common and many, all referring in detail to initiatives on the engagement of society in global affairs, and promoting their participation. International, regional and national entities have identified their focus and priorities and formulated their own vision on the information society. The following are but illustrative examples: In the international level the UN and International Telecommunications Union (ITU) resolutions on the WSIS in general[42]; and more specific in connection to the digital economy (e-trade) like the Seoul Declaration that relates to developments in the field of customer engagement at different instances.[43] Regionally, among the principles of internet governance declared in the 2011 by the Committee of ministers of the Council of Europe is the empowerment of

[39] His famous 1,200 pages publication on the information age has even been compared to Max Webber's Economy and Society by Giddens; the trilogy includes: The Network Society, The Power of Identity, and End of Millennium (Castells 1996, 1997, 1998).

[40] Supra note, 26. Fuchs on the Internet and Society, and a social theory in the information age. He is not a radical determinist but considers that new phenomena deserves innovative assessments in combination with traditional social sciences methods. He is a proponent of a critical theory in regard to ICTs and society. See also Hofkirchner (2007) on more of self-regulatory theories and critical theory in connection to the networked society.

[41] Find a complete reasoning in his article: Webster (2002).

[42] Texts and developments are available in the WSIS webpage at: http://www.itu.int/wsis/documents/background.asp?lang=en&c_type=res. Additional documents, reports and follow up reviews are also accessible on the same webpage at: http://www.itu.int/wsis/index.html. The WSIS declaration of principles can be found at: http://www.itu.int/wsis/docs/geneva/official/dop.html.

[43] See the OECD website for information on policy and recommendations on the internet economy: http://www.oecd.org/internet/ieconomy/, information economy: http://www.oecd.org/sti/ieconomy/measuringtheinformationeconomy.htm and consumer policy in context: http://www.oecd.org/sti/consumer/consumersinthedigitaleconomy.htm.

internet users.[44] The European Union has a much more sophisticated commitment the field of participation in regional governance and economic development, this last converging in the digital agenda for Europe, referenced more in detail below.[45] An explicit customer policy strategy was set even earlier to empower EU customers[46]; replaced by a new European Consumer Agenda, and complemented with numerous related commitments also on areas outside the economic context.[47] Besides, the formation of virtual and global communities, and a kind of "experiential governance" performed by digital activism disseminated mainly though social media, evidences the informal institutionalization patterns that are configuring collective, democratic and coordinated civic action. The society refines its participation style as it becomes more experienced, as in "learning in the making."

The information society participates in the internet governance system. Within the institutional framework that was proposed above, its activity relates most closely to the *regulability* principle on its applications and content layers, because it includes institutional cooperation practices and self-regulatory competences and *multistakeholderism* principle, which sheds some light about the nature of society's constructive and active roles. To integrate the diversity of understandings on the information society, some principles could be introduced. Most of them reflect the substance of the WSIS "key principles of the information society for all."[48] Agreement on these essentials would contribute to science with a theoretical, empirical and institutionally grounded approach that could embrace multidisciplinary and evolving understanding of social phenomena.

The information society principles that could guide the protection of a sustainable networked society could be summarized in three groups: The first would seek

---

[44] The principle reads: "Users should be fully empowered to exercise their fundamental rights and freedoms, make informed decisions and participate in Internet governance arrangements, in particular in governance mechanisms and in the development of Internet-related public policy, in full confidence and freedom." The full text is availableonline at: http://www.coe.int/t/informationsociety/documents/CM%20Dec%20on%20Internet%20Governance%20Principles_en.pdf.

[45] Information society as a concept was already mentioned in official documents a decade ago when the transition to the digital knowledge-based economy was starting to be a priority. In fact, the launch by the Commission of the *e*Europe initiative took place already in 1999, followed by the eEurope2002, the eEurope2005, and the i2010 and most recently the Digital Agenda (DA). This last is part of the Europe 2020 strategy, aimed at the optimal development of the potential of information and communication technologies (ICTs), to promote innovation, economic growth and progress. One of the most relevant pillars on inclusion and empowerment is Pillar VI. Actions that support it are explained in detail online at: http://ec.europa.eu/digital-agenda/en/our-goals/pillar-vi-enhancing-digital-literacy-skills-and-inclusion. See also Sect. 4.

[46] European consumer policy strategy 2007–2013, available onlineat: http://ec.europa.eu/consumers/overview/cons_policy/doc/EN_99.pdf.

[47] The full text of the Agenda is available at: http://ec.europa.eu/consumers/strategy/docs/consumer_agenda_2012_en.pdf. Consumer empowerment, according to it, is based in four pillars related to safety, knowledge (awareness), enforcement and redress, and alingnment between policy and socio economic change. A working document on knowledge enhancement is recommended, also available online at: http://ec.europa.eu/consumers/strategy/docs/swd_document_2012_en.pdf.

[48] See *supra* text accompanying note 40.

to realize the ideological vision of the times: *participation*: all inclusive, deliberative, proactive, associative, reflexive governance (making extensive use of regulatory impact assessment tools); The second, *empowerment*, defining the priorities for the vision's proper development: freedom, trust in the own's other's and state competences, confidence in the system and processes, skills, knowledge, self-regulatory capacities, non-deterministic dependence of technology but control of the ICTs resources and solutions; and last, attending to the tactics and methods that are compatible with social processes, *cooperation*: promotion of the binding force of collaboration, trust, methodical, productive connections, networking. The focus on media, and technology must shift to one more balanced were the society can have control over those resources and its own processes, aware of its potential and preventing exclusion and the prevalence of disputes and division that have characterized recent societal manifestations, some of which are still resisting change.[49]

The extent to which a critical theory is implemented in this analysis of the information society is limited but valuable. The critical theory Fuchs has brought forward is convincing in its lack of conformity and desire for social change. It considers alternative ways to develop society by exposing its potential, departing from its essence and looking into bridging the differences between what it "is," and what it "could become."[50] His concerns on the unrealized *–democratic*-participatory possibilities of social arrangements are of chief importance; it could be added that they presuppose freedom and the institutionalization of civil liberties. Also cooperation and sharing for the public good. Critical information theory is much more complex, for example, according to Fuchs, it must guide a social struggle, heavily drawing from the Marxian approach.[51] But the most relevant contributions to this section is that empowerment is needed to achieve social goals, and these, could be realistically measured by the potential of society. The struggle to succeed would be the most efficient if it takes place through enlightenment of people, along with the development of ethics more

[49] This would be the case, for instance of the property law structures that are deeply challenged in their formulation, legitimacy and applicability by the new digital economy logic of abundance, difussion and egalitarian forces. Authors like Fuchs consider that networks oppose ownership and compel the atomization of captalism, as networks are expansion and redistribution of resources and with them, of power. Information being the most important comodity in this context and the content that provides the mediums with meaning. Networks are in essence a negation of individual ownership and the atomism of capitalism. Global economic networks and cyberspace.

[50] Fuchs *supra* note, 37.

[51] Marx's works [in particular reflections from his economic and philosophic manuscripts: Marx (2012), interprets Fuchs, talk of cooperation as the concerted use of resources and socialization for the purpose of liberation. He also explains that cooperation could be an objective dimension of an ethic that strives for self-realization and inclusion through self-determination, instead of competition and abuse that would lead to the gain of some at the expense of others. In this sense, Marx ideology indeed suggests that competition separates men from their essence. Although cooperation at least theoretically would maximize the chances for success, collective action can also degenerate, and so the benefits of leaving collaboration to the hope of being inherent to society is dangerous. It also denies individual competences and characteristics. Cooperation can be taught from a very pragmatic point of view of convenience and sharing of risks and responsibilities like it is proposed in the field of Conflict Management and Alternative Dispute Resolution, but cannot be imposed. Collaboration, as most legal systems of the world establish, is voluntary and manifests through instruments like agreements.

consistent with the networks. Movements on cooperative information society, and cooperative cybernetics have proliferated in the past decade. Capurro, for example, also grounds his theory on the social sphere and assigns to the networks ethics a primordial task of advancing freedom for the digital world.[52] The Convergence Model of cooperative cybernetics that Bradley developed exhibits additional values. She has argued that a good ICT society is one that seeks equality and the common good, develops from the bottom-up, performs integratively and is humane.[53]

An ideological view of the layers of the internet and ICTs that are in contact with the end users is present in contemporary new media discourse because of the management of access, flow and identities that converge on the Web 2.0 concerning all players and combining all stakes. Governance actors should incorporate this approach and institutionalize accordingly. It is at this level, very close to all users turn into producers that the democratization of society can take place, but in as much as a transformative power could be applied to technologies, before the semantic Web 3.0 unfolds in a social "regression" process where it would effectively place all control on the networks.[54] Without complete empowerment of all stakeholders, it would be difficult to reach a stage of value that is both powered by self-structured and generated information and enhanced human participation.

4 Information Society Empowerment Though the Enhancement of Self-regulatory Capacities and Its Practical Applicability in the Field of Conflict Management

The global network society changes at a different pace if to study each of its dimensions separately: the tools provided by technologies of the times are unevenly distributed. Many institutional agreements on *economic structures* (production, distribution and use of resources) appear to contradict some *political structures* (governance), and advancement tends to disregard the differing capacity of *cultural structures* to absorb change. Scale is one of the most obvious reasons why homogeneous and coordinated development is challenging. Nonetheless, the logic of the networks gradually penetrates all, to a different degrees of success. The contradictions that arise in the assessment of global and regional social institutions makes proposing new institutional formulations by policy or legislation convenient. There is a clear incentive to regulate, and a high risk to overdo it.

Social change is too affected by resistance, a natural attachment to the "old ways" as well as to the corresponding competences that are already acquired by

[52] Capurro and Hjørland (2003).

[53] For a complete look into the social informatics field consult Bradley's convergence model in: Bradley (2010) and (2006).

[54] This evolution signals the integration of data that presuposes the semantic web 3.0, highly collaborative, proactive and constructive. It would lead to the management of content by the web, enabled to recombine data and information and understand it, in a way an "smart" entity capable of processsing content intelligently using data mining processes. For an accessible explanation of the semantic web, consult: Yu (2007). On the future of an integrative Web 3.0 see: Gruber (2008).

experience. Laws and policy could prevent fragmentation with more careful consideration of these factors, to help a smooth transition where the bonds of society could be strengthen or at least preserved. A bottom up approach has always been valued, it is a pragmatic and effective way to influence compliance with laws and appreciation for policies. This is especially true in Europe where the governance scheme is founded on reflexive processes, and the regulatory action seeks to take place at the closest possible distance to the subjects and their problems or interests.[55]

To focus on what would constitute effective social empowerment, the role of private internet governance stakeholders must be reviewed in detail. This takes place at the intersection between the social and behavioural sciences and ICTs. In accord to the principles proposed above on ICTs governance and the networked information society, the way in which this analysis propose coordination requires that public institutions endorse and promote freedom of contract, self-reliance, self-regulation and cooperative skills/competences. These aspects may be partially resolved with a drastic return to basics in legal theory as in the doctrines on freedom of contracting when it was first conceptualized.[56] This, for the creation of a private order that goes beyond merely organizing the production and distribution processes to where it seems most needed: an order that can integrate differences, manage conflict and resolve disputes effectively. Conflict management features resulting on ADR methodologies are purely based on voluntary engagement, and effective as long as they are practiced according to their integrative principles. Self-regulation competences are recognized by the legal system and most recently acknowledged as a fundamental component for the success and sustainable development of the digital economy in Europe.[57] They influence conflict management styles and the effectiveness of ADR methodologies. The same could be said of ODR schemes if these are not solely mediatizing traditional formal processes.

4.1 Self-regulation and Human Competence

The notion of empowerment that is presented here is a buzzword in the general public policy debate about ICTs governance. Gaining control, power, helping our selves, achieving describes the meaning of the word. Empowerment has become a precondition to be active in the highly cooperative networked information society that places much more responsibilities on private groups and individuals than other forms of social, legal economic and political systems existing before. A way to institutionalize new interactions is to innovate with rules and practices. New

[55] The principles of EU conferral, subsidiarity, proportionality are some of the Union's founding principles. Read more in the EU webpage at: http://europa.eu/scadplus/constitution/competences_en.htm. See also *supra* note 6 on reflexive governance, and the writings on political communication: Jessop (2003).

[56] Recommended classical reference books on freedom of contract, among the many available are: Mensch (1981), Kessler and Fine (1963) and Pound (1909). With a more recent application of perspective in: Reichman and Franklin (1999) and Haufler (2013).

[57] *Infra* note, 81.

rules should be dynamic, adjustable, and new practices could begin from the adoption of preventive, reflexive and proactive legal and political principles.[58] If to solve new problems with older tools instead, recognizing the dangers of overregulation is especially important. The benefits of predictability and stability should be balanced with the need for flexible and effective governance.

Empowerment is a concept that has to be evaluated much further, grounded on the different fields where it is required. Here it is going to be framed within the broader theory of self-regulation, and linked to personal autonomy and motivation. Cooperation, which logically would refer to more than one individual or group does not exclude but compels the contribution of independent parties towards achieving same goal. Similarly, participation is essential when describing associative interaction considering that it is about involvement and engagement, becoming part of a collective process. Thus, capacity is a component for any agent to be meaningfully linked to regulatory processes.

Self-regulation is also the root of the civil law systems, the clearest explained through the laws and principles of the law of contracts and obligations reflected in constitutional level provisions on individual freedoms.[59] Freedom to contract being of paramount importance to define the extent to which a person in the legal

[58] The proactive law approach is an innovative vision interested in integrating preventive law philosophy, ADR principles and contract management. It develops by influence of the Nordic School of Proactive law (http://www.proactivelaw.org/) that supports its theoretical and practical developments. Consult the works of Helena Haapio, and also, for instance: Sorsa (2009).

[59] Examples of the principle of contractual freedoms are explicitly established in legal systems around the world, and in particular in constitutions and civil codes and legal acts that are based in the Napoleonic code of 1804 (Spanish, German and Swiss legislation have their roots in the Roman Law tradition of the 19th Century just as most of the civil law codes across Latin America that uphold to the maximum the principle of freedom of contract). Article 1134 of the French Civil Code, reads: "Les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites. Elles ne peuvent être révoquées que de leur consentement mutuel, ou pour les causes que la loi autorise. Elles doivent être exécutées de bonne foi." See also some examples on the Spanish Constitution Art.8 and art.53, and art.1255 of the Spanish Civil Code; German Constitution art.2(1) and its law of obligations (albeit its dramatic changes in favour of a new consumer protection oriented policy to modernise a civil code first enacted in the year 1900. The reforms entered into force in 2002, marking a path in the direction determined by supranational legislation); Chilean Civil code art.1545, Colombian National Constitution of 1991 articles 13 and 16; Colombian Civil code art.1602 (valid contracts constitute law between the parties); an example of jurisprudencial reasoning on this respect is also available online at: http://www.corteconstitucional.gov.co/relatoria/2008/c-1194-08.htm.), etc. Doctrinal development of the principles can be found in classical reference texts such as in Ourliac and de Malafosse (1969) and Pothier et al. (1839). Robert H. Small. T. Jurisprudencial sources and doctrine have also developed the theory in connection to the economic system of free markets where commerce is expected to flourish auspiced not by the state but by private agency and the market forces. In Europe, most recently, the law of obligations and contracts has found a harmonizing option in the so-called consumer protection laws. These specific developments aim at restating and diffusing precisely what the traditional values that were already present in legislations of member states guarantee on individual freedoms and the co-regulatory power of private persons. Only, that consumer protection laws establish limits and specific protection measures that aim at empowering the population and enhancing their trust in the system. In sum, in a legal system where economic freedom is promoted, the state must facilitate private regulatory activities through legally enforceable agreements that permit an efficient exchange of products and services.

system is entitled to create and modify rights and duties that are enforceable.[60] This topic deserves a deeper -*but brief*- reflection that can be explained by exploring self-determination theories, the importance of which resides in the extent of the impact that legislation can realistically have on people's behaviour. Legitimacy of rules and effectiveness of regulations have everything to do with the degree to which subjects can identify with norms, and how institutional formulations can or have to be incorporated to behaviour. People are more prone to comply with rules that are "their own," rules that match with their individual or collective sense of obligatoriety. In the organismic dialectical perspective of Deci and Ryan, it is only when the environment supports autonomy that integration of behaviour and relevant regulation is conducive to effective and constructive self-regulatory action. They also explain the relevant causalities between formal and informal institutions and self-determination, taking into account different theories such as the Basic Needs Theory, that connects action with wellbeing, and mental health supported by the works of Kasser, Sheldon, Ryan and Reis, Roscoe, Chirkov, Hayamizu and Tanaka, etc.[61] Drawing from their work, one could deduct that restrictive institutional arrangements could undermine people's sense of competence, autonomy and relatedness. As a result motivation for compliance and performance can be—*proportional*—the direct consequence of the capacity allowed by a social and legal system and how much it achieves a sense of competence.

Empowerment, thus, acquires meaning only if it translates on allowances to exercise free will and self-determination; the acknowledgment of the importance of free will is to recognize an ontological reality of human beings and the existence of subjective rights. ADR Methods do that in the field of conflict management, one that contributes the most to a peaceful, harmonious society. The ICTs have heightened and increasing interest in ADR methodologies, especially for economic agents. First, commercial transactions in the open geography of the networks pose jurisdictional challenges that ADR can solve, but most importantly, they promote integrative, collaborative solutions consistent with the spirit of the times. In Europe, where all the focus has been placed on economic arguments and emphasis is so explicitly reduced to consumer and trade, the potential of the field in terms of human and social development seems to have been trivialized. On one hand, any institutionalization of ADR is welcome and useful, if to call attention about its benefits. On the other, the confined space where it has been developed and the formalities assigned to its practices could be misleading. No empirical study is available on that people in general will embrace unfamiliar forms of dispute resolution just because they exist; not even when formally institutionalized. Furthermore, in the cyberspace, people and institutions could be less inclined to trust systems that are not common, as well as incapable of implementing the tools necessary for their successful application.

The 2007–2013 EU Consumer Policy Strategy, sets as its main objective "to empower EU consumers." It also assigns importance to understanding consumers'

[60] For a contemporary analysis consult also the doctoral thesis by Soro Russell (2012), and in connection to ADR, Julio (2012).

[61] As referenced By Deci and Ryan (2012).

behaviour and promoting autonomy by advocating free choices, accurate information, transparency of the markets, and the institutionalization of their rights and their effective protection.[62] Although these priorities are set to be based on indexes for qualitative assessment, first they are limiting, and second, they do not consider the overall capacity of society to respond to such expectations, reflections of independence and freedoms.[63] Outside remained the fundamental dimensions on freedom, self-reliance and confidence from the side of the institutions and the population on their self-regulatory power. In addition, one more challenge for public policy and legislative development is over institutionalization, or the excessive reliance on that regulations can significantly alter human development and social behaviour on their own. The capacity of rules is much more limited whereas the possibilities of a constructive conflict management culture diffusion through indirect public action and informal institutional development could be much greater.

