TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Business and Governance

Department of Law

Salla Rautiola

IMPACT OF PERSONAL DATA PROTECTION REFORM ON PROCESSING DIGITAL EVIDENCE

Bachelor Thesis

Supervisor: Ph.D Agnes Kasper

Tallinn 2017

I hereby declare that I am the sole author
of this Bachelor Thesis and it has
not been presented to any other
university of examination.

Salla Rautiola

“.....”..... 2017

The Bachelor Thesis meets the established requirements

Supervisor Agnes Kasper

“.....”..... 2017

Accepted for examination “.....”..... 2017

Board of Examiners of Law Bachelor’s Theses .....

Table of Contents

Abbreviations

ACPO	Association of Chief Police Officers
AEPD	Agencia Española de Protección de Datos
BCR	Binding Corporate Rules
BWB	Austrian Competition Agency
CIL	Customary International Law
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSP	Cloud Service Provider
DPD	Data Protection Directive
EC	European Commission
ECHR	European Convention of Human Rights
ECJ	European Court of Justice
ECtHR	European Court of Human Rights
EEA	European Economic Area
ENISA	European Union Agency for Network and Information Security
EPIC	Electronic Privacy Information Centre
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IEC	International Electrotechnical Committee
ISO	International Organization for Standardization
ISO/IEC JTC	Joint Technical Committee established by ISO and IEC
IT	Information Technology
OECD	Organization for Economic Co-operation and Development
OLAF	European Anti-Fraud Office
OSINT	Open Source Intelligence
SCC	Standard Contractual Clauses
SOCMINT	Social Media Intelligence
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights

Introduction

Information technology is a central feature of modern society. Individuals worldwide use a wide range of different electronic tools for communication, working, entertainment and preservation. Digital domain serves as easily accessible and cost efficient platform for a great number of different activities. Therefore, it is not only praised by individuals but large multinational corporations as well. Due to high volume of content that is produced mundanely, investigators have discovered the significant value of digital domain in legal proceedings. With high probability, any modern investigation or legal dispute involves digital evidence.

However, novelty of digital domain and its complexity raise both national and international jurisdictional issues. In order to provide secure data transfers, harmonized legislation is highly demanded. On the 5th of May 2016, the European data protection Regulation (EU) 2016/679 entered into force. Due to the complex relation between information society and an individual, detailed analysis on legal aspects of digital evidence and privacy will be provided in the argumentative part of this work. The thesis is constructed in accordance with the research question of **what are the impacts of personal data protection reform on processing digital evidence in international context.**

Due to momentum and fragile nature of digital evidence, traditional investigation methods are difficult to apply in digital domain. In order to remain the admissibility of digital evidence through the investigation, certain stages and criteria must be fulfilled. Rules and principles for such investigations are set in a number of international guidelines but there is no internationally binding procedure for it. Therefore, methods for search and seizure of digital evidence are subjects for international confusion. In contrast to traditional documented evidence, digital evidence is not bound to location: cloud computing is yet another novel ground for legal concerns.

Privacy is a traditionally recognized human right. Despite the binding treaties, novel threats have, however, occurred due to information technology improvements. Modern individuals tend to be aware of the importance of privacy. Yet, privacy in public spaces, such as in social network, is often neglected. Therefore, reasonable expectations for privacy have been questioned in modern societies. Such uncertainty has rapidly transferred from social network to abuse of governmental authority. In order to avoid authoritarian offenses, unified legislation is required and the role of Customary International Law will be discussed in context of modern data privacy.

Current legislative instruments are whether not binding or considered as vague. Moreover, the issue of different legal regimes bring another aspect to the discussion. The European post-war data privacy legislation is considered as advantageous in detail but territorial. Therefore, transnational data flow is rarely facile. Cooperation with foreign States requires additional evaluation and administration in order to provide secure data handling for the European Union citizens. Furthermore, Asia is continuously increasing its importance in international trade and communication. Conflicts arising from jurisdictional differences will be analyzed in context of international data privacy.

Under the last chapter, detailed discussion on the Data Protection Reform will be provided. The main elements of the reform and how they shape the framework of modern data protection: will there be significant harmonization only within the European Union or between the third countries as well. It is also observed whether the reform produces novel obstacles for cross-border discovery. The connection between an individual and the Data Protection Reform will remain in the core. The European Commission's reasoning and opinions serve as a platform for the analysis.

To conclude the work, the author will provide an interpretation of the inferences observed in the thesis. This empirical research pursuits to address the conflicts in data protection and processing digital evidence. The effect of the Data Protection Reform on processing digital evidence, and its impact on individual's privacy rights will be observed in detail. In order to identify the valid law and legal norms, this thesis is written in qualitative and comparative, literature based methods. Argumentative sections are provided in accordance to a number of academic sources and official policy documents. Relevant principles are supported by case law.

1. Digital Evidence

1.1. Nature of Digital Evidence

Current legal procedures and jurisdictions are challenged due to technical nature of information society. John S. Atkinson argues[1] that due to complexity of digital evidence, previous methods for collecting evidence would be impractical for modern investigation purposes. Atkinson states[2] that interaction with computers is the ground for creating such high volume of potential digital evidence. Any data that is collectible from a device has the potential to be digital evidence. Although, Information Technology (IT) is often included in legal disputes and investigations, the jurisprudences tend to lag behind because of momentum and complexity of technology.

Any data that is stored or transferred via technological means, and is used to support a claim, is considered as digital evidence. Therefore, any investigation and legal dispute, civil or criminal, involves digital evidence with high probability. Presented evidence must, however, be relevant, reliable, complete, authentic, and proportionate. It shall not support just a certain perspective or part of the theory but present a complete view. In order to make digital evidence admissible for court proceedings, it must be validated through proper multi-staged investigation process. Furthermore, IT practitioners are often consulted.

According to Atkinson[3], there are two major categories of digital evidence. The first category consists of evidence that meets the admission criteria discussed above, and is used in court proceedings.[4] The second category considers evidence according to which it is reasonable to suspect that an individual is involved in unlawful activities.[5] Atkinson remarks[6] that such data requires a search warrant or justification for further investigation. Search warrants in Digital Age will be discussed later in this chapter. Despite the increasing significance of digital evidence, importance of traditional evidence shall not be excluded. According to Atkinson[7], it is important to remain traditional methods alongside the modern ones, especially when digital traces are not linkable to the suspect.

[1] Atkinson, S. J. Proof is Not Binary: The Pace and Complexity of Computer Systems and the Challenges Digital Evidence Poses to the Legal System. Birkbeck Law Review 2014, 2 (2), pp. 245-262.
[2] *Ibid*
[3] *Ibid*
[4] *Ibid*
[5] *Ibid*
[6] *Ibid*
[7] *Ibid*

1.2. International Rules and Principles

1.2.1. ISO/IEC 27037

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) constitute a joint technical committee ISO/IEC JTC 1. In 2012, ISO/IEC JTC 1 prepared an International Standard document ISO/IEC 27037[8], for operations in processing digital evidence. The document was prepared in cooperation with Subcommittee SC 27. ISO/IEC 27037 sets rules and international standards for individuals who operate in the field of identification, gathering, acquisition and preservation of digital evidence. Via these standards, investigation will promote admissibility of potential evidence.

Digital evidence arise from a number of different electronic sources: databases, networks, communication devices, downloads etc., which is why it is fragile in nature. Therefore, proper measures to ensure the authenticity and integrity of data is necessary. The International Standard is also addressed to decision-makers, such as judges, whose responsibility is to evaluate the reliability of digital evidence. However, ISO/IEC 27037 does not rule the measures that fall outside the scope of identification, gathering, acquisition or preservation. For that reason actual legal proceedings, disciplinary procedures or analysis methodology are not ruled under this document.

ISO/IEC 27037 does not override laws or specific legal requirements. Nevertheless, it harmonizes the potential exchange of digital evidence between different jurisdictions. Therefore, the users of this document are required to implement these guidelines in requirements for evidence under their national law. ISO/IEC 27037 complies with ISO/IEC 27001[9] and ISO/IEC 27002[10]. Moreover, this International Standard is encouraged to be read in liaison with other national and international provisions for digital evidence and the investigation of information security related incidents.

1.2.2. The Association of Chief Police Officers

[8] Joint committee of International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 21037, 2012. www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en (18.2.2017)
[9] Joint committee of International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27001, 2005. (Reformed in 2013) www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en (18.2.2017)
[10] Joint committee of International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27002, 2005. (Reformed in 2013) www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-1:v1:en (18.02.2017)

In March 2012, Police Forces in England, Wales & Northern Ireland adopted the 5th version of the Association of Chief Police Officers (ACPO) Good Practice Guide for Digital Evidence[11]. It is to assist law enforcement and investigations in digital incidents, mainly in the United Kingdom (UK). The Good Practice Guide is disclosable under the Freedom of Information Act 2000, and it does not fall under the Government Protective Marking Scheme. Previous, the 4th, version was focused on evidence emerging from computers. However, the reform embraces the diversity of IT: variety of digital sources are encompassed under the 5th version of the Good Practice Guide.

The ACPO Good Practice Guide provides four principles of digital evidence. According to the first principle, any piece of digital evidence shall be equally recognized and treated to physical and documentary evidence. Furthermore, laws and rulings shall apply to both digital and documentary evidence. Law enforcement agencies (LEAs) or any persons connected to those agencies through employment, shall not change or modify data. Due to momentum and constantly altering nature of IT systems, the nature of digital evidence is fragile. Therefore, the second principle provides that any person accessing the original data must have a competent right to do so.

In order to prevent any third parties from accessing data unlawfully, the third principle of the ACPO Guidelines regulate the necessity of an audit trail. Therefore, any actions taken on digital evidence should be recorded properly. This is not only to protect the evidence from unauthorized users, but to provide the authenticity, reliability and admissibility of the evidence. However, the overall responsibility for ensuring proper and lawful processing of digital evidence falls on the person who is in charge of the investigation. The fourth principle therefore ensures that the law and the four principles set in the ACPO Good Practice Guide for Digital Evidence are being pursued.

1.2.3. The European Anti-Fraud Office

The European Anti-Fraud Office (OLAF) ruled a set of international Guidelines on Digital Forensic Procedures[12] in 2016. It is to provide proper chain of evidence via identification, acquisition, representation, compilation, analysis and storage of digital evidence. Only admissible

[11] The Association of Chief Police Officers. The ACPO Good Practice Guide for Digital Evidence, 2012. www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (17.02.2017)
[12] The European Commission. The European Anti-Fraud Office. Guidelines on Digital Forensic Procedures for OLAF Staff, 2016. ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf (18.02.2017)

evidence is legitimate in disciplinary, administrative and legal proceedings. The OLAF Guidelines implement Article 4(2) of Regulation (EC) 883/2013[13] and Article 7(1) of Regulation (EC) 2185/96[14]. However, due to high volume of collected data, digital proceedings often tend to be unfavourable for privacy. Therefore, the OLAF Guidelines do not only regulate rules for securing digital evidence but they imply data protection provisions as well. Although, the OLAF Guidelines mostly tend to comply with the Instructions to Staff on Data Protection, other internationally recognized standards such as ISO/IEC Standard 27037 and the ACPO Good Practice Guide for Digital Evidence are implemented as well.

1.2.4. Convention on Cybercrime

In order to harmonize legislation on computer related crimes, the Council of Europe (CoE) drafted Treaty No. 185, Convention on Cybercrime[15]. Treaty No. 185, commonly known as the Cybercrime Convention, was opened for signature in Budapest on the 23rd of November in 2001, and it entered into force in 2004. The Cybercrime Convention is considered to be the first multilateral treaty to regulate network security, computer networks and misuse of such systems. According to the preamble of the Convention[16], it aims to balance the interest of law enforcement and fundamental human rights, such as privacy and political freedoms. In order to fight cyber crimes efficiently, the Convention stresses the necessity of cooperation between State and private industry.

In 2001, the Cybercrime Convention introduced certain facilitations to international investigations, such as expedited preservation of data. As author has observed in previous sections, high volume, momentum and fragility create challenging circumstances for digital evidence processing. Due to rapid overall transformation of IT based services, the value of the Cybercrime Convention is, however, questioned in context of modern demand. For instance, the ascent of Social Media has created a new platform for not only cyber criminals but for investigators as well. The Cybercrime Convention was drafted to contribute legislative issues on the Internet but it is lacking transparent regulations and procedural requirements.

[13] Regulation (EU, EURATOM) No 883/2013 of the European Parliament and of the Council concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (EURATOM) No 1074/1999. OJ L 248, 18.9.2013, Article 4(2).
[14] Council Regulation (EURATOM, EC) No 2185/96. OJ L 292, 15.11.1996, Article 7(1).
[15] Convention on Cybercrime. The Council of Europe. Budapest, Treaty No. 185, 23.11.2001.
[16] Convention on Cybercrime, preamble.

According to Amalie M. Weber[17], there are three major jurisdictional issues with the Cybercrime Convention: lack of criminal statutes, lack of procedural powers, and lack of enforceable mutual assistance provisions with foreign states. Weber remarks[18] that in 2001, international cooperation on cybercrime was rather an exception, which is why the Cybercrime Convention provisions are difficult to apply in modern digital environment. Although, there is a large number of states that provide jurisdictional statutes criminalizing computer related offenses, more resources are required to operate proper investigations. Weber therefore states[19] that in order to operate successful cyber crime investigations, transparent cooperation is necessary. In case a state refuses to cooperate and assist in an investigation, it is likely to be an obstacle for harmonized jurisdiction. The Cybercrime Convention does not provide such cooperation obligations.

In 2004, the Electronic Privacy Information Center (EPIC)[20] also filed their statement[21] of disagreement with the Cybercrime Convention provisions. According to the statement[22], the Convention jeopardizes civil liberties due to lack of adequate privacy protections and dual-criminality requirement. EPIC states[23] that adoption of the Cybercrime Convention and invasive methods of investigation would threaten legal protections provided in the US Constitution. According to the Article 14 on Search and Seizure of Stored Computer Data[24], individuals are required to disclose decryption keys to ease LEAs accessing the data. EPIC also notes[25] that the Conditions and Safeguards[26] are vague and do not provide detailed protection of privacy.

