Doktori (PhD) értekezés

Dr. Simó Ferenc Zoltán

Debrecen
2023

DEBRECENI EGYETEM MARTON GÉZA
ÁLLAM-ÉS JOGTUDOMÁNYI DOKTORI ISKOLA

PRIVACY REGULATORY CONCERNS PRESENTED BY EVOLVING TECHNOLOGIES

Készítette:

Dr. Simó Ferenc Zoltán

Témavezető:

Dr. Fézer Tamás, egyetemi tanár

A doktori program címe: Az állam- és a jog változásai Közép- és Kelet Európában

A doktori iskola vezetője: Dr. Szabadfalvi József, egyetemi tanár

A kézirat lezárva: 2023. július31.

DEBRECEN

2023

NYILATKOZAT

Alulírott, dr. Simó Ferenc Zoltán, büntetőjogi felelősségem tudatában kijelentem, hogy a Debreceni Egyetem Martonn Géza Állam-és Jogtudományi Iskolában a doktori fokozat megszerzése céljából benyújtott, **Privacy Regulatory Concerns prescated by Evolving Technologies** című értekezésem saját önálló munkám, a benne található, másoktól származó gondolatok és adatok eredeti lelőhelyét a hivatkozásokban (lábjegyzetben), az irodalomjegyzékben feltüntettem.

Kijelentem, hogy a benyújtott értekezéssel azonos tartalmú értekezést más egyetemen nem nyújtottam be tudományos fokozat megszerzése céljából.

Tudomásul veszem, hogy amennyiben részben vagy egészben sajátomként mutatom be más szellemi alkotását, vagy az értekezésben hamis, esetleg hamisított adatokat használok, és ezzel a doktori ügyben eljáró testületet vagy személyt megtévesztem vagy tévedésben tartom, a megítélt doktori fokozat visszavonható, a jogerős visszavonó határozatot az egyetem nyilvánosságra hozza.

Debrecen, augusztus 22, 2023.

RECOMMENDATION OF THE SUPERVISOR

We all experience a boom in the development of technology. This dynamic development, however, also results a certain lag in the response of legislation and jurisprudence. As modern technology aims to make life comfortable and safe in some aspect, it also gives birth to new challenges and dangers that force lawmakers and the judiciary to establish safeguards that attempt to minimize the negative effects of the application of such technologies. Data protection issues and privacy concerns are among the top fundamental rights concerns in the application of new surveillance tools (e.g. drones), artificial intelligence, machine learning, internet of things (IoT) and other modern technologies. While the phenomenon has been with us for over two decades now, lawmakers failed to decide on what approach they should follow when designing laws and attitudes for the new technologies. Sporadic, sector specific and neutral legislation can all be experienced depending on the jurisdiction analyzed, however, there has been no perfect approach emerged yet that may serve as a beacon for all countries in the world.

The author's work provides for an attempt to gather the various approaches academics and lawmakers have on the topic, to systemize them and to criticize them, all in the light of proposing a way forward. The author took a somewhat subjective approach when deciding on the jurisdictions dragged into the pool of comparison. The choice can be justified by several considerations: history of regulation, amount of cases courts had a chance to deal with, model laws in place, potential to be pioneers and others. The European Union obviously has a central point in the dissertation, while the U.S., China, Italy, the UK and even Hungary often contributes to the analysis on their unique approaches.

The thesis also subjectively selects from the modern technologies it aims to scrutinize, focusing mostly on the use of drones and the privacy issues the application of these instruments invoke. While privacy concerns in the application of modern technologies can certainly be relevant to several areas of jurisprudence (e.g. criminal law, constitutional law, public administration law, tort law), the author aims to follow a mostly private law oriented approach when giving us a blueprint of his research through the lines of the dissertation. Tort law has a special role in the thesis as the last chapter is dedicated entirely to this important column of the law. As privacy torts reflect the concerns of the society with regard to the application of drones and other modern technologies, this decision of the author can easily be understood. It is not always easy to maneuver in the maze of all the various legal domains when approaching the

problems the use of modern technologies induce for the lawmaker and for the courts, the candidate could deliver a narrative that merges most areas while still maintaining the private law element focusing on the individual person's privacy rather than on some more general approaches.

The author built his work on an impressive array of works and referred to them properly assisting the reader to identify which idea or statement is coming from somebody else's perspective and which one is his own proposal or criticism. I believe the thesis is an interesting contribution to the otherwise lively and active academic discussion on the use of modern technologies in the context of privacy issues.

Debrecen, 17th August 2023

Dr. Tamás Fézer, PhD
professor of law
supervisor

Contents:

Introduction:

The aims and scope of the dissertation:

The primary aim of my dissertation, among the numerous exploring challenges and encounters posed by novel technologies, is to address the question of what it all really means for individual privacy. Extensive changes presented by novel technologies to the way we contact and communicate with each other, with groups, communities and organizations and with the world in general are currently being ushered in, and some of these have fairly noteworthy implications/consequences for and long term effects on personal privacy and the concept(s) in connection with novel technologies and their regulation(s). While it sounds true that cultures keep changing, I propose there are parts of the present culture that we should target to preserve or, at least, maintain a level of control. Personal privacy is one of these significant particles of our culture, including all nations with different preferences while defining privacy. Even if there might be an urge for standardization and harmonization, as key concepts/principles, mostly in the European Union, and around world. The right to privacy is such a basic, universal expectation, or sometimes, a hope that it is seldom as obviously articulated as it is sensed, and rarely more keenly felt than when it is in danger. But how can we protect it in the face of major changes to our ways and means of communication? How can we have the benefits that the technology has to offer without at the same time sacrificing autonomy, anonymity, and our choice(s) over who is allowed to know us and what we are doing, or what my intention are? Privacy in the context of novel technologies is very much about how we define privacy or how a (legal) culture defines it and how we define our expectation of privacy in interactions with others through complex, intricate electronic systems and connections. A conscious effort is vital to safeguard and guarantee that we do not accept gradually and unintentionally a deletion of our rights to privacy. Scholars often feel the need to assess the privacy implications of using new technologies by inquiring: What does novel technology mean for the individual and his or her well-being? Does it diminish or support individual autonomy, choice, sense of security, trust? What information does it generate about individuals and how it is applied and controlled? What controls exist to protect the

reliability of the transaction? In an ideal world, this assessment should take place before the event; if not there is a chance that any intrusions on privacy will slow the pace and extent to which the new service or novel technology will be included or incorporated (or even welcomed) by the very public/audience targeted they are created and designed for. Whatever the case may be, the assessment should not take place only once, but be an ongoing (re)evaluation of the impact on our private lives. The urgent need to protect our privacy, particularly in the light of the reception of new technologies, is one of the reasons why many governments have recently proposed to extend privacy protections to the private sector. Opinion polls demonstrate that the public is progressively concerned about the effect of contemporary novel technology on privacy. Lots of scholars and people interviewed about it say that privacy is a very significant social issue, and the way that commercial organisations handle personal seems one of the sources of discontent information. Moreover, the reasons for the ever-growing concern can be connected to the unstoppable progresses and expansion in information technology. Against this milieu should consider the effects on (personal) privacy of novel (and rapidly changing) technologies and the way they have been applied to the services we receive as parts of our everyday life.

It often seems that overwhelmed by novelty, the law/regulation, as it is often claimed, cannot keep up with novel/innovative technology. The novel forms of digital technologies and their ability to interconnect have only reinforced the legitimacy of re-examining the relation between privacy, regulation and novel technologies.

All through my dissertation, I intend to highlight that one of the possible sources of confusion created by idea that, for instance, regulation can be observed as a lone sort of law or scheme designed with the sole purpose: regulating the regulated. As Jonathan B. Wiener sensibly assumestes that regulation is seen as if it derives in one type and has a solitary effect on technology, though, realisticly, the diversity of the types of technologies can be observed[1]. His comment, seventeen years later, turns out to be as solid as it was

[1]WIENER, Jonathan B.:*The regulation of technology, and the technology of regulation*. Technology in Society, Vol. 26, Iss. 2-3, 2004, 483-500. (Doi: https://doi.org/10.1016/j.techsoc.2004.01.033) See: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1960&context=faculty_scholarship[accessed 17 Aug 2020]Also: BUNCH, Bryan H. – HELLEMANS, Alexander: *The History of Science and Technology: A Browser's Guide to the Great Discoveries, Inventions, and the People Who Made Them from the Dawn of Time to Today*. Houghton Mifflin Harcourt,Boston, 2004.orMCCLELLAN, James E. – DORN, Harold: *Science*

then, and with the unstoppable march of high-tech, it shakes the foundation of legal institutions/concepts and their protection, such as privacy.

The main points of my dissertation circulate around the following questions:

1. Is there a need for modification in the context of personality protection, which may be justified by the diverse nature of individual technologies?

The need for modification in the context of personality protection arises from the rapid advancements and diverse nature of technology in today's world. As new technologies emerge and evolve, they often bring novel challenges and risks to the protection of individuals' personalities and personal information.

2. Taking into account that typically administrative law is the first to respond to new technologies, the question arises as to what legislative attitudes can be inferred for civil courts?

The legislative attitudes primarily characterize the response to new technologies in the field of administrative law. However, this approach can also serve as inspiration for civil courts. The civil courts, dealing with civil law matters, can also recognize the possibilities and impacts of new technologies in their legal system. New technologies such as automated systems, artificial intelligence, or block chain solutions can be advantageous in various areas for the functioning of courts and the efficiency of legal proceedings. Learning from legislative attitudes can help civil courts become acquainted with and understand these new technological developments, and their application can accelerate, simplify, or enhance legal procedures.

3. What regulatory trends of novel technologies have emerged in response to the growing issues of privacy protection?

In response to the increasing personality protection issues, several technological regulatory trends emerged between 2017 0nd 2021.It is essential to note that technological regulatory trends are continuously developing/evolving, and novel challenges and issues/concerns in data privacy and personal protection seem to have emerged. Some measures have been

and Technology in World History. Johns Hopkins University Press, Baltimore, 2006. Available: https://books.google.hu/books?id=YnqLfVRJ3AkC&printsec=frontcover&hl=hu&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [accessed 23 Jul 2020]

taken by governments, organizations, and tech companies to safeguard the rights and safety of users.These trends indicate that data privacy and personal protection are becoming increasingly crucial in the digital world, and efforts are continuously being made to improve user rights and safety alongside technological progresses. However, it seems necessary to keep track of the evolving regulatory and technological developments and "novelties" in this field, as the landscape continues to evolve, alter and adjusted in order to satisfy the needs of all "players" connected.

Conceptual and Theoretical Framework and the subject matter of analysis

The spreading and application of novel technologies is often go together with uncertainties or obscurities as to their long-term non-anticipated or non-welcomed effects, regarding virtually every field of existence, comprising, for example, guidelines/directives regulatory systems/, privacy protection and so on. Novel technologies carry queries (and many issues) on the limits/constrains of the regulation like the fine contour between destructive and affirmative as well as progressive outcomes is frequently problematic to draw, and even to discovery. With the comparative analyses of the regulatory models aimed to regulate novel, evolving, progressive and revolutionary "machineries", such as drones, AIs and biometric systems, I intoned to point out some major loopholes and short-comings that might be avoided by the development of the progressive attitude by the regulators, on one hand, and the cooperative attitude by developers of novel techs on the other. In order to prevent the influx of privacy concerns, I propose that the need to regulate and to adjust regulations again and again should be questioned. Though the method how to achieve it could be and will be different, caused by diverse norms combined with cultural disparity between countries may show alterations in the ratification, comprehension and enforcement, let alone compliance, too.

It seems vital to point out that the difficulties presented by the clash of interest between novel technologies and regulations appears to lead to even more privacy concerns, due to the fact that a great number of the public appear to suffer from the *Flawed LawSyndrome*: the drive to call law or regulation obsolete or faulty (severed) and the urge to solve the nuisances by concentrating on the law, rather than applying other possibilities

to fix the assumed gaps (Legal Solutionism)[2]. Still, I may advise to pay more attention to a revisionist method in order to revitalize and try out newer methods as, for instance, self-regulations.

Legal normative questions through a multidisciplinary approach:

Researching the theoretical and practical correlations of legal normative questions through a multidisciplinary approach offers several advantages:

1. Multifaceted approach: Multidisciplinary research can allows experts from various fields and sectors such as law, economics, sociology, political science, or psychology to collaborate and jointly examine legal issues. This amalgamation of different aspects and viewpoints can lead to a richer and more comprehensive understanding, especially when issues and concerns seem to progress faster than solutions.