4.2 Applications of Private Regulatory Capacities

ADR methodologies belong to the study and theory of conflict, where most of the most reputable and well known scholarly work can trace its origins to (Menkel-Meadow 2000). Negotiation and mediation are the most collaborative and independent types whereas conciliation utilizes the law as the primary standard for decision making and arbitration closely resembles traditional adjudicatory processes. The use of ADR methodologies is anyway based on free will and consent because at least in their purest forms, they can be used only when the parties voluntarily agree on their application, or on an outcome that results from their methods (to include the cases where mediation and conciliation are integrated to judicial processes and they are compulsory). Negotiation is a universal activity; all people negotiate, on daily basis, with or without noticing. It takes place in disregard of skills, awareness or acknowledgement. Negotiation is the core collaborative method in the conflict management and ADR fields. Gerard Nierenberg discussed the importance of attending to negotiation styles in everyday life from the late 1960s.[64] His views included a comprehensive description of negotiation explaining that it includes any exchange aiming at transforming relationships. From his time, and after the ADR movement re-emerged four decades ago, it has been agreed by scholars and practitioners that the skills that effective negotiators

[62] Consult the Monti report, available online at: http://ec.europa.eu/bepa/pdf/monti_report_final_10_05_2010_en.pdf.

[63] The Directorate General of Health & Consumers and the Directorate General Joint Research Center created a unique measure of consumer empowerment named the Consumer Empowerment Index. It considers three main dimensions: *Consumer skills*, *Awareness of consumer legislation* and *Consumer engagement*, claiming that it encompases the concept.

[64] Gerard Nierengberg (1968) is considered to be the father of the art of negotiation, his book "The art of Negotiating" popularized the discipline.

should possess are not limited to the cognitive but most importantly related to the emotional and conative transferable social abilities that could influence relationships. Thus, this understanding speaks of competences, rooted on personal development that cannot be transformed without critical efforts at accepting certain ethics, adopting its models and revising personal attitudes, and beliefs systems.[65] A twofold argument results from here: first, it is not likely that the more we use alternative methods, the better we perform; second, formal institutionalization of ADR methods per se has no power to affect society and conflict resolution styles positively. It follows that to develop a complete (in the operational meaning, sustainable) legal system linked to people, besides the use of its regulatory capacity it has to reflect sociological facts. Conscious adoption of ADR principles is also possible, and could be supported by policies and general civil laws.

The regulation of ADR processes is the subject of debate. Proposers argue that it compliments consumer protection legislation, preserves important principles by the establishment of deterrents and sanctions, and protects other legal rights. Opposers believe that it not possible to impose non-adversarial forms of dispute resolution against their own ethics of voluntariety, stiffing the process and reclaiming authority over an arena that is and should continue to be managed privately. To preserve the essence of integrating and associating methods for dispute resolution, the logic of adjudicatory processes, certainty, formalism, and focus on the outcome should be kept distant. Until very recently the legislator had little incentive to intervene, or did it as a co-regulator to back up when required, for instance by providing remedies to the breach of contracts or allowing avenues to action for liabilities in the absence of agreements.[66] Some societies have been acquainted with these methods, and states very supportive of their functioning. Countries with long standing tradition of ADR are the United Kingdom, Sweden, Netherlands, Canada, Australia, etc.[67]

The convenience of ADR methods has been measured in terms of cost, efficiency, preservation of vital relationships, close control of the processes and outcomes, flexibility and confidentiality. They match the innovation requirements of the times, with their constant generation of responses to conflict. Although they have been around for long, they could be considered to belong to the group of regulatory innovation. Others are for instance the movement on preventive law, dynamic/reflexive law and the proactive legal practice. All of which share a spirit much more consistent with internet governance and networked information society principles than traditional processes, in that they are collaborative, flexible, seek to satisfy the self and common interests (by integrating instead of distributing) attending to the core of conflicts, have the capacity to resolve rather than solely settle a dispute, are associative and are not affected by the constraints imposed by the doctrine of the rule of

[65] Thompson (1990) and Gelfand et al. (2011).

[66] Extra contractual responsibility or its equivalent in the Common Law Legal Tradition: tort. See the two approaches in the following texts: Schlechtriem (1988) and Tolsada (2001).

[67] These are the places where theoretical developments have also been most prolific.

law. These methodologies overcome the flaws of competitive dispute resolution mechanisms and focus primarily on reaching a common understanding.[68]

4.3 The Influence of Conflict Management Styles and the Information Society on the Effectiveness of ADR Methodologies

ADR methods are procedural solutions but are not reduced to the designation of a simple sequence of neutral events.[69] Besides their methodological relevance, these processes are rich in substance, and communicate identifiable conflict management styles.[70] Countries with ADR tradition also have a sophisticated conflict management approach that commonly embraces a principle based negotiation -also called collaborative, associative, or integrative- style.[71] In contrast, it is common that competitive negotiation styles prevail where no ADR tradition exist or when ADR is institutionalized by law or through mimetic organizational efforts. Nonetheless, the skills and competences required for transformative conflict management can be learned, much more so when people are growingly interconnected, exposed to constant cross border interaction and realizing the convenience of collaboration over competition in negotiating their transactions and resolving their disputes. ADR is trendy, gaining popularity as word on its benefits spreads, in particular because it can accommodate differing social, legal and cultural determinants and overcome the same type of barriers.

The real value of ADR resides in its transformative power by creating a sense of self control (empowerment) and the effect of recognition (participation). Individuals are restored their independence to gain confidence and strength to solve their problems and decide on their personal affairs. Well guided and informed collaborative ADR processes can produce stable, friendly and efficient outcomes; it is a truism in the conflict management field that these characteristic define a successful result (which could be an enforceable agreement or a peaceful disassociation) and facilitate compliance.[72] This describes non-intrusive methodologies that could eventually incorporate the use of technical tools so that the

---

[68] Explained in detail in Solarte Vasquez (2014).

[69] *Ibid*., 66.

[70] For a recent approach on the specifics of assisted negotiation consult Wall and Dunne (2012), and on the relativizing the influence of style in the field of assisted negotiation, a study by Wall and Kressel (2012). See also Ross and Stittinger (1991) writing on the wiser context of dispute resolution

[71] In the conflict management literature from the Harvard negotiation project and on, the terms, adversarial and associative, positional and principled and destructive and constructive are also of common use.

[72] Essentials on the negotiation theory studied and proposed by Ury and Fisher. See also *infra* note, 77.

mediatizing effect of technology is put deliberately at the service of ADR processes not only in the sense of a medium or platform but also to increase understanding. It is necessary to research further, from the technical and the social and behavioural sciences perspectives, whether progress in artificial intelligence, and the replacement of some human activities by algorithmic chains, would help to prevent disputes and resolve conflicts.[73] Staging ADR online is not enough, in this sense the very fashionable ODR of recent years is not equivalent to ADR, unless it excludes the traditional formats and constraints of adjudicatory and adversarial methodologies.

4.4 Online Dispute Resolution

It was discussed above how the internet and other ICTs governance has evolved from its conceptual origins a decade ago, together with the WSIS. However, it has been emphasized that its "official" working definition still stands on that stakeholders of all sectors, in their respective roles shape the development and use of internet (according to this text, all other ICTs too). It is difficult to find a more proper public participation forum for civil engagement and empowerment than e-governments; and for the private exercise of transactional and relational freedoms than e-commerce and the social web.[74] ODR could be part of both environments and progress with the rest of the web towards its semantic stage.[75]

ODR comprises all dispute resolution processes that are mediatized by ICTs. All methodologies can be included in this category as it strictly refers to the medium or platform that supports human interaction. The increasing use of ODR, especially in the United States, and its formal institutionalization in Europe has an effect on the conflict management practice in general. It suggests that ODR should be a concern of policy makers and practitioners. The first documented ODR scheme was available in 1996, but only after the year 2000 the service passed from being experimental to become an entrepreneurial activity.[76] It could be said that in

[73] Replaceable and instrumental support would be software for legal informatics, visualization tools, data mining, retrieval and systematizing of information, translation services and virtual meeting environments to record sessions and progress during proceedings. One project of the last sort is being the subject of research by the faculty of Industrial Engineering at Aalto University in Finland. For detailed information access the URL.

[74] "Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the Internet". Consult documents of the WSIS webpage and the sections above developing the concept of ICTs governance principles.

[75] *Supra* note, 51.

[76] In Woodley (2012). A section with the history of ODR is referenced in detail. And for a review on its evolution see: Schultz (2011).

the EU, ODR is also going through a serious institutional stage with regulations against the ADR framework on cross-border disputes and consumer protection legislation.[77]

All ADR mechanisms could have a mirror online, in addition ICTs specific solutions have tried to innovate on services such as in fully automated negotiation sites, incorporating artificial intelligence components.[78] Mediation and arbitration have been the most prevalent forms of ODR. Facilitation, mediation and negotiation are part of the integral business strategy of online companies such as eBay, Google, and Amazon.

The E-government presence could also expand its influence to the judiciary, if only to go from the electronic filing and management of documents towards the virtual courtroom for any possible court dispute. In this context to resolve the problem of distance only, not to delegate control of the judicial process or to impart procedural justice. In the private scope, at least so far, negotiation continues being a human activity and it seems reasonable to state that inert technology cannot be expected to transform conflicts without human intervention.[79] Innovative technical solutions could facilitate cross cultural exchange if they temper positional attitudes affected by prejudice, distrust, resentment and similar barriers to constructive transactions, or be a logistic support when distance is a barrier.

5 ADR and ODR Institutionalization Processes in the European Union and the Digital Agenda

The ADR movement is sufficiently old for experts and practitioners in the conflict management field, to have become a "traditional" approach already. The integrative dispute resolution and lawyering style that ADR methods support has also been

[77] EU legislation should also be compared with the broader UNCITRAL developments on ODR aiming at establishing international normative standards on these processes and their practice. See: Preamble 2 draft Procedural Rules and A/CN9/WG III/WP112 UNCITRAL Working Group III (Online Dispute Resolution) Note by the Secretariat 28. February 2012, These rules do not focus on harmonization or subject matter i.e. consumer protection legislation but with a much more pragmatic vision intend to have the most applicability to high volume and low cost disputes in general.

[78] See: Bellucci and Zeleznikow (2005).

[79] To create a cooperative relationship, improve communication and influence people's perceptions positively. In transactions mediated by technology in particular, where the human factor is reduced, more objective interaction is possible reducing strain, reducing negative emotions and diminishing the positive as well. Technology can also distract if the user interfaces are not transparent and well mapped but this belongs to the field of human-computer interaction in the computer science domain. All those converging disciplines actively explore applications for conflict management support, in the search for solutions beyond the mere replication of analogous processes in the internet or the mobile technologies. For a contrasting perspective, look in Alexander (2005). Blurring the disctinction between diffusion and mere reach.

theorized long ago.[80] However, the formal institutionalization trend and regulation efforts in the EU to formalize these methodologies is recent, and very much connected to the interest in supporting the development of the digital economy and the emergence and increase application of ICTs technologies to human exchange in trade. Rules on ADR *-and ODR-* in Europe are part of a broader range of supranational actions that seek to support the Digital Agenda for Europe linked to a consumer protection aim.[81] This is one of its most overlooked weaknesses. Not only is the scope limited to certain aspects of cross border commerce instead of expanded to any field and addressing issues of people's empowerment in general, but also limiting in the way it minimizes the transformative potential of collaborative ADR in practice.[82] The Digital Agenda was announced in 2010, the re-launch of the single market in the same year, followed by the Single Market Acts in 2011 and 2012; both key strategic objectives of the EU within the threefold Agenda 2020 European Growth Strategy.[83] The Digital Agenda is one of the seven flagship initiatives, the first of the priorities for smart growth; and although it is together with these efforts that ADR and ODR institutional developments occur, they could have been considered in connection to other targets and about different flagship initiatives, especially if the purpose was not only focused on economic considerations. The goals of the Digital Agenda are summarized in 7 pillars and two additional areas: scoreboard (to report on progress assessment, a very important feature demonstrating a mature level on the EU reflexive governance evolution) and the international nature of the European progress on all the fields considered.[84] These last 9 dimensions are further subdivided into actions, a total of 125 from which the following can be said to have relevance in the field of private participation in the ICTs governance model of empowerment and social development if the emphasis was put on preventive regulatory development instead of on a defensive and limited model:

---

[80] ADR was long unregulated, separating it from adjudicatory processes and increasing its popularity in fields that need the most agility such as commercial law and international trade. This is also believed to have favoured a continuous, undisturbed evolution. On integrative and principled conflict management a classic text, explaining the core strategy of the Harvard Negotiation program, is Getting to Yes: Fisher et al. (2011). In perspective: Schneider (2013). Also consult the work of Louis M. Brown on preventive law for applications of perspective, for instance in his classical publications: Brown (1956) and Brown and Brown (1975). Preventive law proposes a problem solving and creative lawyering style that aims at practicing a less adversarial legal profession.

[81] Available Online at: http://ec.europa.eu/digital-agenda/digital-agenda-europe.

[82] Consumer Protection Policy Strategy for Europe 2007–2013. Available at: http://ec.europa.eu/consumers/strategy/index_en.htm#intro.

[83] The Monti Report: A New Strategy for the Single Market: Report to the President of the European Commission is available Online at: http://ec.europa.eu/bepa/pdf/monti_report_final_10_05_2010_en.pdf, on the Single Market Acts I and II consult: http://ec.europa.eu/internal_market/smact/index_en.htm. Details and documents on the Agenda 2020 can be found online at: http://ec.europa.eu/europe2020/index_en.htm.

[84] See the section defining these goals online at: http://ec.europa.eu/digital-agenda/en/our-goals/international.

Pillar I Digital Agenda:

Action 1: Simplifying pan-European licensing for online works Action 4: Wide stakeholder debate on further measures to stimulate a European online content market, Action 9: Updating the eCommerce Directive, Action 10: Member States to implement laws to support the digital single market, Action 12: Review the EU data protection rules, Action 13: Complementing the Consumer Rights Directive, *Action 14: Explore the possibilities for Alternative Dispute Resolution*, *Action 15: Consult the stakeholders on collective redress*, Action 16: Code of EU online rights, and Action 103: Adopt and implement the key digital single market proposals of the Digital Agenda.

Pillar III Trust and Security:

Action 28: Reinforced Network and Information Security Policy, Action 37: Foster self-regulation in the use of online services, Action 123: Proposal for Directive on network and information security and Action 125 Expand the Global Alliance against Child Sexual Abuse.

Pillar V Research and Innovation:

Action 54: Develop a new generation of web-based applications and services.

Pillar VI Enhancing digital literacy, skills and inclusion:

Action 57: Prioritize digital literacy and competences for the European Social Fund, Action 58: Develop a framework to recognise ICT skills, Action 59: Prioritise digital literacy and skills in the 'New skills for jobs' flagship, Action 61: Educate consumers on the new media, Action 62: EU-wide indicators of digital competences, Action 64: Ensure the accessibility of public sector websites, Action 66: Member States to implement digital literacy policies, and 126: Grand Coalition for Digital Jobs and Skills.

Pillar VII ICT-enabled benefits for EU society:

Action 84: Support seamless cross-border eGovernment services in the single market, Action 89: Member States to make eGovernment services fully interoperable, and Action 91: Member States to agree a common list of key cross-border public services.

These were steps taken by the Commission to boost the economy and promote prosperity in the region. In the field of ADR and ODR initiatives were effectively developed within the digital market priorities connected to e-commerce. E-commerce belongs to Action 9, and justified on the promise that the digital market reprents for the European Economy. An e-commerce directive was issued in June of the year 2000.[85] The goal is set to at least half of EU consumers

[85] The full text of the directive is available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT, to consult in detail policy, legislative process and reports visit the corresponding page at: http://ec.europa.eu/internal_market/e-commerce/communications/2012/index_en.htm, including the updated e-commerce Action plan 2012–2015 accessible online at: http://ec.europa.eu/internal_market/e-commerce/docs/communications/130423_report-ecommerce-action-plan_en.pdf where explicit references to ADR and ODR are made in detail.

purchasing online, 20 % of which should be doing it across borders by 2015. E-commerce, according to the reports submmited to the Commission, is poorly developed, and the conclusions on extensive research and consultation revealed that the main problem is lack of trust in the market; the consultation included a section on ODR which showed that people are unaware of its existence and benefits.[86] The EU adopted in 2008 Directive 2008/52/EC on certain aspects of mediation in civil and commercial matters with the purpose of building trust in the process of mediation within the EU. The directive did not propose any other form of ADR but lists well known advantages of asssited negotiation over adjudicatory processes. A short implementation period followed, and for the most part resulted in strict compliance. Mediation is enshrined in supranational and member states legislation eversince and awareness on its formal aspects is growing. An optimistic interpretation of these processes is that opportunities to spread ADR and preventive law principles in a large scale have become available to complement access to justice strategies and in general a healthy conflict management system for the whole Europe. Unfortunately their formal adoption, lacking in cultural meaning and appeal has failed to deliver the expected advantages.[87] The interpretation of country reports after the transposition clearly revealed the cultural resistance to change and lack of identification with mediation. Countries where no ADR tradition existed did not benefit in the least from the new laws on mediation or conciliation. This was the case of Bulgaria, Italy, Lithuania, and Estonia, for instance.[88] Where increase on trade or mediated dispute resolution indexes were recorded, mere correlational evidence was found. Sweden and the UK have and ADR culture strongly established. The interpretation by the EU, however, detected weaknesses on the fractioned schemes and the lack of use of latest ICTs technologies alone. No section of it assesses comprehensively the cultural obstacles for the incorporation of ADR into the European system except than the problem of language. Country specific factors, embedded in the conflict management and dispute resolution culture should have been studied in dept.[89] Solid institutionalization of principles does not follow the passing of laws, or the

[86] Revise the summary report online at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf.

[87] All reports and documentation on policy making supporting records, consultation and impact assessments are available online or linked at: http://ec.europa.eu/consumers/redress_cons/adr_policy_work_en.htm. This is a revealing test of society's readiness: http://ec.europa.eu/public_opinion/flash/fl_299_en.pdf. For an author's view on the potential of ADR in the field of e-comercein particular, consult Brannigan (2004). Revise the summary report online at: http://ec.europa.eu/internal_market/consultations/docs/2010/ecommerce/summary_report_en.pdf. Also find a complete doctrinary analysis of the EU consumer legislation and its current challenges in Weatherill (2013). EU consumer law and policy.