1.3. Legal Issues of Processing Digital Evidence

1.3.1. Search in Digital Age

As observed in the previous section, suspicious data requires a search warrant for further investigation. Orin S. Kerr[27] however states that handling of digital files demands a two-stage

[17] Weber, M. A. The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal 2003, 18 (1), pp. 425-446.
[18] *Ibid*
[19] *Ibid*
[20] Electronic Privacy Information Centre is a leading, non-profit, civil liberties organization. It has globally observed and reported privacy developments since 2001.
[21] Electronic Privacy Information Centre, Statement to the United States Senate, 2004. epic.org/privacy/intl/senateletter-061704.pdf (18.2.2017)
[22] *Ibid*
[23] *Ibid*
[24] Convention on Cybercrime *supra* nota 15, p 8, Article 14 on scope of procedural provisions.
[25] Electronic Privacy Information Centre *supra* nota 21, p 9.
[26] Convention on Cybercrime *supra* nota 15, p 10, Article 8 on conditions and safeguards.
[27] Kerr, S. O. Search Warrants in an Era of Digital Evidence. Mississippi Law Journal 2005, 75 (4), pp. 84-145.

process. He argues[28] that traditional seizure of the physical devices, and electronic search to collect the relevant data from the device are both necessary to reach a complete and valid collection of evidence. Kerr states[29] that such two-stage process however challenges the current legislation as the current regulations on warrants presume traditional, single-stage searches. Kerr argues[30] that computer search involving investigations require specified warrant procedure for modern context.

Kerr remarks[31] three major issues when reflecting the current system in digital domain: should the warrant describe the physical or the digital search, how the search area would be described, and would the timing of the electronic search follow the traditional regulation on physical warrant operation. When performing a traditional search, authorities pursue to find specific items. However, when a crime is committed in cyber domain, it might not be obvious which data is actually desired. Neither is clear, whether a warrant should describe the physical location of the device, the device itself, or the location where the electronic search will take place. In order to make digital evidence admissible for litigation, there must be a transparent chain of evidence. Therefore, Kerr states[32] that record-keeping regulations should be precise for electronic search.

1.3.1.1. The Spar Case in Austria

As observed above, vague legislation regarding e-discovery creates uncertainty. Moreover, digital evidence is barely ever located on one device only. Issues do not necessarily require a trans border element because legal difficulties occur within national scope as well. In 2013, the Austrian court made a significant ruling on digital evidence related to search warrants. Viktoria H.S.E. Robertson[33] observes the judgment of the incident, its meaning and impact on other European jurisdictions.

Spar is one of the major food retailers in Austria.[34] However, on the 6th of August in 2013 Spar became a subject to anti-competitive agreement and dawn raid related investigations operated by

[28] *Ibid*
[29] *Ibid*
[30] *Ibid*
[31] *Ibid*
[32] *Ibid*
[33] Robertson H.S.E. V. The Spar Cases in Austria: Shaping the Legal Framework for Digital Evidence Gathering During Competition Dawn Raids. Oxford University Press, Journal of European Competition Law & Practice 2016, 7 (3), pp. 205-211.
[34] *Ibid*

the Austrian Competition Agency (BWB).[35] According to Robertson[36], the BWB operated their investigation at Spar business premises in Maria Saal but accessed company data in Salzburg, outside the premises defined in the warrant. Robertson remarks[37] that the remote access was operated via forensic software. The Austrian Cartel Court extended the search warrant on the 20th of August 2013, a day after the search at the premises. Robertson states[38] that Spar argued the investigation having breached procedural rules and being therefore carried out unlawfully.

The Supreme Cartel Court's judgement held[39] that in this case the investigation was operated on a group of companies, and that the corporate legal structure may be overlooked when issuing search warrants for collecting digital evidence. Robertson states[40] that after Spar claimed the BWB for exceeding the search warrant by searching for data outside the premises, the BWB argued that the search warrant did not only cover the electronic data that was physically located at the business premises. Instead, Robertson remarks[41] that all data that is accessible from the premises, should be covered by the warrant. The Court's ruling upheld the BWB's statement.[42] Due to international business models, legislation that denies access to digital files in foreign servers is inapplicable for modern investigation purposes.

According to Robertson[43], when carrying out the investigation, the BWB was accompanied by two IT-specialists. She states[44] that when searching the laptops at the business premises, encryption was turned on but the owner refused from cooperating. Therefore, the IT-specialists decided to run forensic software that was created for Criminal Law investigations. An external expert stated[45] that without a Criminal Law search warrant, use of such software was unsuitable and irrelevant for competition law investigation. Robertson observes[46] that the case gained wide media attention, and created discussion on use of forensic software in digital evidence gathering; which authorities

[35] *Ibid*
[36] *Ibid*
[37] *Ibid*
[38] *Ibid*
[39] *Ibid*
[40] *Ibid*
[41] *Ibid*
[42] *Ibid*
[43] *Ibid*
[44] *Ibid*
[45] *Ibid*
[46] *Ibid*

shall use such software, and which forensic software may actually be used in business investigations.[47]

As Kerr remarked[48] modern investigation requires two-stages. In the Spar case, lack of up-to-date legislation on collecting digital evidence caused confusion: what does the search warrant actually cover. The same issues that Kerr raised in his article, are virtually seen in the Spar case. However, the Austrian judgement did gain international legislative attention: according to Robertson[49], after the Spar case, the EC ruled that under Regulation 1/2003[50] investigators may use their own forensic IT-equipment to search IT environment and other electronically stored data. Moreover, Robertson states[51] that the right to access also covers mobile devices, external storage services, and private devices at the premises.

1.3.2. Use of Predictive Coding in Litigations

When discovering electronic evidence, ambiguity is not limited to issues regarding location or stages of search process only. In order to promote and facilitate e-discovery by identifying relevant documents, predictive coding has been developed to review the materials. The software is not, however, yet fully approved for legal procedures, which creates a ground for another legal discussion. Wallis M. Hampton states[52] that due to uncertainty, a number of attorneys are unwilling to use it as a primary review tool in litigations. Nevertheless, Hampton argues[53] that predictive coding offers various different functions as it can be used, for instance, to identify and review relevant documents, organize and prioritize the discoveries, or analyze the results. Furthermore, predictive coding is flexible in nature as it may be applied during different stages of investigation.

Predictive coding is claimed to be time and cost efficient method to review relevant documents but it does, however, have its limitations and downsides as well. Hampton remarks[54] that inequality between the coding programs may challenge equality principle in litigation process. Moreover, he

[47] *Ibid*
[48] Kerr *supra* nota 27, p 9.
[49] Robertson *supra* nota 33, p 10.
[50] Council of the European Union. Regulation 1/2003 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. Brussels, OJ L 1, 04.01.2003.
[51] Robertson s*upra* nota 33, p 10.
[52] Hampton, W. M. Predictive Coding: It's Here to Stay. E-Discovery bulletin, Thomson Reuters 2014. www.skadden.com/sites/default/files/publications/LIT_JuneJuly14_EDiscoveryBulletin.pdf (30.03.2017)
[53] *Ibid*
[54] *Ibid*

argues[55] that a significant deficiency with predictive coding is its inability to analyze files such as videos, graphic and audio with sufficient level of reliability. Therefore, admissibility of the evidence presented in court may not be adequate. Furthermore, Hampton stresses[56] that involvement in development process of the search methodology may cause disproportionate advantages by gaining irrelevant or damaging data about the opposing party.

In 2012 a significant court decision was ordered by Judge Andrew Peck in case *Monique Da Silva Moore et al. v. Publicis Groupe & MSL Group*[57]. Peck decided that predictive coding used for the employment discrimination litigation was appropriate.[58] His decision was upheld later in the U.S. District Court by Judge L. Carter Jr, who after balancing the potential weaknesses and advantages concluded that the use of predictive coding was reasonable.[59] Peck stated in his decision the following: ”Until there is a judicial opinion approving (or even critiquing) the use of predictive coding, counsel will just have to rely on this article as a sign of judicial approval. In my opinion, computer-assisted coding should be used in those cases where it will help "secure the just, speedy, and inexpensive" (Fed. R. Civ. P. 1)[60] determination of cases in our e-discovery world.”[61]

1.3.3. Validating Digital Evidence for Judicial Purposes

As observed above, in order for digital evidence to be admissible in court, it must meet certain criteria. Before evaluating whether digital evidence is admissible, it shall go through a verification process. Richard Boddington, Valerie Hobbs and Graham Mann[62] observed that the complexity of digital evidence creates challenges for legal practitioners. Therefore, the authors state[63] that the digital domain, in which the evidence is originated, transferred and processed, shall be examined. However, the authors argue[64] that the techniques of digital forensics used to aid the second-stage of digital investigation, should be legally defined in detail.

---

[55] *Ibid*
[56] *Ibid*
[57] United States District Court, Southern District of New York, Monique *Da Silva Moore, et al. v. Publicis Groupe & MSL Group, No. 11 Civ.1279 (ALC) (AJP),* 2012.
[58] *Ibid*
[59] District Court Upholds Judge Peck’s Order Endorsing Computer Assisted Review. New York, KrolLDiscovery Pulse, Case Law 2012. www.ediscovery.com/pulse/case-law/detail/26415/ (15.04.2017)
[60] Federal Rules of Civil Procedure, Rule 1. Scope and Purpose 1937, amended in 2016.
[61] United States District Court, Southern District of New York (2012) *supra* nota 57, p 13, Opinion and Order.
[62] Boddington, R., Hobbs, H., Graham, M. Validating digital evidence for legal argument. Australian Digital Forensics Conference, Edith Cowan University Research Online 2008.
[63] *Ibid*
[64] *Ibid*

Due to fragility of digital evidence, different investigation stages are necessary for successful investigation process. The authors remark[65] that negligent actions may result in incomplete or false evidence. In order to avoid improper handling, the authors observed[66] six stages which must be examined carefully: investigative domain that consists of preservation, locating, selecting, validating, and legal domain concentrating on constructing and final presentation. According to the authors[67], in order to isolate and stabilize the evidence scene, the preservation stage is significant: only after sufficient operation of preservation, adequate identifying of digital evidence is possible. The authors state[68] that after locating the devices containing digital evidence, it is important to select relevant evidence only for further proceedings. According to the authors[69], the validity of the data is examined in the validation stage, during which any claims can be verified.

In order to avoid failures in legal domain phase, the evidence must be constructed in proper manners. As the authors state[70], investigative stages are necessary due to the complexity of digital domain. However, the investigators do not have the sufficient degree of legal knowledge to analyze whether the evidence is significant for the case. Therefore, the authors remark[71] the importance of legal practitioners: they shall test the digital evidence collected in investigative stages, and evaluate its suitability in legal argument. Finally, after the digital evidence has been carried through each stage mentioned above, only supporting arguments will be presented in the court.

1.4. Digital Evidence and Cross-border Data Protection

1.4.1. The OECD Guidelines

In 1980, the Organisation for Economic Co-operation and Development (OECD) introduced an international Guidelines on the Protection of Privacy and Transferred Flows of Personal Data[72]. The Document is considered as one of the first international set of data privacy principles, and majority of the OECD Member countries have implemented these Guidelines in their national legislation alongside the Data Protection Directive 1995/46/EC (DPD). The OECD

[65] *Ibid*
[66] *Ibid*
[67] *Ibid*
[68] *Ibid*
[69] *Ibid*
[70] *Ibid*
[71] *Ibid*
[72] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), 2013. www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (03.03.2017)

Recommendation recognized that although national laws and data protection policies differ, the Members share a common pursuit to protect individual's privacy and liberties.[73] Therefore, the Guidelines presented in the Recommendation are addressed to apply to personal data processed in the public and private sectors.[74] The Guidelines were revised in 2013, after the Regulation 2016/679[75], General Data Protection Regulation (GDPR) was introduced by the European Commission (EC) in 2012.

According to basic principles of international application set out in Part Three of the Recommendation[76], reasonable measures should be taken to ensure uninterrupted and secure data transfers to, and within, abroad. Unless the receiving country does not observe the OECD Guidelines or provide adequate data protection, Member countries should not set any restrictions for data transfers.[77] Moreover, it is stressed that the transfer shall not circumvent domestic privacy laws.[78] As the DPD was not directly applicable, Contracting States were able to apply it partly or set other restrictions regarding data privacy. In the OECD Guidelines[79] it is, however, stated that the Member countries should avoid introducing laws, policies or practices that could directly create obstacles to international personal data transfers.

The revised Guidelines introduced in 2013 constituted the first update of the OECD Guidelines presented in 1980. Those new Guidelines comply with global dimension and modern personal data transfer challenges. According to the OECD[80], two themes serve as a core for the updated Guidelines: risk management and improved interoperability. In addition to revised Guidelines, the update introduces[81] a number of new concepts: national privacy strategies, privacy management programs, and data security breach notifications. In the twenty-first century, cyber crimes are globally recognized as a threat to national security, due to which the OECD has introduced tasks for Governments as well. Implementation of the GDPR is obvious in the revised Guidelines, as the obligations regarding data security breach notification are set under articles Articles 33[82] and 34[83] of the Regulation.

---

[73] *Ibid*
[74] *Ibid*
[75] OJ L 119, 4.5.2016.
[76] The OECD Guidelines (1980) *supra* nota 72, p 14.
[77] *Ibid*
[78] *Ibid*
[79] *Ibid*
[80] 2013 OECD Privacy Guidelines, 2013. www.oecd.org/internet/ieconomy/privacy-guidelines.htm (15.04.2017)
[81] *Ibid*
[82] OJ L 119, 4.5.2016, Article 33 on notification of a personal data breach to the supervisory authority.
[83] OJ L 119, 4.5.2016, Article 34 on communication of a personal data breach to the data subject.