2. Deep comprehension: Dialogue and collaboration among researchers with diverse backgrounds may assist to reveal, even expose hidden interaction/associations and causal connections that can otherwise remain elusive. As a result, a greater variety of insights into the societal, economic, and psychological factors underlying legal norms can be achieved as a sort of progressive outcome.

3. Informed decision-making: The multidisciplinary approach allows researchers and decision-makers to achieve and enhanced grasp on the consequences and impacts of legal norms on society and various stakeholders. This appears to contribute to making more informed decisions and more effective legislative processes.

4. Novel solutions and innovations: The combination of knowledge and methodologies from different disciplines can yield novel solutions and innovations for addressing legal issues. These innovative approaches/methods can improve; even boost the efficiency and fairness of the legal system.

5. Understanding societal challenges: Legal normative questions often intertwine/overlap with societal challenges such as environmental protection,

[2]LEENES, Ronald: *Regulating New Technologies in Times of Change*. In: REINS, Leonie (Ed.): *Regulating New Technologies in Uncertain Times*. Springer, The Hague, 2019, 5-6.(Doi: https://doi.org/10.1007/978-94-6265-279-8_1)

privacy protection, human rights, or technological advancements/regulation. Multidisciplinary research can assist to comprehend these challenges/issues and identify legal solutions that best fit the social and environmental contexts and so on.

6. Enhanced communication: Improved communication among researchers with varied and different backgrounds can facilitate better understanding of legal norms and related issues for a wider audience. Consequently, communication between the legal system and the affected individuals can also improve.

In conclusion, a multidisciplinary approach to researching legal normative questions fosters collaboration and knowledge sharing across various disciplines, leading to a more profound understanding and more effective solutions for the legal system.

Comparison of European Union Legislation and Anglo-Saxon Legislation in the Light of Technology Regulation:

European Union (EU) legislation and Anglo-Saxon legislation represent different legal systems, with distinct approaches to technology regulation.

1. Sources of Law and Legislation: In the European Union, legislation primarily originates from secondary legal sources, such as regulations and directives, as well as from national laws of member states. EU institutions, such as the European Parliament and the European Commission, collectively create laws that apply to EU member states.In the Anglo-Saxon legal system, the fundamental source of law is precedent (case law), which is based on previous court decisions. The United Kingdom, for example, includes the English common law, where court decisions play a significant role, and there is no constitutional court.

2. Technology Regulation: In recent years, the EU has increasingly focused on technology regulation, especially concerning data protection and digital taxation. A prominent example of this is the General Data Protection Regulation (GDPR), which establishes uniform data protection rules across the European Union.The Anglo-Saxon legal system traditionally adopts a more flexible approach to technology regulation, for the most part owing to its precedent-based nature. In the United Kingdom, rules regarding data protection are determined at the national level, though there is no doubt about the fact that GDPR has also greatly influenced the implementation/execution of stricter regulations.

3. Social and Cultural Factors: The EU comprises a wide range of diverse (seemingly vastly different) cultural and legal backgrounds, resulting in a diversity of legislative approaches. It can be stated that one of the main goals of the European Union is to harmonize (or at least, to attempt to harmonize) the various legal systems among member states, which might pose a considerable amount of challenges and necessitate adaptation in technology regulation.The Anglo-Saxon legal system relies on the principle of precedent, allowing courts to actively shape and develop the law while adapting to new technological challenges. Thus, it looks that the English legal system encourages/supports innovation and a willingness to evolve the law for the sake of going forward.

To conclude, one can say that the differences between EU and Anglo-Saxon legal systems in technology regulation come from the sources of legislation and the cultural and legal contexts. Both systems have their advantages and disadvantages, and both strive to adapt to the rapidly changing technological landscape. Technological advancements/progresses continue to present challenge/issues/concerns to the regulatory authorities of both legal systems.

Comparative overview of the technology regulatory models (in the European Union (EU), the United States (USA), and the United Kingdom (UK))

1. The technology regulatory model in the European Union (EU): The EU is well-known for its strict data protection regulations, which were established by introducing the General Data Protection Regulation (GDPR) in May 2018. This (relatively) new regulation implemented unified data protection rules within the EU, guaranteeing fundamental rights for citizens regarding data/privacy protection. In addition, the EU has developed regulatory directives that govern electronic communications and consider the rapid advancement/progress of technology.

2. The technology regulatory model in the United States (USA): In the USA, technology regulation can differ significantly within different states. Data protection and regulation of technology services are more fragmented, lacking a single comprehensive data protection law like the EU's GDPR, although recently a measurable interest has been directed to GDPR from the USA, supposedly because of its relatively successful existence.. However, there are federal laws, such as the Consumer Privacy Act, that provide some level of protection concerning data collection and consumer data handling.

3. The technology regulatory model in the United Kingdom (UK): In 2020, the United Kingdom left the European Union (Brexit), and as a result, the data protection provisions outlined in the GDPR no longer automatically can be applied to the country. Nonetheless, the UK has established its own data protection laws, such as the Data Protection Act of 2018, which offer data privacy protection similar to the GDPR.

During the comparison, it is important to note that technology regulation and data protection laws in all three regions are subject to continuous changes, and further developments may occur over time. Given the rapid advancement of technology and increasing demands for data privacy, it is expected that there will be additional modifications and enhancements to the regulatory models in the future.

"Consumer privacy issues are a "red herring": You already have zero privacy - get over it" Scott McNealy[3]

Chapter 1 Privacy and technology in an international context: highlights and definitions[4]

Privacy is valued, mostly in cultures where individualism is crucial because personsneed to have power overthe access to their body and to information about their ownalternatives, and, of course, privacy can support a vast variety of productss. In addition, it is able to protect intimacy among friends/relatives and coworkers and build trusting relations of tolerance among acquaintances, and uphold dignity, since it can be uncomfortable to unveil secret or hasty thoughts or opinions, or to expose one's naked body or other private spaces. Privacy can contribute to our individuality, self-worth, and autonomy as well; and can protect us from several emotional or psychological harms connected to unwanted publicity. However, one should not fail to remember that privacy can also upholdnoteworthy political and legal "merchandises", as well as property rights,

[3] CEO of Sun Microsystems,Scott McNealy, told a group of reporters and analysts Monday night at an event to launch his company's new Jini technology. (January 1999) It seems crucial to remember that Sun Microsystems is a member of the Online Privacy Alliance, an industry coalition that seeks to head off government regulation of online consumer privacy in favor of an industry self-regulation approach.
Available: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ [accessed 30 Sep 2020]

[4]This chapter of my dissertation is based on: SIMÓ, Ferenc Zoltán. *Privacy in Context: Info-tech based society and the revolutionary effects ofdrones/phones/biometrics*JURA 25: 2 pp. 458-469. , 12 p. (2019)

fraud prevention, and non-discrimination. However, one should not forget to remember the darker side, too, since privacy can be disvalued as well. Privacy is therefore, as A. E. Cudd and M. C. Navin states too, not an absolute good. Instead, if we propose to unveil the circumstances in which privacy is satisfactorily valuable to justify the protection of privacy rights, one shouldinitiate philosophical and legal exploration into the realms of privacy, the content of privacy, and the goods and harms that privacy protection could cause. Székely Iván argues that „behind the anomalies currently besetting the notion of privacy – anomalies that arise from different cultural, political and social milieus both at the group and at the individual level – there lies a common conceptual element: individuals and small communities carry an increasing weight vis-`a-vis the external world"[5]. In addition, he presumes that the notion of freedom of information exposescomparableinconsistencies even if one examines it from diversestandpoints, such as, geographical, cultural or political, or studies it in the context of history[6]. The virtual/technological period has brought novel issues and threats related to privacy (and its protection), as innovative technologies bring about newspecies and extents of the intrusion/invasion of privacy. The innovations associatedwith PCs and smart technologies have picked up the pace of statistical studies, while the Internet and the IoT have extremely rushed communication, sharing and compilation of information[7].

While the idea of 'privacy' is often respected and honoured,[8] one may accept the fact that "modern" obsessions and considerations with privacy are fundamentally rooted in the twentieth century, predominantly the years following the Second World War, which

[5]SZÉKELY Iván:*Freedom of Information versus Privacy: Friends or Foes?* In: GUTWIRTH, Serge – POULLET, Yves – DE HERT, Paul – DE TERWANGNE, Cécile – NOUWT, Sjaak (Eds.): *Reinventing Data Protection?* Springer, Dordrecht, London, 2009, 293.

[6] As it can be seen in:SZÉKELY Iván: *Central and Eastern Europe: Starting from Scratch*. In: FLORINI, Ann (Ed.): *The Right to Know: Transparency for an Open World*. Columbia University Press, New York, 2007.

[7]CUDD, Ann E. – NAVIN, Mark C. (Ed.): *Core Concepts and Contemporary Issues in Privacy*. Springer International Publishing, (AMINTAPHIL: The Philosophical Foundations of Law and Justice 8), 2018. https://doi.org/10.1007/978-3-319-74639-5_1 [accessed 9 Jan 2019]

[8] The word itself has a long history, authorities cited for the word 'Privacy' in the *Oxford English Dictionary Online*(Oxford University Press, Oxford, 1989–2005) dates back to the early seventeenth century and before. Also, Gale Encyclopaedia of American Law defines it as follows: "In constitutional law, privacy is the right of people to make personal decisions regarding intimate matters; under the common law, it is the right of people to lead their lives in a manner that is reasonably secluded from public scrutiny, whether such scrutiny comes from a neighbor's prying eyes, an investigator's eavesdropping ears, or a news photographer's intrusive camera; and in statutory law, it is the right of people to be free from unwarranted drug testing and electronic surveillance".BATTEN, Donna (Ed.): *Gale Encyclopaedia of American Law*. Gale Cengage Learning, New York, 2010, 176.

might not be a shocking surprise due to the terror of the WW2. Though the clear-cut reasons may be different and change over time, one may not fail to see the connections between the terrifying events of the War and the rise of the rise of the modern understanding of privacy. As any European civilian lawyer will confirm, the European Convention on Human Rights,[9] with its important provision for security of private life alongside its protection of freedom of expression,[10] was a direct response to the numerous and wide-ranging intrusions on personal integrity that happened during the war years. Though the War years are over, at least in Europe, but not forgotten, and in Europe it still represents as a kind of fortification against organized authority, and expressively not only one limited to the authority of the state.[11] Austin Sarat argues that we live in an age of new modalities of social interaction as well as new reproductive technologies and the revolution of biotechnology. Each of these things appears to foreshadow a world without privacy, or, at least, a world in which the meaning of privacy is radically transformedboth as a legal idea and as a lived reality.[12] Before going into the abyss of the multifaceted and complicated task of defining privacy, one must understand why the topic is significant or crucial and why privacy law is one of the most exciting developing fields of legal study. Thus, my intention is far from clarifying and entangling its complexity, my attempt is to shed a light on the burdensome "channels of communication" among the triad of privacy, (novel) technology and regulation. While legally defining privacy and certain rights relating to personalityin connection with the applied terms of personality, László Sólyom emphasises the fact even if one analyses terms such as autonomy, dignity and so on, one must not forget that it is only worth examining them in a socio-historical context, which defines and foreshadows the ever-changing nature of the term[13]. He goes on to observe that any analysis of the formerly mentioned topic should be based on and related to in the particular era in which one intends to analyse it. Others, like Iván Székely focuses on the complexity of the term, and he argues that there are different manifestations of privacy, thus it could be seen as a social trend, or as a worth, or as a right, in print or unrecorded, or

[9] Opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 June 1952).

[10]Ibid. Article 8 and Article 10 respectively.

[11]KENYON, Andrew T. – RICHARDSON, Megan (Eds.): *New dimensions in privacy law: international and comparative perspective*. Cambridge University Press, New York, 2006.

[12]AUSTIN, Sarat: *Whither privacy: an introduction*. In: *A world without privacy: what law can and should do?* Cambridge University Press, New York, 2015.