[88] See: http://ec.europa.eu/consumers/redress_cons/adr_study.pdf.

[89] The European Commission states that in the EU by now, more than 750 institutionalized ADR schemes are currently into place. See: http://ec.europa.eu/consumers/redress_cons/adr_odr_eu_en.htm and the source report again: http://ec.europa.eu/consumers/redress_cons/adr_study.pdf

establishment of convincing public policies, even at the national levels.[90] The proportion of consumers who order goods or services using Internet ranked highest in the Netherlands and the United Kingdom, 58 and 55 % according to the Eurobarometer analytical report from 2010 on Consumer attitudes towards cross-border trade and consumer protection in the EU.[91] These countries, before the EU initiatives on ADR were issued, were acquainted with ADR methods and a wide spectrum of dispute resolution methodologies were already available, and appreciated. In Contrasts, the study concluded that Bulgaria and Italy showed the lowest occurrence of both domestic and cross-border e-trade. The data interpreted the same way confirms that their institutional systems had little or no tradition in the use of non-adjudicatory resolution methodologies.

The latest legislative provisions on ADR systems were enacted in 2013. The Directive 2013/11/EU on Consumer ADR and the Regulation (EU) No 524/2013 on Consumer ODR were issued with the purpose of unifying the regime, and to improve the functionality of the system.[92] Again, with a normative approach, the EU is attempting to reach full ADR coverage, and better ADR services provided by specialized and professional entities. In terms of technological advancement the regulation is modest in requiring the formation of a single European ODR platform where to submit and resolve all relevant disputes electronically. The directive is more general in that it seeks to benefit consumers and traders, online and offline, in domestic and cross-border situations. These rules are anyway responsive, steaming from policy assessment mechanisms and a step ahead in assigning relevance to a subject that would have advanced at a much slower pace outside of the EU Digital Agenda. It is possible that they will promote a more committed integration process through exchange. They clearly push states to allocate resources for training, education, and consumer awareness programs, another pillar of this legislative development.

A concerning aspect of this institutional path is that little if any empowerments is encouraged by policy or legislation. Personal competences are not tackled and will not been enhanced in the absence of deliberate efforts to formulate policies that are fully in accord and consistent with the vision about new governance structures and the existence of new patterns in the relationships and exchange naturally emerging form the interdependence and generative power of the networked information society. These considerations should at least create more interest and invite research.[93] The arguments that will be most compelling can derive from the direc-

[90] Consult The Directorate General for Health and Consumers reports for comparison between Estonia: http://ec.europa.eu/consumers/redress_cons/docs/MS_fiches_Estonia.pdf And the United Kingdom: http://ec.europa.eu/consumers/redress_cons/ecc_united_kingdom_en.htm, for instance.

[91] Read online at: http://ec.europa.eu/consumers/consumer_empowerment/docs/report_eurobarometer_342_en.pdf.

[92] The policy development and preparatory works can be consulted online at: http://ec.europa.eu/consumers/redress_cons/docs/adr_citizen_summary_en.pdf.

[93] See the data collected in this statistical report: http://www.idate.org/fic/revue_telech/462/C&S43_UDEKEM-GEVERS_POULLET.pdf on measures of engagement of customers in the EU.

tion that technology is taking and the increasing role of smart technology in everyday life. Perhaps for tech-savvy societies ODR and artificial intelligence combined will be more convenient solutions to the slow increment in the use of ADR, but many other variables can play important roles, such as ICTs penetration, just to mention one. No conclusions can be drawn in the absence of well designed, behavioural sciences research.

6 Concluding Remarks; from the Thread of Consumer Protection to the Definition of an European Dispute Resolution Culture

In previous works it has been already stated that "Formal institutionalization efforts in the European Union, are proven insufficient to benefit commerce, improve the accessibility to justice and/or enhance the collaborative human interaction that the adequate use of ADR and ODR methodologies could bring about."[94] On one hand, public policy and other regulatory expressions that are basic in design allow the implementation of corrective measures; room for these actions anticipates the possibility of failure. But on the other, assigning value to temporary rules is difficult and implementation is costly. The balance between flexibility and an output for long-term systemic effects of public intervention, it is not easy to achieve but it is facilitated by the practice of reflexive and participative governance models that match the social requirements and competences of the times.

This book chapter has attempted to connect the global governance reality effectively influenced by the ICTs and its effect on society and the role that individual empowerment and competences reflected in self-regulatory capacities could play in it. A field where these qualities could thrive is conflict management. The European Union, a leader in reflexive governance deals with both aspects, ICTs and ADR development but circumscribed to a policy field, missing on the potential of fully integrating principles of the two to advance human capital and the realization of regional political, social and economic goals through constructive association and cooperation. The virtue implicit of the networks self-generated arrangements could be expanded to many other fields of public life to promote the formation of a dispute resolution culture compatible with complexities and uncertainties of a working process of making sense of our globalized world.

Concrete proposals that this chapter has developed are: to depart from a broad and inclusive object when invoking concepts of ICTs governance; in this way, referring also to topics on applications, content and behaviour; to accept the influence of ICTs in all governance instances and relationships, redefining power,

[94] *Supra* note, 66.

public interest and political intervention as much as private affairs and interaction, and institutionalize general collaborative principles in the concerned fields; to share the control on the ITC resources and exploit their potential without reducing human development to the adoption of technical solutions; to regulate wisely, with general and less intrusively public policy and normative proposals that could validate and incorporate private contributions in the classical format, agreements, co-regulation and concerted action; and to commit to implement all of these understanding at all levels so the ICTs really can become generative of data but also of substantial content and social development.

In regard to ADR instruments to support e-commerce and the digital market, disillusion could continue if a holistic implementation of their philosophy is not implemented. In this chapter different arguments have been proposed to consider nowadays collaboration and association essential components of a good conflict resolution strategy so that the developing ADR and ODR systems of the EU do not turn into meaningless rituals for replicating more of the same old competitive conflict management styles. Technology is an enabling medium and a growingly supportive mechanism to expand human abilities, but it still requires control. For this reason a priority for public policies should be education and human competences development in as much as a sustainable economy has always been, including consideration of variables affecting the changes and according to determining factors such as culture, access, and capacities.

Responsibilities should not be all assigned to the supranational entities. The European Union members must take the priorities set by policy seriously and engage in understanding their meaning, potential and implications. Compliance alone is a hollow action. In the area of redress mechanisms, even if formulated restrictively within the customer protection field, it offers innumerable opportunities for social progress, confidence in the electronic single market and the promotion of cross border e-commerce only scratching the surface of possibilities.[95] Constructive conflict management and ADR have practically no detractors. They are applicable to all organizational levels. The administration of procedural justice prevalent in all legal systems would also benefit from methodologies of administration of justice of other kinds. The logic of the networks and ethics of the interconnected information society can change the conflict management culture of the most developed states. This could be set to be another deliberate integration policy for the EU guided by the values of cooperation, empowerment (self-regulation), self-reliance (freedom), effectiveness and regulatory dynamism.

[95] Four to five decades ago the ADR movement became popular because it sought to resolve the problems of unsatisfactory dispute resolution practices and alleviate the costs of adversarial litigation endured by society and the public institutions. In the European Union nowadays, their normative consideration attends to very different motivators. The spread or e-commerce urges legal development to adapt to technical and social innovative practices as part of optimizing and expediting transactions through incremental deregulation.

References

Alan, W. (2001). Regulations and Standards for Online Dispute Resolution: A Primer for Policymakers and Stakeholders. *ODR News*, February 15, 2001.

Alexander, N. (2005). Mobile mediation: How technology is driving the globalization of ADR. *Hamline Journal of Public Law & Policy, 27*, 243.

Baldwin, R., Cave, M., & Lodge, M. (2011). *Understanding regulation: Theory, strategy, and practice*. Oxford: Oxford University Press.

Banisar, D. (2011). The right to information and privacy: Balancing rights and managing conflicts. *World Bank Institute Governance Working Paper*.

Barnett, R. E. (2014). *The structure of liberty: Justice and the rule of law*. Oxford: Oxford University Press.

Bellucci, E., & Zeleznikow, J. (2005). Developing negotiation decision support systems that support mediators: A case study of the Family_Winner system. *Artificial Intelligence and Law, 13*(2), 233–271.

Bennett, C. J., & Howlett, M. (1992). The lessons of learning: Reconciling theories of policy learning and policy change. *Policy Sciences, 25*, 275–294.

Black, J. (2001). Decentring regulation: Understanding the role of regulation and self-regulation in a "post-regulatory" world. *Current Legal Problems, 54*, 103–147.

Black, J., Lodge, M., & Thatcher, M. (Eds.) (2005). *Regulatory Innovation: A Comparative Analysis*. Cheltenham: Edward Elgar. Civic Consulting (2011) Consumer market study on the functioning of e-commerce and internet marketing and selling techniques in the retail of goods. Available at http://ec.europa.eu/consumers/consumer_research/market_studies/e_commerce_study_en.htm

Bradley, G. (2006). Social informatics—from theory to actions for the good ict society. In *Social Informatics: An Information Society for all? In Remembrance of Rob Kling* (pp. 383–394). Berlin: Springer.

Bradley, G. (2010). The Convergence Theory on ICT, Society, and Human Beings: Towards the Good ICT Society. *Information and Communication Technologies, Society and Human Beings: Theory and Framework*, *30*, 30–48.

Brannigan, C. (2004). Beyond e-commerce: Expanding the potential of online dispute resolution. *Interaction, 16*, 15–17.

Brown, L. M. (1956). The Law Office. A Preventive Law Laboratory (pp. 940–953). *University of Pennsylvania Law Review*.

Brown, L. M., & Brown, H. A. (1975). What counsels the counselor-the code of professional responsibility's ethical considerations-a preventive law analysis. *Val. UL Rev., 10*, 453.

Capurro, R., & Hjørland, B. (2003). The concept of information. *Annual review of information science and technology, 37*(1), 343–411.

Castells, M. (2008). The new public sphere: global civil society, communication networks, and global governance. *The ANNALS of the American Academy of Political and Social Science, 616*(1), 78–93.

Castells, M. (2011). *The rise of the network society: The information age: Economy, society, and culture* (Vol. 1). Hoboken: Wiley.

Cutler, A. C., Haufler, V., & Porter, T. (Eds.). (1999). *Private authority and international affairs*. Albany: Suny Press.

Da Silva, J. S. (2007). Future internet research: The EU framework. *ACM SIGCOMM Computer Communication Review, 37*(2), 85–88.

Deci, E. L., & Ryan, R. M. (2012). Overview of self-determination theory. *The Oxford Handbook of Human Motivation*.

DeNardis, Dr. Laura, The Emerging Field of Internet Governance (September 17, 2010). Yale Information Society Project Working Paper Series. Available at SSRN: http://ssrn.com/abstract=1678343

Deutsch, M., Coleman, P. T., & Marcus, E. C. (Eds.). (2011). *The handbook of conflict resolution: Theory and practice*. Hoboken: Wiley.

Epstein, R. A. (2009). *Principles for a free society: Reconciling individual liberty with the common good*. New York: Basic Books.

Eurobarometer. (2011) *Special report on Consumer empowerment*. Report nr 342. Available at http://ec.europa.eu/consumers/consumer_empowerment/docs/report_eurobarometer_342_en.pdf

European Commission. (2000) *Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)*, Directive 2000/31/EC of 8 June 2000. Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML.

European Commission. (2011). *Communication from the Commission "Towards Single Market Act", COM(2010) 608*. Available at: http://ec.europa.eu/internal_market/smact/docs/single-marketact_en.pdf

European Commission. (2012) *Communication "A coherent framework to build trust in the Digital single market for e-commerce and online services"*. http://ec.europa.eu/internal_market/ecommerce/communication_2012_en.htm

Fuchs, C. (2007). *Internet and society: Social theory in the information age*. London: Routledge.

Fuchs, C. (2010). Theoretical foundations of defining the participatory, co-operative, sustainable information society. *Information, Communication & Society, 13*(1), 23–47.

Fuchs, C., Hofkirchner, W., Schafranek, M., Raffl, C., Sandoval, M., & Bichler, R. (2010). Theoretical foundations of the web: cognition, communication, and co-operation. Towards an understanding of Web 1.0, 2.0, 3.0. *Future Internet, 2*(1), 41–59.

Gelfand, M. J., Fulmer, C. A., & Severance, L. (2011). *The psychology of negotiation and mediation*.

Gibbons, L. J. (1996). No regulation, government regulation, or self-regulation: social enforcement or social contracting for governance in cyberspace. *Cornell Journal of Law and Public Policy, 6*, 475.

Giddens, A. (1979). *Central problems in social theory: Action, structure, and contradiction in social analysis* (Vol. 241). Oakland: University of California Press.

Giddens, A. (2013). *Social theory and modern sociology*. Hoboken: Wiley.

Gruber, T. (2008). Collective knowledge systems: Where the social web meets the semantic web. *Web semantics: science, services and agents on the World Wide Web, 6*(1), 4–13.

Habermas, J. (1987). *The philosophical discourse of modernity*. Twelve lectures.

Habermas, J. (1996). *Contributions to a discourse theory of law and democracy*. Cambridge: Polity Press.

Hilbert, M., & López, P. (2011). The world's technological capacity to store, communicate, and compute information. *Science, 332*(6025), 60–65.

Hofkirchner, Wolfgang. (2007). A critical social systems view of the internet. *Philosophy of the Social Sciences, 37*(4), 471–500.

Julio, C. B. (2012). Libertad de Contratación, Orden Público y sus repercusiones en el marco de la Arbitrabilidad. *Indret: Revista para el Análisis del Derecho, 2*, 1–31.

Levi-Faur, D. (2011). Regulation and regulatory governance. *Handbook on the Politics of Regulation*, pp. 1–25.

Martens, B., & Turlea, G. (2012). *The drivers and impediments for online cross-border trade in goods in the EU*. Digital Economy Working Paper 2012/1.

Menkel-Meadow, C. (2000). Mothers and fathers of invention: The intellectual founders of ADR. O*hio State Journal on Dispute Resolution*, 16, p 1.

Mill, J. S. (1859). *1975, on liberty in three essays*. Oxford: Oxford University Press.

Misztal, B. (2013). *Trust in modern societies: The search for the bases of social order*. Hoboken: Wiley.

Mitchell, W. J. (2004). *Me++: The cyborg self and the networked city*. Cambridge: MIT Press.

Mueller, Milton L. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge: MIT Press.

Nierenberg, I. G. (1968). *The art of negotiating, psychological strategies for gaining advantageous bargains*. USA: Hawthorn Book a Division of Elsevier-Dutton, New York Press.

Perillo, J. M. (2004). Robert J. Pothier's influence on the common law of contract. *Texas Wesleyan Law Review, 11*, 267.

Planiol, M., & Ripert, G. (1959). *Treatise on the civil law* (pp. 153–55). Eagan: West Publishing Company.
Poblet, M. (2011). *Mobile technologies for conflict management*. Berlin: Springer.
Pothier, R. J., Le Trosne, M., & Aguesseau, H. F. (1839). *A treatise on the law of obligations, or contracts: 2* (Vol. 2). Robert H. Small.
Rawls, John. (1971). *A theory of justice*. Oxford: Oxford University Press.
Ross, L., & Stittinger, C. (1991). Barriers to conflict resolution. *Negotiation Journal, 7*(4), 389–404.
Russell, S. (2012). *O. El contrato normativo: análisis de una categoría*. Crónica del acto de defensa de tesis doctoral hispano-francesa (UCM, 3.7. 2013).
Schultz, T. (2011). *The roles of dispute settlement and ODR* (pp. 135–155). Berlin: Kluwer.
Solarte-Vasquez, M. C. (2013). Regulatory patterns of the internet development: Expanding the role of private Stakeholders through Mediatized "Self-regulation". *Baltic Journal of European Studies, 3*(1), 84–120.
Solum, L. B., & Chung, M. (2003). Layers principle: Internet achitecture and the law. *The Notre Dame Law Review, 79*, 815.
Thompson, L. (1990). Negotiation behavior and outcomes: Empirical evidence and theoretical issues. *Psychological bulletin*, 108(3), 515.
Tiilikka, P. (2013). Access to information as a human right in the case law of the European court of human rights. *Journal of Media Law*, *5*(1), 79–103.
Trubek, D., & Trubek, L. G. (2007). New governance and legal regulation: complementarity, rivalry, and transformation. *Columbia Journal of European Law, 13*(3), 539–564.
Utterback, J. M. (1996). *Mastering the dynamics of innovation*. Boston: Harvard Business Press.
Vansteenkiste, M., Niemiec, C.P., & Soenens, B. (2010). The development of the five mini-theories of self-determination theory: an historical overview, emerging trends, and future directions. In T.C. Urdan, & S. A. Karabenick (Eds.) *The Decade Ahead: Theoretical Perspectives on Motivation and Achievement (Advances in Motivation and Achievement* (Vol. 16, pp. 105–165), Bingley: Emerald Group Publishing Limited.
Solarte Vasquez, M. C. (2014). *The institutionalization process of alternative dispute resolution mechanisms in the european union*. L'Europe Unie/United Europe: The Estonian Legal Developments Experience.
Voss, J. P., Bauknecht, D., & Kemp, R. (Eds.). (2006). *Reflexive governance for sustainable development*. Cheltenham: Edward Elgar Publishing.
Wall, J. A., & Dunne, T. C. (2012). Mediation research: A current review. *Negotiation Journal, 28*(2), 217–244.
Wall, J., & Kressel, K. (2012). Research on mediator style: A summary and some research suggestions. *Negotiation and Conflict Management Research, 5*(4), 403–421.
Weatherill, S. (2013). *EU consumer law and policy*. Edward Elgar Publishing.
Woodley, A. E. (2012). Resolving the world's commercial disputes: An integrated model for e-learning and ODR. *International Journal of Technology Policy and Law, 1*(2), 217–233.
World Bank. (2012) *Governance indicators*, database available at http://data.worldbank.org/datacatalog/worldwide-governance-indicators
Castells, M. (1996). *The information age: Economy, society and culture (Vol. I): The rise of the network society*. Cambridge MA/Oxford UK: Blackwell Publishers ISBN: 1-55786-616-3 / 1-55786-617-1 (pbk)
Castells, M. (1997). *The information age: Economy, society and culture Vol. II: The power of identity*. Malden MA/Oxford UK: Blackwell Publishers ISBN: 1-55786-873-5/ 1-55786-874-3 (pbk)
Castells, M. (1998). *The information age: Economy, society and culture Vol.III: End of millennium*. Malden MA/Oxford UK: Blackwell Publishers ISBN: 1-55786-871-9 (alk.paper)/ 1-55786-872-7 (alk. paper)
Castells, M. (2004). 1. Informationalism, networks, and the network society: a theoretical blueprint. *The Network Society, 3*, 3–45

Fisher, R., Ury, W. L., & Patton, B. (2011). *Getting to yes: Negotiating agreement without giving in*. London: Penguin

Gelbstein, E., & Kurbalija, J. (2005). *Internet governance: issues, actors and divides*. Diplo Foundation

Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment

Hendriks, C. M., & Grin, J. (2007). Contextualizing reflexive governance: the politics of Dutch transitions to sustainability. *Journal of Environmental Policy & Planning, 9*(3–4), 333–350.