1.4.2. Procedures for Cloud Forensics

In the twenty-first century, cloud computing is recognized as a central feature of modern network services. It provides a foundation for a service through which information can be shared to a large number of customers and other users. Cloud works via the Internet and anyone having an access may use the cloud services. The United States National Institute of Standards and Technology[84] defined cloud as: ”a model for enabling convenient, on-demand network access to shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”[85] Due to its flexibility and cost efficiency, cloud computing has attracted an enormous number of mundane users: not only civil individuals store their data on cloud but easily manageable cloud computing has established its status as a major tool in corporations as well.

Despite the substantial advantages, cloud computing does comprise severe privacy and data protection concerns. The software, shared resources, and information that is stored on cloud service locate on a remote server. Joe Kong[86] remarks that when transitioning to cloud computing, one transfers the responsibility and legal right to process their data to the cloud service provider (CSP). In order to discuss the personal data privacy concerns in the context with cloud forensics in detail, relevant models of cloud computing must be introduced. Henry Chang[87] identifies those three models as software as a service (SaaS) and platform/infrastructure as a service (PaaS/IaaS). The European Union Agency for Network and Information Security (ENISA)[88] argues[89] that the Iaas models provide the largest amount of information for digital forensics as potential evidence. IaaS is also more convenient to investigate as SaaS and PaaS provide highly limited access for acquisition, due to which investigators must often rely on the information provided by the CSPs.[90]

[84] American non-regulatory agency and a measurement science, standards, and technology laboratory.
[85] Mell, P., Grance, T. The NIST Definition of Cloud Computing. Special Publication 800-145, U.S. Department of Commerce, National Institute of Standards and Technology, 2011. nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. (18.04.2017) Cited in Kong. (Kong, J., Xiaoxi, F., Chow, K.P. Introduction to cloud computing and security issues; Cheung, A.S.Y., Weber, R.H. (ed.) Privacy and Legal Issues in Cloud Computing. UK, Edward Elgar Publishing Limited: USA, Edward Elgar Publishing, Inc. 2015.)
[86] Kong, J., Xiaoxi, F., Chow, K.P. Introduction to cloud computing and security issues; Cheung, A.S.Y., Weber, R.H. (ed.) Privacy and Legal Issues in Cloud Computing. UK, Edward Elgar Publishing Limited: USA, Edward Elgar Publishing, Inc. 2015.
[87] Chang, H. Data protection regulation and cloud computing; Cheung, A.S.Y., Weber, R.H. (ed.) Privacy and Legal Issues in Cloud Computing. UK, Edward Elgar Publishing Limited: USA, Edward Elgar Publishing, Inc. 2015.
[88] Centre of expertise for cyber security in Europe.
[89] European Union Agency for Network and Information Security (ENISA). Exploring Cloud Incidents, 2016.
[90] *Ibid*

According to ENISA[91], there are three potential types of forensics in cloud environment: before incident, live, and post incident, out of which the first one is considered as the most valuable type of forensics in cloud environment. ENISA remarks[92] that the CSPs are obliged to perform actions such as activity records and detection of misanthropic behavior. In order to provide transparent and therefore legally satisfying assistance in digital forensics, the CSPs must introduce these preliminary actions in the agreement between them and the client. According to ENISA[93], live forensics pursuit to collect information from a live and currently running system before they are being switched off. Such data is often time sensitive and is often lost during traditional forensics.

Legal challenges in cloud forensics occur due to jurisdictional differences. Despite the fact that the EU citizens' data should not be transferred to jurisdictions with inadequate level of data protection, Chang states[94] that personal data that is stored in cloud locating outside the EU is a subject to that foreign jurisdiction. As observed above, European legislation requires search warrants for further forensics. Chang, however, remarks[95] that foreign jurisdictions may allow interferences without such requirements. Furthermore, according to ENISA[96], the procedures regarding the CSPs obligations during investigations are not defined under any specific regulation. Due to jurisdictional issues, Chang argues[97] that before concluding the agreement, CSPs should inform the customers that their personal data will fall under foreign jurisdiction.

Procedures for cloud forensics are complex because of a number of issues in different stages. The remote nature of the data and multi-jurisdictional environment hinder the access of investigators. According to ENISA[98], cloud specific tools should be developed alongside the development of cloud technology. Such tools would harmonize the standards for digital forensics in cloud environment. Furthermore, in addition to non existent tools and policies, ENISA stresses[99] that neither the LEAs have any agreement with the CSPs regarding cooperation in cloud investigations.

[91] *Ibid*
[92] *Ibid*
[93] *Ibid*
[94] Chang s*upra* nota 87, p 16.
[95] *Ibid*
[96] European Union Agency for Network and Information Security s*upra* nota 89, p 16.
[97] Chang s*upra* nota 87, p 16.
[98] European Union Agency for Network and Information Security s*upra* nota 89, p 16.
[99] *Ibid*

2. Privacy in Digital Domain

2.1. Legal Instruments

Privacy is a fundamental human right. It is recognized under Article 7 in the European Union Charter of Fundamental Rights[100] as well as in a number of other international treaties. Secondary law is created to specify the legal issues in modern circumstances. However, the concept of universal individual privacy is mostly a creation of Western culture and remained unknown in many cultures until the twenty first century.[101] Due to a high volume of production, analysis and distribution of data, increasing usage of sophisticated information and communication technology (ICT) is often considered as a threat to modern demand of privacy. Opinion polls hold that individuals are globally concerned over privacy violations and surveillance, now more than ever.[102] Therefore, proper national and international, up to date, privacy legislation is highly demanded.

2.1.1. Early Stages of Privacy Legislation

Oliver Diggelmann and Maria Nicole Cleis[103], suggest that the right to privacy was internationally recognized as a human right even before the unilateral treaties. However, the events of the second World War are generally recognized as major reasoning for such advanced privacy legislation in Europe. Today data protection is divided into personal data and sensitive personal data. Personal data refers to data from which a living individual is identifiable[104]. Sensitive personal data, instead, is personal data that consists of racial or ethnic origins, political opinions, religious beliefs, health records, sexual life or any other data that may be used for discriminatory purposes[105].

Diggelmann and Cleis state[106] that instead of an obvious single essence of the right to privacy there are two competing core ideas. The authors remark[107] that the main functions of privacy are to

[100] OJ C 326, 26.10.2012, Article 7 on right to private and family life.
[101] van den Hoven, J., Blaauw, M., Pieters, W., Warnier, M. Privacy and Information Technology. Stanford Encyclopedia of Philosophy 2014.
[102] Banisar, D., Davies S. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. The John Marshall Journal of Information Technology & Privacy Law, Journal of Computer & Information Law 1999, 18 (1), pp. 1-108, pp. 3-12.
[103] Diggelmann, O., Cleis, M. N. How the Right to Privacy Became a Human Right. Human Rights Law Review 2014, 14 (3), pp. 441-458.
[104] Information Commissioner's Office, Key Definition of the Data Protection Act. co.org.uk/for-organisations/guide-to-data-protection/key-definitions/
[105] *Ibid*
[106] Diggelmann s*upra* nota 103, p 18.
[107] *Ibid*

create distance between an individual and society, and to protect primitive community norms. According to Diggelmann and Cleis[108], almost every proposal included two guarantees during the codification process: protection for one's home and correspondence. Diggelmann and Cleis observe[109] that the protection of home is to provide physical protection and distance from society as well as one's private life at home. Protection of correspondence, instead, is to provide protection against unwanted interactions and interferences[110].

2.1.1.1. Universal Declaration of Human Rights

The Universal Declaration of Human Rights[111] (UDHR) is a milestone document in developing fundamental freedoms, such as international privacy. It was adopted by the United Nations General Assembly in Paris in 1948, where 48 countries voted in favor of the Declaration.[112] It was drafted by an international group of representatives with vary backgrounds.[113] The Article 12 of the UDHR provides: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[114]

2.1.1.2. European Convention on Human Rights

In 1950, the CoE drafted an international convention to protect fundamental human rights and freedoms in Europe. On 4th of November in 1950, all forty-seven CoE Member States signed the Convention in Rome, Italy. The European Convention on Human Rights[115] (ECHR) entered into force in 1953.[116] Article 8 of the ECHR provides: "Everyone has the right to respect for his private and family life, his home and his correspondence. 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

[108] *Ibid*
[109] *Ibid*
[110] *Ibid*
[111] Universal Declaration on Human Rights, United Nations General Assembly. The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world. It sets out, for the first time, fundamental human rights to be universally protected. Paris, 10.12.1948
[112] Diggelmann s*upra* nota 103, p 18.
[113] United Nations, Universal Declaration of Human Rights. www.un.org/en/universal-declaration-human-rights/ (10.02.2017)
[114] Universal Declaration on Human Rights, Article 12 on arbitrary interference.
[115] European Convention on Human Rights. The Council of Europe. The European Convention on Human Rights sets forth a number of fundamental rights and freedoms. Rome, 4.11.1950.
[116] Council of Europe, European Court of Human Rights commentary. www.echr.coe.int/pages/home.aspx?p=basictexts (08.02.2017)

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."[117]

2.1.2. Privacy Protection Instruments in Modern Context

As observed in previous chapters, privacy violations in Information Age often occur in cyberspace. Therefore, digital evidence has a significant importance in modern investigations. Postwar privacy legislation from the mid twentieth century is, however, difficult to apply in modern IT involving offences. While the UDHR and ECHR aim to protect individual's privacy mostly in relation to physical appearance, one's privacy in digital era shall be protected via secondary law as well. Although the Cybercrime Convention protects equipment and systems from interference and attacks, it excludes the human aspect of the Internet actors. Modern individual should be provided secured communication, confidentiality, and online privacy via proper jurisdiction.

2.1.2.1. ePrivacy Directive

In 2002, European Parliament and Council drafted Directive 2002/58/EC on Privacy and Electronic Communications.[118] Directive 2002/58/EC, commonly known as ePrivacy Directive, concerns personal data protection and privacy of the Internet users in the Information Age. It is aimed to harmonize the provisions between the Member States and, therefore, provide secure data flow within the EU. E-Privacy directive supplements the European directive on protection of personal data but is, nevertheless, applicable beyond the scope of the DPD. However, it is not applicable on public state security and defense, or criminal law.

In order to modernize privacy legislation within the EU, the EC prepared a proposal for an ePrivacy reform[119] in January 2017. As mentioned above, it is important for legislation to follow the fast changing pace of IT-based services and applications. According to the proposal, daily applications such as WhatsApp, Facebook Messenger and Skype would fall within the scope of the reform[120].

[117] European Convention on Human Rights, Article 8 on right to respect for private and family life.
[118] OJ L 201, 12.7.2002.
[119] European Commission. Proposal for an ePrivacy Regulation, 19.02.2017. ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (15.04.2017)
[120] *Ibid*

User consent would reach higher appreciation, and metadata and communications would be more secured. However, according to the proposal, consent would be no longer required for cookies.[121]

2.2. Why Privacy Matters

Privacy is not only to protect individual interests but democratic society as well. According to Daniel J. Solove[122], privacy matters due to certain central features. Solove states[123] that in order to maintain the trust within society, neither governments nor private sector companies shall limit individual's right to privacy or use any personal data to influence the citizens. He argues[124] that in modern societies, both physical and informational boundaries are being established to protect one's private life. As Diggelmann and Ciel observed[125], privacy is to provide protection from actions that aim to break those boundaries.

In the Information Age, political rights are in the center of privacy concerns. Such sensitive information shall be processed in accordance with the regulations regarding sensitive personal data. Solove states[126] that it is important that freedom of thought and speech, as well as freedom of social and political activities remain as one's private concern. Therefore, an individual should be the one deciding whether to share or publish that information. Solove argues[127] that individuals should be eligible to act privately online, without having to fear misuse of their personal data[128].

2.2.1. European Data Protection Principles

Information Commissioner's Office (ICO) observes[129] that European data protection follows eight principles, which are also implemented in the GDPR[130]. According to ICO[131], personal data must always be processed fairly and lawfully. In case there is no precise purpose, or the personal data is invalid, inadequate, or irrelevant, processing shall not take place: data minimization[132]. As

[121] *Ibid*
[122] John Marshall Harlan Research Professor of Law from George Washington University Law School.
[123] Solove, D. J. 10 Reasons Why Privacy Matters, Privacy + Security Blog, 2014. www.teachprivacy.com/10-reasons-privacy-matters/ (08.02.2017)
[124] *Ibid*
[125] Diggelmann s*upra* nota 103, p 18.
[126] Solove s*upra* nota 123, p 21.
[127] *Ibid*
[128] *Ibid*
[129] Information Commissioner's Office, Data Protection Principles. ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/ (25.04.2017)
[130] OJ L 119, 4.5.2016, Article 5 on principles relating to processing of personal data.
[131] Information Commissioner's Office s*upra* nota 129, p 21.
[132] OJ L 119, 4.5.2016, Article 5(1)(d).

observed above, admissibility is the legal basis for using digital evidence as solid prove in court proceedings. Therefore, ICO remarks[133] that personal data must be accurate before processing.

The GDPR addresses the importance of processing for precise purpose. After the data is unnecessary in relation to that purpose, it must either be removed or pseudonymised as soon as possible. Furthermore, ICO observes[134] the rights of data subjects: no processing that is not in accordance with the GDPR shall take place. Unauthorized and other unlawful processing must be prevented via technical and organizational means.[135] Moreover, data transfers to third countries serves as a core theme of the GDPR. Sufficient level of data protection shall be provided to European data subjects wherever their data is being processed. Therefore, ICO addresses[136] that the eight principle prevents any data transfers to countries with insufficient level of protection.

2.3. Privacy in Public Spaces

Social Network has gone through significant improvements after the DPD was drafted in 1995. Although the Internet users of modern societies have knowledge on anonymity, privacy and data protection, high volume of personal information is given and published online. After smartphones and applications became available to consumers in the early 2000's, continuous access to social network has been facilitated. Therefore, risks and criminal offenses in public online spaces are challenging to solve in accordance with the current legislation. Momentum of ICT development has created a whole new perspective for data privacy.