[13]SÓLYOM László: *A személyiségi jogok elmélete.*Közgazdasági ég Jogi Kiadó, Budapest, 1983, 14.

as a opinionated aim, or even as a profitableproduct or service.[14] One of the bravest moves done by Szabó Máté Dániel can nicely demonstrate how complex it is to define privacy as a term. To emphasise this fact, he calls his study only an "attempt". He calls our attention to the fact that even the effort to translate the word *privacy with its full spectrum of meaning and content* is doomed to failure or it narrows down the concept unnecessarily. But he assumes that *privacy* should be defined even if it clearly poses difficulties and it can be dangerous as well[15]. According to John T Soma, we should turn to Professor Roger Clarke, a pioneer in the field of privacy and IT, who describes individual privacy as consisting of four dimensions: the psychological, the sociological, the economic, and the political. Psychologically, people require private space to preserve a sense of individual identity. Sociologically, people need the opportunity to connect and interact with others, but without the continual threat of being watched. These two dimensions of privacy have long been recognized (and more or less honoured). Without a doubt, as the Eighteenth Century British philosopher Jeremy Bentham wrote in describing his vision of the ultimate prison (the "Panopticon"), "the most important point [is] that the persons to be inspected should always feel themselves as if under inspection …."[16] More recently, the economic and political dimensions have come to be recognized as critically important as well.[17] Privacy has been described in a U.S. Supreme Court decision as a right more fundamental than any of the rights enumerated in the Bill of Rights. The Constitution of the United States is a living and evolving document, although its (r)evolution might be seen difficult in the light of its rigid nature. Though written at the birth of the country in a pre-Industrial 18th century, these founding documents were designed to adjust to times of yet unknown technology such as phono/photographs and telegraphs/phones, audio-visual recordings and transmission, and, surprisingly, the digital era and the Internet. It is well known and discussed that the Declaration of Independence and the Constitution state and guarantee certain inalienable rights, including the right to liberty and the pursuit of happiness. The conclusion might be that if

[14]SZÉKELY Iván [2009] op. cit., 293-294.

[15]SZABÓ Máté Dávid: *Kisérlet a privacy fogalmának meghatározására*. Információs társadalom, Vol. 5, No. 2, 2005, 44-54. Availablehttp://epa.niif.hu/01900/01963/00013/pdf/infotars_2005_05_02_044-054.pdf [accessed 30 Sep 2020]

[16]BENTHAM Jeremy: *Panopticon or the Inspection House*. Letter V (1787), available athttps://cryptome.org/cartome/panopticon2.htm [accessed 19 Apr 2019]

[17]SOMA, John. T.–RYNERSON, Stephen D. – KITAEV, Erica: *Privacy Law in a nutshell*. West Academic Publishing, West, 2014, 1-3.

statutes, laws and regulations, not directly and explicitly protect such rights these rights mustbe included by a certain reality of common law. The common law embodies the heredity for a right to privacy, a right to be free from persecution and/ör exposure. Nevertheless, there might be some questions arisen. Some go as far as to criticize that the recognition of any right not explicitly declared in the formerly mentioned founding documents, judgmentally calling it 'judicial legislation', thereby upsetting the balance of powers by captivating/assuming the legislature's role, Warren and Brandeis claim that "the elasticity of our law, its adaptability to new conditions, the capacity for growth, which has enabled to meet the wants of an ever changing society and to apply immediate relief for every recognized wrong, have been its greatest boast.[18]" Moreover, it seemsessential to note that any right to privacy was also subject to the explicit right of Free Speech set forth in the First Amendment of the Bill of Rights. As it can be seen, Warren and Brandeis were responding to technological developments, particularly, the arrival of instant photography and audio recordings in the late nineteenth century. The novel technologies had launched a tabloid industry that profited on the most prurient interests without caring to modern morals. The harms of privacy invasion are assumed to be categorized as one of four types: first, intrusion into one's private life and affairs; second, public exposé of discomfortingpersonal6confidentialdetails/information; third, unwanted publicity of private individuals; and, the last, misappropriation of a name or likeness for financial advantage.The article sets forth the basis for reading into the common law as yet identified rights. First identifying the harm, a right of privacy is predicated on mental anguish and feelings, that in and of themselves, were an actionable right to protect.While slander and libel would stop false representations, they bore no way to stop an invasion of private facts. Copyright law that could protect individual letters had become inadequate/obsolete with the rapidly evolving technology that could disgorge one's privacy without stealing or copying any tangible items. Rights in property, and even to the exclusive right to control publication of one's labour, could not express the privacy rights in their entirety, as no property is physically divested. Contract law would not go far enough. A judicial declaration of public morality, private justice, and general convenience would not support a finding for breach of confidence in an implied contract if there were no prior relation between the parties. Criminal law could not be used to enforce privacy rights absent specific legislation that would allow the State to intervene in a "private" civil matter. Still, there must be some sort of privacy right, a right to one's own personality, or peace of mind, or even the right to be let alone.

[18]WARREN, Samuel D.–BRANDEIS, Louis D.: *The Right to Privacy*. Harvard Law Review, Vol. 4, No. 5, 1890. Available: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf[accessed 19 Apr 2019]

Therefore, Warren and Brandeis set forth the injuries, potential remedies, and basis for a true right to privacy.This rule would protect one from publication of one's private matters with few exceptions: first, privileged communications are the domain of libel/slander; second, speaking gossip and oral communication are outside the purview of privacy rights; third, consent to publication is an outright defence; and, lastly, whiletruth andmalice are irrelevant to a breach of privacy action.As time went on, actions to enforce rights of privacy against individuals were repelled by the rights to free speech and freedom of the Press. Since today's tabloid industry attests, public personas, celebs and even those thrust into the public debate without their consent or action, must now grapple with a paparazzi bent on exposing their most minute and private facts.With regard to the right of privacy from the government however, the Supreme Court has recognized Constitutional protections. For instance, in Griswold v. Connecticut, 381 U.S. 479 (1965), the Court envisioned the right to privacy as emanating from the "penumbras" of the Bill of Rights. More recently, the Court, in Lawrence v. Texas, 539 U.S. 558 (2003), unwanted the penumbral theory, viewingas an alternative to the substantial due process rights guaranteed by the Fourteenth Amendment as a Constitutional basis of the right to privacy. However, privacy attracted scant explicit legal attention until 1890, when Warren and Brandeis supported explicit lawfulacknowledgment of privacy as a right. The fourth amendment to the U.S. Constitution guarantees the right to be secure it one's person, houses, papers, and effects against unreasonable search or seizure. The first amendment affords people free exercise of religion and freedom of speech, the press, and assembly - freedoms we associate with freedom of conscience. In *Stanley v. Georgia,*[19]this amendment was cited as limiting the government's competence to control the contents of thoughts. The Fifth Amendment ensures that people cannot be required to testify against themselves, and the fourteenth amendment provides that they cannot be deprived of life, liberty, or property without due process of law. In addition, one needs to see that two other areas of law have also evolved in a way that is protective of privacy. In tort law, there are four categories of individual protection: first, intrusion upon a person's privacy, seclusion, or personal matters; second,openexposé of personal, discomfortingdetails/information; third, public disclosure of a person in a false light; fourth, appropriation of another's name, image, or other aspect of identity, for one's advantage or profit, without that person's consent. However, the second area is the most controversial. It is because the controversial treatment of privacy in

[19]Stanley v. Georgia, 394 United States (1969), it recognizes a right to possess privately pornographic materials in one's home despite legitimate prohibitions on sale or purchase of these materials.

the law arises in the recent Supreme Court decisions that recognize "procreative rights"[20][21] As we can see the complexity of the term privacy has long been recognized by scholars, one of them is the Constitutional scholar William Beaney, he observes in an article shortly after the U.S. Supreme Court's landmark privacy judgment in *Griswold v. Connecticut*, "even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right.[22]" Undeniably, there is no doubt about the "fact" that the only certainty in defining privacy is that it is a concept that is extremely flexible, and its definition is elusive. Although, Soma John. T, Stephen D.Rynerson and Erica Kitaev agree that the notion of privacy depends on the experience, interests, and agenda of the person interpreting it and the socio-political context the definition is offered in. For most individuals, though, privacy's definition does not rely on some philosophical foundation, but rather is a simple, even instinctive/spontaneous idea.[23] Ironically, Inness Julia C states that "exploring the concept of privacy is similar to an exploration of an unknown/uncharted swamp. We start on firm ground, noting the common usage of "privacy" in everyday conversation and legal argument; it seems it will be a uncomplicated/effortless task to locate the conceptual and moral core of such an frequently-used term. But then the ground softens as we discover the confusion underlying our privacy intuitions.[24]" Also she goes on to observe that even if one turns to the legal and philosophical literature on privacy hoping that one can get a grip on the idea of privacy. Instead of finding it, nothing but chaos can be found; since the literature lacks an accepted account of privacy's definition and value, but she also ask whether we need a unified explanation of privacy at all or not. In addition, the Supreme Court of the United States delivered an opinion authored by Justice Byron White. After an extensive discussion of jurisdiction, White concluded that the Court was authorized to consider the virtues of the

[20]SCHOEMAN, Ferdinand David: *Privacy and social freedom*. Cambridge University Press, Cambridge, 1992, 12-13. (Doi: https://doi.org/10.1017/CBO9780511527401)

[21]Those "proactive"rights recognized (by Schoeman F. D.) are the following (non definitive)list: to choose a marriage partner (Loving v. Virginia), to use birth control (Griszvold v. Connecticut, Eisenstadt v, Baird, Carey v.Population Services International), to become a parent (Skinne v. Oklahoma), to have access to abortion services (Roe v.Wade), and, at least in the setting of a marriage, the right to engage in unregulated sexual practices (Bowers v, Hardwick).

[22]BEANEY, William M.: *The Right to Privacy and American Law.* Law and Contemporary Problems, Vol. 31, No. 2, Privacy, 1966 Spring, 253, 255. Available: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3107&context=lcp [accessed 16 Jan 2021]

[23]SOMA – RYNERSON – KITAEV:op. cit., 1-3.

[24]INNESS, Julia C.: *Privacy, Intimacy and Isolation*. Qxford University Press, Oxford, 1992, 3-4.

case and reversed the judgment of the Georgia Supreme Court. The Court recognized that there is a zone ofprivacy surrounding every individual that the state may protect from invasion by an abusive press. It also recognized that the twentieth century had seen "a strong tide running in favour of the so-called right of privacy." The Court noted, however, that this case did not involve the appropriation of a name or a photograph, a physical intrusion into a private area, or a publication of false, defamatory, or otherwise private information.[25] My short overview has already indicated that there are a number of fundamental problems associated with the concept or idea of privacy, moreover, irrespective of the conclusion drawn on the basis of the formerly mentioned ideas; the debate about the impact of technology on privacy protection in the world on is set to continue. Unlike several European countries that have one law covering all sorts of personal information and a national commissioner or an authority to enforce it, there is diversity and inconsistency in the kinds of information and locations that are covered by privacy laws in the USA. Moreover, the USA does not have an official who supervises a national privacy policy. Even Hedricks assumes that if there were such an official, it would be able to, at least, assist individuals solve complaints about record keeping and report to Congress what new legislation was necessary to preserve privacy rights in the face of rapidly advancing computer technology[26].The concept of a person's right to be free from irrational governmental intrusion is fundamental to all human rights. Opinion polls constantly have revealed that Americans support stronger privacy laws and are mistrustful that large organizations use personal data for secondary purposes without their knowledge or consent. A lot of people view privacy laws as the individual's major defence against undue encroachment by large institutions a sort of legal shield or weapon for fending off the computer-equipped giants dominating society. In America, theoretically, the *Privacy Act of 1974*,[27] enacted as part of the Watergate-era reforms, regulates practically all government conducts of personal data. Practically, most scholars (and laymen) as well, such as Even Hendricks, Trudy Hayden, Jack D. Novik argue *the Privacy Act* is a feeble and unsuccessfully, even disappointingly enforced statute. As a result, there are only

[25]STAPLES, William G: *Encyclopedia of privacy*.Greenwood Press, London, 2007, 159.

[26]HENDRICKS, Even – HAYDEN, Trudy –NOVIK, Jack D.: *Your right to privacy: a basic guide to legal rights in an information society*. Southern Illinois University Press, Carbondale, Edwardsville, 1990.

[27] 5 U.S.C. 552a : https://www.law.cornell.edu/uscode/text/5/552a [accessed 15 Feb 2018]

minimal restrictions on federal agencies' compilation, utilization, and exposé of privatel data/information.