Jessop, B. (2003). Governance and meta-governance: On reflexivity, requisite variety and requisite irony. *Governance as Social and Political Communication*, 142–172. Manchester: Manchester University Press.

Kessler, F., & Fine, E. (1963). Culpa in contrahendo, bargaining in good faith, and freedom of contract: A comparative study. *Harvard Law Review, 77*, 401.

Marx, K. (2012). *Economic and philosophic manuscripts of 1844*. Mineola: Courier Dover Publications.

Mensch, B. (1981). Freedom of contract as ideology. *Stanford Law Review, 33*, 753–772

Mueller, M., & McKnight, L. (2004). The post-.COM internet: toward regular and objective procedures for internet governance. *Telecommunications Policy*, 28(7), 487–502

Ourliac, P., & de Malafosse, J. (1969). *Histoire du Droit privé* (2ème ed., p. 114). Paris: Presses Universitaires de France.

Pound, R. (1909). Liberty of contract. *Yale Law Journal, 18*, 454–487

Ramsbotham, O., Miall, H., & Woodhouse, T. (2011). Contemporary conflict resolution. In Polity, M. Deutsch, P. T. Coleman & E. C. Marcus (Eds.), *The handbook of conflict resolution: Theory and practice*. Hoboken: Wiley

Reichman, J. H., & Franklin, J. A. (1999). Privately legislated intellectual property rights: Reconciling freedom of contract with public good uses of information. *University of Pennsylvania Law Review, 147*, 875–970

Schlechtriem, P. (1988). Borderland of tort and contract-opening a new frontier, The. *Cornell Int'l LJ, 21*, 467.

Schneider, A. K. (2013). Beyond theory: Roger Fisher's lessons on work and life. *Negotiation Journal, 29*(2), 171–177.

Sørensen, E., Torfing, J., Peters, B. G., & Pierre, J. (2012). *Interactive governance: Advancing the paradigm*. Oxford: Oxford University Press.

Sorsa, K. (2009). The proactive law approach: A further step towards better regulation. Tala, J. & Pakarinen A.(Eds.), Changing Forms of Legal and Non-Legal Institutions and New Challenges for the Legislator-International Conference on Legislative Studies in Helsinki. National Research Institute of Legal Policy. *Research Communications* 97, 35–70

Tolsada, M. Y. (2001). *Sistema de responsabilidad civil, contractual y extracontractual*. Dykinson.

Webster, F. (2002). Theories of the information society. *International Library of Sociology*.

Yu, L. (2007). *Introduction to the semantic web and semantic web services*. Boca Raton: CRC Press.

Concepts and Problems Associated with eDemocracy

Pawan Kumar Dutt and Tanel Kerikmäe

Abstract Information and communications technology (ICT) plays a major role in modern society. The Internet has certain unique factors which make eParticipation and eGovernance particularly appealing, namely the size and extent of the Internet, which enables it to be a medium whereby information can be very widely dispersed. This in turn has made political participation easy online. However, there is also a propensity of ICT to be used to interfere with our right to privacy. There is a need to factor in present and future requirements in the scope of eDemocracy and eGovernance generally, and one of the key issues is the devising of methods to narrow the prevailing digital divide. There is also more need for creation of adequate support tools to enable the user to navigate through vast contents, while also engaging and interacting in a meaningful manner with others. For eDemocracy to flourish, what is needed are newer versions of ICT, interest in eDemocracy (both by the government and public), suitable legislation, financing, and a generally conducive environment for enhancement of democratic ideals. However, by its very nature, technology is not inherently democratic. To indulge in eParticipation, we need to understand the concept of ePersonality. This in turn leads us to the question of what is an ePerson? In order to enable the ePersonality to flourish, the authors propose the need to create a parallel online universe, where rights and liabilities mirror those found in our various earthly conventions and declarations related to human, cultural and political rights, but where the distinction between the real world and the online world persists—thereby creating a situation wherein the twain shall coexist but never meet. This is the cloned heaven specially made for Trishanku, a concept taken from Hindu mythology in an attempt to find the answer for the future from our past.

P.K. Dutt (✉)
Tallinn University of Technology, Tallinn, Estonia
e-mail: pawan.dutt@ttu.ee

T. Kerikmäe
Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia
e-mail: tanel.kerikmae@ttu.ee

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_13

1 Concept

1.1 Introduction

The role of information and communications technology (ICT) in modern society in conjunction with the Internet cannot be underestimated. Although governments in most developed countries around the world have used digital technologies for a very long time, it was only after the mass scale advent of the Internet and technologies associated therewith in the 1990s that the potential for interaction between the government and society took a giant leap.[1] In particular, it has led to the enhancement of the democratic process. This in turn has spurred further research efforts in this field throughout the world. This leads us to the study of the eDemocracy situation, and its main branches, namely eVoting and eParticipation and the phenomenon of the Internet which makes it all possible.

The Internet has certain unique factors which make eParticipation and eGovernance particularly appealing, namely the size and extent of the Internet, which enables it to be a medium whereby information can be very widely dispersed (especially when compared with the print medium); it helps us to understand, for instance, how Egyptian protestors were able to increase their numbers at a very high rate, much to the chagrin of their government which was unable to control this rapid explosion of information and freedom on the Internet.[2]

Further, the possibility for online users to remain anonymous and the general inexpensiveness of the Internet allow the Internet to be extremely effective in a high risk environment.[3] In a way, this could be said to reflect the anonymity offered only by a secret ballot in a democratic process, although traditionally public debate and enactment of legislation has, by its very nature, been a very public exercise of one's democratic rights.

Also, the characteristics of information exchanged, which in certain ways mimics how human societies in the past depended on oral forms of communication. The Internet allows for communication and interactivity which is almost instantaneous, just as in such tribal societies.[4] Thus, some researchers believe that the cyberspace is changing the law at a very fundamental level, and hence, it may not be enough to merely try to adapt existing rules to govern the Internet.[5] One can also draw a contrast between text-based legal positivism which insists on clarity and ease of flow of authority in a vertical manner (from ruler to ruled) on the one hand with older societies based on oral traditions/customs and modern ICT-driven societies. In these non-text-based societies, the essential features are surprisingly similar—being namely flexibility and ease of access in a multi-centric and horizontal system—which

---

[1] Hood and Margetts (2007), p. 202.

[2] Duvivier (2013), p. 41 at footnote 159, where Ghonim (2012) is quoted.

[3] *Id* 43, where in footnotes 173 and 174 the role of annoymity vis-a-vis public exercise in the legislative process as ruled in the US Supreme Court case John Doe (2010) is discussed.

[4] Howes (2001), p. 41.

[5] Duvivier (2013), p. 48 where Howes (2001) is widely quoted.

actually is how legal interactivism is defined nowadays.[6] eGovernance is usually seen as a basis of better service of people, development and innovation. As pointed out by some researchers, there have always been barriers to development.[7] When in 1445, Gutenberg invented the printing press, Western Europe recognised it quickly. However, in areas where absolutism was the rule, the printing press was seen as an evil. It seems that any development of technology available to public would create networks, raise the knowledge, ease the communication, and therefore, the citizens are harder to control.

1.2 The Changes Seen Consequently in Modern Society

When compared with the past, it could be considered that political activism in the modern digital era is not as taxing as it used to be in the past. Thus, where at one time, a civic-minded activist-citizen would have been expected to take the time out to educate him with regard to the issue at hand and subsequently to compose a letter, to address it to the correctly identified recipient of the political message and then to actually post that letter out, things are different today. Nowadays, it is the norm for eLegislating requests to make use of personal data that is already stored in an online database, and further, only a click of a button to dispatch the eMessage through ICT means straight from the online user/participant's computer to the political representative's office. This whole process has become so much more easier, cheaper and less bothersome, that it has actually given rise to the use of terms such as "slacktivism" or "clicktivism", the image being one of utter lack of serious responsibility on the part of the eParticipant.[8]

Qualitywise, it is thus to be noted with some concern that positions articulated online by eParticipants often tend to be defined by their spontaneity (which should be actually read as a hasty decision based on the general knowledge, morals and viewpoint) and a form of herd mentality.[9]

Thus, it can be seen that eLegislating efforts can now have a greater impact in the world of politics, given their potential to empower citizens by giving them an opportunity to counter those privileged forces which could afford to pay full-time lobbyists to do their conventional lobbying/campaigning for them, often to the detriment of the ordinary citizen. This in itself is a very positive change, which if handled correctly can lead to further enhancement of democracy, since it harnesses ICT to bring about social development and political change.[10]

---

[6] Howes (2001), p. 39.

[7] Acemoglu and Robinson (2013), pp. 213–216.

[8] Duvivier (2013), p. 55.

[9] Cynthia et al. (2012), pp. 132–133.

[10] Duvivier (2013), p. 76.

1.3 Words of Caution

However, before we get carried away by the euphoria of technology and its supposed fruits, a word of caution is due. Our modern democratic societies in Europe, built from the ashes of the Second World War and sheltered zealously from the debilitating numbness of the Cold War, have one singular premise that overrides all other aspects—and that is respect for fundamental rights. Yet, these very fundamental rights are exposed to risks from digital tracking and other surveillance technologies, products of the very ICT that we built to liberate our modern selves from the ghosts of our non-digital past.

What we are waking up to, with increasing disconcert, is the unbecoming reality of the propensity of ICT to be used to interfere with our cherished right to private life. This is partly due to the rapid technological developments in the field of ICT and also the slowness of the legal frameworks and safeguards to adapt to these changes.[11] Questionable practices of some democratic governments in enacting legislations, which allow broad surveillance of their citizens, have given rise to a bewildering array of capabilities and practices which have in turn made citizens to stop and think about the direction in which their societies are heading. This has in turn had an adverse effect on participation by citizens in social, cultural and political spheres, because of the real and present danger of undermining of the reasonable quest for confidentiality, or the rights to freedom of expression and information under Article 10 of the European Convention on Human Rights (ECHR). Some recent issues, such as protection of journalist's sources and the safety of the concerned persons (as so elaborately brought out in the case of Edward Snowden who was formerly associated with intelligence agencies of the United States of America (USA)), if not resolved can actually cause long-term damage to democracy itself.[12]

Article 8 of the ECHR binds Council of Europe member states to secure the right to respect of private and family life, home and correspondence, and consequently, states have an obligation to refrain from interfering with fundamental rights (i.e., a negative obligation) coupled with an obligation to actively protect the above rights (i.e., a positive obligation).[13]

Of particular interest to us is the modern day tendency of our citizens to rely on electronic devices (both fixed and mobile) in order to communicate with others, participate in various activities and generally to better manage their lives on a daily basis. But these devices are unfortunately double-edged weapons—since they all have the latent potential to collect and store all kinds of data and personal information. This includes, but is not restricted to, geographical locations and data

[11] See Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (2013), para 1.

[12] *Id* at para 2.

[13] *Id* at paras 3 and 4.

regarding Websites visited. This can lead to unlawful surveillance of a user's daily activities and can also result in leakage of sensitive personal information which can reveal in an intimate manner the details of a person's wealth, physical well-being, interest in political matters, beliefs or sexual orientation, etc. Over a period of time, this can all be collated and it gives rise to a detailed data bank about a particular person and his immediate circle of family and friends.[14]

These intrusive digital technologies can be used positively to develop new services for consumers/taxpayers for legitimate, commercial and law enforcement purposes. But conversely, these same technologies can be grossly misused, to the extent that they actually harm personal liberties and freedoms.[15] Further, the conflicts and collisions between European legal acts such as the ECHR and the EU Charter on fundamental rights pose a challenge as well.[16]

What is of relevance is the compliance of all such data collecting technologies with the appropriately applicable safeguards in the field of human rights. These cover the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, etc., which should incorporate the principle of proportionality. Also relevant are the safeguards set out in the convention for the protection of individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and in its additional protocol, Recommendation CM/Rec(2010)13 on the protection of personal data in the context of profiling, the Budapest Convention for combating cybercrime which may cover unlawful surveillance and tracking activities in cyberspace, etc. Thus, it is vital to increase awareness among users of such digital technologies as well the developers of such technologies who should be sensitised to the concepts of "privacy by design" and "privacy by default".[17] Further, under Article 13 of CM(2011)175 dated 15 March 2012, being the Internet Governance—Council of Europe Strategy 2012–2015, emphasis is laid upon efforts to maximise the potential of the Internet to promote democracy by encouraging Internet governance, promotion of citizen's participation by online means, developing secure eVoting procedures and promoting greater transparency through Internet governance. The universality of human rights can also be revisited from the angle of eDemocracy.[18]

Equally important is the need to factor in present and future requirements in the scope of eDemocracy and eGovernance generally, and one of the key issues is the devising of methods to narrow the prevailing digital divide. There is also more need for creation of adequate support tools to enable the user to navigate through vast contents, while also engaging and interacting in a meaningful manner with others.[19]

---

[14] *Id* at para 5.

[15] *Id* at para 6. Also see Walker and Grytsenko (2014).

[16] Kerikmäe (2014).

[17] *Id* at paras 7 and 8.

[18] Kerikmäe and Nyman-Metcalf (2012).

[19] Kotsiopoulos (2009), p. A-2.

It is therefore important that while introducing, implementing or reviewing eDemocracy, steps must be taken to ensure that it fully complies with obligations of human rights and fundamental freedoms, enhances democracy, complements traditional democratic processes and widens participatory choices for the electorate, respects citizens' trust in democracy and makes the entire process transparent, responsive and accountable. Public deliberation and participation are the key in this democratic process. Also equally important is the need to use education and public awareness methods to address the digital divide issue which can potentially exclude and discriminate against people. Further, a lot depends upon the use of technology-neutral means, including open-source solutions and open standards and specifications.[20]

1.4 A Brief Glimpse of the Dangers

It should be noted that eDemocracy is susceptible to certain dangers, both technical and non-technical in nature. The fact is that technology is not always neutral in scope. This gives rise to the need to inculcate a general awareness of the characteristics of the technology in use.[21] Further, technology is an enabling tool which can serve to enhance democracy, but it is not the solution.[22] To be effective, eDemocracy tools should be designed to work in a secure fashion, and this responsibility vests upon the institution incharge of the eDemocracy project.[23] One good recommendation in this regard is to make the source code open for the public. This serves to enhance trust as it enables free and fair inspection of the solution. Such open-source codes promote transparency, interoperability, accessibility and also encourage inclusiveness in the field of eDemocracy.[24]

It must also be noted that although Internet-based electoral campaigns can be surprisingly cost-effective; when compared with traditional electoral campaigns, there is a risk of oversimplifying issues into a "yes" or "no" situation. This situation of a zero sum game can lead to citizens being misled and tricked into voting contrary to their true intentions.[25]

Typical responses from citizens, especially in terms of quality, indicate that a heightened discussion of politics online did not necessarily translate into acquisition of higher levels of knowledge in the field of politics and further, qualitywise, most online political posts by citizens tend to be reflective of their own opinions and

[20] See Recommendation CM/Rec(2009)1 para 6.

[21] See *id*, Appendix thereto, Principle of eDemocracy 52.

[22] See *id*, Principle 50.

[23] See *id*, Principle 53.

[24] See *id*, Principles 54–57.

[25] Duvivier (2013), p. 51.

prejudices. Often there is nothing new or educative on display.[26] These online posts can actually be seen as, to an extent, encouraging further polarisation among those who hold political discussions over the Internet. It would thus be incorrect to assume that online discussions would lead to an exalted level of deliberative democracy.[27]

Thus, even if one were to assume that citizens could be coaxed, through the use of specially designed online forums, to indulge in political discussions in an orderly and civil manner, there is always the risk that such discussions could be distorted or disrupted, given the inherent propensity of ordinary online participants to remain just ordinary and lacklustre in their outlook thus the need for rules.[28]

Further, given the complex nature of legislation, it is easy for voters to become confused. Often citizens act with a herd mentality. Adding affiliation to certain groups or thinking processes can thus lead to polarisation of opinions, especially when there is increased interest of political and other interest groups in eLegislation campaigns.[29]

Furthermore, it would appear that eRegulation would empower the inclusiveness and, therefore, democracy. If one were to look at the situation in totalitarian states—for example in North Korea, mobile phones were even banned once (2004). Now, their usage is allowed, but it is not possible to call outside the country or to use free Internet. Becoming a citizen's Europe, the EU should give green light to innovation but do it with great care, avoiding problems of violation of privacy and possible use of the new technologies by terrorists. That is one of the reasons in glorifying legal norms that would lead to certainty, user-centricity and balance between the interests of stakeholders. Several mistakes and failures in creating more unified Europe should be sufficient lessons to avoid elitism and non-inclusiveness and ignoring the democratic process.

1.5 Suggested Safeguards

Hence, in the specific case of technology, certain safeguards are mandatory and worth considering. As mentioned previously, eDemocracy software should necessarily be open-source software, which should be liable to inspection or certification by an independent body.[30] It is further recommended that stakeholders in eDemocracy projects should draft contracts for eDemocracy applications which specify an open-source clause. This is especially beneficial since open-source software and applications provide open frameworks. This in turn leads to

[26] Feezell et al. (2009), pp. 9, 16.

[27] Sherman (2011), p. 102.

[28] Dutton and Peltu (2007), p. 21.

[29] Duvivier (2013), p. 54.