Due to popularity of social media, it is a unique platform for investigators. In order to perceive the volume of transferred data, the Intelligence and Security Committee of Parliament stated the following on 2015 report: "The internet carries the communications of 2.4 billion internet users. In one minute, those 2.4 billion transfer 1,572,877 gigabytes of data, including 204 million emails, 4.1 million Google searches, 6.9 million messages sent via Facebook, 347,222 posts to Twitter and 138,889 hours of video watched on YouTube."[137] Lilian Edwards and Lachlan Urquhart

[133] Information Commissioner's Office *supra* nota 129, p 21.
[134] *Ibid*
[135] OJ L 119, 4.5.2016, Article 5(1)(f).
[136] Information Commissioner's Office *supra* nota 129, p 21.
[137] Intelligence and Security Committee. Privacy and security: a modern and transparent legal framework, 2014. Cited in Edwards and Urquhart (Edwards L., Urquhart L. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? Oxford University Press, International Journal of Law and Information Technology, 24, 279–310, 2016.)

observe[138] how LEAs use social media intelligence (SOCMINT)[139] and open source intelligence (OSINT) for prosecution and investigation purposes. They state[140] that soon after London riots in 2011, LEAs discovered the value of ICT in investigating crimes and misanthropic behavior.

Edwards and Urquhart argue[141] that much of OSINT derives from social media, due to which privacy expectations have become vague. Furthermore, the authors note[142] that a large amount of SOCMINT and OSINT contain identifiable personal information that falls within the scope of Article 8 of the ECHR and creates the framework for the DPD and GDPR. The primary instrument regulating intelligence investigation by LEAs is the Regulation of Investigatory Powers Act 2000[143] (RIPA). It was drafted by the Parliament of the United Kingdom to regulate public authorities. Edwards and Urquhart remark[144] that in case the gathering and processing of personal data are operated by police to prevent a crime, RIPA allows it to be excluded from Data Protection Law. According to RIPA[145], data subject is neither asked to provide their consent for such actions nor have they right to request access to their personal data. The authors state[146] that it is nevertheless important to define proportionate policies when balancing privacy and public interest.

Tony Ward states[147] that images captured by surveillance cameras are common form of digital evidence presented in litigations. He refers[148] to Rose LJ in Attorney General's Reference No 2 of 2002[149], in which she remarks that despite the technology, images are always analyzed via human resources. Reliability of such images is therefore vague. Furthermore, according to the ACPO Guidelines[150], as judgements yet relies on human analysis, surveillance camera images are not considered as reliable enough to meet the admission criteria. Therefore, they should not be used

[138] Edwards, L., Urquhart, L. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? Oxford University Press, International Journal of Law and Information Technology 2016, 24 (3), pp. 279–310.
[139] Depending on individual's privacy settings, such as friends-locks, passwords or encryption, social media may be recognized either as open or closed source of information.
[140] *Ibid*
[141] *Ibid*
[142] *Ibid*
[143] Regulation of Investigatory Powers Act 2000. The Parliament of United Kingdom. The United Kingdom, 28.07.2000.
[144] Edwards s*upra* nota 138, p 23.
[145] Regulation of Investigatory Powers s*upra* nota 143, p 23.
[146] *Ibid*
[147] Ward, T. Surveillance, Cameras, Identification and Expert Evidence. Pario Communications Limited, Digital Evidence and Electronic Signature Law Review 2012, 9, pp. 42-50.
[148] *Ibid*
[149] Rose LJ. Attorney General's Reference (No 2 of 2002). Publications & records of the Parliament, UK, 2003. lexisweb.co.uk/cases/2002/october/attorney-generals-reference-no-2-of-2002 (16.04.2017)
[150] Ward s*upra* nota 147, p 23.

as evidence in court. According to the General's Reference[151], Rose LJ, however, stated that despite the Guidelines, such evidence should be admissible if it supports the guilt of the accused.

2.4. Mass-surveillance

Privacy rights are often balanced with national security. However, in order to fight both national and international terrorism via mass-surveillance, systematic interference with citizens' right to privacy is often inevitable. In order to fulfill the definition of mass-surveillance, a population is either partly or entirely surveilled by governments, governmental organizations or judicial systems. Despite the fact that surveillance camera images are often used as digital evidence, mass-surveillance often result in violating one's right to privacy as well as their social and political freedoms. When it comes to cyberspace, crimes are often difficult to trace because of technical complexity and cross border elements. Data privacy has a status as a fundamental right in many jurisdictions but it is unclear whether data protection is still an optional obligation or if it already has obtained status as a binding rule of Customary International Law.

Roger Clarke suggests[152] that data retention as such is a risk of mass-surveillance. Because individuals are often monitored for identification purposes, Clarke argues[153] that mass-surveillance should be considered as a higher privacy risk than personal and location surveillance. Categorized and discriminative surveillance is prohibited under EU law but yet Clarke states[154] that the current legislation relating to destruction of evidence is promoting personal surveillance. Clarke encapsulated his thoughts by citing Caspar Bowden: "It is incompatible with human rights in a democracy to collect all communications or metadata all the time indiscriminately. The essence of the freedom conferred by the right to private life is that infringements must be justified and exceptional."[155] Therefore, Clarge argues[156] that any access to personal data without judicial warrants should be prohibited.

[151] *Ibid*
[152] Clarke, R. Data retention as mass surveillance: the need for an evaluative framework. Oxford University Press, International Data Privacy Law 2015, 5 (2), pp. 121-132.
[153] *Ibid*
[154] *Ibid*
[155] Bowden, C. Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of [the UK] Parliament. Blog Privacy Strategy, 2014. Cited in Clarke (Clarke, R. Data retention as mass surveillance: the need for an evaluative framework. Oxford University Press, International Data Privacy Law 2015, 5 (2), pp. 121-132.)
[156] *Ibid*

2.4.1. Privacy as Customary International Law

Monika Zalnieriute identifies[157] three major legal issues in relation of data privacy and mass-surveillance; first of which is the relationship between national security and crime prevention. There are numerous search and interception techniques used to prevent national security threats, such as terrorism. Zalnieriute argues[158] that if data privacy had the status as binding rule of Customary International Law (CIL), it could facilitate the cooperation between the EU and the third countries. Before the GDPR becomes applicable in 2018, there is no directly applicable international treaty on data protection, due to which international uncertainty occur.

Although, systematic surveillance exercised by governments is not necessarily a new phenomenon, modern threat of terrorism has blurred the line between target-specific and mass-surveillance. Zalnieriute argues[159] that neither the modern sources of data nor the jurisdictional differences are the main obstacles for recognizing privacy as a CIL: identifying an unwritten character of CIL is difficult due to complex nature of CIL itself. Despite the complexity of CIL, Zalnieriute states[160] that the discussion of accepting data privacy as a principle of CIL should be approached through two doctrines often known as traditional and modern. Traditional approach has, however, gained criticism for its positivistic nature. Therefore, modern custom was created as an alternative to the traditional one, and to modernize CIL as a source of international law.[161]

2.4.2. Case study (37138/14), S*zabó and Vissy v. Hungary* [162]

The case of two nationals of Hungary, Máté Szabó and Beatrix Vissy, is a mass-surveillance concentrated case law ruled by the European Court of Human Rights (ECtHR) in 2016. According to the judgement[163], Hungarian legislation was inadequate to provide sufficient security against secret anti-terrorist surveillance. The Press Release of the Court remarked[164] that the applicants were both employed in a non-governmental warding company (Eötvös Károly Közpolitikai Intézet). The chain of events began in 2011, when the Hungarian police announced Anti-Terrorism

[157] Zalnieriute, M. An international constitutional moment for data privacy in the times of mass--surveillance. Oxford University Press, International Journal of Law and Information Technology 2015, 23, pp. 99-133.
[158] *Ibid*
[159] *Ibid*
[160] *Ibid*
[161] *Ibid*
[162] European Court of Human Rights, *Szabó and Vissy v. Hungary* (37138/14), 2016.
[163] European Court of Human Rights. Press Release on case *Szabó and Vissy v. Hungary* (37138/14), The Registrar of the Court, 2016. www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY-prel.pdf (11.02.2017)
[164] *Ibid*

Task Force department starting to operate.[165] Existence of the department was qualified under Hungarian Law, Act no. XXXIV of 1994 on the Police[166], according to which the secret intelligence force would be eligible to operate secret house searches, investigate phone and e-mail recordings, interfere mail traffic and communications without given permission.

In June 2012, Szabó and Vissy filed a constitutional claim stating that the secret intelligence actions breached their right to privacy under the Article 8 of the ECHR. The Constitutional Court dismissed the claim, and it was submitted to the ECtHR in 2014.[167] When examining the case, the ECtHR stated that although the applicants were potentially targeted group, the Hungarian legislation directly affected all households and users of ICT systems.[168] Furthermore, the Hungarian law did not provide a possibility to submit a complaint in case of suspicion of privacy interception.[169] Due to the circumstances mentioned above, the ECtHR held that Szabó and Vissy would be considered as victims of privacy violations under the ECHR.[170]

In 2016, the ECtHR observed that the safeguards provided in the Hungarian legislation 7/E (3) on Surveillance[171] were not adequate enough.[172] According to the judgement[173], secret surveillance measures did not serve the original purpose and were therefore considered as abuse of authoritarian power. Furthermore, the ECtHR held that the actions of secret surveillance were not supervised by judicial means.[174] Hungary is a party to the Cybercrime Convention[175] and yet such offenses took place in 2016. It is important to protect citizens' privacy to limit authoritarian power. Neither this case nor the decision can prevent governments from passing mass-surveillance approving legislation but equivalent cases will be taken to the ECtHR with high probability.

2.5. Right to Be Forgotten

[165] *Ibid*
[166] National Legislative Bodies / National Authorities of Hungary, Act no. XXXIV of 1994 on the Police. Hungary, 1994.
[167] European Court of Human Rights (2016) *supra* nota 163, p 25.
[168] *Ibid*
[169] *Ibid*
[170] European Court of Human Rights (2016), *Szabó and Vissy v. Hungary* (37138/14) *supra* nota 162, p 25.
[171] Act no. XXXIV of 1994 on the Police s*upra* nota 166, p 26. 7/E (3) on Surveillance.
[172] *Ibid*
[173] European Court of Human Rights (2016), *Szabó and Vissy v. Hungary* (37138/14) *supra* nota 162, p 25.
[174] *Ibid*
[175] Council of Europe, Chart of signatures and ratifications of Treaty No. 185. www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

In 2014 The European Court of Justice (ECJ) ruled that under certain conditions, EU citizens shall request removal of their personal data from search engine results. As the citizens of modern societies strongly rely on the information available on the Internet, the judgement in Google Spain has been considered to have a significant impact on modernizing data privacy legislation. After the judgement, attention has been paid to publicly available personal information, its content and accessibility. However, the Google Spain ruling was based on the DPD, which only included the bare principle for data erasure under Article 12.[176] Article 17 of the GDPR[177], instead, provides a detailed explanation and scope for the right to be forgotten.

2.5.1. Case Study (C-131/12), *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*[178]

Spanish national Mario Costeja Gonzáles submitted a complaint together with Agencia Española de Protección de Datos (AEDP) against local newspaper La Vanguardia Editions SL, Google Spain and Google Inc., in 2010[179]. The claimant stated that when entering his name in Google Search, the search results would grant links to two separate pages of old issues of La Vanguardia, which included unfavorable real-estate auction announcement from year 1998.[180] The auction was ordered due to Mr Costeja Gonzáles' social security debts.[181] The debt was, however, settled a number of years ago, due to which the information was no longer valid or relevant but harmful to Mr Costeja Gonzáles' reputation.[182] He ordered La Vanguardia to either remove or anonymize the pages, and Google Spain to take reasonable technical measures to hide the links from the public.[183]

The AEDP held that La Vanguardia had published the announcement in accordance with law and rejected the complaint but, however, requested Google Spain and Google Inc. to remove Mr Costeja Gonzáles' data from the search result index.[184] The Spanish National High Court, received complaints from Google Spain and Google Inc, and eventually the case was handed to the ECJ

[176] European Commission, Factsheet on the "Right to Be Forgotten" ruling (C-121/13). ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (3.3.2017)
[177] OJ L 119, 27.04.2016. Article 17 on right to erasure ('right to be forgotten').
[178] European Court of Justice, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (C-131/12), 2014.
[179] Court of Justice of the European Union, Press Release No 70/14 on case *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (C-131/12),* Curia, Press and Information, 2014. curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (11.2.2017)
[180] *Ibid*
[181] *Ibid*
[182] *Ibid*
[183] *Ibid*
[184] *Ibid*

where it was stated that as the operator of the search engine Google Spain and Google Inc. would be considered as data controllers.[185] According to the DPD[186], controller is responsible for identifying the purposes and means of processing data. Despite the fact that Google Spain is a subsidiary of Google Inc., and therefore has a seat in a non-member state, such establishment shall act in accordance with the EU Directive. The ECJ concluded that outdated and irrelevant information about the complaint was not compatible with the current data protection legislation.[187]

2.5.1.1. Internet and Jurisdiction after Google Spain

Despite the significance of Google Spain judgement, it has attracted criticism as well. According to Eleni Frantziou, implications arose because the judgement did not provide an exhaustive definition of the right to be forgotten. When analyzing the judgement, Frantziou holds[188] that the reasoning was only little based on fundamental rights but on the DPD. Furthermore, Frantziou criticizes[189] the weak consistency with the ECHR, due to which the balance with other European fundamental rights were set in risk. The judgement[190] held that data subject's rights should override the public interest in principle, and be avoided only under certain circumstances.

Popular point-to-multipoint networks, such as official newspapers, serve public interest to which citizens are granted an access. The publications may, however, contain harmful, irrelevant and invalid personal information. Miquel Peguera[191] remarks the difference between data protection offences and defamation: for actual offenses there is the AEDP but defamation falls outside the scope of any data protection authorities. Peguera states[192] that due to vague distinction between the two, Google has refused to erase publications such as outdated pardons, charges and lawsuits. Peguera states [193] that unless the publication is related to national security, such information is often outdated and, therefore, irrelevant for public informational purpose.