However, I need to emphasise the fact that I do not attempt to presentancomprehensiveinventory of philosophical definitions of privacy; rather, I try to apply some of the common philosophical posi tions to demonstrate the fluidity and complexity of this concept. By declining to support any of the particular definitions, I endeavour to provide an objective and comprehensive account of what exactly "privacy" is to certain individuals in an international arena. But if one needs to consider other ideas, I might add that American lawyers would almost definitely refer to the paradigmatic work of Warren and Brandeis,[28] which preceded the twentieth century by only a couple of years, and its later revision by Prosser.[29]However, such lawyers may include that historical factors, such as the human/civil rights movement of the 1960s and 1970s actually provided the so-called modern conception of rights as basic to a democratic policy or by implication, democracy, in the United States. In addition, the above-mentioned American lawyers would not hesitate to call our attention to the fact that the influence of these movements, such as the black movement and other ethnic movements, has not died or become extinct with the passing of time. On the contrary, it still has and will have an overarching influence on shaping the concept of privacy. In addition to these essentials English lawyers seem to observe that privacy has been part of the foundation of English law ever since at least the case of *Entick* v. *Carrington*[30] but sometimes find it complicated to clarify emerging concerns about privacy with the exception of as a European phenomenon swept to England under the impetus of the European Convention. Such analyses, however, appear to underestimate the technological/scientific and commercial progresses that seem to have shown the way to novel pressures for privacy protection.[31]Kenyon Andrew T. and Megan Richardson argue that "while the European influence is real and of undoubted significance, there is also a certain prosaic utilitarianism to contemporary English legal discussions

[28]WARREN – BRANDEIS:op. cit.,193. Indeed not only American lawyers commonly cite this, as authority for 'privacy' as 'The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right'.

[29]POSSER, William L: '*Privacy*'. California Law Review, Vol. 48, No. 3, 1960, 383. (Doi: https://doi.org/10.2307/3478805)

[30] Entick v. Carrington(1765) 19 St Tr 1029

[31]KENYON – RICHARDSON: op. cit.

about privacy, which suggests a distinction from the dignitarian rights-based approaches of continental Europe. If England can be seen as the first home of utilitarianism, it can also be acknowledged that while utilitarians might use the language of rights their ultimate concerns are with social welfare: the 'greatest happiness for the greatest number', as put by Jeremy Bentham and John Stuart Mill."[3233]

Most European countries have been founding rights on notions of personal integrity and dignity[34]. Scholars agree that constitutional privacy is commonly understood to mean the right of persons to be free from unwanted and unwarranted governmental intrusions. These rights or "autonomy interests" have been found to include reproductive freedom; family relationships; sexuality; personal autonomy; decisions about dying and death; and informational privacy, though this list may vary and I assume that it is doomed to be revisited time after time. Constitutional privacy also embraces the right of the individual not to have certain private data gathered, preserved, or disseminated by the government or by implication, any other authorities. Constitutional law and other acts as well and consequently restrict intrusions into certain areas or communications. The Hungarian Constitution or as it is commonly known, the Fundamental Law of Hungary affirms the commitment of Hungary and assures the protection of the rights of persons in the *National Avowal*section by stating that "human existence is based on human dignity and [....] that individual freedom can only be complete in cooperation with others. Also, there can be found in the Hungarian Civil Code Act V of 2013, *part three: rights relating to personality (Title XI)*. Under the title, *General Provisions and certain rights relating to personality,* one can find the necessary protection of rights relating to personality.*Section 2:42* (1) assures us that everyone is entitled to freely practice his or her personality rights within the framework of the law and within and with respect to the rights of others, and to not be impeded in exercising such right by others. It also states, as it is similarly can be seen in the Fundamental Law of Hungary that (2) Human dignity and the related personality rights

[32]Kenyon and Richardson also keenly observe that though Mill at least endeavored to recognize rights as entailing 'vastly more important,and therefore more absolute and imperative' social utilitites: 'Utilitarianism' in MILL, John Stuart (Ed.): *Utilitarianism, On Liberty, Essay on Bentham: together with selected writings of Jeremy Bentham and John Austin*. Collins, London, 1962, 321.

[33]KENYON – RICHARDSON: op. cit., 2-3.

[34]Article 6(3) TEU states that "fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the *constitutional traditions common totheMember States*, shall constitute *general principles of the Union's law*" (my emphasis).

must be respected by all. Personality rights are protected under this Act. Also, (3) Personality rights shall not be considered to be violated by any conduct if the person affected has given prior consent thereto. And, in addition, in *Section 2:43* specifies personality rights and observes that those on the subsequent list, particularly, shall be construed as violation of personality rights: any violation of life, bodily integrity or health; any violation of personal liberty or privacy, including trespassing;discrimination; any breach of integrity, defamation; any violation of the right to privacy protection and personal data;any violation of the right to a name; any breach of the right to facial likeness and recorded voice.[35] One of the most discussed/debated rights in the urgent need of protection is personal data protection; therefore, it gives ways to generate more and more debates. Decades before the boom of the Internet of the 1990s, most of the European countries were focusing on protection of personal privacy by limiting data access. The German state of Hesse, for instance, passed the first law granting individuals control of their personal information in 1970.[36] Indeed, the term "data protection" entered the European lexicon from the German word "Datenschutz." Three years later, Sweden could be admitted as the leading figure to protect and safeguard privacy legally.[37] While much of the fundamental public concern that motivated these early efforts assumed to have grown from (legit) historical concerns about the potential abuses of compilations of personal/private information, technological developments were the immediate stimulus, as both statutes were enacted in response to proposals to combine separate government archives into computerized databases. According to Székely Iván, Hungary was among the first to build a legal and institutional system and the associated practice of treating transparency and free admission to unrestricted data not as a separate entity but as an organic novel element of the new and comprehensive info rights system. The Hungarian model, as the early models in many other countries, depict a dichotomy between state and non-state information, signalling that the prime objective of the new system was to shatter the state's monopoly on information. The model identifies two fundamental info/data categories: privateinformation and public interest related data. There is one fundamental rule for each category: the right of autonomy in the former along with openness in the

[35] Act of V on the Civil Code/Polgári törvénykönyvről. 2013.évi. V. törvény. 2:43. §

[36] Hessisches Datenschutzgesetz [HDSG] [Data Protection Act of the German Federal State of Hessen], Sept. 30 1970, v 7.10.1970 GVB1, Hesse I § 625 (Ger.).

[37] Datalag (1973:289) [Data Act] (Swed.).

latter[38]. The concerns are deeply rooted, especially if we take a look at its connection, or rather relationship, with the development of technology over the last fifty year. Legal concerns has gone as far as it seemed reasonable or necessary, as, in Hungary a bill relating tothe amendment of the Hungarian Data Protection Act was submitted to the Hungarian Parliament on June 19 in 2018. The bill aims at the implementation of Directive 2016/680 and the amendment of the Hungarian Data Protection Act regarding the application of the General Data Protection Regulation (GDPR).Directive (EU) 2016/680 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, and repealing Council Framework Decision 2008/977/JHA.[39]The *Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information* was promulgated on the 26th of July 2011and also provides protection and in order to ensure the right of informational self-determination and the freedom of information, and to facilitate the implementation of the Fundamental Law, pursuant to Article VI of the Fundamental Law, and adopts the Act on the fundamental rules applicable in connection with the protection of personal data and the enforcement of the right to access and disseminate data of public interest and data public on grounds of public interest, and on the authority empowered to monitor compliance with its rules. The Hungarian Parliament has recently adopted legislation with the aim of harmonising the national data protection rules with the rules of the GDPR, and supplementing the national rules in areas not regulated by the GDPR. The Parliament implemented Act XXXVIII of 2018 ("*Amendment*") in an extraordinary session and the new regulations entered into force on 26 July 2018. As a kind of background, the entry into force of the GDPR created a "patchwork" regulation in which besides the GDPR, the national data protection act - *Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information* ("*Act*") - and several laws regarding sectors stayed in force in unaltered form. This appears to have led to (embedded) contradictions in the regulations and general legal

[38]SZÉKELY Iván [2007] op. cit.

[39]https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN [accessed 9 Jan 2019]

uncertainty surrounding the subject.[40] Though the new legislation is not a comprehensive review of all data protection-related regulations, it aims to clarify some important issues regarding the correspondinguse of the Act and GDPR. The Amendment represents a majormove to harmonize the national enactment with the GDPR, but it leaves some loopholes (for instance, harmonization concerning the sectoral regulation of data protection). These will presumably be subject to broader data protection reform that is expected in the autumn session of Parliament. In this transition period, the assistance of qualified legal advisors to achieve compliance[41] with the GDPR and the multiple national data protection laws is of even higher importance. The query is that how grim those concerns I havestated are, to answer theissue, Péterfalvi Attila nand his co-editors cannot provide a suitable one, and these scholars appear to trust in the passing of time.[42] Others, such as Klein Tamás and Tóth András concentrate on two characteristics of innovations, "disruptive" and "unknown" innovations, but these scholarschiefly focus on legal issues related to technological innovations and connected concerns,for instance,protection of data,cyber law, robots, and unmanned aircrafts.[43] It looksnoticeable that the progression of political integration in EU has moved onsignificantly since the period of the initialefforts at enacting privacy and data protection.The main bodies of the European Unionapplyconsiderably more pressureand power over patterns of economic directives in the European Union. One canacknowledge as well that each member state of the EU advocate separate laws connected to issues and concerns related to privacy issues, the extent of the theprotection of privacy has been drivenchiefly by the EU for the past decade. The the privacy system of the EU will be re-evaluated as a "national" policy, in spite of its several member states. The basis of the protection of privacy in the EU comes from

[40]https://www.schoenherr.eu/publications/publication-detail/amendments-to-the-hungarian-data-protection-act/ [accessed 9 Jan 2019]

[41]See, for instance: Framework for Demonstrable GDPR Compliance: A mapping of the Nymity's Privacy Management Accountability Framework. Available:https://info.nymity.com/hubfs/Landing%20Pages/GDPR%20Toolkit/Accountability_Roadmap_for_Demonstrable_GDPR_Compliance.pdf [accessed 10 Sep 2020]

to GDPR Compliance Obligations

[42]PÉTERFALVI Attila–RÉVÉSZBalázs –BÚZÁS Péter (Eds.): *Magyarázat a GDPR-ról*. Wolters Kluwer, Budapest, 2018.

[43]KLEINTamás –TÓTH András. (Eds.): *Technológiai jog-Robotjog-Cyberjog*. Wolters Kluwer, Budapest, 2018.

Directive 95/46 (Data Protection Directive)[44]. This was a product of the state-rundesign/methodsof regulations backed by the OECD Guidelines[45], which had created a random collection of diverse system of privacy protectionall the way through Europe. The Data Protection Directive was intenaim of the directive to protect data, was to synchronizethe legistlation of data protection in Member States, thuslessen difficulties to economic motion within the EU when maintaining or even improving, where it is necessary, the rights to privacy.

1.1 Data protection versus privacy:

As soon as one intends to study the changing and challenging theatre of war of (novel) technologies and privacy, including the (urgent) issues of regulation, one needs to deal with and define data protection and privacy. In most cases, it seems that they are the same but many ongoing debates suggest that these two, though sometimes confused as one, they are not the same. For instance, Gloria González Fuster argues the GDPR is a law, solely to protect data, but privacy and protectin cannot and should not be treated as they were the same things[46]. When she debates whether it is even possible to disentangle data protection and privacy, Gloria González Fuster concludes that "[t]o envisage law as continuously renegotiating the meaning of the words of law obliges to refrain from any determination of the content of legal notions that wouldbe valid in abstract, and to accept meaning as in a constant state of flux. It cannot beconcluded from the evidence gathered, thus, whether the right to the protection ofpersonal data generally comprises some specific elements, or whether it does not.Similarly, it cannot be inferred that the EU right to the protection of personal datahas been completely disconnected from the right to privacy in EU law. What needs to be emphasized, in any case, is that the connection between EU

[44]Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en [hereinafter *Data Protection Directive*] [accessed 19 Apr 2019]

[45]Organization for Economic Co-operation and Development (OECD): The OECD is a group of 30 countries committed to the promotion of democratic governance and economic development. As part of these efforts, the members of the OECD join forces to produce a variety documents, including model treaties, reports, and recommendations to support an methodical/logical international system and assist trade not just between its members, but between all interested nations.