[30] See Appendix to Recommendation CM/Rec(2009)1 Guideline on eDemocracy 57.

opportunities to share not only developments in this field but also costs incurred for maintenance purposes.[31] Using open-source software standards and specifications has the added benefit of ensuring interoperability of the varied technical components and services that comprise an eDemocracy tool, which in turn may have been obtained from varied sources, sometimes across borders.[32] Further, such initial processes to ensure openness in the eDemocracy software can help to prevent situations in the future whereby eDemocracy stakeholders feel tied down to a single vendor of software solutions.[33]

Another recommendation worth noting is the necessity of having an independent body appointed by the public authority (which is charged with introducing eDemocracy tools into society) which is empowered to carry checks on the eDemocracy tool and to evaluate it quantitatively and qualitatively to ensure its proper applicability, functioning and security.[34] This is particularly of essence when one considers that eDemocracy tools are often targeted at those who are unable to be physically present at a particular place to partake in democratic functions, and this list includes but is not limited to travellers, those living outside the territory, persons with reduced mobility and people whose absence can be explained by reasons of a personal nature.[35]

1.6 Detailed Analysis of eDemocracy

Having spoken briefly about eDemocracy and its attractive features and potential pitfalls in the preceding part of the introduction, it would be helpful to study this phenomenon in detail. It should be noted that eDemocracy comprises of the use of ICT (including the Internet) in order to enhance the democratic process. It can also be used to implement newer democratic processes within a democratic society. What is aimed for is the idea of making democratic processes more accessible to citizens, which in turn is hopefully linked to more expansive and direct participation of the citizenry in decision-making on issues which are primarily in the realm of public policy. Theoretically, eDemocracy is billed to be the grand enabler of broader public influence in policy outcomes which relate most to the citizens. This is hoped to be achieved by the belief that when more individuals from society are involved, the result is more transparent and subject to greater scrutiny and accountability. This in turn leads to greater legitimacy at the political level, and the adoption by governments of policies which are more in tune with the actual needs of the electorate.[36]

---

[31] See *id*, Guideline 58.

[32] See *id*, Guideline 59.

[33] See *id*, Guideline 60.

[34] See *id*, Guideline 71.

[35] See *id*, Guideline 74.

[36] Kotsiopoulos (2009), p. A-7.

It should be noted that eVoting (although vitally important and considered by many as the most popular of eDemocratic functions) is an important aspect, and the term eDemocracy itself leads to a much wider import and has presently expanded into every facet of the democratic system. The beauty of eDemocracy lies in the fact that it can be designed to be implemented on the vertical plane (from public authorities at various levels at the top and directed downwards, or from citizens at the bottom and directed upwards) or on the horizontal plane.[37] It should however be noted that in order to prosper eDemocracy requires on the one level political will and leadership, and also education, training and measures to cater to the requirements of broad-scale inclusion.[38]

For eDemocracy to flourish, what is needed are newer versions of ICT, interest in eDemocracy (both by the government and public), suitable legislation, financing, and a generally conducive environment for enhancement of democratic ideals.[39] On the other hand, eDemocracy is constrained by challenges such as willingness on the part of the various stakeholders to engage confidently in democracy by electronic means, the divisions in society in the digital and social spheres, and general availability and reliability of technological means in this field.[40]

Other significant barriers to eDemocracy include differences in understanding the role of democracy and the interests of the various stakeholders. Also of worry are lack of resources, shortcomings in the organisation and inability of the structure to meet the challenges which arise.[41] This is often accompanied in tandem by the potential risks attached to eDemocracy of the spectre of misuse (both technical or political) and a bland denial of the opportunities that ICT creates for reaching decisions.[42]

For eDemocracy to function effectively and with suitable safeguards, rules and regulations are a must. Of particular importance are security issues, namely "security of the information that is collected, security of the data that is accessed and stored, including compliance with data protection requirements, security of the mass of documents created, security of the entire voting process, Internet security, networking security and information system security".[43]

Thus, one researcher refers to eDemocracy as the way the Internet can serve as a medium to enrich our democratic processes and thus allow for greater interaction between the government and the governed, at the same time allowing for feedback from the community to enhance good governance.[44]

---

[37] See Appendix to Recommendation CM/Rec(2009)1 Principle of eDemocracy 59.

[38] See *id*, Principles pp. 63, 64.

[39] See *id*, Principle 68.

[40] See *id*, Principle 70.

[41] See *id*, Principle 71.

[42] See *id*, Principle 72.

[43] See *id*, Principle 78.

[44] Kotsiopoulos (2009), p. A-7 where in footnote 1, Clift (2003) is quoted.

All in all, the concept of eDemocracy is hoped by many to provide the means for enhanced participation with the help of the Internet, mobile communications and other forms of modern technology.[45]

It is therefore essential to see that eDemocracy is more akin to the path taken, rather than the end destination. As a process, it involves the use of ICTs in the field of democratic processes, and to further this aim there should be strategies and techniques (with goals of transparency, involvement and frank opinion formation by the masses) put into place.[46]

It must be noted that even though eDemocracy is seen as being synonymous with online forums and concepts such as eVoting or eConsultations, it is more than just being about technology. Further, the use of ICTs can often add an extra layer of bureaucratic red-tapism, making the whole experience even more slower. Thus, eDemocracy is not about "push button" democratic processes nor is it a ready-made solution for countering the democratic deficit which has seeped into our modern day societies.[47]

All of the above is remarkable, when one actually sees the dissonance between the optimism displayed by such eDemocracy initiatives and what has been actually achieved on the ground. What is needed are Web-based mechanisms which actually go beyond non-deliberative mechanisms such as voting, ePetitions, etc., and venture into the field of complicated online deliberation.[48]

Since eDemocracy has still not succeeded in becoming a more pivotal feature of democracy, there is need for an introspection in this regard. It is obvious that in its lack of acceptance by societies, there lie the undeniable facts of technical and societal issues. One key aspect is the registration of a secure, private and safe online identity for citizens. This is essential to enable elections and other interactions between the masses and the governing bodies. Such technical obstacles notwithstanding, there are also prevalent vested interests involving politicians, corporate houses, media and trade union interests, etc., which see such direct eParticipation as a potential threat to their own self-interest.[49]

Added to this are the more familiar objections of direct democracy, namely that eDemocracy can encourage dangerous populism and demagoguery in the political leadership. Further, it can bring forth the cascade of inequalities, stemming from the digital divide between the haves (with access to ICT tools which allow eDemocracy) and the have-nots. Thus, by its very nature, technology is not inherently democratic. This gets even more murkier when one sees the financial opportunities that arise for certain vested groups from the potential expenses which modern innovations in the field of eDemocracy can entail.[50]

---

45 See *id*, p. A7.

46 See *id*, p. A7 where in footnote 2, Mendez (2007) is quoted.

47 See *id*, p. A8 where the NGO access2democracy is quoted.

48 Perez (2013), p. 67.

49 Kotsiopoulos (2009), p. A-8.

50 See *id* at p. A8 where in footnote 5, Barney (2000), is quoted.

1.7 The Type of Citizen Around Whom eDemocracy Revolves

One researcher has contrasted between two seemingly opposite models of democracy. One is the "Plato" model which can be loosely associated as focussing on an increase in the powers of the experts in the bureaucratic institutions of the state.[51] In his work "The Republic", Plato supports political power for those sections of society (notwithstanding the fact that they may be in minority) that possess knowledge of how to use such power correctly. This elite body functions in a form which could be termed as enlightened paternalism, and not as totalitarianism.[52]

These in today's world would be the experts who could be expected to guide modern society through the complicated maze of international law dealing with wide ranging topics such as economy, environment, security, etc. These are seen as areas where genuine public participation and/or transparency are perceived as being merely wishful thinking. This is in contrast to the model of "Open government or eDemocracy" which emphasises upon empowerment of the whole body of citizens to participate in the political process. Here, more weightage is given to the capacity of citizens to engage in meaningful contribution towards the political process. The key differences of this approach from Plato's model are namely: the questioning of privileged access to knowledge of the technocrat and the insistence upon the ideal of harnessing collective wisdom for better public good—both by facilitating production of knowledge built upon through collaboration and by allowing for a mechanism to check the process of bureaucratic work through external checking. Thus, for example, the "Open Government Directive" (OG Directive) of President Obama of USA provides for participation of the public by contribution of ideas which can be used by the Government to adopt policies which are more in tune with society's needs.[53]

This is a vein of thought which is also expressed by Popper, K. in his book wherein knowledge is described as being achieved through collective means of debating and arguing. Further, the right to criticise government policies is seen as helping in the growth of the faculty of reason itself.[54]

One researcher considers the model of citizenship that is used for eDemocracy purposes and has developed the concept of the "punctuated citizenship". The researcher hopes to draw attention to the underlying tension between a highly idealised vision of eDemocracy vis-a-vis the actual ground reality.[55] The author will expand upon this concept in more detail in subsequent pages.

---

[51] Perez (2013), p. 68.

[52] See *id*, p. 70 where in footnote 23, Plato. *The Republic,* is discussed.

[53] See *id*, p. 72.

[54] See *id*, p. 74 where in footnote 36, Popper, K. *The Open Society and Its Enemies* is discussed.

[55] See *id*, p. 68.

2 Definitions and Categorisation

2.1 The Different Sectors of eDemocracy

The different sectors of eDemocracy are laid down as follows. eDemocracy is basically all about eParticipation—it is a concept which has the potential to move forward involvement of/by/for citizens in the various democratic processes to a higher level.[56]

For eParticipation to truly succeed, the key requirements are to use ICT to help the system to become open, accessible and free for participation. Petitions are seen as an effective tool that helps the public to communicate directly with Parliament on matters of public importance. It should be noted that true success can only be measured when an individual's petition will be considered on an equal footing with a petition which has been signed by a large number of supporters.[57]

As an example, one can see the Scottish Parliament which has devised an electronic petitioning system called ePetitioner. Its main characteristics are that it allows the petition to be viewed online, to read additional related information online, a possibility to allow supporters to append their identity to the petition online and to allow participation in an online forum where they can voice their views (either in support or against) on each ePetition. An easy to read and short summary highlighting the key points raised is also helpful in focussing attention. Further, to make sure that the petitioners do not feel forgotten, they are kept informed of the progress made while their petition is under study in Parliament. Similar such measures are used in Germany and England.[58]

Other activities that reveal different types of eParticipation are Online Chats (for open communication between public and government officers), Online Meetings (where official meetings of the legislative branch are Webcast live), Online Meeting Places (where citizens can meet and exchange ideas), Online Debates (where electoral candidates can answer questions and hear what voters have to say), Online Protests (as seen from the events of the recent Arab Spring and demonstrations in Kiev, Ukraine, the public can use ICT and mobile phones to mount spectacular democratic protests that can rock the political class), Online Town Halls, Online Voting and Blogs.[59]

On a more elementary level, eDemocracy can be defined as the utilisation of ICT within the four corners of a political process by sectors which are democratic in nature.[60] It encompasses the following:

---

[56] Kotsiopoulos (2009), p. A-9.

[57] See *id*, p. A12 and also see footnote 16, where the researcher Macintosh (2003) is quoted.

[58] See *id*, p. A12.

[59] See *id*, pp. A13–A14.

[60] See Clift (2003).

eGovernment: The use made, most commonly, by administrative agencies to deliver public services and information to common citizens by effective use of electronic and ICT services.[61]

eParliament, which entails the usage of ICT by members of government for the purposes of involving citizens in a more active manner by allowing for better information and improved management of communication. It concerns legislative, consultative and deliberative assemblies at various levels. It can help to ensure a more deliberative form of democracy with greater participation by all stakeholders.[62] eParliament thus constitutes parliamentary processes in the nature of legislation which is assisted by electronic means, ICT enabled ballot processes and higher degrees of transparency.[63] For this, it is essential that eParliament enables greater communication between citizens and leaders, so that there can be greater input from citizens both in terms of preparing agendas and finalising decisions.[64]

eLegislation, which deals with the usage of ICT to make legislative procedures such as drafting, commenting, consulting, amending, voting and publishing laws by elected members more transparent, more readable and thus makes the public more aware about the laws.[65]

eJustice, wherein ICT is used in order to improve the efficiency of the justice system and the quality of justice. It includes communication through electric means, exchange of data and also access to judicial information.[66] ICT helps to speed up the proceedings in court, to provide online tracking of case proceedings, the use of videoconferencing techniques in court rooms, etc. [67] eJudicial advocacy: Interestingly enough in USA, eDemocracy has been used to attempt to influence judges in matters which are deemed of public importance by sending them messages—both online and through post.[68] This is an extension of American opinion culture, whereby the public chooses winners of reality TV shows, etc.[69]

eMediation, which entails the usage of ICT to help resolve disputes without requiring the opposing parties to be physically present in the same room.[70]

eEnvironment, which uses ICT for the purposes of greater public participation in the assessing, planning, protecting and using of natural resources.[71]

---

61 Duvivier (2013), p. 18.

62 See Appendix to Recommendation CM/Rec(2009)1 Principle of eDemocracy 36.

63 Kotsiopoulos (2009), p. A-9.

64 See Appendix to Recommendation CM/Rec(2009)1 Guideline on eDemocracy 43.

65 See *id*, Principle on eDemocracy 37.

66 See *id*, Principle 38.

67 See *id*, Guidelines on eDemocracy 46 and 48.

68 For example, see Sacks (2012).

69 Duvivier (2013), p. 20.

70 See Appendix to Recommendation CM/Rec(2009)1 Principle of eDemocracy 39.

71 See *id*, Principle 40.

eElections, eReferendums and eInitiatives use electronic means for the purposes of holding elections, referendums and initiatives.[72] eElectioneering has been further defined as involving the use of ICT to help voters to elect politicians. It should be noted that the use of the electronic medium for the promotion of electioneering and related activities was, unsurprisingly, the first step in the nascent stages of eDemocracy.[73]

eVoting, which entails the usage of ICT for casting of the vote by remote means, thereby making the process speedier, better monitored, votes get electronically registered and participation is not hampered by distances or handicaps.[74] eVoting thus essentially comprises electronic versions of the electoral processes, citizen's referendums and other public policy opinion garnering initiatives.[75] Referendums can of course vary in political nature and context—ranging from referendums to be organised in Scotland and Catalonia on the one hand and the recent referendum allegedly conducted in Crimea. This shows the political situation which can affect voting in general and eVoting in particular.

eConsultation, which uses ICT to allow the collection of opinions of target groups on specific issues. Decisions reached finally may thus be directly or indirectly influenced, although there is no obligation to act in accordance with the opinions so garnered.[76] This is also known as eRulemaking: This registers inputs from the pubic (by way of their online comments), to administrative rules proposed by the government. However, often the comments of the public are disregarded by the administrative agencies, thereby putting a question mark on the reason why these comments were invited in the first place![77]

eInitiatives, which allows the usage of ICT by citizens to develop, initiate and forward political proposals.[78]

ePetitioning, which is the use of ICT by citizens to sign online petitions and to thus deliver a protest or recommendation to a democratic institution. This helps to foster greater debates n democratic circles.[79] This is based on the premise that ICT can be used by the public to actually influence how laws are drafted and enacted.[80] Petitioning the Government for relief or change by expressing one's ideas, hopes

---

[72] See *id*, Principle 41.

[73] See also Macnamara and Kenning (2010) for an interesting insight into e-electioneering.

[74] See Appendix to Recommendation CM/Rec(2009)1 Principle of eDemocracy 42.

[75] Kotsiopoulos (2009), p. A-9.

[76] See Appendix to Recommendation CM/Rec(2009)1 Principle of eDemocracy 43.

[77] Duvivier (2013), p. 19 at footnote 47, where Assateague Island National Seashore, Personal Watercraft Use (2003) is quoted as an example. This case is available at http://www.gpo.gov/fdsys/pkg/FR-2003-05-30/html/03-13578.htm. Accessed 2 Apr 2014.

[78] See Appendix to Recommendation CM/Rec(2009)1 Principle of eDemocracy 44.

[79] See *id*, Principle 45.

[80] Duvivier (2013), p. 22.

and concerns itself is not, per se, a new activity.[81] Thus, for example, we can see this right to petition being mentioned in the Magna Carta.[82] In the English Bill of Rights 1689, the right to petition is also specifically provided.[83] The First Amendment of the US Constitution also states that people have the right to petition the government for redressal of their grievances.[84] An interesting version of an active online ePetitioning site can be seen in the case of United Kingdom.[85]

eCampaigning helps the public to engage with one another through the usage of ICT, thereby mobilising and influencing the shaping or implementation of policies which have a bearing on the public.[86]

ePolling/eSurveying uses ICT to obtain opinions from the public.[87]

2.2 Further Categorisation of Models

As enumerated by a researcher, eDemocracy models could also be categorised as comprising of two main types, namely the consultative mode, where communication flows in a vertical manner between the citizen and the state, and the participatory model, where interaction takes place in multiple directions and in a more complex manner.[88]

2.3 A Holistic Approach

There exists a third and more holistic form of categorisation, wherein increased transparency with regard to governance and government affairs (e.g. a government run official Website), increased participation by active citizenry in the decision-making process (e.g. eConsultation) and increased deliberation among citizens by means of forums, is stressed upon.[89]

---

[81] See Borough of Duryea et al. (2011) at page 2495. http://scholar.google.com/scholar_case?case=14079373987044019788&hl=en&as_sdt=6&as_vis=1&oi=scholarr. Accessed 2 Apr 2014.

[82] See Magna Carta (1215), para 61. http://www.nationalcenter.org/MagnaCarta.html. Accessed 2 Apr 2014.

[83] See English Bill of Rights (1689) http://avalon.law.yale.edu/17th_century/england.asp. Accessed 2 Apr 2014.

[84] See U.S. Constitution, First Amendment, http://www.law.cornell.edu/constitution/first_amendment. Accessed 2 Apr 2014.

[85] See http://epetitions.direct.gov.uk/. Accessed 2 Apr 2014.

[86] See Appendix to Recommendation CM/Rec(2009)1 Principle of eDemocracy 46.

[87] See *id*, Principle 47.

[88] Chadwick (2003), pp. 9, 13, 14.

[89] Kotsiopoulos (2009), p. A9.

3 In the EU and Switzerland

The Lisbon Strategy (adopted in March 2000) led to the development of the eEurope Action Plan for the exploitation of the ePotential in Europe. Subsequently, the "i2010 eGovernment Action Plan—Accelerating eGovernment in Europe for the Benefit of All" laid emphasis on, interalia, bridging the digital divide, increasing efficiency and effectiveness, ensuring data privacy and security, and in particular—strengthening democracy and participation by citizens in Europe. Under this citizens were sought to be empowered by means of offering of extended information, discussion and participation rights. To enable the citizens to control politics, eVoting and eElections are seen as the key.[90] Further, to create a society based on information and knowledge, other steps such as the use of computer aided expert systems and knowledge databases are required for community formation and to create public memory.[91]

3.1 Important Legal Aspects of eDemocracy in the EU

Some of the important legal aspects of eDemocracy in the EU are covered by the following documents. First is the Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for evoting (Adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies). Next comes the Recommendation CM/Rec(2009)1 of the Committee of Ministers to member states on electronic democracy (edemocracy) (Adopted by the Committee of Ministers on 18 February 2009 at the 1049th meeting of the Ministers' Deputies). Then, there is the Declaration by the Committee of Ministers on Internet governance principles (Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies). And finally, there is the Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (2013).

3.2 Salient Features of These Legal Documents

The author presents some of the salient features of these legal documents:

The Principles of edemocracyas outlined in Rec(2009)1 broadly deal with certain truisms, namely that eDemocracy is in addition to and complements traditional

[90] Meier (2012), pp. 2–3.