---

[185] European Court of Justice (2014) *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (C-131/12) s*upra* nota 178, p 27.
[186] OJ L 281, 24.11.1995, Article 2(d) on definitions.
[187] *Ibid*
[188] *Ibid*
[189] *Ibid*
[190] European Court of Justice (2014) *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (C-131/12) s*upra* nota 178, p 27.
[191] Peguera, M. In the aftermath of Google Spain: how the 'right to be forgotten' is being shaped in Spain by courts and the Data Protection Authority. Oxford University Press, International Journal of Law and Information Technology 2015, 23, pp. 325–347.
[192] *Ibid*
[193] *Ibid*

3. Data Protection Directive

3.1. Current Phase

The European Data Protection Directive has been the source of European data protection law for longer than two decades. Provisions of the directive have been implemented to national laws of the Member States across the EU. In order to give an international overview of applicable data protection law across the EU, the European Union Agency for Fundamental Rights and the CoE together with the Registry of the ECtHR prepared a Handbook on European data protection law in 2014.[194] The Handbook consists of the major data protection principles and their backgrounds: the European data protection rules, data subject's rights and transborder data flows are discussed in the light of the DPD, which is the core source of the principles presented in the Handbook. However, instead of unifying the legislation, the Directive only harmonized it

According to the Handbook[195] , the DPD is not necessarily a data protection framework itself but a substance given to the principles set in Convention 108[196]. It is stressed that when the DPD became applicable in 1995, all fifteen EU Member States were also Contracting Parties to Convention 108.[197] It is observed in the Handbook[198] that the Court of Justice of the European Union (CJEU) has stated the following: "Directive 95/46 is intended [...] to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. [...] The approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the EU. Accordingly, [...] the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete."[199]

[194] The European Union Agency for Fundamental Rights, the Council of Europe. Handbook on European data protection law. Publications Office of the European Union, Luxembourg, printed in Belgium, 2014.
[195] *Ibid*
[196] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Council of Europe. The first binding international instrument to protect the individuals from abusive gathering and processing of personal data. Strasbourg, No. 108, 28.1.1981.
[197] *Ibid*
[198] *Ibid*
[199] The Court of Justice of the European Union, Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24.11.2011. Cited in the Handbook on European data protection law (The European Union Agency for Fundamental Rights, the Council of Europe. Handbook on European data protection law. Publications Office of the European Union, Luxembourg, printed in Belgium, 2014, p 18.)

The DPD applies to all countries of the European Economic Area (EEA). Despite the harmonization, the DPD did not solve the issue of transferring data to third countries. Personal data shall only be transferred to non-contracting states if an adequate level of protection is guaranteed. Therefore, in 2000 the EC drafted an EEA relevant decision[200] on the protection provided by the Safe Harbour privacy principles, which are also presented in the Handbook. The Safe Harbour agreement was a transatlantic agreement with the US that aimed to promote the harmonization of data protection rules and adequacy between the European States and the US. However, in 2015 the CJEU stated that the protection provided via Safe Harbour agreement was not, however, adequate enough to protect the European citizens' data privacy in the US.[201] Therefore, the agreement was invalidated after allowing transatlantic data transfers for fifteen years.[202]

3.2. Cross-border Discovery Conflicts

Digital evidence is an internationally recognized form of evidence in modern legal proceedings. As observed above a high volume of data is being produced continuously. Therefore, numerous devices are sources of not only personal data but of potential evidence as well. Due to international communication and connections, such data often locates abroad, outside the national legislation. Jurisdictional differences, however, tend to build conflicts and obstacles for investigations and international litigations.

3.2.1. The European Union and United States

The EU has developed an advanced and harmonized data protection legislation. The US instead has a broad approach towards privacy: what is known as personal data in the US, is considered as personal sensitive data in the EU[203]. However, as observed in previous chapters, the European data protection rules tend to be territorial, which limits data transfers to third countries. When the US investigations and legal proceedings require data gathering from the EU, conflicts tend to occur.

[200] Commission Decision 2000/520/EC. The European Parliament and the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. Brussels, OJ L 215, 25.8.2000.
[201] Gibbs, S. What is 'safe harbour' and why did the EUCJ just declare it invalid?. The Guardian 2015. www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection (29.03.2017)
[202] *Ibid*
[203] The Sedona Conference. The Sedona Conference Practical In-House Approaches for Cross-Border Discovery and Data Protection, 2016.

Seth Berman remarks[204] that the US law generally presumes that a company owns all the data it stores and regulates. Berman therefore notes[205] that data subjects' rights or data privacy violations, are rarely recognized as a concern. He states[206] that the US litigation is strongly based on civil procedure rules, according to which one shall start storing relevant data as soon as it is probable that a lawsuit will occur.

According to Berman[207], in the international context, Rule 26 of the Federal Rules of Civil Procedure[208] creates legal obstacles for data transfers. The Rule 26 provides the following: "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defence - including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter."[209] Berman observes[210] that according to Rule 26, any litigate party may have to search their own devices for any relevant data. Furthermore, the US scope for data subjects is even broader. According to Berman[211], the US litigants are obliged to store any data that could potentially be relevant to the future litigation without precise purpose.

In Europe the DPD remains applicable until May 2018. The Directive provides that companies do not gain arbitrary right to use data during possession because in Europe but data subjects maintain the ownership to their personal data that is possessed by third parties. As well as the DPD, the GDPR regulates exposure of private data: one's data shall not be exported to third countries if sufficient data protection jurisdiction is not provided in that State. According to Berman[212], the US is not considered as a state with sufficient degree of data protection, due to which electronic discovery conflicts occur. Moreover, the legal nature of the Directive enables national jurisdictional differences within the EU Member States. Those differences will be, however, unified by the GDPR as it is directly applicable as such.

[204] Berman, S. Cross-border Challenges for e-Discovery. Business Law International 2010, 11 (2), pp. 123-132.
[205] *Ibid*
[206] *Ibid*
[207] *Ibid*
[208] Federal Rules of Civil Procedure, Rule 26 - Duty to Disclose; General Provision Governing Discovery.
[209] Federal Rules of Civil Procedure, Rule 26 - Duty to Disclose; General Provision Governing Discovery. Cited in Berman (Berman, S. Cross-border Challenges for e-Discovery. Business Law International 2010, 11 (2), pp. 123-132.)
[210] Berman s*upra* nota 204, p 31.
[211] *Ibid*
[212] *Ibid*

However, Berman[213] states that the European territorial limits on data transfers are not only inconsistent with the US rules but with multinational corporations as well. Therefore, in 2009 the EC published Article 29 Data Protection Working Group, Working Paper 158[214] to address the issue. According to Berman[215], the Working Paper manages to recognize the issue of applying the European territoriality rules in businesses but it does not, however, offer any solution to it. According to the Working Paper[216], before exposing any data, corporations should balance the proportionality with the demand. In order to solve this issue, several suggestions are presented in the Working Paper[217] : anonymizing the data; avoidance of collecting unnecessary data, use of trusted third parties to handle the data, and filtering data within the EU before transferring it to the US. These suggestions are also specified under the GDPR.

The GDPR will not only cover individuals but businesses that have operations in Europe as well. Gabriela Zanfir stresses[218] that in case a multinational corporation, such as Facebook, Apple and Google, offers services for EU citizens, new data protection rules must be implemented. According to the Commission[219], the European citizens should be provided secure and confidential processing of personal data outside the EU as well. However, Zanfir states[220] that in case the data is efficiently anonymized, it will not fall within the scope of the GDPR. Identifiable personal data should be pseudonymised as soon as possible.[221] Furthermore, pseudonymization reduces the privacy risks of the data subjects, and ease data processors and controllers to meet data-protection obligations.[222]

3.2.1.1. Blocking Statutes

Due to excessive discovery intrusions by foreign litigants, a number of Civil Law countries, especially Germany and France, have imposed blocking statutes to protect the privacy of their citizens. Vivian Grosswald Curran states[223] that the US courts are not pleased with these statutes

[213] *Ibid*
[214] Article 29 Data Protection Working Group, Working Paper 158. The European Commission. The document goes on to set out guidelines for EU data controllers when trying to reconcile the demands of the litigation process in a foreign jurisdiction with the data protection obligations of Directive 95/46/EU. Brussels, 11.2.2009.
[215] Berman s*upra* nota 204, p 31.
[216] Working Paper 158 s*upra* nota 214, p 32.
[217] *Ibid*
[218] Zanfir, G. The right to Data portability in the context of the EU data protection reform. Oxford University Press, International Data Privacy Law 2012, 2 (3), pp. 149-162, pp. 153-155.
[219] Working Paper 158 s*upra* nota 214, p 32.
[220] Zanfir s*upra* nota 218, p 32.
[221] OJ L 119, 27.04.2016, preamble (78).
[222] *Ibid*, preamble (28).
[223] Grosswald Curran, V. United States Discovery and Foreign Blocking Statutes. Louisiana Law Review, A Louisiana Law Review Symposium of the Civil Law 2016, 76 (4), pp. 1141-1149.

that jeopardize the fundamental rights of the US plaintiffs by decreasing their ability to discover evidence. Vise versa, the European litigants are concerned over the US discoveries and the risks they impose to fundamental rights of the European citizens. Grosswald Curran observes[224] that these Roman Law inspired blocking statutes invalidate the obligation of the German and French to assist their opponent in litigation. However, in Germany and France the requesting judge is obliged to provide a specific description on what information is insisted and how it is relevant to the case, which is not a common practice in the US.

In 1970 the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters[225] was introduced to facilitate international discovery policies. Through the Convention, the Contracting States desired to establish joint provisions on mutual recognition of legal requests for discovery. However, in case *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa*[226], the US Supreme Court held that on a case-by-case basis, the Hague Convention could be circumvented by the rules set in the Federal Rules of Civil Procedure[227]. Moreover, there was only a small number of parties to the Convention[228], which dilutes its competence. Article 23 of the Hague Convention provides the following: "A Contracting State may at the time of signature, ratification or accession, declare that it will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries."[229]

In the aftermath of case *Moses Strauss et al. v. Crédit Lyonnais, S.A*[230] a French advocate was arrested and prosecuted after investigating a French national under the US District Court orders. Furthermore, such discovery for foreign litigations was criminalized under French Law No 80-538[231] that provides the following: "Subject to international treaties or agreements and laws and regulations in force, it is forbidden for any person to request, seek or communicate, in writing, orally or in any other form, documents or information of an economic, commercial, industrial,

[224] *Ibid*
[225] Hague Conference on Private International Law. The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters. Hague, 01.02.1970.
[226] United States Supreme Court, *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa,* 482 U.S. 522, 1987.
[227] Federal Rules of Civil Procedure. The United States 1937, (amended in 2016).
[228] Hague Conference on Private International Law (1970) s*upra* nota 225, p 33.
[229] *Ibid*, Article 23.
[230] United States District Court Eastern District of New York, *Moses Strauss et al. v. Crédit Lyonnais, S.A,* (1:06-cv-00702), 2007.
[231] French Law No 80-583 on the communication of economic, industrial, financial, or technical documents or information to foreign individuals or legal entities, 16.07.1980.

financial or technical nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures or in the context of such procedures." The Statute has prevented any judicial cooperation involving personal data disclosure to the US. In 2018, the GDPR will however unify the legislation regarding data transfers to third countries. According to the doctrine of supremacy of EU law[232], the GDPR will therefore have an impact on blocking statutes.

According to Agnes Kasper and Eneli Laurits[233], the US court has, however, established a five-sector test to avoid confusion among the US litigants. The test aims to evaluate whether the foreign piece of electronic evidence should be eligible for e-discovery[234]. According to the five-sector test[235], one should evaluate the importance of the discovery, the degree of its specificity, whether the information has originally aired within the US, are there any alternative security measures to protect the data, and if there is a possibility for undermine in interests. Kasper and Laurits state[236] that after balancing the five matters mentioned above, one shall decide whether to comply with the foreign blocking statute or the US order. The authors remark[237] that the US litigants shall not comply with them both.

3.2.2. Privacy Concepts in Asia

Asia is highly diverse in culture, politics and legal systems. A number of Asian states follow the Anglo-American Law traditions, while others belong to the Civil Law family. Moreover, religious traditions have entailed significant features to a number of Asian national jurisdictions. Therefore, there is no unified legal norms in Asia but numerous mixed jurisdictions. Asian states are, however, significant participants in international trade and modern communication, which is why it is important to discuss the Asian data protection rules in context with the EU and US. According to Allan Chiang[238] the Hong Kong's Personal Data Ordinance was the first data privacy related jurisdiction in Asia. Chiang states[239] that after it came into force in 1996, eleven other Asian states

[232] European Court of Justice, *Van Gend en Loos v Nederlandse Administratie der Belastingen*, (Case 26/62), 1963.
[233] Kasper, A., Laurits, E. Challenges in Collecting Digital Evidence: A Legal Perspective; Kerikmäe, T., Rull, A. (ed.) The Future of Law and eTechnologies. Tallinn, Springer International Publishing Switzerland 2016.
[234] *Ibid*
[235] *Ibid*
[236] *Ibid*
[237] *Ibid*
[238] Chiang, A. Foreword for Greenleaf, G. Asian Data Privacy Laws: Trade and Human Rights Perspectives. New York, Oxford University Press 2014.
[239] *Ibid*

have implemented similar, yet incomplete, rulings in their national laws. Such trend discloses the growing concern over privacy in Asian nations as well.

As observed above, privacy is a fundamental human right that is a platform for personal data protection. Therefore, Greenleaf states[240] that all the Asian countries that are members of the CoE, are obliged to apply Article 8 of the ECHR, which is why a majority of the Asian countries have implemented privacy in their constitution. However, due to cultural differences the Asian values are much different from the European ones. Michael C. Davis states[241] that Asian values promote anti-democratic society structure. Davis further notes[242] that due to lack of such cultural prerequisites, East-Asian societies are considered as unsuitable to imply Western privacy principles.