[46]GONZALEZ FUSTER, Gloria: *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer, New York, 2014. (DOI 10.1007/978-3-319-05023-2)

personal data protectionand privacy is contingent, and that it is not stable"[47]. Thus, I vote for separation of the protection of privacy and data with bearing in mind their necessary entanglement. We need to admit that these notion (data and privacy, and their protection)are distinct, though entwined, concepts/notions, coming in Europe from distinct, though intertwined, sources of law, which, in turn, makes it even more difficult to grasp for those unfamiliar with them. űalso, when we consider biometric data protection, Pedro Miguel Freitas, Teresa Coelho Moreira,and Francisco Andrade states that "[b]iometric data should be understood, for the purposes of the regulation, as anytechnical means of retrieval or confirmation of the identity of a natural living personusing their physical, physiological or behavioural characteristics. Also, "[…] some biometric data must also be considered as sensitive data and the processing sensitive biometric data is generally forbidden, but there are exceptions such assituations whenever there is a free informed consent or if someone is—physicallyor legally—incapable of giving consent, and there is the need of protection of his/hervital interests, among many others. Anyway, the sensitive nature of biometric datameans that it can only be used in very restrictive and specific situations"[48]. Others scholars, such as Hyunghoon Cho, Daphne Ippolito and Yun William Yu assume three notions of privacy seem relevantwhile examining contact-tracing systems that "[…] (1) privacy from snoopers, (2) privacy from contacts,and (3) privacy from the authorities"[49]. And, in addition, they also inform us, as I have already done, that they do not rigorously definewhat it means for information to be private, though some populardefinitions include information theoretic privacy, k-anonymity, and differential privacy[50].The difference might

[47]GONZALEZ FUSTER, Gloriaop. cit., 268.

[48]FREITAS, Pedro Miguel –COELHO MOREIRA, Teresa –ANDRADE, Francisco: *Data Protection and Biometric Data: European Union Legislation.* In: JIAN, Richard –AL-MAADEED,Somaya–BOURIDANE, Ahmed [et. al.] (Eds.): *Biometric Security and Privacy Opportunities & Challenges in The Big Data Era*. Springer, New York, 2017, 420.

[49]CHO, Hyunghoon –IPPOLITO, Daphne–YU,Yun William: *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs.* Available:https://arxiv.org/pdf/2003.11511v2.pdf[accessed 17 Sep 2020]

[50]See, for example:SHANNON, ClaudeElwood:*Communication theory of secrecy systems*. Bell system technical journal, Vol. 28, No. 4, 1949, 656–715. (Doi: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x) Available: https://www.cs.virginia.edu/~evans/greatworks/shannon1949.pdf [accessed 17 Sep 2020] or/and SWEENEY, Latanya:*k-anonymity: A model for protecting privacy*. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10, No. 05, 2002, 557–570 available: https://epic.org/privacy/reidentification/Sweeney_Article.pdf[accessed 17 Sep 2020]and DWORK, Cynthia –MCSHERRY, Frank –NISSIM, Kobbi [et. al.]:*Calibrating Noise to Sensitivity in Private Data Analysis*. In: HALEVI, Shai –RABIN, Tal (eds.): *Theory of Cryptography. Lecture Notes in Computer Science*, Vol. 3876,

be seen clearer in the light of the explanation given by Meg Leta Jones and Margot E. Kaminski, they argue that "[d]ata protection is more akin to what many in the United States call *data privacy* or *information privacy*: protections that attach to data sets (of personal data) that are stored and analyzed en masse. They also state that while the majority the American people considerprivacy;tend to visualizedefending individuals from the giving out of a specificbit of damaging/risky detail, or against particularly intrusive information collection[51]. Although it opens up another debate among American scholars, since it seems to create a tension between privacy and free speech, protected by the First Amendment, though courts have already renowned that privacy is needed for speech, too[52]. Another "standard" connected to privacy for American citizens is the Fourth Amendment[53], which guardspersons against non-warranted government surveillance that defies a "reasonable expectation of privacy"[54] Also, this amendment stress protections for the residence, and has been struggling til merely lately with dealing withextensive surveillance in public places, ordone online.[55]Obviously, the difference between data protection and privacy is present in European/Continental regulations/acts as well, and I will discuss it a bit later in relative detail, the EU does it more formally than the USA. EUacts overtly guard them as "fundamental rights[56]". First, it is essential for us to realize that difference is notworthy between rights under Constitutional law of the USA and rights under the law in the European Union. Whilst the U.S. Bill of Rights is a catalog of constraints on the government based on person's protections, the EU Charter includes a list

---

Springer, Berlin, Heidelberg,2006, 265-284. (https://doi.org/10.1007/11681878_14) Available:https://people.csail.mit.edu/asmith/PS/sensitivity-tcc-final.pdf[accessed 17 Sep 2020]

[51]SOLOVE, Daniel J: *Uderstanding Privacy*. Harvard University Press, London, 2008, 10–11, 106–07, 161–64.

[52] See, for instance, the discussion between VOLOKH, Eugene–SCHWART,Paul M.: *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*. Stanford Law ReviewVol. 52, No. 5, 2000, 1049.(Doi: https://doi.org/10.2307/1229510); SCHWART, Paul M.: *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*.Stanford Law Review, Vol. 52, No. 5, 2000, 1573-1584. (Doi: https://doi.org/10.2307/1229521)

[53] Available: https://www.law.cornell.edu/constitution/fourth_amendment [accessed 9 Sep 2020]

[54]See, for example: Katz v. U.S., 389 U.S. 347 (1967).

Available: https://www.law.cornell.edu/supremecourt/text/389/347 [accessed 9 Sep 2020]

[55]See: Kyllo v. United States, 533 U.S. 27 (2001) focusing on the protection for the home.

Available: Kyllo v. United States, 533 U.S. 27 (2001) and Carpenter v. United States, No. 16-402, 585 U.S. (2018) Available: https://supreme.justia.com/cases/federal/us/585/16-402/case.pdf [accessed 9 Sep 2020]

[56]Convention Art. 8; Charter Arts. 7, 8. Available:https://www.echr.coe.int/Documents/Convention_Eng.pdfand https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data [accessed 9 Sep 2020]

of rights to services provided by the state, as they are often called, positive rights, and not exclusively negative rights. Theyembrace:education paid maternity leave, preventative healthcare, and environmental protections. However, it appears important to note that the completion of fundamental rights has not finished in the European Union. These rights are frequently weighed against one another, and from time to time against other the interests of the current administratio, applying a method to human rights called proportionality analysis.[57]Consequently, to declare that data protection is a fundamental right in the Europen Union is not to declare that courts intend tooverturn laws all the time that influence it. Privacy and data protection as fundamental rights are not even close to beingabsolute; they are interrelated, but not the same.[58] Other scholars, Serge Gutwirth and Paul De Hert, for instance, endeavor to differentiate between data protection and privacy as two different resources for concentrating onauthority discrepancies and differences: privacy all the way through needing opacity as a check on power, and data athe protection of datall the way through instituting processes and transparency tools of channeling power when it's exercised[59]. Fundamentally, Privacy law forbids definiteactions and verifies info transfers, whilstthe law of data protection at its heartattempts to arrange for the rules and regulations for processing data[60]. Another scholar,Hielke Hijmans, observes that privacy heads towards fuzzierprinciples/standards, whereas data protection encompasess a more defined rules.[61]Data protection, too, might have a different scope, that is to say, it can be seen as broader and as well as narrower than privacy. Data protection is restricted to casing

[57]EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. Available: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf [accessed 9 Sep 2020]

[58]See, for example:GONZALEZ FUSTER, Gloria–GUTWIRTH, Serge: *Opening up personal data protection: A conceptual controversy*. Computer Law and Security Review, Vol. 29, Iss. 5, October 2013, 531-539.Or Editors: LEENES,Ronald–Van BRAKEL,Rosamunde –GUTWIRTH,Serge –DE HERT, Paul (Eds.): *Data Protection and Privacy: (In)visibilities and Infrastructures.* Springer,New York, 2017. (Doi: 10.1007/978-3-319-50796-5)

[59]GUTWIRTH, Serge –DE HERT, Paul:*Privacy, data protection and law enforcement. Opacity of the individual and transparency of power*.In:CLAES, Erik –DUFF, Antony–GUTWIRTH, Serge (eds.):*Privacy and the criminal law*. Intersentia,Antwerp/Oxford, 2006, 61-104. (ISBN 90 5095 545 2)

Available: https://works.bepress.com/serge_gutwirth/5/ [accessed 10 Sep 2020]

[60]HOOFNAGLE, Chris Jay–VAN DER SLOOT, Bart –ZUIDERVEEN BORGESIUS, Frederik: *The European Union general data protection regulation: what it is and what it means*. Information and Communications Technology Law, Vol. 28, Iss. 1, 2019, 65-98. (DOI: 10.1080/13600834.2019.1573501)To link to this article: https://doi.org/10.1080/13600834.2019.1573501 [accessed 10 Mar 2020]

[61]See: HIJMANS, Hielke: *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*. Springer, New York, 2016.

personal data as opposed to putting a stop to an intrusion intohomes, but tracks that data outer of more conventionally private contexts.

Data protection law frequently relates to other balancing fundamental rights besides privacy, for instance, the right to non-discrimination.[62] Other scholars, for instance, Patrizio Campisiconceptualizes privacy as follows: "[t]he word privacy is a general term which encompasses both different areas of study and real life situations. It is commonly accepted"[6364]that the common phrase privacyis able to presume somewhat diverse implications as depicted in […] and specified in the following, in depth, one refers to decisional privacy when we refer to the right of the individual to decide concerning his life without any unnecessaryintrusion;spatial privacy.[65]When we denote the individual's right to have his own personalphysical spaces, which cannot and should not be violated without one's explicit consent; intentional privacy when we refer to the right of the individual to prohibit/preventfurther contact/connection of apparent events. For example, discussion/talks in public, or uncoveredskin texture, for instance, circulating/distributing pictures or photos);Informational privacy can refer to the individual's right to determin the limits to the admission/right to use toprivate info which signifies whichever info that may perhaps be applied/exploited inany way to recognize/classify aperson. Though it seem vital to note that some data which may not look private info can turnout to be one that identifies a person in the near future. Obviously, no clear-cutrestrictions/margins can be seen among the specifiedassociations […]. In relation to the use, a certainconceptualization of privacy might beselected as widespread, the other characteristics still being vaued for considering in the evaluation of privacy. Nevertheless, owing to the impressiveprogress of IT in the last

[62]See, for instance: *Handbook on European non-discrimination law*. 2018 Available:https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf [accessed 10 Sep 2020]

[63]*Privacy & biometrics building a conceptual foundation*. NSTC, Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics. Tech rep, September 2006. Available: https://www.hsdl.org/?view&did=463913[accessed 10 Sep 2020]

[64]WOODWARD,John D. Jr.:*The law and use of biometrics*. (Doi: https://doi.org/10.1007/978-0-387-71041-9_18) In: JAIN, Anil K. –FLYNN, Patrick –ROSS, Arun A. (Eds.): *Handbook of Biometrics*. Springer, New York, 2008.

[65]This term sometimes seems the closest to the definition of privacy offered by environmental psychology as I will examine later in order to get a wider picture connected to the elusive nature of the term privacy.

twenty or so years, info privacy has assumed a major rolewithin the recentdevelopment considered[66].

1.2 Private Spaces under the reign of IT: Privacy defined by psychology and its uneasy relation toits own concept of privacy, data protection, and confidentiality: legal/psychological issues and concerns.

Studies and researches on privacy can be found in anthropology, architecture, cultural geography, environmental design, ethology, history, law, philosophy, and sociology, as well as clinical, counselling, developmental, educational, environmental, and evolutional and social psychology. As a consequence of differences in definition, language and purpose, of the numerous methods and approaches, it seems problematic and challenging to connect one study to another. In vexing moments, it look as if the differences were irresoluble, even contradictory, and that the state of affairs could not be solved[67]. There has not been agreements on whether privacy is a condition of the individual, a quality of the place, a progression, an objective, an individual or group attitude or an observable/recognizable behavior. Thought we are aware of the fact that law and psychology are two different disciplines, defining privacy with a different drive and determination, one must recognize the necessary entanglement of them. The definition of privacy coming from different sources and prospective is worth studying, especially if one acknowledges that the connotations of privacy itself keep changing, leaving gaps, loopholes to fill in, and, more often, the understanding of the word may be intertwined. One of the basic assumptions is that personal space and privacy are vital for individual andcommunity comfort, security and quality of life. Irwin Altman defines privacy as the "selective control of access to the self or one's group." Thus, privacy involves control over the immediate environment. It is essential for the individual to be able to shape and personalize space. Privacy characterizes and embodies a dynamic process of openness and closeness to others[68]. Consequently, privacy variations might be recognized with physical

[66]CAMPISI, Patrizio: *Security and Privacy in Biometrics: Towards a Holistic Approach.* In: CAMPISI, Patrizio (Ed.):*Security and Privacy in Biometrics*. New York, Springer, 2013, *3*.