[91] See *id*, p. 160.

processes of democracy. The essential point is that good governance is the key to eDemocracy. Further, eDemocracy offers an opportunity for enhancing participation in the civic processes by helping to disseminate information and encouraging deliberation, thereby enabling better decision-making at the political level. Being new technology, it is hoped to be more attractive to young people. It should be noted that its goals are transparency, accountability, accessibility and responsibility, along with fostering greater trust in the political process. However, to be properly designed and implemented, information should be widespread, nationality should be eschewed in favour of long-term residence and integration, citizen participationship should be heightened and citizen should be empowered, included and allowed to debate.[92]

The issues related with eVoting as outlined in Recommendation Rec(2004)11 are as follows. There is an increased emphasis by various governments to make the voting process suitably designed to attract voters and also to ease the voter's convenience. For this, eVoting can play a pivotal role. However, the question arises as to how to make eVoting fool-proof.

eVoting must also comply with core legal standards. Some of the principles covered herein are universal suffrage, which is an essential consideration and hence the system should be easy to understand and use. eVoting should be considered as an optional means of voting. Also important is the concept of equal suffrage, hence a voter should only be allowed to cast one vote. The voter should not be able to vote in the same election using multiple voting channels. Free suffrage should be ensured as voting must be free and fair. The voter should be able to change their decision with regard to their voting choice at any point in the eVoting process before he actually casts his vote. The previous choice should not be recorded in the system. In accordance with the principle of secret suffrage, it should be impossible to authenticate the identity of the voter. The votes should remain anonymous at all times.[93]

It should be noted that national digital smart/ID cards such as those adopted by Estonia, Italy and other nations have made authentication easier and more reliable, thus enabling smoother eVoting procedures.[94]

Equally important is the adherence to strict procedure and safeguards in this process. For this, it is essential that the following issues are focussed upon[95]:

Transparency: Voters should understand and have confidence in the eVoting process. The functionality of the process should be public knowledge. The opportunity to practise voting on the system before the actual casting of the electronic vote is beneficial. Also required is free and lawful access to the system by neutral experts and observers.

---

[92] Appendix to Recommendation CM/Rec(2009)1 Principles of eDemocracy 1–34.

[93] Recommendation Rec(2004)11of the Committee of Ministers to member states on legal, operational and technical standards for evoting. Appendix I, Legal Standards, Principles.

[94] Kotsiopoulos (2009), p. A-27.

[95] Recommendation Rec(2004)11. Appendix I, Legal Standards, Procedural Safeguards.

Verifiability and accountability: The authorities must be able to verify and certify the components of the eVoting system. A duly appointed independent body of experts should verify the security of the system. There should be a possibility of recounting the eVotes which have been cast. Re-run of the elections should be allowable by the system.

Reliability and security: The possibility of fraud in the elections should be avoided. Serious issues that affect the eVoting system, namely malfunctioning of the system, breakdown of parts or denial of service attacks via the Internet should be especially catered for. Access to the central infrastructure, servers and electoral data should be closely monitored and controlled. Command and control should be dual based, and concentration of all powers in a single individual should be avoided. Further, the voting data should be encrypted. The voter's authentication information should be delinked from the voter's final decision at a specific stage in the eElection process.

The biggest fear of course is to verify that people are not selling their voter ID codes, especially in view of the fact that eVoting cannot be supervised at a voting station.[96]

One way around this tricky situation is to use electronic voting machines in voting stations. However, even these can have their faults, and hence, there is emphasis on researching ways to ensure that citizens know their votes have been counted. But this verification process can also be counterproductive, as it could potentially violate the principle rule of secret ballots.[97] Although the more sophisticated computer programs can overcome such hurdles, a key factor is also the prevailing political culture.[98]

Also in Rec(2009)1, "enablers, challenges, barriers and risks" to eDemocracy are studied in detail. Therein a host of enabling factors such as political will, trust and transparency, access to technology, user friendliness, accountability for citizen's inputs, etc., are enumerated.[99] It is also stressed how important it is that citizens should not be misled, lied to, and that there is no defamation, incitement, hatred or discrimination in the course of eParticipation.[100] Certain other key features that should not be overlooked are the main goals of forming rules to regulate eDemocracy is to ensure empowerment and to provide adequate safeguards.[101] Similarly, while anonymity and confidentiality have their advantages, voter identity and authentication should not be compromised in the course of eDemocracy.[102] Disclosure of public information should certainly go hand in hand with

[96] Kotsiopoulos (2009), p. A-10.

[97] Kotsiopoulos (2009), p. A-10.

[98] See also Recommendation Rec(2004)11, where concepts such as operational standards for eVoting (Appendix II), Technical requirements (Appendix III) and security issues in the pre-voting, voting and post-voting stages (para.77 onwards) are considered in detail.

[99] Appendix to Recommendation CM/Rec(2009)1 Guideline on eDemocracy 79.

[100] See *id*, Guideline 80.

[101] See *id*, Guideline 81.

[102] See *id*, Guideline 83.

confidentiality of the interests of the concerned stake holders.[103] When personal data are held by public authorities, it must be safeguarded against abuse and misrepresentation.[104] Also since eDemocracy methods are prone to misuse, there must be a zero-tolerance attitude towards such breaches.[105] It is particularly important that eDemocracy rules and regulations should safeguard human rights and fundamental freedoms.[106] The truth is that eDemocracy goes hand in hand with eSecurity, which includes security of information, data, documents, voting processes, Internet access, networking and ICT.[107] It is also important that there are appropriate levels of security in place, for each setting.[108] Further, standardisation of document formats, system applications and architecture, etc., should be rigorously pursued in order to simplify and speed up political documentation and decision-making.[109]

In this connection, it is interesting to note a case study of eVoting in Austria wherein an analysis of Rec(2004)11 was conducted. Since this recommendation comprises of legal standards, operational standards and technical requirements, specific instances of technical attacks during the eVoting period and countermeasures were studied in detail. Different types of attacks were noted during the eVoting period. They are described as follows:

3.2.1 Distributed Denial of Service Attacks[110]

This attack was noticed at least three days before the eElection by the staff who were providing security for the eVoting exercise. An Austrian organisation which was involved with issues related with the social uses of ICT published a particular Web tool. This Web tool was showcased as a server availability checking tool. It allowed users with computers to conduct a stress test on the eVoting system (at all times, several times of the day) to verify its availability, in an ostensibly legal fashion. This sophisticated tool written in javascript allowed a single computer to produce a heavy load on the Web server of the eElections. Further, this particular type of attack was well distributed (although managed centrally), thus making it difficult to detect the attackers or to block them. This attack worked on the basis of computer users who participated willingly (albeit unwittingly).

A suitable countermeasure was developed to stop this attack. However, it showed the various practical issues that arose with this type of distributed denial

---

103 See *id*, Guideline 84.

104 See *id*, Guideline 85.

105 See *id*, Guideline 87.

106 See *id*, Guideline 92.

107 See *id*, Guideline 96.

108 See *id*, Guideline 97.

109 See *id*, Guideline 98.

110 Ehringfeld et al. (2010), pp. 228–230.

of service attacks (dDoS) attack, namely: blocking all incoming traffic online from a particular source IP, although a common and effective measure, would have been unsuitable in this instance as it would have deprived an unknown number of voters from voting in this eElection. Further, last minute software changes or adaptations as counter measures to such dDoS attacks could possibly invalidate the certification for the eVoting exercise, thereby invalidating the whole election.

Thus, it was shown that the most effective counter measure was that eVoting was used as an additional voting possibility and was scheduled before the paper ballot election. In this way, legally speaking, it was possible to annul the eVote and enforce the paper ballot system instead. Therefore, a recommendation was made to alter Article 45 of Rec(2004)11 to the effect that remote eVoting should end before the paper ballot election commences and that eVoters should be informed in case of an annulment of the eVote so that they may cast the paper ballot instead.

3.2.2 Phishing Attacks[111]

A political party set up a Website which was deceptively similar to the official voting Website. Even the voting process was copied. The URL used was also deceptively similar. All of this was done to mislead the potential eVoters. Thus, it was hoped by the political party to gain sensitive data from the eVoters, or to cause irritation and annoyance to the eVoters.

Subsequent research showed that effectively counterattacking such a phishing attack requires the following acts, namely an official Website of the eElection should be established, and it should provide a single window system for all information related with voting in that eElection.

Further, it should be well advertised (in accordance with Article 46 of Rec(2004)11, especially since empirical data showed that most users navigated directly to the Website by manually entering the official URL into their browsers, or searched for the name of the election with the help of an Internet search engine.

Also in this regard, the Internet search engines should be actively monitored based on typical queries and their responses, phishers should be acted against immediately and decisively, domain names which are confusingly/deceptively similar to the official Uniform Resource Locator (URL) should be bought out in advance, the validation certificates used for proofing the integrity of the official Website should be of the highest order, and the eVoting Websites should be hosted exclusively within the exclusive domain space of the government.

The security layer of the citizen card used for the purposes of authentication should only allow access online if the connection is based on Hypertext Transfer Protocol Secure (HTTPS) and the connection should be exclusively to a government-related domain (which is not freely obtainable by non-government sources).

---

111 See *id*, pp. 230–232.

The registration and use of domain names which are deceptively similar to the official eElection domain name, immediately prior to and after the eElection period, should be carefully monitored with extra vigilance.

3.2.3 Smear Campaigns[112]

These are designed to discredit the eElections by referring to them as unreliable, insecure or controverted. This is done by playing upon eVoter's irrational fears regarding the inherent non-transparency of the eVoting process.

In this particular eElection, an anonymous smear campaign was conducted by the use of a false video purporting to show how the eElection result was subverted. It was alleged that an eVote cast in favour of one candidate instead led to marking on the electronic ballot sheet in favour of another candidate.

To counter this, it was necessary to set up an incident response team to quickly react to such potential public relations disasters, and to do so via a public communication channel which was already in place and well established.

3.2.4 Buying of eVotes[113]

Attempts were made to discredit the eElections by use of advertisements in the form of false flyers which offered to pay eVoters for casting their votes in the presence of the election observers of a specific political party. Generally, in elections, it has been observed that only when votes are cast in secret then there is no possibility for the briber to supervise the voter. However, it is theoretically possible to buy a vote in all forms of elections which are conducted remotely, including in eElections. This could be countered through the use of Article 51 of Rec(2004)11 which states that the voter in an eVoting system should not be provided with any proof with regard to who was infact voted for by him. It is also recommended to establish that an eVoter is aware of his responsibility to cast votes freely and secretly.

3.3 eDemocracy in Switzerland

Also in this connection, it is pertinent to see how eVoting is regarded in Switzerland, which although outside the EU is very close to it at the same time. eVoting is seen as a powerful tool in Switzerland, with potential to increase participation among the voters, improving voting quality and thereby helping political

---

112 See *id*, pp. 232–233.

113 See *id*, pp. 234–235.

rights to be implemented within a democratic set-up. Risks regarding integrity of the system and issues pertaining to the digital divide though still persist. On the whole, the Swiss experience in this field (which has been ongoing since 1998) has shown the substantial benefits of eVoting, namely meeting the citizen's need for simplicity and convenience in democratic procedures; catering for voters with disabilities or citizens living abroad, who may prefer to use their home computers for the purposes of eParticipation; its inclusive nature, whereby more voters are incorporated into the democratic process, similar to the introduction of postal ballots of the past; and counting of votes electronically, thus reducing the risk of human error.[114] The overriding feature though is that of trust, namely trust in the eVoting environment and in one's computer.[115]

On the other hand, the risks associated with eVoting have been found to be the digital divide, security and confidentiality (which can only be ensured if personal data and the ballot are kept separately from each other) and information overload (which is sometimes sought to be countered by reducing information intake—a process which in turn encourages irrational and populist tendencies). Another area of concern is the lack of transparency, since a new set of technical skills is required to deal with the three main aspects of eParticipation, namely: data generation, data transformation and data storage. In the past, a citizen could feel a sense of control over the democratic process of voting by helping to count the votes. However, this is now done electronically and is too sophisticated for the average voter to comprehend or to connect with.[116]

Of the various eVoting systems studied, the one used in Geneva is most interesting. The voting card (along with other paraphernalia) is mailed to the voters well in advance of the voting date. The voting card can be used only once (thus ensuring the one man, one vote principle) and is valid only for the coming election. The verification process is enabled by entering of an individual identification number (which is stated on the ballot sheet). On entering the correct number, the system connects the voter to a secure server. Here, the voter enters his vote. The system restates the choice made and the voter confirms it by giving his date of birth and the unique PIN code which can be obtained by scratching the ballot sheet. Lastly, the voter receives a confirmation from the system that his vote has been registered.[117]

It is pertinent to note that in Swiss usage, eVoting is fast gaining popularity and is second only to postal ballots, whereas traditional ballot box voting is a distant third.[118]

---

114 Gerlach and Gasser (2009), pp. 3–4.

115 See *id*, p. 4.

116 See *id*, p. 5.

117 See *id*, p. 7.

118 See *id*, p. 9.

4 The Approach Taken in USA

4.1 Introduction to the Scenario in USA

As we are aware, USA is a world leader in Internet-related activities, both commercial and non-commercial. It is also a typical Western-styled democracy, along with being also the richest and most powerful nation in the world. Issues such as low voter turnout, low accountability of politicians and general disdain of the youth towards the political system are also highly visible in USA.[119]

In USA, it should be noted that information is disseminated in vast numbers, directly leading to increased transparency. However, citizen's involvement and/or participation in the decision-making process is very sparse.[120]

There is a lot of focus on deliberative initiatives such as online forums and citizen's communication with elected representatives (including call-in radio shows where citizens can speak personally with elected representatives and some of the data are then posted on a Website). Then, there are participation initiatives such as forums for receiving feedback from citizen's, initiating proposals on a ballot, provision for online bidding as a form of eProcurement (which in effect allows for the widening of eDemocracy by allowing businesses to openly and freely participate in Government tenders in a transparent fashion) and provisions for receiving feedback from citizens with regard to drafting the budgetary needs of the town/city. A large part of eParticipation is reserved for transparency initiatives such as blogs of an official nature which are set up and maintained by specific public departments to provide information directly to the constituents and not routed through intermediaries such as the press, Webcasting of activities of the legislature at various levels, use of RSS feeds, etc.[121]

Thus, we can see that eDemocracy in USA is mostly about providing transparency to the whole political process. This allows citizens to use their ICT tools to monitor official activities. This, in turn, is hoped to increase vigilance and interest among the voters. It also helps to curb dishonest practices by politicians.

Incidents such as the online protests in 2012 against two US legislative Acts designed to counter piracy, namely the Protect IP Act ("PIPA") and the Stop Online Piracy Act ("SOPA") showed how easily and effectively companies such as Google, Wikipedia and Facebook were able to mobilise public support and make the US politicians aware of public opposition to the above-mentioned proposed Acts. This was done in a very different manner than the lobbying actions that are usually conducted by "old economy" companies. This may even serve as an indication of how the web-universe is a very different and multidimensional entity

---

[119] Kotsiopoulos (2009), pp. A-24–A-27.

[120] Peart (2007), p. 8, where this is attributed to prevailing American political culture.

[121] See Kotsiopoulos (2009), pp. A-25–A-26, where examples like those of Virginia's Governor Kaine's two call-in radio shows monthly and the discussion forum (http://gov.ca.gov/ask) which was used by Governor Arnold Schwarzenegger when he was in power in California, are provided.

when compared with the image of a flat eDemocratic ideal that one perceives eParticipation to comprise of.[122]

It must however be noted that the romantic vision of the emergence of ICT as a saving grace for the tottering system of modern representative democracy in Western countries such as USA (which are battling lack of public participation, disenchantment of young voters and a perceived lack of trust in politicians) has not really played out to its full potential.[123] There exists a view of great disillusionment with eDemocracy.[124] This view has been buttressed by various research activities which indicate that various eDemocracy tools such as online consultations, eForums, etc., have not really helped ICT to live up to its full potential of influencing policy changes and decision-making.[125]

Perhaps this is an indicator that the so-called cyber-democrats were wrong about their early optimism regarding the capabilities of ICT, and in their belief that simply placing the correct platform in place would serve as a guarantee for increased civic participation in the manner espoused by an electronically mediated deliberative democracy.[126]

Despite these setbacks, the enthusiasm of governments to engage in more projects related with eDemocracy continues unabated, especially as seen in the US with the OG Directive of President Obama—which stresses on the principles of transparency, participation and collaboration in the running of the government.[127] This in turn has led to the setting up of "open government" portals, the ability to single-handedly access high-value data from the databases of federal agencies, and development of initiatives such as Regulations.gov, the Open Government Dashboard, and Challenge.gov.[128]

This in turn has influenced other countries such as Canada, United Kingdom, Australia, etc.[129] Further, over 60 countries have signed the Open Government Declaration (OG Declaration) of 2011, being an international platform for domestic reformers committed to making their governments more open, accountable and

---

122 Perez (2013), p. 63.

123 Shane (2012), p. 3.

124 Ostling (2010), p. 4.

125 Dahlberg (2011), p. 866.

126 Perez (2013), p. 65.

127 Orszag (2009) Memorandum from the Director for the Heads of Executive Departments and Agencies. Executive Office of the President of USA. p. 1. http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf. Accessed 2 Apr 2014.

128 Perez (2013), p. 66.

129 See for Canada—http://data.gc.ca/eng. Accessed 2 Apr 2014. United Kingdom—http://data.gov.uk/ Accessed 2 Apr 2014. Australia—http://www.finance.gov.au/blog/2010/07/16/declaration-open-government/ Accessed 2 Apr 2014.

responsive to citizens.[130] Such activity has also spread to international organisations such as the World Bank and others.[131]

4.2 The Flaws Which Are Perceived by some Scholars in the USA System

In one research study conducted in USA,[132] an eParticipation consultative process was found to suffer from the following flaws namely that the search engine which supported the consultation Website was inadequate and unreliable (thereby rendering the collection of information difficult). Further, the collection of all the relevant data was a time-consuming and expensive affair, and was compounded by the fact that the entire maintenance of the system was consigned to just one man.[133] Also the participants in this program were inevitably experts, as the general public refrained from participating in most such complex and heavily loaded issues. The situation turned worse because the general public were cynical about their role in the online consultation process and its actual impact on the influencing of government policy. Further, many members of the public preferred to write directly to the politicians, avoiding the agency.[134] In this scenario, some of the ways to improve the system could include greater accessibility to information, possibility of follow-up action, support from higher authorities and being consistent.