The idea of illiberal culture is also seen in William Case's classification[243], according to which Asian states can be divided into three categories based on the degree of their democracy: democratic, semi-democratic, and authoritarian regimes. Greenleaf, however, observes[244] that although Asia is still considered as semi-democratic region, western privacy principles continuously influence legislation in the Asian states. Greenleaf argues[245] that the importance of the previously discussed OECD Guidelines is nevertheless also effective in Asia as their significance does not necessarily lay on the number of members but its influence as a standard. Therefore, despite the fact that Japan and Korea are currently the only Asian members of the OECD, Asian data privacy policies could be harmonized by implementing the Guidelines in Asian non-member states as well. According to Greenleaf[246], the main question is, however, whether democratic laws could actually be efficiently applied in semi-democratic circumstances.

[240] *Ibid*
[241] Davis, M. C. The political economy and culture of human rights in East Asia. Jindal Journal of International Affairs 2011, 1 (1), pp. 48-72.
[242] *Ibid*
[243] Case, W. Politics in Southeast Asia: Democracy or Less. Psychology Press 2002.
[244] Chiang s*upra* nota 238, p 34.
[245] *Ibid*
[246] *Ibid*

4. Data Protection Reform

4.1. Regulation (EU) 2016/679

According to Viviane Reding[247] the EC has identified three main data protection related challenges: the prominent capabilities of modern technologies, the increase of global data transfers, and LEA's accessing personal data now more than ever.[248] The development of modern technologies, mobile devices, and the Internet services bring benefits to not only individuals but to businesses and public authorities as well. In order to gain trust and increase economy, Reding argues[249] that the personal data must be secured, especially when the data is stored in the cloud. In order to improve European legislation and its suitability in the digital age, the EC disclosed the EU Data Protection Reform in January 2012.[250] The Regulation constitutes a modern and unified framework for international data protection within the EU.

The text of the Regulation was published in the EU Official Journal on the 4th of May in 2016.[251] It entered into force twenty days later, and will be applicable from the 25th of May in 2018.[252] Alongside with the Regulation 2016/679 the European Parliament and the Council drafted Directive (EU) 2016/680[253] which is to be applied on Police and Criminal Justice Sector. In the Press Release[254], published in December 2015, the EC states that complexities, legal uncertainty and administrative costs have occurred due to differences in national implementations of Directive 95/46/EC, which was introduced at a time when majority of modern devices, services, platforms or any other data protection challenging applications were not yet existing. The Regulation 2016/679 is considered as a significant improvement in unifying and strengthening the European citizens' fundamental rights and freedoms in the digital age but it also plays a major role in promoting the Digital Single Market within the EU.[255]

[247] Vice-President of the European Commission in 2010-2014. ec.europa.eu/archives/commission_2010-2014/reding/ (12.4.2017)
[248] Reding, V. The upcoming data protection reform for the European Union. Oxford University Press, International Data Privacy Law, 2011, 1 (1), pp. 3-5.
[249] *Ibid*
[250] European Commission's Directorate General for Justice and Consumers. Reform of data protection rules. The European Commission, 18.1.2016. ec.europa.eu/justice/data-protection/reform/index_en.htm
[251] *Ibid*
[252] *Ibid*
[253] OJ L 119, 4.5.2016.
[254] European Commission. Press Release on the Data Protection Reform, Questions and Answers. The European Commission Press Release Database, MEMO/15/6385, 21.12.2015, Brussels. europa.eu/rapid/press-release_MEMO-15-6385_en.htm (29.3.2017)
[255] *Ibid*

Due to modernization of electronic devices and ascent of social media, international communication has reached a new, global dimension. According to Reding[256], data subjects should have the right to know how and by whom their personal data is being gathered and processed, and what would be their rights to access, correct or delete the data. The EC complies with Reding as it states[257] that the objective of the Regulation is to grant the individuals more control over their personal data[258] and therefore strengthen their rights in the online environment, where transparency and clear policies are often lacking. Moreover, due to the global dimension of data protection, in 2011 Reding requested[259] unified data protection rules for actions involving third countries: European citizens should be able to enjoy the same data protection rights as the third country nationals would enjoy in the EU. Via international data protection standards, the Regulation ensures a strong enforcement of the rules when transferring European citizen's data to any third countries or to international organizations[260], and reinforcement of the European single market.

4.2. Data Protection in the Twenty-first Century

Directive 95/46/EC was considered as a milestone document in development of personal data protection. Viviane Reding addresses[261] that the DPD cherished two basic pursuits of the European integration: the protection of fundamental rights and freedoms, and the development of internal market through free flow of data within the EU. However, as observed earlier, instead of unifying the codification, the DPD only ensured similar data protection legislation in the Member States, due to which data controllers were forced to process data with different data protection laws. Therefore, unnecessary administrative burdens and costs occur. Via directly applicable Regulation, Reding estimates[262] that companies would be led to savings of €2.3 billion a year.

The EC's Data Protection Reform contains new legislative instruments. The pursuit of those instruments is to initiate significant improvements regarding legal basis, the rights of data subjects and responsibility of data controllers. Moreover, personal data protection regarding international data transfers, and police and criminal justice authorities will be updated through the reform.

[256] Reding (2011) *supra* nota 248, p 36.
[257] European Commission (2015) *supra* nota 254, p 36.
[258] OJ L 119, 27.4.2016, Chapter III Rights of the data subject
[259] Reding (2011) *supra* nota 248, p 36.
[260] OJ L 119, 27.4.2016, Chapter V Transfers of personal data to third countries or international organisations.
[261] Reding,V. The European data protection framework for the twenty-first century. Oxford University Press, International Data Privacy Law, 2012, 2 (3), pp. 110-129.
[262] *Ibid*

According to Reding[263], Article 16 of the Treaty on the Functioning of the European Union (TFEU)[264] serves as a new legal basis for the Regulation and the Directive. By providing right to protection of personal data, Reding states[265] that one is granted the fundamental right to data protection that applies to all Union policies. Previously legal bases for regulating personal data processing and protection were rather distinct. However, Reding argues[266] that via Article 16 TFEU the legal bases will be unified across the EU.

The CJEU has held in several decisions[267] that regardless of whether or not a cross-border element is involved, the rules regarding personal data protection, data processing activities, and free flow of such data within the EU shall remain applicable. Moreover, Reding stresses[268] that activities that do not fall inside the scope of Union law activities, would also fall outside the scope of the Regulation 2016/679 and the Directive 2016/680. However, as much as globalization has affected the need for adequate data privacy legislation, it is necessary to provide regulations for domestic data processing activities as well. According to Reding[269], Article 16 TFEU does not distinct domestic and cross-border processing operations. She therefore stresses[270] that as the Directive will provide harmonized regulations regarding operations within the EU, the investigational work of LEA's would facilitate.

Strengthening individuals' control over their personal data is a major element of the GDPR. According to Reding[271], a major obstacle for individuals to purchase goods on the Internet is the concern over their privacy. Therefore, Reding states[272] that through high level of unified data protection, the European citizens would enhance the digital economy and digital single market, and furthermore, economic growth and competition within the EU. By three major measures and improvements, Reding argues[273] that individuals' are granted more control over their data: clarifying their consent, specified scope of the right to be forgotten, and right to access and right

[263] *Ibid*
[264] OJ C 326, 26.10.2012, Article 16 (ex Article 286 TEC).
[265] Reding (2012) *supra* nota 261, p 37.
[266] *Ibid*
[267] CJEU Joined Cases C-465/00, C-138/01, and C-139/01 *Rechnungshof*; Case C-376/98 *Germany v Parliament and Council*; Case C-491/01 *British American Tobacco and Imperial Tobacco*, cited in Reding (Reding,V. The European data protection framework for the twenty-first century. Oxford University Press, International Data Privacy Law, 2012, 2 (3), pp. 110-129.)
[268] Reding (2012) *supra* nota 261, p 37.
[269] *Ibid*
[270] *Ibid*
[271] *Ibid*
[272] *Ibid*
[273] *Ibid*

to data portability. Prior to applicability of the GDPR, consent that is legally valid in one Member State, may be invalid in another which initiates uncertainty and inequality between the processes operated in different European states. Moreover, Reding states[274] that the GDPR introduces an obligation on controllers, according to which they are obliged to inform the data subject of estimated period for the data storage, and their rights to it. Such measures encourage to complete and maintain the admissibility criteria for data that can potentially be used for litigation purposes.

4.2.1. eDiscovery in Context of the Reform

The GDPR aims to facilitate international data transfers within and outside of the EU. According to Reding[275], Article 45[276] of the GDPR, which complies with the OECD recommendation on cross-border cooperation in the enforcement of laws protecting privacy[277], is to provide measures for international cooperation between the EC and the supervisory authorities outside the EU. Furthermore, Reding states[278] that legal issues regarding investigations and inspections are facilitated by Articles 51[279] and 54[280] of the GDPR which set legal bases and conditions for efficient cooperation between supervisory authorities. Moreover, Reding remarks[281] that in case the EC approves the adequacy of data protection, transferring personal data to third countries or international organizations by police and criminal justice authorities may now be admissible.

Legal obligation is a legitimate ground for international data transfers. In order to legitimize an e-discovery, the EC must recognize the sufficiency of data protection level in that third country. Lawrence Ryz and Tracey Stretton remark[282] that the GDPR only applies to European legal obligations. Therefore, requests arising from the US law, or that are made by American regulators or LEA's may not meet the criteria for legal obligation. As observed above, such jurisdictional differences and obstacles, create a number of international e-discovery conflicts and challenges.

[274] *Ibid*
[275] *Ibid*
[276] OJ L 119, 4.5.2016, Article 41 on monitoring of approved codes of conduct.
[277] The OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy 2007. www.oecd.org/sti/ieconomy/38770483.pdf (14.04.2017)
[278] Reding (2012) *supra* nota 261, 37.
[279] OJ L 119, 4.5.2016, Article 51 on supervisory authority.
[280] *Ibid*, Article 54 on rules on the establishment of the supervisory authority.
[281] Reding (2012) *supra* nota 261, 37.
[282] Ryz, L., Stretton, T. EU Data Protection Gains A Sword To Go With Its Shield. Association of Corporate Counsel, ACC Docket, 2015. www.ediscovery.com/cms/pdf/EU-Data-Protection-Gains-Sword-to-Go-with-Shield.pdf (15.04.2017)

Ryz and Stretton state[283] that when implementing the DPD, a number of Member States ruled that data transfers to third countries should be either authorized by or notified to local Data Protection Authorities. However, the authors stress[284] that the GDPR does no longer require such approval in case the other requirements of the GDPR are met. Ryz and Stretton therefore conclude[285] that this would drastically decrease the administrative costs of multinational corporations that depend on EU Model Contracts. Furthermore, unlike the DPD that only applies to data controllers, the GDPR sets a number of specified obligations on data processors as well. Ryz and Stretton argue[286] that such change may substantially affect e-discovery and service providers.

4.2.2. New Instruments for Data Transfers

In order to protect Europeans citizens' privacy during personal data transfers to third countries, the EC has established[287] different tools and rules to ensure sufficient level of data privacy outside the EU. One of those tools is the adequacy decision. After the EC has assessed necessary elements, it may decide whether the third country provides level of data protection that is equivalent to that in the EU. Now the EC may however apply the adequacy decision on LEAs as well.[288] Furthermore, the reform enables partial adequacy[289] in case where the third country only has a specific territory or particular sector that is considered to fulfill the adequacy requirements.

In the absence of adequacy decision, the reform introduces a number of alternative measures to provide secured data transfers.[290] The previous instruments such as standard contractual clauses (SCCs) and binding corporate rules (BCRs) are being formalized and expanded.[291] SCCs may now be applied in the contracts between European processors and the ones in the third countries.[292] Furthermore, the scope of BCRs has been expanded as it may now be applied in a group of different companies engaging in the same economic activity.[293] Furthermore, the GDPR provides completely new instruments; approved codes of conduct, and certification mechanisms are

[283] *Ibid*
[284] *Ibid*
[285] *Ibid*
[286] *Ibid*
[287] European Commission, Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalized World. Brussels, 10.01.2017.
[288] OJ L 119, 4.5.2016, Article 36(2).
[289] OJ L 119, 27.4.2016, Article 45(1) and OJ L 119, 4.5.2016, Article 36(1).
[290] European Commission (2017) *supra* nota 287, p 40.
[291] *Ibid*
[292] OJ L 119, 27.4.2016, Article 46(2)(c)(d).
[293] *Ibid*, Article 46(2)(b).

flexible instruments enabling establishment of sufficient safeguards for data transfers between public authorities.[294] Moreover, the use of derogations is specified under the GDPR.[295] Finally, the EC will be enabled to establish international cooperation mechanisms, such as mutual assistance arrangements in accordance with the GDPR.[296]

[294] *Ibid*
[295] OJ L 119, 27.4.2016, Article 49.
[296] *Ibid*, Article 49(1), second subparagraph.

Conclusion

Information technology is in the center of modern society that is strongly built upon digital domain. A great variety of electronic tools are being used for communication, entertainment, preservation and commercial purposes. Digital domain is an easily accessible and cost efficient platform for not only civil persons but multinational corporations, LEAs and investigators as well. Due to high volume of data produced on a mundane basis globally, digital domain has reached a significant status in legal proceedings: any modern investigation or legal dispute, civil or criminal, involves digital evidence with high probability. However, the complexity of online environment and information society create both national and international jurisdictional challenges.

Contents that may potentially become digital evidence emerge in a number of different mundane electronic sources: communication devices, social networks, databases, downloads, etc. Therefore, any data that is stored or transferred by using electronic means, and is used to support a claim, is considered as digital evidence. In order for digital evidence to be admissible for court proceedings, it must be relevant, reliable, complete, authentic, and proportionate. Before such admissibility can be verified, the investigation should follow the structure of proper multi-staged investigation process. Negligent actions during the investigation may lead to incomplete or even false evidence.

Although there is a number of international instruments setting rules and principles regarding digital evidence processing, unified legislation for international digital forensics is still lacking. Previous provisions and regulations are yet outdated in the modern context, as personal data and privacy concerns are recognized as a main concern in the online environment. In order to operate a proper investigation, one's privacy must not be interfered at any time. Therefore, when investigators desire to search suspicious personal data, search warrant is required for further proceedings. However, traditional approaches do not satisfy the demand of digital forensics which are challenged due to multiple locations and jurisdictions.