[67]MARGULIS, Steven. T.:*Conceptions of privacy: current status and next steps*. Journal of Social Issues, Vol. 33, No.: 3, 1977, S-21. (Doi: https://doi.org/10.1111/j.1540-4560.1977.tb01879.x)

[68]See: ALTMAN, Irwin:*Theenvironment and social behavior.*Brooks/Cole, Monterey, 1976, 18.orALTMAN, Irwin:*A Conceptual Analysis.*Environment and Behavior, Vol. 8, Iss. 1, 1976, 7-29.

or even psychological barriers wherever individuals seek to separate or protect themselves from the intrusion of others. This seems to be importantin one's home, but also in the work environment or duringrelaxation or free time activities. Privacy also includes visual and auditory exclusivity[69]. Steady or transitionally occupied places produce place attachment and are often accompanied with ties to personal objects such as furniture, pictures, and souvenirs that mark the appropriation. Appropriation is often defined as a particular emotional relation to an object. The appropriated object could become part of the identity of the individual[70], and might be seen as one of the most important factors while defining the quality of life[71]. The appropriation of space has in essence a social function in the sense that the individual or the group marks control over the space[72], which in line produces a feeling of security. When appropriation is not shared with others, or only with one's group, control is absolute. Personal space can be defined as the invisible boundary surrounding each and individual into which others might not intrude without affecting and/or causing discomfort. Also, it can be realized that personal space regulates communications/collaborations, and its extension relies on environmental variables. Its functions are twofold: protection, in which it acts as a buffer against various interpersonal threats, and communication purpose, in which it regulates and defines which sensory communication-channel, such as touch, visual, or verbal can and are supposed to be applied. Consequently, interpersonal spaces/distances can be seen as signals for understanding the specific relationship of two individuals. There are various social determinants of personal space such as culture and ethnicity, age and gender[73]. Contrary to

(https://doi.org/10.1177/001391657600800102)or ALTMAN, Irwin–CHEMERS, Martin M.:*Culture and environment*. Brooks/Cole, Monterey,1980.

[69]Check, for example: SUNDSTROM, Eric–TOWN, Jerri. P.–RICE, Robert. W. [et. al.]:*Office noise, satisfaction and performance*. Environment and Behavior, Vol. 26, Iss. 2, 1994, 195–222. (Doi: https://doi.org/10.1177/0013916594026002O4)

[70]KOROSEC-SERFATY, Perla. (Ed.):*Appropriation of space.* In: SERFATY-GARZON, Perla:*Proceedings of the third International Architectural Psychology Conference*.Louis Pasteur University, Strasbourg, 1976. orBARBEY, Gilles: *L'appropriation des espaces du logement: Tentative de cadrage théorique*. In: KOROSEC-SERFATY, Perla. (Ed.): *Actes de la 3ème Conférence Internationale de Psychologie de l'Espace Construit Strasbourg, France*. Université de Strasbourg Press, *Strasbourg*, 1976, 215-218.

[71] See, for example: STEG, Linda –DE GROOT, Judit I. M.: *Environmental Psychology:An introduction*. John Wiley & Sons Ltd, Chichester, West Sussex, 2019.(DOI:10.1002/9781119241072)

Available: http://www.wiley.com/go/permissions [accessed 7 Oct 2020]

[72]PROSHANSKY, Harold M.:*The City and Self-Identity*. Environment and Behavior, Vol 10, Iss. 2, 1978. (Doi: 10.1177/0013916578102002),available: http://eab.sagepub.com/content/10/2/147 [accessed 7 Oct 2020]

personal space, territoriality is perceptibly bordered by limits and tends to be home or workplace centered. It is a defined and protected space and is always an expression of identity and attachment to a place[74]. Also, territories are controlled spaces that serve to enable the personalization and regularization of intrusion. Of course, for environmental psychology the emphasis is often on the physical surroundings, this focus, however, with the crystal clear realization and acknowledgement that there are no physical settings that are not a social, legal, cultural and psychological as well.

1.3 Under the reign of IT: Privacy, data protection, and confidentiality: legal/psychological issues and concerns

Privacy and confidentiality have been getting growing attention from the public and from both branchesof governments(executive and legislative) all around world. Newspapers, scientific-scholarly papers/studies, and even books, popular literature, and have already recognized the mounting concentration of individual data records and the growing capacity of computer and communication/information technologies to assist connection, retrieval, and distribution of personal information. The public concern has been reflected in actions of the European Union[75] and of many countries, including the USA. Some public distressesses have been reflected in governmental actions as well. For example, the EU's data protection laws have long been considered as a standard in the world[76]. Over the last 25 or so years, technology has transformed our lives in several ways no-one could have dared to imagine. Also, this fact has put pressure on the regulation procedure and on the regulatory body to review the existing rules. Consequently, in 2016, the European Unionimplemented theGDPR, one of its greatest endeavours in present years.

---

[73]AIELLO, J.R. (1987). *Human Spatial Behavior*, In: D. Stokols –I. Altman (Eds.): *Handbook of Environmental Psychology*. New York: John Wiley & Sons, pp. 359-504 or Aiello, J. R. –Thompson, D. E., & Baum, A. (1981). *The symbiotic relationship between social psychology and environmental psychology: Implications from crowding, personal space, and intimacy regulation research*. In J. H. Harvey (Ed.): *Cognition, social behavior and the environment*. Hillsdale, New Jersey: Lawrence Erlbaum Associates, pp. 423-438.

[74]Sommer, Robert: *Personal Space: The Behavioural Basis of Design*. Prentice-Hall, New Jersey.1969

[75]See, for instance, Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert (eds.): Data Protection and Privacy: (In)visibilities and Infrastructures. Springer, New York. 2017 or Serge Gutwirth, Ronald Leenes, Paul De Hert (eds.) - Data Protection on the Move: Current Developments in ICT and Privacy_Data Protection. Springer, Dordrecht. New York. 2016

[76] See: Marini Alice, Alexis Kateifides and Joel Bates (DataGuidance) and Gabriela Zanfir-Fortuna, Michelle Bae, Stacey Gray and Gargi Sen (Future of Privacy Forum): Comparing privacy laws: GDPR v. CCPA 2019

Its objective is to substitute Data Protection Directive of 1995 that was implemented when the Net was could only reach its embryonic stage. The GDPR is now known as law across the EU. In order to be efficiently implemented, Member States have been given two years to guarantee that it is entirely implementable in their countries by May 2018. The announcement of regulations, and implementation of administrative guidelines/procedures have demonstrated the rivet attention of legislators and government executive given to what they see as the urgent need to reassure the public that its rights of privacy are protected in the attainment, the amassing and maintenance of data records. At the same time, government officials diagnose that timely and relevant information in statistical form is desirable, and even compulsory for making decisions in both sectors, public and private. Producers as well as users of survey data have been concentrating on apparent and professed amassed difficulties in directing surveys and censuses of individuals and households. However, several reasons have been recommended for the reported increasing problematic issues, changes in living and working conditions, over-surveying, disappointment about the validity of survey results, and so on. Still, privacy and confidentiality has mentioned prominently as a contributory cause. First, it seems important to define *privacy vs. data protection and confidentiality*, since there is an ongoing debate in the world whether these words may mean or refer to the same for their users.

Concerns of interrelatedness: privacy, data protection and confidentiality:[77]

In the EU recognizes human dignity as an absolute fundamental right. In this notion of dignity, privacy or the right to autonomy and private/personal, life, in control of information about you, to be let alone, plays a pivotal role. Privacy is often valued as a social value, not merely an individual right. In history, in the United States of America, privacy has frequently been viewed and considered as a major component of freedom, the right without any state intrusions. Though thedifference between Europe and the rest of world is relative (even virtual) since privacy is a crucial component considered throughout the European Union. Almost each country in the world recognizes or be aware of the importance of privacy in some way, be it in their constitution, fundamental law or in other

[77] Available: https://www.snia.org/sites/default/files/Hibbard_DSI_2015_Privacy-vs-Data-Protection-v2-revision.pdf [accessed 10 January 2021]

acts/provisions. Furthermore, privacy is recognized as a universal human right while data protection is not, or some scholars predict, at least, not in the near future. The right to private/personal life and/or privacy is enshrined in the Universal Declaration of Human Rights (Article 12)[78], the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7). There are some examples of activities considered private might include: a medical examination, activities within your own home, using a bistro bathroom, going into the office of a reproductive health provider. In general, one can state that any action for which you have the reasonable expectation of privacy.Most things done in public places would not be considered private, although privacy laws leave a substantial amount of grey area as to what might be considered "public." In the USA, the Fourth Amendment of the U.S. Constitution protects against searches that violate your reasonable expectation of privacy, That can be loosely defined as something for which society as a whole would consider legitimate. The 1967 Supreme Court case *Katz v. United States* held that the government may not record a conversation made from a public phone booth (with the glass door shut), even if the recording device is on the outside since the individual making the call has a reasonable expectation of privacy. One may have a reasonable expectation of privacy within his or her home; your office (if closed to the public); and most post and delivery sent or received through the Postal Service, to name a few examples. Though, one might have a much more limited expectation of privacy when out in public places and none with respect to things left in the trash outside your home. Also, privacy is the control over the magnitude, timing, and conditions of sharing oneself, since it reflects on one's intention, these might be seen as physical, behavioural, or intellectual with others one might desire or feel the need to share. For example, persons may not want to be seen entering a place that may contribute to stigmatizing or to being threatened by probable stigmatization them, such as a psychological counselling centre undoubtedly and evidently identified by signs on the front of the building. The evaluation of privacy also includes consideration of how scholars, scientist or (mental) health care professionals access information from or about potential

[78] Available: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf and, consult: https://www.standup4humanrights.org/layout/files/30on30/UDHR70-30on30-article12-eng.pdf [accessed 10 January 2021]

clients, patients and/or participants[79]. Moreover, one can identify, at least, four main areas of privacy that are of specific interest concerning data protection and privacy laws and practices: information privacy, bodily privacy, territorial privacy, and communications privacy[8081]. Information privacy can be defined as the declartion by persons, groups or institutes/organizations to make a decision for themwhat time, how and to what extent info/details about them is transferred to others. Bodily privacy concentrates on a person's physical being and any intrusion thereof. Such an intrusion can be recognized as a form/procedure or method of genetic testing, drug testing or body cavity searches. Territorial privacy[8283]is mostly concerned with setting limitations on the ability of one to intrude into another individual's surroundings or environs. Environment is not restricted to the home of the individual concerned; it might be demarcated as the workplace or public space and environmental considerations can be extended to an international level. Incursion into an individual's territorial privacy characteristically comes in the form of video surveillance[84], or closed-circuit television (CCTV), ID checks and usage of related technology and procedures. Surveillance of the public using CCTV is common in numerous regions all around the world. Since the arena of similar technologies are rapidly developing, the use of body worn video cameras has been presented as a novel, innovative form of surveillance, frequently applied in law enforcement, with cameras placed on a police officer's chest or head. Video surveillance has already created substantial debate about balancing its use with individuals' right to privacy even when in public[85]. Communications privacy includes the protection of the means of correspondence, together

[79]https://www.research.uci.edu/compliance/human-research-protections/researchers/privacy-and-confidentiality.html

[80]To get to know more up-to-date information, visit: https://iapp.org/resources/glossary/

[81]See: https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/1-introduction-to-the-inquiry-5/the-meaning-of-privacy/ [accessed 11 January 2021]

[82]KÖNIGS Bastian, Florian Schaub, Frank Karlg and Michael Weber: Towards Territorial Privacy in Smart Environments. Conference: Intelligent Information Privacy Management (Privacy 2010), AAAI Spring Symposium Project: Context-adaptive Privacy Mechanisms. Available: https://www.researchgate.net/publication/236657460_Towards_Territorial_Privacy_in_Smart_Environments [accessed 11 January 2021]

[83]BANISAR David and Simon Davies: Privacy and human rights: an international survey of privacy laws and developments. The John Marshall Journal of Computer and Information Law. Vol. XVIII. January 1999

[84]Samantha Adams, Nadezhda Purtova, Ronald Leenes (eds.) - Under Observation_ The Interplay Between eHealth and Surveillance-Springer International Publishing, New York 2017

[85]See, for instance: Demetrius Klitou: Privacy-Invading Technologies and Privacy by Design_ Safeguarding Privacy, Liberty and Security in the 21st Century Asser Press/Springer, New York 2014

with postal mail, phone conversations, e-mail and other forms of communicative behaviour and device, machine or toll of technology. Overall, it can be stated that privacy is about people, a kind of sense of being in control of access that others have to ourselves, but also a right to be protected, and it is in the eye of the clients/patients, not the (mental) health care professionals.