Thus, it can be seen that eDemocracy often works in theory, but not in practice. Further, continued political support is the key to success for eDemocracy projects, since they require a lot of active intervention and this consumes a wide variety of resources.[135]

4.3 A View of the OG Directive in this Regard

The OG directive, when seen objectively, has shown the following positive effects, namely that it has given rise to a change in mindset. Thus, the government is perceived to be more transparent and participatory than in the past. It has also helped

---

130 See The Open Government Partnership comprising of over 60 countries. http://www.opengovpartnership.org/. Accessed 2 Apr 2014.

131 See The World Bank ICT Sector Strategy at http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:23118048~menuPK:8432091~pagePK:210058~piPK:210062~theSitePK:282823,00.html. Accessed 2 Apr 2014.

132 Perez (2013), p. 86.

133 See *id*, p. 87.

134 See *id*, p. 87.

135 See *id*, pp. 116–117.

like-minded members of the public (including ordinary citizens, experts and academics) to come together and discuss open governance. Further, it has led to a development of technology to help support and run eGovernance-related activities.[136]

However, there are some negative aspects too, especially when one considers whether there has been any improvement in democratic practices thanks to the OG Directive. One view is that continuity of the political support in regard to the OG Directive in the long run gives rise to uncertainty which therefore limits the potential of this program. Also too much faith is put in the belief that the technology itself will spur change in the social environment. This viewpoint ignores barriers such as sociological and psychological ones which in reality inhibit adoption of digital democratisation. The biggest challenges still remain in respect of creating public interest in eDemocracy.[137]

Convincing people that their views are important to the Government is especially difficult when officials view the public as being ignorant, ill informed and valueless.[138] A bigger challenge to eDemocracy is the fact that citizens are more often likely to be neither alert nor motivated enough to engage in online political engagement.[139]

4.4 The Road Ahead

Thus, one scholar sees the following as the key to development and progress of eDemocracy in USA[140]: He proposes building motivation by using online communities and social media. There is also a need to understand the limitations of the online medium and to interject into the online dialogue with the help of human and technological intermediaries to help enrich the content. Prioritising specific issues/areas for more intensive civic engagement is an important task. However, the question arises as to who will determine these specific issues and what effect this will have on expectations of democratic neutrality?[141] Creating/encouraging new technologies to develop eLiteracy and online deliberation is also very helpful, as is supporting political intermediaries such as interest groups, non-government organisations, academics, press, etc., to deepen democratic engagement.

136 See *id*, p. 118.

137 See *id*, p. 119.

138 Stromer-Galley et al. (2012), p. 93.

139 Perez (2013), p. 122.

140 See *id*, pp. 127–128.

141 Perez (2006), p. 122.

4.5 Involving Citizens of USA in the Legislative Process

4.5.1 Petitioning in USA and the Growing Role of eLegislation

Traditionally, in USA, legislative processes relating to the federal system of government have been difficult to access for common citizens. However, eLegislation is changing this because of its ability to communicate voter's thoughts to legislators with the help of ICT. But, as was seen in the example above of the protests against SOPA in 2012, there can be some negative aspects, namely: manipulating members of the public by playing on their emotions, the anonymity of the protestors online and the use of (temporary) deprivation of services by influential Websites (such as Google, Wikipedia, etc.) to attract the attention of Internet users, often in favour of the opinions voiced by the owners of the Websites. Thus, it is apparent that eLegislating can be used in a constructive manner and also abused in an obstructive manner, and it is pertinent that common citizens are made aware of both sides of the coin.[142]

Given the large numbers of common people who use social media, it is but natural that the Internet will also be used for activities which are of a civic or political nature.[143] Thus, where earlier political speeches were given in the streets and parks to mould public opinion, a lot of such activities have now shifted into the realm of the electronic media.[144]

4.5.2 Historical Perspective

In the past, petitioning was most commonly exercised through the medium of letters or the gathering of multiple signatures on a petition.[145] Although the US Congress was not obliged to enact legislations on the basis of such petitioning by the public, the petitions were nonetheless reviewed in a serious manner.[146]

---

[142] Duvivier (2013), pp. 10–11.

[143] Sherman (2011), p. 96.

[144] Duvivier (2013), p. 17. Also note pp. 11–12 where the influence of social media in political transition is discussed. For example, the Facebook Webpage dedicated to Mr. Khaled Said who had died allegedly at the hands of Egypt's secret police in 2010 led to a revolution on the streets of Egypt leading to the overthrow of the Egyptian government. Another stark example is the clever use of an online, state of the art electioneering campaign named Project Narwhal by Mr. Obama for the elections in 2012 to the office of the President of USA. This was more successful than the Website launched by his rival Mr. Romney, which performed unsatisfactorily.

[145] See *id*, p. 26. Although there are historic reasons for their declining power at the Federal level, [in 1844, a rule was passed in USA whereby petitions would be referred to committees instead of being brought to the attention of the whole House of Representatives. This in effect meant that they could now be conveniently ignored under the guise of action by the committee (See p. 28)]. It should be noted that in 2012, 186 initiatives and referendums at the state level were voted for by citizens in 39 states of USA. (See p. 32).

[146] See *id*, p. 28.

4.5.3 The Role of ICT in this Regard

From the above, it is clear that petitions and referendums, per se, fail in giving any role in legislation making at the Federal level in USA to citizens. But it is hoped that by the use of ICT, this can be changed. To give citizens a chance to share their collective expertise and information, there are some new possibilities in USA.[147] Thus, the White House has come out with an electronic petition platform incorporated in its "We the People" Website.[148] If petitions cross the stipulated threshold of signatures, then the USA administration promises to respond with their reply.[149]

It should be noted, that just like in other democracies, the voice of the citizens in USA is only audible to the politicians during elections. But laws are enacted during periods between election cycles, and it is not possible for voters to compete with vested interest groups who use expensive lobbyists to influence legislators. Opinions voiced at town hall meetings or correspondence by post/telephone is often not enough to get the citizen's feeble voice across to the legislators at the time when public opinion actually matters the most—during the actual drafting and enacting of laws.[150] The use of ICT by voters to register their feedback with politicians is envisaged differently by different researchers—some see such online activism as being merely a "difference-of-degree" form rather than a "difference-in-kind" form, when compared with traditional activism.[151]

4.6 Difference Between Europe and USA

The European lead is exemplified by experiments such as those of Switzerland, Estonia and the UK. Meanwhile, the US emphasises in transparency rather than participation.[152]

Two key issues that arise as problem areas are related with voter identification and the different voting systems involved. The fact is that most Europeans have a unique identification number which is issued by their respective governments. This is the most important component of eVoting. Citizens in USA do not have such a numerical form of identification. Secondly, in USA, the political system is based around the principle of "the winner takes it all". This means that a politician

147 See *id*, p. 37.

148 See http://www.whitehouse.gov/blog/2011/09/22/petition-white-house-we-people. Accessed 2 Apr 2014.

149 Thus, in response to a petition to secure resources and funding, and begin construction of a Death Star by 2016, which crossed the required threshold of signatures, a Government response was guaranteed. For the response, please see https://petitions.whitehouse.gov/response/isnt-petition-response-youre-looking. Accessed 2 Apr 2014.

150 Duvivier (2013), p. 39.

151 Karpf (2010), p. 9.

152 Kotsiopoulos (2009), p. A-71.

standing for elections in USA has a lot more to lose than his European counterparts who follow the "proportional representation" voting system. Thus, the European model is less prone to corruption or fraud.[153]

5 The eCitizen Question

5.1 Differing Views on eParticipation for Citizens

One researcher has compared the different approaches adopted by Steven Clift and Ann Macintosh.[154] According to him, Clift proposes to be proactive in building up the structures of eDemocracy and to construct a community of networks thereby facilitating ways for people to enter into political discussions which can then be used to influence good governance. The Macintosh approach is to use government funding to enable academic researchers to build and operate tools which allow the public to communicate with the legislative and executive branches on issues of public importance.[155]

However, it should be noted that research has shown that the existence of an "informed citizen" is a myth, particularly since it has been observed that most citizens are less informed and are prone to taking shortcuts when it comes to decision-making, and hence they need to be guided by intermediaries such as political parties, civic groups, mass media, etc.[156] Those who hold this view also point to the barriers which exist in our society towards a wider form of engagement of the public in a democratic set-up, namely: "epistemic scarcity, attention scarcity and motivational scarcity".[157]

Further, research has shown that Internet-based democratic set-ups work best in an open-structured environment where social and technological entrepreneurs are actively involved. However, once the eDemocracy project is streamlined, centrally coordinated and furnished with a structured framework then the motivation and enthusiasm levels often crash.[158]

5.2 Citizen Archetypes

In this connection, it is interesting to note that one scholar has raised a distinction between various citizen archetypes. He defines citizens as being either the "info-lite" citizen who is passive, not very inclined to research and makes his political choices based on his limited experiences, or the "push-button citizen" who is willing to

153 Kuzelewska and Krasnicka (2013), p. 353.

154 Kotsiopoulos (2009), p. A 14, where in footnote 21, Rilley CG is quoted.

155 See *id*, pp. A-14–A-15.

156 Perez (2009), p. 47.

157 Perez (2013), p. 76.

158 See *id*, p. 80.

exercise his right to vote and participate in referenda, but still shies away from active deliberation, or finally the "actualizing citizenship", who is most comfortable with open governance and fullsome participation of the public in the government process. Thus, eDemocracy technologies used by the Government should be mindful of these different types of citizens and their individual capacities. In this context, the scholar asserts that eDemocracy is "democratic space where anyone can stake a claim to be heard and respected and all proposals have a chance of being acted on".[159]

5.3 The Punctuated Citizen

A different approach is that of the "punctuated citizenship".[160] This definition acknowledges the above listed three citizenship types as coexisting in each of us, and that we ceaselessly vacillate between these three states. However, a citizen is neither constantly actualized nor continuously passive.[161] Further, since punctuated citizenship accepts that citizens have limitations when it comes to knowledge, attention and motivation, then their participation in the political process is punctuated, unstable and not maintainable over long periods. However, there exists a certain amount of latent political activity in all citizens, and this should be exploited for the purposes of eDemocracy.[162]

6 ePerson–ePersonality–eParticipation and the "Trishanku" Effect

To indulge in eParticipation, we need to understand the concept of ePersonality. This in turn leads us to the question of what is an ePerson? These questions are closely linked with our digital personalities. A recent study showed that there are at least four types of digital personalities, all of which are possible due to the influence of ICT in our everyday lives. These digital personalities vary from those who seek efficiency by going online to those who value increasingly sophisticated connectivity between various devices.[163] Perhaps one can look towards the ancient writings of Hinduism to draw surprising parallels to today's riddle of ePersonality. In the Hindu Epic "Ramayana", authored by Valmiki (the exact date of authorship is unknown but it is believed to be several thousand years old), the concept of Trishanku is explored in the 60th Sarga (chapter) in the Baalkaanda.[164]

---

[159] See *id*, p. 122–123.

[160] See *id*, p. 124.

[161] Muller (2011), p. 3.

[162] Perez (2013), p. 125.

[163] Please see this press release from IBM (2012).

[164] Please see an online version of the Ramayana, along with its English translation here: http://valmiki.iitk.ac.in/index.php?id=translation. Accessed 2 Apr 2014.

Trishanku was an Indian King who wished to travel to Heaven in his own mortal body. Such an act was not permissible under the laws of Heaven. Trishanku prayed to the sage Vishwamitra to help him attain his goal. The wise sage agreed to this request and lifted Trishanku to the very gates of Heaven. However, here the entry of Trishanku was blocked by Indra, the King of Gods. Thus, pushed off Heaven, Trishanku fell towards the earth, beseeching the sage for help. Enraged at this turn of events, the sage created an alternate heaven for Trishanku, complete with clones of galaxies, stars and even Gods. This cloned Heaven is believed to be a southern version of the Ursa Major Constellation which is found in the Northern Hemisphere. Seeing this absurdity, the Gods proceeded to the mighty sage and worked out a face saving compromise which was agreeable to both parties. It was decided that Trishanku could stay in a heaven, but not in the original Heaven. Instead he could stay in the cloned version of Heaven, suspended upside down, for all eternity.[165] Here, he is neither subject to the laws of earth nor is he required to follow the laws of Heaven, a victim instead of compromise.[166]

The author is of the view that a similar fate awaits an ePerson who is enmeshed in the digital world of Internet and ICT. In order to enable the ePersonality to flourish, one must create a parallel online universe, where rights and liabilities mirror those found in our various earthly Conventions and Declarations related to human, cultural and political rights, but where the distinction between the real world and the online world persists—thereby creating a situation wherein the twain shall coexist but never meet. Once such a Trishanku's cloned Heaven exists, then it is easier to identify the boundaries which can then be blurred sufficiently so as to create a semblance of similarity between the two distinct worlds. Thus, one's human rights in the digital medium would mirror the human rights found in real life but would not be considered as being the same. Acceptance of such a state of affairs makes the concept of the punctuated citizen more easier to follow, because such citizens—namely the passive, the willing and the active, already exist in our non-digital worlds, and they thus mirror those that we see online.

7 Conclusion

7.1 Some Eternal Truths

Thus, we can see that eDemocracy can develop only when ICT and the Internet evolve further.[167] As was outlined by the OECD way back in 2003 in its article titled "Engaging Citizens Online for Better Policy-making", some important points raised were that technology is not the solution, it simply enables us to reach towards the solution. Further, information must be provided online for success of

[165] Please see another English version of the story of Trishanku here: http://www.valmikiramayan.net/bala/sarga60/bala_60_prose.htm. Accessed 2 Apr 2014.

[166] Calamur (2012).

[167] Kotsiopoulos (2009), p. A-15.

the eDemocracy system. But it should not be forgotten that information in terms of quantity cannot override quality. Also the online consultations should be actively promoted and effectively moderated to be successful. Also to be noted are the cultural factors which can affect citizen's online behaviour and subsequent engagement. These are distinct from the technological barriers.[168]

The author thinks that these points are still relevant today, after more than 10 years. Also what needs to be noted is the convenience that the practice and usage of Internet has brought into our lives. eVoting is thus the pinnacle of convenience in today's time and age.[169] But given the propensity of ICT networks to be subjected to surveillance or being hacked into, the bigger question that the author poses is whether we should fear the proverbial big brother?

Perhaps it is also pertinent to explore ePersonality from a different angle, hence the reference to the metaphorical "Trishanku" who is symbolic of the modern day ePerson, fully immersed in the digital world of Internet and ICT. His existence can flourish only in a parallel online universe, where rights and liabilities mirror those found in our various earthly Conventions and Declarations related to human, cultural and political rights, but where the distinction between the real world and the online world persists—thereby creating a situation wherein the twain shall coexist but never meet. By accepting this metaphor from ancient Hindu mythology, we can appreciate the concept of the Punctuated Citizen. Such citizens—namely the passive, the willing and the active, already exist in our non-digital worlds, and they thus mirror those that we see online.

7.2 What eDemocracy Needs?

7.2.1 Political Willpower

As stated by one researcher, political willpower is important for this venture, along with adequate human resources and capital, both of which are allocated much in advance.[170] Coordination between various government agencies is the key, because efficiency and cost savings can help the eDemocracy program. Given adequate time, the process can evolve under the glare of open participation and free flowing of information, coupled with support of a technical nature. A well staffed government agency alone can help ICTs to fulfil eDemocracy ideas in eGovernance by developing policies and monitoring the issues.[171] The Estonian example shows that once the technical requirements are met (with the usage of digital signature cards, multiple PINs, card readers, etc.) and the people have been adequately exposed to

[168] See *id*, p. A-53.

[169] Alvarez et al. (2008), p. 3.

[170] Clift (2004), p. 5.

[171] Kotsiopoulos (2009), p. A-53.

such technologies so as to make them feel comfortable using them, then acceptance for eVoting will grow steadily.[172]

7.2.2 Citizen's Involvement

When citizens stop voting or participating in the political process, it is indicative of the sad fact that they have lost hope and do not believe that their views matter to their government.[173]

The present state of affairs as far as democracy is concerned is rounded up in this quote from the report of a consultation paper: "We live in an age characterised by a multiplicity of channels of communication, yet many people feel cut-off from public life. There are more ways than ever to speak, but still there is a widespread feeling that people's voices are not being heard".[174]

The UK Government's eDemocracy strategy visualises the following key, related components, namely: democracy needs participation of the people which in turn is on the decline in the traditional sphere; citizens nonetheless remain motivated enough to dedicate time, effort and energies in matters which are of relevance to them; and ICT is changing society and can consequently help in broadening the engagement of the citizens in public policy matters. But the key to eDemocracy is democracy and not technology.[175]

7.2.3 Effective Consultation Techniques

The UK Government's Code of Practice on eDemocracy offers specific criteria for consulting online. These include timing of consultation—so that the consultation can have actual impact and is taken into account at each stage. Also needed is clarity about the questions asked, those who are questioned, the time frame and the purposes of the questions. A key feature is simplicity and conciseness of the consultation document. Widespread availability of all documentary information to all interested parties is especially helpful. Also time for collecting responses—ranging from twelve weeks or more for the consultation—is important. An analysis of the responses should be open-minded, and reasoned decisions must be the norm. And above all, a coordinator should be appointed to monitor and evaluate consultations, so that the lessons learned are shared and not forgotten.[176]

---

172 Beckert (2011), p. 4.

173 Kotsiopoulos (2009), p. A-54.

174 UK Government (2002), p. 8.

175 Kotsiopoulos (2009), p. A-55.

176 UK Government (2002), pp. 1–2.

7.3 Summary of Case Study Results

Two researchers have looked into certain examples and have stated in respect of Estonia that it has developed remarkably in the field of eDemocracy initiatives. Further, Internet is highly prevalent in Estonia. However, the democracy deficit and the general lack of faith in the government offices and working style remains.[177] Although voter turnout at elections to the European Parliament in Estonia has increased to up to 43 % (in 2009) when compared with 2004 when there was no provision for eVoting and voter turnout stood at 27 %, the link with eVoting is considered to be smaller in magnitude.[178] In the case of Italy, problems exist because of the deep digital divide, which has made eDemocracy inconsequential to a large proportion of the Italian populace.[179]

Switzerland has a strong federal structure. There is also a steady tradition of direct democracy, since any citizen has the right to initiate a vote on any issue of significance, provided that a certain number of co-signatories sign in. The use of ICT in such a situation would be ideal. However, as one researcher suggests, eVoting has not become generally acceptable because of arguments ranging from the risk factors, costs, the issue of digital divide to the aspect of its detrimental effect on the symbolism associated with the physical act of voting. This may also explain why some political parties still oppose it.[180]

Conversely, in the case of Latin America, one researcher suggests that eParticipation is often used as a ruse merely to advertise government activities and to attract funding, instead of improving democracy in general.[181]

Another researcher suggests that all the eParticipation requirements are unlikely to be met by any single, general size, sophisticated e-tool. This is especially so because of the various languages, cultures and technical skills that one sees in human society. These differences only serve to exclude some groups from eDemocracy.[182]

7.4 ICT and Democracy

Thus, the role of ICT in eDemocracy can be summed up as follows, namely that ICTs may not be used to their fullest value in a democratic set-up, unless the leaders want them to be so used. ICT usage in democracy is not faultless. Adaptation would depend on conditions, cultural and legal issues, and also on how it is

177 Peart and Diaz (2007), p. 13.

178 Beckert (2011), p. 1.

179 See *id*, p. 22.

180 Mendez (2007), p. 15.

181 Welp (2007), p. 16.

182 Kotsiopoulos (2009), p. A-65 where in footnote 88, Macintosh (2003) is quoted.

followed up subsequently. Success cannot be taken for granted, as it may differ in different countries and may be changed by new leadership. Also ICT has immense value and can help to enrich democracy with new tools. Thus, for eDemocracy to succeed—articulation, deliberation and dedication are important.[183]

7.5 Dangers of eDemocracy

As outlined by access2democracy NGO, eDemocracy is not bereft of dangers. If eDemocracy is not rightly implemented, it can become a tool in the hands of politicians for enforcement of wrong policies under the excuse of populism. Further, the threat to privacy is real, especially in the absence of accountability and transparency. There is also a need to be on the alert against malpractices and scam practices in the guise of online eDemocracy Websites which are designed to rip off innocent citizens by promising them access to policy-making. Mocking citizens (who are already disillusioned with politics) by the use of half-baked eDemocracy projects risks increasing public ire.[184]

Further, as a report stated back in 2003, there is a danger of fatigue creeping into the eConsultation process, particularly when there is a lack of suitable feedback from the government to the people. This in turn stokes the fires of disillusionment. There is also a need to institutionalise the process for analysing citizen's inputs and contributions, both solicited or otherwise. All of this is compounded by the lack of studies on eEngagement that clearly draw a link between such engagement and consequent influences on the decision-making process, leading to actual changes in government public policy.[185] The author feels that one decade later these issues still persist and are relevant.