In order to search both the physical devices and digital contents the search should be operated in two stages: traditional seizure of the physical devices, and electronic search to collect the necessary data. Current legislation does not provide applicable laws for such two-stage process, as the regulations regarding search warrants are structured for traditional seizures. Further issues arise when cross-border element is involved. Despite the different national legislations, the OECD Guidelines are globally recognized as a ground for personal data privacy. After they were revised

in 2013, two new themes were included: risk management and improved operability, which are both important for modern commercial centralized communications.

The importance of harmonized personal data privacy principles becomes distinct when using cloud services. This flexible and cost efficient service has attracted an enormous number of mundane users; individuals and corporations. Cloud computing does however comprise severe data privacy concerns: when transferring data to cloud service, one's personal data becomes a subject to foreign jurisdiction, which potentially induce cross-border conflicts regarding data privacy. Furthermore, the remote nature and multi-jurisdictional environment of cloud computing hinder the access of investigators. Currently there is neither specific legislation regarding cloud forensics nor international agreements between LEAs on cooperation.

In Europe, privacy is however a fundamental human right recognized under a number of international treaties. Modern individual must be guaranteed physical protection and distance from society, and right to private life at home. Furthermore, developed privacy legislation promotes democratic society structure. The increased usage of sophisticated ICT systems are often, however, considered as a threat to modern demand for privacy. Moreover, increased popularity of social media has affected the common expectations for privacy. The distinction between public and private information is rather vague as individuals share and publish data regardless the privacy risks that may occur.

Privacy settings set by an individual play a major role in the online environment and digital investigations. Having weak privacy settings may emerge as an open account to which anyone is able to access, while limited access and secured account requires a search warrant or court order before accessing legally. Much of OSINT does however emerge from social media. Such data is often identifiable, due to which it falls under the scope of Article 8 of the ECHR and must therefore be protected from interferences. Although, digital communications are highly valued by LEAs when investigating crimes and misanthropic behavior, proportionate policies between privacy and public interest should be balanced.

Furthermore, national security is often balanced with personal data privacy rights. In order to fight modern terrorism, states and authorities tend to interfere citizens' privacy rights via systematic surveillance. Data captured from surveillance cameras is a common form of digital evidence presented in litigations. Despite the technology, the captures are nevertheless analyzed via human

resources, which is why their validity does not necessarily complete the admission criteria. Therefore, such material should not be used as an evidence unless it substantially supports the quilt of the accused.

Despite the fundamental status of privacy, it is yet unclear whether personal data protection is an optional obligation or binding rule of CIL. Since 1995, Directive 95/46/EC has been the main source of European data protection law. It was aimed to ensure equality in data privacy protection and processing of personal data between the Member States. The DPD is applicable not only within the EU but in EAA as well. However, before the GDPR becomes applicable on the 25th of May in 2018, there is no common policy that is directly binding in nature. Instead, the European Member States have implemented the provisions of the DPD in their national laws. Despite the European level Directive, Member States and governments may pass laws allowing data privacy interferences.

In order to avoid acquisition of however wrongful data, one shall be eligible to request removal of invalid and therefore irrelevant, unnecessary or harmful personal data. Judgement in Google Spain case held that data subject's rights should override the public interest. The principle commonly known as the right to be forgotten is a substantial feature of the GDPR. It improves individual's control over their own data by increasing the number of obligations on controllers. Furthermore, such provision will promote democracy and one's control over their reputation.

Instances involving a cross-border element to third countries are yet more challenging to solve. Under EU law, data transfers to countries with inadequate level of data protection, such as the US, are not permitted. Due to strict territoriality of the European data protection legislation, data transfers to third countries are limited. Therefore, EC drafted an EEA relevant decision in 2000: the Safe Harbour agreement aimed to promote the data transfer cooperation between the US and the European States. In 2015, the agreement was, however, declared invalid due to insufficient data protection provisions in the US. Transferring data between two different jurisdictions challenge transnational e-discovery, investigations and legal proceedings.

The European provisions regarding data transfers are not only inconsistent with the US but with multinational corporations as well. Therefore, a number of Civil Law countries, especially France and Germany, have imposed Roman Law inspired blocking statutes to protect the privacy of their citizens against excessive discovery intrusions. The Hague Convention provided that Contracting

States shall refuse to disclose documents for pre-trial discovery purposes. Furthermore, French Law forbids any constitution of evidence for foreign judicial or administrative procedures. The US courts are not, however, pleased with such blocking statutes as they invalidate the obligation of German and French to assist their opponent in litigation, and therefore jeopardize the fundamental rights of the US plaintiffs.

Prominent capabilities of IT, increased number of global data transfers, and LEAs continuously accessing personal data are the three main challenges regarding data protection. In order to overcome these challenges, the EC disclosed the EU Data Protection Reform in January 2012. On the 4th of May in 2016 the official text of Regulation 2016/679 was published, and it will be applicable from 25th of May 2018. Due to national differences in implementations of the DPD, legal uncertainty and unnecessary administrative costs occur. Therefore, the directly applicable Regulation is considered as a significant improvement in unifying personal data protection provisions across the EU. Furthermore, free flow of data reached through the Regulation will promote the European Digital Single Market.

The objective of the Regulation is to provide individuals more control over their personal data. By clarifying one's consent, specified scope of the right to be forgotten, and the right to access and right to data portability, control is given to the data subjects themselves. Due to jurisdictional differences, consent that was previously given in one Member State, could be legally invalid in another. Such uncertainty created inequality between European States, and challenged digital cooperation and assistance. Furthermore, the controller will be obliged to inform the data subject about the estimated period of strong their data, and their further rights to it. This will not however only promote data subjects' right to control their data. Via such measures, admissibility criteria for data will be complete and maintained.

In the online environment where transparency and specified policies are yet lacking, individuals will be guaranteed sufficient level of data protection regardless to where their data is being transferred to. European citizens should be able to enjoy the same level of protection as the third country national enjoy in the EU. The Regulation therefore ensures a strong enforcement of the rules regarding data transfers to third countries, via which international transfers will be facilitated. However, prior to transferring European citizen's data, there must be a legitimate ground for it. As the GDPR will only be applicable to European legal obligations, requests arising from the US jurisdiction may not meet the criteria for legal obligation. Furthermore, when implementing the

DPD, a number of Member States ruled that personal data transfers to third countries should be either authorized by or notified to local Data Protection Authorities. The GDPR does not require such approval in case the other requirements set in the Regulation are met.

The DPD introduced the principle of adequacy decision, prior to which the EC assessed detailed elements before deciding whether or not that third country had sufficient level of data protection. The principle remains as a core in the Reform but shall now be applied on LEAs as well. Moreover, further improvements and alterations are being made. In order to facilitate transfer policies, tools such as SCCs and BCRs are extended to apply to a larger group. In addition to partial adequacy decision and extensions, the Reform introduces a number of new instruments to provide security for international personal data transfers: approved codes of conduct, and certification mechanisms are flexible instruments that may now be used to establish sufficient safeguards for data transfers between public authorities. Furthermore, the GDPR specifies the use of derogations and enables the EC to establish international cooperation mechanisms, such as mutual assistance arrangements.

The European Data Protection Reform is not only a distinct set of rules to protect one's data privacy but there is a strong connection to a global context as well. In order to collect digital evidence for both domestic and international purposes, jurisdictional harmonization is demanded. The GDPR will provide unified ground for European data protection legislation, which facilitates evidence acquisitions. Via stringent and detailed regulations, uncertainty and vague implementations will be voided. Therefore, admissibility of potential evidence will become complete and well maintained.

By giving more control to data subjects, arbitrary intrusions will decrease which promotes individual's fundamental right to privacy. Supremacy of the EU law and directly binding nature of the Regulation will unify the European data protection law. Challenging intercourses may however occur due to national Criminal Laws, as seen with the French blocking statutes. To what extent such national restrictions are applicable after the GDPR becomes applicable, remains as national challenge to solve. However, in case a Member State fails to meet the obligations set under the Regulation resulting in violations or damages, an individual may rely on EU law before national courts.

The author of this thesis agrees that modern investigation processes are being challenged due to outdated legal instruments. Furthermore, she argues that despite the significant unification,

the Data Protection Reform will not resolve all the issues observed in this thesis. The Reform is addressed to protect individual's personal data from interferences, and by giving the control to data subjects themselves, privacy and democratic society is being promoted. However, issues regarding investigation processes are left unsolved. The author argues that privacy and data protection are not sufficient as such to provide an adequate ground and framework for digital forensics.

The GDPR provides that in relation to third countries and international organizations, the EC and supervisory authorities shall take proper measures to develop international cooperation and mutual assistance during investigations. However, the author of this thesis remarks that the tools for such improvements are left unidentified. Although the measures are described in the GDPR, it is down to the Member States to decide how to operate them. Furthermore, those provisions regarding cooperation concern the Member States only. Despite the new instruments to facilitate the sufficient data protection, the GDPR does not resolve the cooperation issue regarding data transfers to third countries.

As observed in this thesis, modern investigation, search and seizure requires multiple stages. Despite the directly applicable nature of the GDPR, the author of this thesis does not consider it to unify the actual investigation process. Instead she stresses the importance of separate instrument, such as the ISO/IEC 27037 and OLAF Guidelines. As it is remarked in this thesis, a large amount of data is transferred internationally within the EU and to third countries. In case there was an instrument such as the ones mentioned above but binding in nature, not only European Member States but third countries as well would face harmonization. Via harmonized rules regarding investigation process, the number of interferences and potential data protection risks would decrease.

As seen in Spar case, technology creates new tools to operate efficient investigations. Forensic software, predictive coding and cloud computing are examples of modern technology tools to facilitate digital forensics and investigation. However, the author of this thesis observes that when only dealing with the privacy and data protection, such technical measures are left without assessment. She argues that an instrument such as the Cybercrime Convention could be used to regulate the technical means and measures. Again, issues however occur due to the legal nature of the Cybercrime Convention: instead of being directly applicable and binding instrument, it must

be ratified. Furthermore, the author of this thesis addresses its outdated nature in the context of modern technologies.

As observed in this thesis, despite the direct applicability of the GDPR, the European Member States may have national legislations that will be in conflict with the Regulation. In order to remark and resolve such conflicts, careful research on both national legislation and the GDPR is necessary. The author of this thesis observes that only after such examining, it is possible to estimate the extent of potential conflicts. For instance, the blocking statutes have restricted data transfers for foreign litigation purposes. Due to supremacy of the EU law, these blocking statutes will no longer hinder the data transfers to the same extent but will likely create conflicts between the national and EU law.

An overall impact of the Data Protection Reform will be to protect individual's right to personal data protection in modern context. However, when it comes to processing digital evidence, other instruments are necessary as well. In order to provide legitimate and secured investigation in digital domain, in addition to personal data protection there should be adequate legal instruments to regulate the technical tools and cooperation with the third countries. The author of this thesis argues that the territorial effect of the GDPR remains within the EU due to which its impact on processing digital evidence in transatlantic context remains vague. However, the European unification regarding data protection law facilitates and clarifies the confusion. Not only the European authorities but those of the third countries as well, will be required to work with one data protection legislation instead of twenty-eight different.

List of Sources

Science books:

1. Case, W. Politics in Southeast Asia: Democracy or Less. Psychology Press 2002.

2. Chang, H. Data protection regulation and cloud computing; Cheung, A.S.Y., Weber, R.H. (ed.) Privacy and Legal Issues in Cloud Computing. UK, Edward Elgar Publishing Limited: USA, Edward Elgar Publishing, Inc. 2015.

3. Greenleaf, G. Asian Data Privacy Laws: Trade and Human Rights Perspectives. New York, Oxford University Press 2014.

4. Kasper, A., Laurits, E. Challenges in Collecting Digital Evidence: A Legal Perspective; Kerikmäe, T., Rull, A. (ed.) The Future of Law and eTechnologies. Tallinn, Springer International Publishing Switzerland 2016.

5. Kong, J., Xiaoxi, F., Chow, K.P. Introduction to cloud computing and security issues; Cheung, A.S.Y., Weber, R.H. (ed.) Privacy and Legal Issues in Cloud Computing. UK, Edward Elgar Publishing Limited: USA, Edward Elgar Publishing, Inc. 2015.

Journal articles:

6. Atkinson, S. J. Proof is Not Binary: The Pace and Complexity of Computer Systems and the Challenges Digital Evidence Poses to the Legal System. Birkbeck Law Review 2014, 2 (2), pp. 245-262.

7. Banisar, D., Davies S. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. The John Marshall Journal of Information Technology & Privacy Law, Journal of Computer & Information Law 1999, 18 (1), pp. 1-108, pp. 3-12.

8. Berman, S. Cross-border Challenges for e-Discovery. Business Law International 2010, 11 (2), pp. 123-132.

9. Boddington, R., Hobbs, H., Graham, M. Validating digital evidence for legal argument. Australian Digital Forensics Conference, Edith Cowan University Research Online 2008.

10. Clarke, R. Data retention as mass surveillance: the need for an evaluative framework. Oxford University Press, International Data Privacy Law 2015, 5 (2), pp. 121-132.

11. Davis, M. C. The political economy and culture of human rights in East Asia. Jindal Journal of International Affairs 2011, 1 (1), pp. 48-72.

12. Diggelmann, O., Cleis, M. N. How the Right to Privacy Became a Human Right. Oxford University Press, Human Rights Law Review 2014, 14 (3), pp. 441-458.

13. Edwards, L., Urquhart L. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? Oxford University Press, International Journal of Law and Information Technology 2016, 24 (3), pp. 279–310.

14. Frantziou, E. Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos.* Oxford University Press, Human Rights Law Review 2014, 14 (4), pp. 761-777.

15. Grosswald Curran, V. United States Discovery and Foreign Blocking Statutes. Louisiana Law Review, A Louisiana Law Review Symposium of the Civil Law 2016, 76 (4), pp. 1141-1149.