The protection of data is about shielding any info concerning and linked to aparticular natural (living) human being. It definitely includes names, dates of birth, pictures, shots of videos, addresses, especially home an email and phone numbers. Other info/details such as IP addresses and contents of communications that can be connected to or provided by end-users of communications services are considered private data, too. Also, it seems vital to note that the concept of protecting data comes from privacy right and in cooperationthey are contributory to safeguarding and supporting values and rights that are valued fundamentally; and to exercise other rights and freedoms, for instance free speech and so on[86]. Data protection has precise goals and objective to guarantee and safeguard the fair processing (treating, dealing with and handling) of personal data, including gathering/assortment, usage, storage) by both the public and private sectors[87].

Confidentiality denotes personal information shared with a lawyer, an attorney, psychologist, physician, therapist, or other individuals that cannot be revealed to third parties without the client's expressed consent. Also, put it differently, confidentiality relates to the management or conduct of information that an individual has revealed in a relationship of trust and with the expectation that it will not be disclosed to others without approval/consent in ways that are inconsistent with the understanding of the original disclosure.During the informed consent process, if relevant, subjects are supposed to be notified of the precautions that will be applied to safeguard data confidentiality and be informed of the parties who will or may have access. This will let subjects make a decision about the acceptability of the protections and the adequacy of the possible release of private information to the interested parties.

Thus, we may conclude that confidentiality is about identifiable data, and can be seen an extension of privacy. It is also a kind of contract about maintenance and who has

[86]https://criminal.findlaw.com/criminal-rights/is-there-a-difference-between-confidentiality-and-privacy.html
[87]https://edps.europa.eu/data-protection/data-protection_en#Privacy

access to classifiable data. For instance HIPAA[88], it protects patients from inappropriate disclosures of "Protected Health Information" (PHI). It is of vital importance in the United States, since any organization or individual who works in or with the healthcare industry or who has access to Protected Health Information (PHI) of US individuals, largely categorised as Covered Entities, Business Associates and Sub-Contractors. And, of course, the list includes: Healthcare Providers, such as hospitals, health clinics and health centres, nursing homes, doctors, dentists, pharmacies/drugstores, chiropractors, and psychologists as well. Employer Group Health Plans such as HMOs, health insurance providers, plans for health provided/supported by companies, programs by the government that pay for health care such as Medicare/aid, and health programs for (combat) veterans. It includes Health Insurance Companies and Healthcare Clearing Houses and Healthcare clearing houses comprise entities that process non-standard health information for a healthcare organization and transforms this data into a different format. Lastly, Business Associates, who can be anybody who works with any of the above mentioned[89].

On the verge of confusion: *confidentiality* vs. *privacy* vs. *data protection*:

Privacy refers to the freedom and autonomy (with self-determination) from intrusion into one's private affairs, and personal information. The fact that the terms *confidentiality* and *privacy* are often used inconstantly and interchangeably make the debates about them e even more complicated, not to mention the bare fact that the situation is almost the same with *privacy* and *dataprotection*. It seems as if these three terms and their definitions overlap each other in our everyday routines. Yet, these terms or notions mean definitely different things, at least, from a legal perspective. Whereas confidentiality is an ethical duty often fortified by an oath, privacy is a right fixed and deeply rooted in the common law. I argue that the comprehension of the difference, which is embedded in these

[88]Health Insurance Portability and Accountability Act of 1996 is United States legislation that provides data privacy and security provisions for safeguarding medical information. It was subsequently revised in 2009 as a Hitech Act & again in 2013 with Omnibus Rule. HIPAA&'s objective was to reform the healthcare industry by reducing costs, simplifying administrative processes and burdens, and improving the privacy and security of Protected Health Information (PHI). Those who conform to the requirements of this act may achieve a HIPAA Compliance Certification based on their merits. See more: https://www.certpro.in/hipaa-compliance-certification/?gclid=CjwKCAjw0On8BRAgEiwAincsHCAV_y4fZ3see-w9aoJndw83vZtvkkerxzPZ-nxSsd_mZv5jtrqCThoCCG0QAvD_BwE

[89]To get to know more about requirements, visit the following site: https://www.certpro.in/hipaa-compliance-certification/?gclid=CjwKCAjw0On8BRAgEiwAincsHCAV_y4fZ3see-w9aoJndw83vZtvkkerxzPZ-nxSsd_mZv5jtrqCThoCCG0QAvD_BwE

notions, privacy, data protection and confidentiality, can contribute to entangle the misunderstanding once signing contracts, founding and forming a client-psychologist relationship, and knowing and understanding your rights and responsibilities in a given situation, at least, in general. When it is expressed that information is *held in confidence*, and thus (is supposed to be) confidential, a person or a client has an expectation that it can be shared only after authorization has been provided, and then only with authorized individuals. Most confidentiality agreements, either written or implied, as with the attorney-client privilege, for instance, stay in effect for an indefinite period. The doctor-patient or psychologist-client relationship founds an implied contract of confidentiality since these health care professionals are in a position to help or assist their patients/clients by gathering and analysing/evaluating/examining otherwise private information. If a psychiatrist asks a psychologist to consult on case, for instance, it would not be a breach of confidentiality. But if the psychiatrist, after the consultation, were to tell your partner that you are terminally ill and nothing to be done, that most definitely would constitute a breach of their ethical duty to keep your information private. Confidential information is frequently handled by financial institutions, for example, banks or insurance companies; hospitals and health care centres; doctors; psychologists, therapists; law firms; companies; religious authorities; and so on. These professionals often have specific rules and regulations for handling confidential information, but others protect confidential information by contract[90]. As it has already been discussed before, the difference may be seen more vibrant in the light of the explanation specified by Meg Leta Jones and Margot E. Kaminski, they state that "[d]ata protection is more akin to what many in the United States call *data privacy* or *information privacy*: protections that attach to data sets (of personal data) that are stored and analyzed en masse. The accumulation of digital dossiers raises not just concerns that disclosure of an individual piece of information will harm someone, but systemic concerns about power, fairness, accuracy, security, and accountability when governments and companies hold large amounts of information about individuals"[91]. They also state that when most Americans think of privacy, they tend to

[90]https://www.research.uci.edu/compliance/human-research-protections/researchers/privacy-and-confidentiality.html

[91]Meg Leta Jones and Margot E. Kaminski: *An American's guide to the GDPR.* Forthcoming in Volume 98, Issue 1 of The Denver Law Review (2020)

visualize protection of persons/human beings from the giving out of a certain bit of damaging/risky info/deatils, or against predominantly intrusive information collection[92].

The concerns of upholding Confidentiality:

Katie Amatruda and Jacqueline Schwarz[93] argue that „Professional mental health therapists swear nothing. Doctors have the Hippocratic oath[94]" in Hungary an oath is taken by fresh psychologists usually before the ceremony[95], and, surprisingly there are three types of oaths, considering the level of the student reached, thus, the University of Szeged has an oath of first-year psychology students, and oath of BA graduate students, and, lastly, one for MA graduate students as well[96].It is interesting, from legal point of view, how these three oath differ. Oath of first-year psychology students as follows: "I, … solemnly pledge that I will observe the rules of the University and the Institute of Psychology. I aim to master the results of science and to carry out my studies with devotion. I declare that I know, understand and abide by the decrees of the Code of Ethics of the Institute of Psychology. During my years of study, I only administer tests, instrumental or other examining processes and researches with professorial guidance. I will strictly keep in secret all information I get to know about research subjects. I pledge that with my knowledge, I will serve my community, for the benefit of the people"[97]. Referring to the Code of Ethics applied by the Institute of Psychology may seem to narrow down the conceptual scope, though it does not contradictory to the wider scope represented by the other two texts of oaths. With respect to the foreseeable prospects and liability of BA graduate students, the oath is slightly modified by including a commitment to "future work" as well, and it reads as: "I, … solemnly pledge that during the course of my future work, I will aim to fully comply with professional and ethical standards. I declare that I got to know and I abide by the competences and boundaries of the Psychology BA diploma. I pledge to faithfully deal with people assigned to my competence, I will do the best I can that serves their interests. I will not misuse the information I possess; I strictly keep

[92] Solove Daniel J: , Uderstanding Privacy harvard University Press, London (2008) 10–11, 106–07, 161–64

[93] Katie Amatruda, PsyD, MFT, CST-T, BCETS and Jacqueline Schwarz, PhD

[94] https://www.psychceu.com/ethics/psychgoodtherapy_index.asp

[95] https://www.psychceu.com/ethics/psychgoodtherapy_index.asp

[96] **https://www.pszich.u-szeged.hu/etika/fogadalom-szovegek/?lang=eng**

[97] **https://www.pszich.u-szeged.hu/etika/fogadalom-szovegek/?lang=eng**

confidential information in secret. I pledge that with my knowledge, I will serve my community, for the benefit of the people"[98]. Strangely though, data protection (as a privacy issue) appears explicitly and directly only in the second and the third "forms" of oath, as if given more content and seriousness to it. The widest on of all three, the last one, for MA graduate students (meaning psychologist), includes a commitment for the whole course of life as a career obligation, and it goes: "I, … solemnly pledge that during the course of my career, I will aim to fully comply with professional and ethical standards of psychologists. I pledge to faithfully deal with people assigned to my competence, I will do the best I can that serves their interests. I will not misuse the information I possess; I strictly keep confidential information in secret. I pledge that with my knowledge, I will serve my community, for the benefit of the people"[99]. It can be stated that confidentiality is the legal and ethical duty of therapists/psychoanalysts/psychotherapists/counsellors/analysts not to disclose or expose anyhow information about their clients to any unapproved or unauthorized individuals. Legally and ethically, the above mentioned health care professionals are bound by statutes/acts and by the profession's code of professional conduct, which may differ nationally or internationally (Code of ethics) not to reveal any information about their clients to unauthorized individuals. Moreover, both legally and ethically, clients have the right to prevent their therapist or psychologist and so on from disclosing any information shared by them in counselling without their (expressed) consent. If one needs to determine the types of confidentiality, there are, at least, two categories of confidentiality are usually documentedconcerning counselling, the first one is*content confidentiality* and the second one is contact confidentiality[100]. The obligation of content confidentiality can be described as: the material or content of the client's conversation with a counsellor not be exposed or revealed by the health care professional. To clarify the difference, it can be specified that disclosures of confidential client information to individuals without right tothat (certain) information are defined as content breaches. Such breaches of confidentiality might have consequences in civil liability to the therapist or the revocation of his or her licence. Thus, contact confidentiality entails that the professional are forbidden to reveal the fact that the client is being seen or visited by

[98] **https://www.pszich.u-szeged.hu/etika/fogadalom-szovegek/?lang=eng**

[99] **https://www.pszich.u-szeged.hu/etika/fogadalom-szovegek/?lang=eng**

[100] http://psychology.iresearchnet.com/counseling-psychology/counseling-ethics/confidentiality-and-legal-privilege/ [accessed 15 January 2021]

the professional. Disclosures to an unauthorized party that the client is meeting the therapist are denoted as contact breaches. Though therapists frequently make tireless efforts and seen determined to avoid disclosures of the identities of their clients, the law usually does not specify matters of contact confidentiality.