As another researcher has stated, ICTs are not an equal opportunities provider for all concerned citizens, since they tend to be inherently undemocratic. The electorate is often divided into the haves (with access to the modern tools and knowledge of their use) and the have-nots.[186]

Looking towards eVoting, the main dangers can be summarised as follows: First is the issue of free and secret voting, for example, in the context of family pressures in voting matters. It is thus presumed that remote voting cannot guarantee the true privacy of a secured voting booth. Secondly the digital divide, which manifests itself in an upper class bias, is an important issue. Such divides (even though subtle at times) are evidence of how eElections are actually less

[183] Clift (2004), pp. 37–38.

[184] Kotsiopoulos (2009), p. A-68.

[185] Macintosh (2003), pp. 24–25.

[186] Kotsiopoulos (2009), p. A-69 where in footnote 93, Barney (2000) is quoted.

representative than traditional electoral processes. The question of culture is related with the civic ritual of casting one's vote physically in a secured voting booth situated in a public area is as much a communal affair, which eVoting insulates a citizen from. Fourthly, complicated structures, namely the technologically complex logistical issues with ensuring the success of eVoting make them more complicated than traditional voting procedures. Lastly, the effects on behaviour are seen when one views voting in an isolated environment (such as at home on a computer). It gives rise to a more individualistic identity (based on self-interest) unlike when one votes in a communal setting, surrounded by others. Further, the perceived threat of eSurveillance online can alter one's voting preferences. All this in particular affects the "floating" voters (similar in context to the swing voter) who can often turn to be the key determinant factor in an election.[187]

Added to the above is the fact that eVoting cannot and should not be compared with eCommerce, since free and fair voting is at the very essence of our democratic roots. Any affront to this principle can delegitimise the entire eVoting process, unlike in a commercial transaction which, if affected, has a limited impact on unrelated transactions. Further issues with transparency, anonymity, security flaws online, symbolism attached with voting, etc., have also been considered elsewhere in this chapter.[188]

7.6 Conclusion

Thus, we can see that eDemocracy and eParticipation are relatively new fields that have their plus points and their pitfalls. Further research is essential to study their long-term effects. eDemocracy has found a lot of takers in Europe and USA. eVoting is a logical expansion of the principle of postal voting and will only get more entrenched as time passes.

The Internet is present all around us and continues to increase its influence in our daily lives. Due to increasing computerisation of public administration, coupled with the need to involve the youth more proactively, there is a need to work on aspects related with convenience, efficiency, cost-effectiveness, etc. All of these can be provided for effectively with eGovernance.[189]

However, if it is not properly implemented, then it can potentially become a carrier of wrongful policies and bad practices. Further, facilities such as eVoting can result in significant alteration of the voting context, with hidden dangers that may someday manifest themselves in surprising ways.[190]

---

187 Oostveen and Van den Besselaar (2007), pp. 2–5.

188 Beckert (2011), p. 3.

189 See *id*, pp. 2–3.

190 Kotsiopoulos (2009), p. A-71.

References

Books

Acemoglu, D., & Robinson, J. A. (2013). *Why nations fail. The origins of power, prosperity, and poverty*. London: Profile books.

Barney, D. (2000). *Prometheus wired*. Vancouver: UBC Press.

Ghonim, W. (2012). *Revolution 2.0: The power of the people is greater than the people in power: A memoir* (pp. 84–85). Boston: Houghton Mifflin Harcourt.

Hood, C. C., & Margetts, H. Z. (2007). *The tools of government in the digital age*. Hampshire: Palgrave Macmillan.

Kerikmäe, T. (2014). EU Charter as a dynamic instrument. In T. Kerikmäe (Ed.), *Protecting human rights in EU: Controversies and challenges of the charter of fundamental rights* (pp. 1–4). Berlin: Springer.

Kuzelewska, E., & Krasnicka, I. (2013). E-voting to the European Parliament and United States Congress. An attempt of comparison. In E. Kuzelewska & D. Kloza (Eds.), *Elections to the European Parliament as a challenge for democracy* (pp. 335–358). Warsaw: Aspra.

Macintosh, A. (2003). Using information and communication technologies to enhance citizen engagement. In J. Caddy, & C. Vergez (eds.) *Promise and problems of E-democracy, challenges of online citizen engagement* (pp. 19–142). France: OECD Publications Service. http://www.oecd.org/governance/public-innovation/35176328.pdf. Accessed 2 Apr 2014.

Meier, A. (2012). *eDemocracy and eGovernment. Stages of a democratic knowledge society*. Berlin: Springer.

Perez, O. (2006). The Institutionalization of Inconsistency: from fluid concepts to random walk. In O. Perez & G. Teubner (Eds), *Paradoxes and inconsistencies in law* (pp. 119–144). Oregon: Hart Publishing. http://upecen.edu.pe/ebooks/Derecho/Teor%C3%ADa%20del%20Derecho/Paradoxes%20and%20Inconsistencies%20in%20the%20Law.%20Oren%20Perez%20and%20Gunther%20Teubner.pdf. Accessed 2 Apr 2014.

Shane, P. M. (2012). Online consultation and political communication in the era of Obama: An introduction. In S. Coleman & P. M. Shane (Eds.), *Connecting democracy: Online consultation and the flow of political communication* (pp. 1–20). The MIT Press. http://mitpress.mit.edu/sites/default/files/titles/content/9780262516464_sch_0001.pdf. Accessed 2 Apr 2014.

Articles

Alvarez, R. M., Hall, E. T., & Trechsel, A. H. (2008). *Internet voting in Estonia*. Resource document. VTP working paper #60. http://vote.caltech.edu/sites/default/files/vtp_wp60.pdf. Accessed 2 Apr 2014.

Beckert, B. (2011). *Evoting in Europe: Why we should look at it, which arguments we should consider and what to expect in the future*. European Parliament workshop. http://www.isi.fraunhofer.de/isi-media/docs/t/de/veranstaltungen/E-voting_arguments_Summary_March_2011.pdf. Accessed 2 Apr 2014.

Chadwick, A. (2003). *E-government and E-democracy: A case for convergence*? Paper presented at the Political Studies Association annual conference, University of Leicester. http://195.130.87.21:8080/dspace/bitstream/123456789/964/1/E-government%20and%20e-democracy%20a%20case%20for%20convergence.pdf. Accessed 2 Apr 2014.

Clift, S. (2003). *E-democracy, e-governance and public net-work*. http://www.publicus.net/articles/edempublicnetwork.html. Accessed 2 Apr 2014.

Clift, S. L. (2004). *E-government and democracy—representation and citizen engagement in the information age*. http://www.publicus.net/articles/cliftegovdemocracy.pdf. Accessed 2 Apr 2014.

Cynthia, R. F., Newhart, M., & Heidt, J. (2012). Rulemaking vs. democracy: Judging and nudging public participation that counts. *Michigan Journal of Environmental and Administrative Law*, *2*, 1. http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1011&context=ceri. Accessed 2 Apr 2014.

Dahlberg, L. (2011). Re-constructing digital democracy: An outline of four 'positions'. *New Media and Society*, *13*, 855–872. http://nms.sagepub.com/content/13/6/855.full.pdf. Accessed 2 Apr 2014.

Dutton, W. H., & Peltu, M. (2007). *Reconfiguring government-public engagements: Enhancing the communicative power of citizens*. Oxford Internet Institute forum discussion paper No. 9. http://www.cyberinet02.inet-tr.org.tr/oii/FD9.pdf. Accessed 2 Apr 2014.

Duvivier, K. K. (2013). E-Legislating. *Oregon Law Review*, *92*(9).

Ehringfeld, A., Naber, L., Grechenig, T., Krimmer, R., & Traxl, M., et al. (2010). Analysis of recommendation Rec(2004)11 based on the experiences of specific attacks against the first legally binding implementation of E-voting in Austria. In R. Krimmer & R. Grimm (Eds.), *Electronic voting 2010 (EVOTE2010) conference proceeding* (Austria) (pp. 225–237). http://www.e-voting.cc/wp-content/uploads/Proceedings%202010/EVOTE2010_finals.pdf. Accessed 2 Apr 2014.

Feezell, J. T., Conroy, M., & Guerrero, M. (2009). *Facebook is… fostering political engagement: A study of online social networking groups and offline participation*. Presentation at the American Political Science Association meeting http://irevolution.files.wordpress.com/2009/09/apsa-feezell-2009.pdf. Accessed 2 Apr 2014.

Gerlach, J., & Gasser, U. (2009). *Three case studies from Switzerland: E-voting*. Berkman Center Research Publication No. 2009-03.1. http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf. Accessed 2 Apr 2014.

Howes, D. (2001). e-Legislation: Law-making in the digital age. *McGill Law Journal*, *47*(39). http://lawjournal.mcgill.ca/userfiles/other/7513733-47.1.Howes.pdf. Accessed 2 Apr 2014.

Karpf, D. (2010). Online political mobilization from the Advocacy Group's perspective: Looking beyond clicktivism. *Policy and Internet*, *2*(4). Article 2. http://davekarpf.files.wordpress.com/2009/03/online-political-mobilization-from-the-advocacy-groups-perspective-1.pdf. Accessed 2 Apr 2014.

Kerikmäe, T., & Nyman-Metcalf, K. (2012). Less is more or more is more? Revisiting universality of human rights. *International and Comparative Law Review, 12*(1), 35–51.

Kotsiopoulos, I. (2009). *Bringing together and accelerating eGovernment research in the EU*. DG Information Society and Media, European Commission. http://www.epractice.eu/files/edemocracy.pdf. Accessed 2 Apr 2014.

Macnamara, J., & Kenning, G. (2010). *E-electioneering 2010: Trends in social media use in Australian political communication*. http://www.academia.edu/830297/E-electioneering_2010_Trends_in_Social_Media_Use_in_Australian_Political_Communication. Accessed 2 Apr 2014.

Mendez, F. (2007). *e-democratic experimentation in Europe: The case of e-voting*. e-Working papers 2007/02. E-Democracy Centre, University of Zürich, Switzerland. http://www.edemocracycentre.ch/files/WP2007-2%20-%20Mendez%20-%20eDemocracy%20Experiences%20in%20Europe.pdf. Accessed 2 Apr 2014.

Muller, M. (2011). *Lurking as personal trait or situational disposition? Lurking and contributing in enterprise social media*. Resource document. IBM research report. http://domino.research.ibm.com/library/cyberdig.nsf/papers/1357B36CA5B3C630852579480052500C/$File/rc25221.pdf. Accessed 2 Apr 2014.

Oostveen, A. M., & Van den Besselaar, P. (2007). *Non-technical risks of remote electronic voting*. Resource document. Idea Group Inc. http://www.social-informatics.net/Encyclopedia_Oostveen2006.pdf. Accessed 2 Apr 2014.

Ostling, A. (2010). ICT in politics: from peaks of inflated expectations to voids of disillusionment. *European Journal of ePractice*, *9*. http://epractice.eu/files/European%20Journal%20epractice%20Volume%209.4.pdf. Accessed 2 Apr 2014.

Peart, M. (2007). *Local e-Democracy initiatives in the United States*. e-working papers 2007/03 for the e-Democracy Centre, University of Zurich, Switzerland. http://www.edemocracycentre.ch/files/WP2007-3-Peart-%20Local%20e-Democracy%20in%20the%20US.pdf. Accessed 2 Apr 2014.

Peart, M. N., & Diaz, J. R. (2007). *Comparative project on local e-Democracy initiatives in Europe and North America*. Resource document. e-Democracy Centre, Faculty of Law, University of Geneva, Switzerland. http://www.edemocracycentre.ch/files/ESF%20-%20Local%20E-Democracy.pdf. Accessed 2 Apr 2014.

Perez, O. (2009). Complexity, information overload, and online deliberation. *I/S: A Journal of Law and Policy for the Information Society*. *Volume*, *5*(1), 43–86. http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Perez_Formatted_02_09.pdf. Accessed 2 Apr 2014.

Perez, O. (2013). Open government, technological innovation, and the politics of democratic disillusionment: (E-)Democracy from socrates to Obama. *I/S: A Journal of Law and Policy for the Information Society*, *9*. http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Perez.pdf. Accessed 2 Apr 2014.

Sherman, B. (2011). Your mayor, your "Friend": Public officials, social networking, and the unmapped new public square. *Pace Law Review*, *31*(1). http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1767&context=plr. Accessed 2 Apr 2014.

Stromer-Galley, J., Webb, N., & Muhlberger, P. (2012). Deliberative E-rulemaking project: Challenges to enacting real world deliberation. *Journal of Information Technology and Politics*, *9*, 82–96. http://www.academia.edu/2497482/Deliberative_E-Rulemaking_Project_Challenges_to_enacting_real-world_deliberation. Accessed 2 Apr 2014.

Welp, Y. (2007). *Democracy and digital divide in Latin America*. e-working papers 2007/01. E-Democracy Centre, University of Geneva, Switzerland. http://research.altec.gr/Ariadne/ariadne8/Democracy_and_Digital_Divide_in_Latin_America.pdf.pdf. Accessed 2 Apr 2014.

Cases

John Doe No. 1 v. Reed, 130 S. Ct. 2811 (2010).

Assateague Island National Seashore, Personal Watercraft Use, 68 Fed. Reg. 32,371, 32,372 (May 30, 2003).

Borough of Duryea, Pennsylvania, et al. v. Charles J. Guarnieri, 131 S.Ct. 2488 (2011).

Legislative Acts and Legal Documents

Magna Carta (1215) paragraph 61. http://www.nationalcenter.org/MagnaCarta.html. Accessed 2 Apr 2014.

English Bill of Rights (1689) http://avalon.law.yale.edu/17th_century/england.asp. Accessed 2 Apr 2014.

U.S. Constitution, First amendment. http://www.law.cornell.edu/constitution/first_amendment. Accessed 2 April, 2014

UK Government. (2002). In the service of democracy: A consultation paper on a policy for e-democracy. http://www.basiccraft.files.wordpress.com/2009/04/in-the-service-of-democracy-2002.pdf. Accessed 2 April, 2014.

Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting (Adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies).

Orszag, P. R. (2009) Memorandum from the Director for the Heads of Executive Departments and Agencies. Executive Office of the President of USA (p. 1). http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf. Accessed 2 Apr 2014.

Recommendation CM/Rec(2009)1 of the Committee of Ministers to member states on electronic democracy (e-democracy) (Adopted by the Committee of Ministers on 18 February 2009 at the 1049th meeting of the Ministers' Deputies).
CM(2011)175 dated 15 March 2012, being the Internet Governance—Council of Europe Strategy 2012-2015.
Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies) https://wcd.coe.int/ViewDoc.jsp?id=2074317&Site=CM. Accessed 2 Apr 2014.

News articles

Calamur, H. (2012). The Trishanku problem. Resource document. *Pragati the Indian National Interest Review*. http://pragati.nationalinterest.in/2012/01/the-trishanku-problem/. Accessed 2 Apr 2014.
IBM Survey. (2012). IBM survey reveals digital behavioral trends for consumers: What is your digital personality? http://www-03.ibm.com/press/us/en/pressrelease/37423.wss. Accessed 2 Apr 2014.
Sacks, M. (2012). Clarence Thomas petitioned by 100,000 progressives to recuse himself from health care cases. Huffington post newspaper. http://www.huffingtonpost.com/2012/02/17/clarence-thomas-petition-recuse-health-care_n_1284610.html. Accessed 2 Apr 2014.
Walker, S., & Grytsenko, O. (2014). Text messages warn Ukraine protesters they are 'participants in mass riot'. The Guardian. http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot. Accessed 2 Apr 2014. It reported that mobile phones of protestors in Kiev were used to locate and pinpoint users by the government.

Related websites

Australia—http://www.finance.gov.au/blog/2010/07/16/declaration-open-government/. Accessed 2 April, 2014.
Canada—http://data.gc.ca/eng. Accessed 2 April, 2014.
United Kingdom—http://data.gov.uk/. Accessed 2 April, 2014.
The Open Government Partnership comprising of over 60 countries. http://www.opengovpartnership.org/. Accessed 2 April, 2014.
The World Bank ICT Sector Strategy at http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:23118048~menuPK:8432091~pagePK:210058~piPK:210062~theSitePK:282823,00.html. Accessed 2 April, 2014.
http://www.whitehouse.gov/blog/2011/09/22/petition-white-house-we-people. Accessed 2 April, 2014.
An online version of the Ramayana, along with its English translation: http://valmiki.iitk.ac.in/index.php?id=translation. Accessed 2 April, 2014.
Another English version of the story of Trishanku here: http://www.valmikiramayan.net/bala/sarga60/bala_60_prose.htm. Accessed 2 April, 2014.