16. Kerr, S. O. Search Warrants in an Era of Digital Evidence. Mississippi Law Journal 2005, 75 (4), pp. 84-145.

17. Peguera, M. In the aftermath of Google Spain: how the ’right to be forgotten’ is being shaped in Spain by courts and the Data Protection Authority. Oxford University Press, International Journal of Law and Information Technology 2015, 23, pp. 325–347.

18. Reding,V. The European data protection framework for the twenty-first century. Oxford University Press, International Data Privacy Law, 2012, 2 (3), pp. 110-129.

19. Reding, V. The upcoming data protection reform for the European Union. Oxford University Press, International Data Privacy Law, 2011, 1 (1), pp. 3-5.

20. Robertson H.S.E. V. The Spar Cases in Austria: Shaping the Legal Framework for Digital Evidence Gathering During Competition Dawn Raids. Oxford University Press, Journal of European Competition Law & Practice 2016, 7 (3), pp. 205-211

21. van den Hoven, J., Blaauw, M., Pieters, W., Warnier, M. Privacy and Information Technology. Stanford Encyclopedia of Philosophy 2014.

22. Ward, T. Surveillance, Cameras, Identification and Expert Evidence. Pario Communications Limited, Digital Evidence and Electronic Signature Law Review 2012, 9, pp. 42-50.

23. Weber, M. A. The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal 2003, 18 (1), pp. 425-446.

24. Zalnieriute, M. An international constitutional moment for data privacy in the times of mass--surveillance. Oxford University Press, International Journal of Law and Information Technology 2015, 23, pp. 99-133.

25. Zanfir, G. The right to Data portability in the context of the EU data protection reform. Oxford University Press, International Data Privacy Law 2012, 2 (3), pp. 149-162, pp. 153-155.

EU legal acts and international conventions:

26. Article 29 Data Protection Working Group, Working Paper 158. The European Commission. The document goes on to set out guidelines for EU data controllers when trying to reconcile the demands of the litigation process in a foreign jurisdiction with the data protection obligations of Directive 95/46/EU. Brussels, 11.02.2009.

27. Commission Decision 2000/520/EC. The European Parliament and the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. Brussels, OJ L 215, 25.08.2000.

28. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Council of Europe. The first binding international instrument to protect the individuals from abusive gathering and processing of personal data. Strasbourg, No. 108, 28.01.1981.

29. Convention on Cybercrime. The Council of Europe. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Budapest, No. 185, 23.11.2001.

30. Convention on Cybercrime, Article 14 on scope of procedural provisions.

31. Convention on Cybercrime, Article 15 (1)(2)(3) on conditions and safeguards.

32. Convention on Cybercrime, preamble.

33. Council of the European Union. Regulation 1/2003 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty. Brussels, OJ L 1, 04.01.2003.

34. Directive 95/46/EC. The European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Luxemburg, OJ L 281, 24.11.1995.

35. Directive 95/46/EC, Article 2(d) on definitions.

36. Directive 2002/58/EC. The European Parliament and the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Brussels, OJ L 201, 12.07.2002.

37. Directive (EU) 2016/680. The European Parliament and Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. Brussels, OJ L 119, 04.05.2016.

38. European Union Charter of Fundamental Rights. The protected fundamental rights regarding dignity, freedoms, equality, solidarity, citizens' rights and justice in the European Union. OJ C 326, 26.10.2012

39. Directive (EU) 2016/680, Article 36 on transfers on the basis of an adequacy decision.

40. European Union Charter of Fundamental Rights, Article 7 on respect for private and family life.

41. European Convention on Human Rights. The Council of Europe. The European Convention on Human Rights sets forth a number of fundamental rights and freedoms. Rome, 04.11.1950.

42. European Convention on Human Rights, Art. 8 on right to respect for private and family life.

43. Hague Conference on Private International Law. The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters. Hague, 01.02.1970.

44. Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Article 23.

45. Regulation (EU) 2016/679. The European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Brussels, OJ L 119, 27.04.2016.

46. Regulation (EU) 2016/679, Article 2 (1)(e) on material scope.

47. Regulation (EU) 2016/679, Article 17 on right to erasure ('right to be forgotten').

48. Regulation (EU) 2016/679, Article 33 on notification of a personal data breach to the supervisory authority.

49. Regulation (EU) 2016/679, Article 34 on communication of a personal data breach to the data subject.

50. Regulation (EU) 2016/679, Article 41 on monitoring of approved codes of conduct.

51. Regulation (EU) 2016/679, Article 45 on transfers on the basis of adequacy decision.

52. Regulation (EU) 2016/679, Article 46 on transfers subject to appropriate safeguards.

53. Regulation (EU) 2016/679, Article 49 on derogations for specific situations.

54. Regulation (EU) 2016/679, Article 51 on supervisory authority.

55. Regulation (EU) 2016/679, Article 54 on rules on the establishment of the supervisory authority.

56. Regulation (EU) 2016/679, Chapter III Rights of the data subject.

57. Regulation (EU) 2016/679, Chapter V Transfers of personal data to third countries or international organisations.

58. Regulation (EU) 2016/679, Preamble (28).

59. Regulation (EU) 2016/679, Preamble (78).

60. Regulation (EU, EURATOM) No 883/2013 The European Parliament and of the Council concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council, and Council Regulation (EURATOM) No 1074/1999. Strasbourg, OJ L 248, 11.09.2013.

61. Regulation (EU, EURATOM) No 883/2013, Article 4(2) on internal investigations.

62. Regulation (EURATOM, EC) No 2185/96 of the European Council concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European

Communities' financial interests against fraud and other irregularities. Brussels, OJ L 292, 11.11.1996.

63. Regulation (EURATOM, EC) No 2185/96, Article 7(1).

64. Regulation of Investigatory Powers Act 2000. The Parliament of United Kingdom. The United Kingdom, 28.07.2000.

65. Treaty on the Functioning of the European Union, The European Union. Sets out organisational and functional details of the European Union. Lisbon, OJ C 326, 26.10.2012.

66. Universal Declaration on Human Rights, United Nations General Assembly. The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world. It sets out, for the first time, fundamental human rights to be universally protected. Paris, 10.12.1948

67. Universal Declaration on Human Rights, Art. 12 on arbitrary interference.

National legal acts of the states:

68. Act no. XXXIV of 1994 on the Police. Hungary, 1994.

69. Act no. XXXIV of 1994 on the Police. Section 7/E on Surveillance.

70. Federal Rules of Civil Procedure. The United States 1937, amended in 2016.

71. Federal Rules of Civil Procedure, Rule 1 - Scope and Purpose. The United States 1937, amended in 2016.

72. Federal Rules of Civil Procedure, Rule 26 - Duty to Disclose; General Provision Governing Discovery. The United States 1937, amended in 2016.

73. Federal Rules of Civil Procedure, Rule 26 - Duty to Disclose; General Provision Governing Discovery. Cited in Berman (Berman, S. Cross-border Challenges for e-Discovery. Business Law International 2010, 11 (2), pp. 123-132.)

74. French Law No 80-583 on the communication of economic, industrial, financial, or technical documents or information to foreign individuals or legal entities, 16.07.1980.

Case law:

75. Court of Justice of the European Union, *British American Tobacco and Imperial Tobacco* (C-491/01) 2002.

76. Court of Justice of the European Union, *Germany v Parliament and Council,* (C-376/98), 2000.

77. Court of Justice of the European Union, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (C-131/12), 2014.

78. Court of Justice of the European Union, Joined Cases C-465/00, C-138/01, and C-139/01 *Rechnungshof, 2003.*

79. Court of Justice of the European Union, Joined cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado,* 2011. Cited in the Handbook on European data protection law (The European Union Agency for Fundamental Rights, the Council of Europe. Handbook on European data protection law. Publications Office of the European Union, Luxembourg, printed in Belgium, 2014, p 18.).

80. European Court of Human Rights, *Szabó and Vissy v. Hungary* (37138/14), 2016.

81. European Court of Justice, *Van Gend en Loos v Nederlandse Administratie der Belastingen,* (Case 26/62), 1963.

82. United States District Court Eastern District of New York, *Moses Strauss et al. v. Crédit Lyonnais, S.A*, (1:06-cv-00702), 2007.

83. United States District Court Southern District of New York, *Monique Da Silva Moore, et al. v. Publicis Groupe & MSL Group,* No. 11 Civ.1279 (ALC) (AJP), 2012.

84. United States Supreme Court, *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa,* 482 U.S. 522, 1987.

eMaterials:

85. Association of Chief Police Officers. ACPO Good Practice Guide for Digital Evidence, 2012. www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (17.02.2017)

86. Council of Europe, European Court of Human Rights commentary. www.echr.coe.int/pages/home.aspx?p=basictexts (08.02.2017)

87. Council of Europe, Chart of signatures and ratifications of Treaty No. 185. www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

88. Court of Justice of the European Union, Press Release No 70/14 on case *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (C-131/12),* Curia, Press and Information, 2014. curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (11.02.2017)

89. District Court Upholds Judge Peck's Order Endorsing Computer Assisted Review. New York, KrolLDiscovery Pulse, Case Law 2012. www.ediscovery.com/pulse/case-law/detail/26415/

90. Electronic Privacy Information Centre, Statement sent to the United States Senate, 2004. epic.org/privacy/intl/senateletter-061704.pdf (18.02.2017)

91. European Commission, The European Anti-Fraud Office. Guidelines on Digital Forensic Procedures for OLAF Staff, 2016. ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf (18.02.2017)

92. European Commission. Press Release on the Data Protection Reform, Questions and Answers. European Commission Press Release Database, MEMO/15/6385, 21.12.2015, Brussels. europa.eu/rapid/press-release_MEMO-15-6385_en.htm (29.03.2017)

93. European Commission, Factsheet on the "Right to Be Forgotten" ruling (C-121/13) 2014. ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (03.03.2017)

94. European Commission. Proposal for an ePrivacy Regulation, 19.02.2017. ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (15.04.2017)

95. European Commission. Viviane Reding, 2014. ec.europa.eu/archives/commission_2010-2014/reding/ (12.04.2017)

96. European Court of Human Rights, Press Release on case *Szabó and Vissy v. Hungary* (37138/14), The Registrar of the Court, 2016. www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY-prel.pdf (11.02.2017)

97. European Union Agency for Fundamental Rights, the Council of Europe. Handbook on European data protection law. Publications Office of the European Union, Luxembourg, printed in Belgium, 2014.

98. Gibbs, S. What is 'safe harbour' and why did the EUCJ just declare it invalid?. The Guardian 2015. www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection (29.03.2017)

99. Hampton, W. M. Predictive Coding: It's Here to Stay. E-Discovery bulletin, Thomson Reuters 2014. www.skadden.com/sites/default/files/publications/LIT_JuneJuly14_EDiscoveryBulletin.pdf (30.03.2017)

100. Information Commissioner's Office, Key Definition of the Data Protection Act. co.org.uk/for-organisations/guide-to-data-protection/key-definitions/ (03.03.2017)

101. Joint committee of International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27001, 2005. (Reformed in 2013) www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en (18.02.2017)

102. Joint committee of International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27002, 2005. (Reformed in 2013) www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-1:v1:en (18.02.2017)

103. The joint committee of International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 21037, 2012. www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en (18.02.2017)

104. Organisation of Economic Co-operation and Development, 2013 OECD Privacy Guidelines, 2013. www.oecd.org/internet/ieconomy/privacy-guidelines.htm (15.04.2017)

105. Organisation of Economic Co-operation and Development, The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013. www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (03.03.2017)

106. Organisation of Economic Co-operation and Development, List of OECD Member countries - Ratification of the Convention on the OECD. www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm (03.03.2017)

107. Organisation of Economic Co-operation and Development. The OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy 2007. www.oecd.org/sti/ieconomy/38770483.pdf (14.04.2017)

108. Rose LJ. Attorney General's Reference (No 2 of 2002). Publications & records of the Parliament, UK, 2003. lexisweb.co.uk/cases/2002/october/attorney-generals-reference-no-2-of-2002 (16.04.2017)

109. Ryz, L., Stretton, T. EU Data Protection Gains A Sword To Go With Its Shield. Association of Corporate Counsel, ACC Docket, 2015. www.ediscovery.com/cms/pdf/EU-Data-Protection-Gains-Sword-to-Go-with-Shield.pdf (15.04.2017)

110. Solove, D. J. 10 Reasons Why Privacy Matters, Privacy + Security Blog, 2014. www.teachprivacy.com/10-reasons-privacy-matters/ (08.02.2017)

111. United Nations, Universal Declaration of Human Rights commentary. www.un.org/en/universal-declaration-human-rights/ (10.02.2017)

Other sources:

112. Bowden, C. Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of [the UK] Parliament. Blog Privacy Strategy, 2014. Cited in Clarke (Clarke, R. Data retention as mass surveillance: the need for an evaluative framework. Oxford University Press, International Data Privacy Law 2015, 5 (2), pp. 121-132.)

113. Chiang, A. Foreword for Greenleaf, G. Asian Data Privacy Laws: Trade and Human Rights Perspectives. New York, Oxford University Press 2014.

114. European Commission, Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalized World. Brussels, 10.01.2017.

115. Intelligence and Security Committee. Privacy and security: a modern and transparent legal framework, 2014. Cited in Edwards and Urquhart (Edwards L., Urquhart L. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? Oxford University Press, International Journal of Law and Information Technology, 24, 279–310, 2016.)

116. Mell, P., Grance, T. The NIST Definition of Cloud Computing. Special Publication 800-145, U.S. Department of Commerce, National Institute of Standards and Technology, 2011. nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. (18.04.2017) Cited in Kong. (Kong, J., Xiaoxi, F., Chow, K.P. Introduction to cloud computing and security issues;

Cheung, A.S.Y., Weber, R.H. (ed.) Privacy and Legal Issues in Cloud Computing. UK, Edward Elgar Publishing Limited: USA, Edward Elgar Publishing, Inc. 2015.)

117. The Sedona Conference. The Sedona Conference Practical In-House Approaches for Cross-Border Discovery and Data Protection, 2016.