1.4 Privacy by Design, Policy and Architecture

The Privacy by Design (PBD) notion proposes that the technology and applicable organizational methods would be able to progress in a privacy-friendly manner from the beginning, wrapping up everyphase from design to distribution and proceduretil disposal and substitution.[101][102] PBD settles on building/improving privacy, also the protection of data, built them into the specifications of the design and structural design of info and the systems of communication systems and technologies.[103] The main design is that protection needs be guaranteed (pro)activelyin place of reacting to events/situatin/changes and to avoid privacy concerns as opposed to planning corrective solutions[104]. We distinguish two approaches: "privacy by policy" and "privacy by architecture." The privacy by policy focuses on the implementation of the notice and choice principles of fair information practices (FIPs), while the privacy by architecture minimizes the collection of identifiable personal data and emphasizes anonymization and client-side data storage and processing. We discuss both approaches with a view to their technical overlaps and boundaries as well as to economic feasibility.[105] When one endeavours to analyse “Privacy by Policy”, it must not be forgotten that, primarily, it can be done through laws and policies, but it also needs

[101]Ontario’s Information and Privacy Commissioner Anne Cavoukian proposed this concept in 2009. She suggests that privacy cannot be ensured only by compliance with regulatory frameworks of regulations; rather, privacy ensurance must and needs to be the default mode of operation of the organizaton.

[102]For more information: https://data.europa.eu/euodp/hu/data/dataset/european-data-protection-supervisor-annual-report-2015[accessed 1 Sep 2020]

[103]*European Data Protection Supervisor– Annual Report 2015*. Publications Office of the European Union, Luxembourg, 2016, 14. Available:https://data.europa.eu/euodp/hu/data/dataset/european-data-protection-supervisor-annual-report-2015[accessed 27 Aug 2020]

[104]BADII, Atta – EINIGMathieu – TIEMANN, Marco–THIEMERT, Daniel– LALLAH,Chattun:*Visual context identification for privacy-respecting video analytics*. Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on. IEEE, 2012. (Doi:10.1109/MMSP.2012.6343470)[accessed 1 Sep2020]

[105]Spiekermann, Sarahand Cranor, Lorrie. *Engineering Privacy*. Software Engineering, IEEE Transactions on. 35. 67 - 82. 10.1109/TSE.2008.88. 2009.

enforcement, without law enforcement, it may remain an empty shell. In this case, it can be true that technology can enable and assist compliance. It is vital to note that damages and intrusion privacy can or may occur owing to actors with ill-intentions, mistakes,government orders or directives as well. If we compare "Privacy by Policy" to or draw a parallel with "Privacy by Architecture", the following differences can reveal themselves: "Privacy by Architecture" is mostly done through technology, it can or might diminishthe (urgent) need to rely on trust and external law enforcement. Thus, intrusions and damages can or may happen iftechnology fails or accessibilityof new data or technologydefeats protections. What might be seen as a preventive force is that "Privacy by Architecture" is often regarded as too costly or restrictive. Ann Cavoukian states that "PbD foundational principles provide a structure for placing privacy data protection in early on, efficiently and realistically into ITs, organizational procedures, architecturesof systems/networks,as well as, without a doubt, the whole governance and supervision systems. PbD attempts to set higher standards for privacy by encouraging and supportingimproved accountability and user confidence. If Privacy by Design provides the "what" to do, then privacy engineering[106] provides the "how" to do it".[107]Privacy by Design has already got its principles appearing in the form of the seven Foundational Principles[108] Demetrius Klitou argues that privacy-invading technologies (PITs) such as Body scanners; Public space CCTV microphones; Public space CCTV loudspeakers and Human-implantable microchips (RFID implants/GPS implants) are, among many others, may pose a considerable threat to privacy. His book presents how and why laws that regulate the design and development of privacy-invading technologies (PITs) can be more effectively guarantee and safeguard the protection of privacy than laws that only regulate data controllers and the use of such novel and advanced technologies. The evidence of his statement is reinforced and validated through a debate on these four specific PITs as case studies. This he attempts to explain how laws/regulations that mandate the implementation

[106]FEIGENBAUM, Joan –FREEDMAN, Michael J.–SANDER, Tomas [et. al.]: *Privacy Engineering for Digital Rights Management Systems*.(ACM Workshop on Security and Privacy in Digital Rights Management)Associated with ACM Communication and Computer Security, Philadelphia, 2001. available: http://www.cs.yale.edu/homes/jf/FFSS-DRM2001.pdf[accessed 13 Oct 2020]

[107]CAVOUKIAN, Ann:*Privacy Engineering: Proactively Embedding Privacy, by Design*. Information and Privacy Commissioner, Ontario, 2014.avilable: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-priv-engineering.pdf [accessed 1 Sep 2020]

[108]https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf[accessed 1 Sep 2020]

of Privacy by Design (PBD) would be able to assist as a practical approach for collectively protection privacy, liberty and security in the 21st Century[109].

Chapter 2 Privacy as related to or is data protection: regulating, defining data.

It sounds like a cliché but the twenty-first century is frequently referred to as the information age. In addition, it is connected to the notion that human activity rely on the exchange of (different types of) information. The so-called modern technologies allow us to assemble/gather, assess, transfer, and process unparalleled quantities of data every second. People now have instantaneous access to information that has not been available before. With this capability/capacity, the risk of mishandling/exploiting people's privacy and its unwanted concerns/consequences grows proportionally, as a consequence, legal concerns and, of course, other related concerns, such as sociological and/or political, have already started to create heated debates in order to search for guarantees that may be able to "defend" privacy with long lasting effects. Obviously, data protection plays an important role in guaranteeing that people may grow confidence in information technology. As I have already described in a previous chapter, there seems to havea lot of turmoil concerning privacy and its connotation and definition, though I do not intend to neglect the importance of privacy as related to data protection. It seems vital for our purpose to devote a shorter chapter to highlight the relevant issues and concerns connected to privacy.

However, the term itself may seem self-explanatory, but "protection of data" normally indicates a compendium of norms/standards that can providethe protection of privacy as well as a wider range of interests.It also admitted that protection of data isdirectlylinked to information technology and expansion that permitaccumulating and applyingcolossal quantity of private data. One can characterize the world by and digitalization and (a drive to) globalization, there is greater than beforeworldwideaccessibility of private data, and the pace of this procedure is sped up by

[109]KLITOU, Demetrius:*Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*. (Information Technology and Law Series (25)), Springer, New York, 2014. (Doi: https://doi.org/10.1007/978-94-6265-026-8_2)

technological inventions as well. There are great amounts of private data being composed, gathered, accumulated, evaluated, allocated and transmitted, with an increase in related "players". One of the major challenges, for instance, is "Big Data[110]", the giganticdata amalgamation to produceeven more data, more postulations and more information (turning into facts) about individuals; the Big Data construction/amalgamation may embracesmart-phones, digitalized Closed Circuit Television, scanning of machine-readable travel passes, post on social media, and so on.[111]

2.1 The GDPR: a brief History in the EU:

The data protection laws of the European Union have long been considered as a criterion in the world. Over the last 25 or so years, technology has altered our lives in many ways nobody could have dared to imagine. Also, this fact has put pressure on the regulation procedure and on the regulatory body to revise the existing rules. Thus, in 2016, the EU implemented the General Data Protection Regulation, one of its greatest accomplishments in current years. Its primary ain has been to substitute the 1995 Data Protection Directive. The GDPR is now known as law across the EU. In order to be smoothly implemented, Member States have been given two years to guarantee that it is completely implementable in their countries by May 2018[112]. The timeline below highlights key dates and events in the data protection reform process from 1995 to 2018.The timeline also offers insights of some of the ways that the GDPR supports our right to data protection[113].

---

[110] According to Zsolt Ződi the definition itself is applied "a rather loose way in the literature," to find out more about this topic, it seems important to be familiar with the following works as well:Zsolt ZŐDI: *Law and Legal Science in the Age of Big Data.* INTERSECTIONS. EAST EUROPEAN JOURNAL OF SOCIETY AND POLITICS, 3 (2): 69-87. or Zsolt ZŐDI: Jog és Jogtudomány a Big Data korában. Állam- és Jogtudomány, 2017/1. sz.,95.o.

[111]KITCHIN, Rob: *Big Data, new epistemologies and paradigm shifts*. Big Data and Society, Vol. 1, No. 1, 2014, p 2. (Doi: https://doi.org/10.1177/2053951714528481) Available: https://journals.sagepub.com/doi/pdf/10.1177/2053951714528481[accessed 17 Aug 2020]

[112] See, for instance:RODRIGUES, Rowena – PAPAKONSTANTINOU, Vagelis (Eds.): *Privacy and Data Protection Seals*. T.M.C. Asser Press /Springer, London, 2018. (Doi: 10.1007/978-94-6265-228-6)

[113]https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [accessed 17 Aug 2020]

One of the key dates is 2016, when Corrigendum to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC, GDPR.[114]One of the Proposals for a Regulation on the protection of individuals with respect to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [First reading] Preparation for the tri-party discussion The European Commission offers two new regulations on ePrivacy and on the rules of the protection of data to be applied to EU institutions (currently Regulation 45/2001) that bring into line the existing rules to the GDPR. Thus, the GDPR is supposed to strengthen an extensive variety of existing rights and launches new ones for individuals including, the right to be forgotten; on request one is permitted to claim that an (or any) organisation delete one's personal data. For example, when one's data are not necessary any longer for the purposes for which they were amassed/accumulated or where one's consent has been withdrawn. In addition, persons have data portability rights, the right to obtain one's private data from an organisation in a frequently used form so that one is able to share it with another. Also, the right not to be profiled, except law or a contract requires it, decisions affecting one cannot be made on the sole basis of automatic/computerited processing. Paul Voigt and Axel von dem Bussche state that the consequenceof GDPR is "[....] a tough negotiation process entailing numerous amendments to the legal text that took 4 years until the adoption of the finalised Regulation. The fragmentation of data protection across EU Member States and the resulting legal uncertainties were considered to constitute an obstacle to the pursuit of economic activities at EU level and lead to a distortion of competition"[115].The aim of the GDPR can be basically summed up as follows: it is primarily an essentially uniform data protection law within the EU. Most of all, this is proposed to reinforce the rights and control options of those whose personal data are processed, for example, data subjects. Personal data should be protected to assume more guarantees, but at the same time their free movement should be guaranteed as well. Art. 5 GDPR set down the data

[114]Corrigendum to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679R%2802%29 and http://data.europa.eu/eli/reg/2016/679/corrigendum/2018-05-23/oj

[115]Rec. 9 GDPR in VOIGT, Paul – VON DEM BUSSCHE, Axel: *The EU General Data Protection Regulation (GDPR):A Practical Guide*.Springer International Publishing AG, Cham, 2017, 2. (Doi: 10.1007/978-3-319-57959-7)

processing principles set down[116], on which the regulation is founded, are in essence similar to those of former versions, considering legality, constraint of purpose, data economy/minimalization), accurateness, restrictions on storage space, integrity and privacy and /or accountability as well as confidentiality the person liable for compliance with these principles[117]. Nonetheless, GDPR has made some changes that need to be considered, as far as companies and private individuals are concerned. The "novel" ideas brought in by GDPR are significant for companies to establish new processes of data protection.

As we have seen it, personal data protection is of primary importance in Europe, with special attention to national features, especially, considering companies and individuals gaining more privacy (equals data) protection. However, it is crucial to realize that as data protection is treated as one of the fundamental rights (with bearing in mind that the "definitions" related and concerned are debated), it is assured by various international and national legal acts.The right to value and respect private and/or family life is guaranteed under Article 8 of the European Convention on Human Rights. In addition, the first international legal act to regulate these subjects (or concerns) in a comprehensive method is the Convention No. 108 for the Protection of Individuals pertaining to Automatic Processing of Personal Data, adopted by the Council of Europe on January 28, 1981. At the level of the EU, the primary legal act was the Directive 95/46/EC on the protection of individuals with reference to the processing of personal data and on the free movement of the data mentioned. Furthermore, the right to personal data protection is safeguarded as well as a fundamental right in Article 8 of the Charter of Fundamental Rights of the EU and in Art. 16 of the Treaty on the Functioning of the EU.

As a starter, in the EU law, besides, Directive 95/46/EC, other legal acts regulated the issue of personal data protection. Significantly, it was harmonized by the provisions of Directive 95/46/EC, which was broad-spectrum and provided a point of reference for the relevant legislation of member states of the EU. The Directive 95/46/EC legalized the right to protection of privacy of each and every natural person with regard to the processing of

[116]See: Art. 5. Principles for the processing of personal data. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016: http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE[accessed on 11 Dec 2020]

[117]FLORIDI, Luciano (eds.): *Protection of Information and the Right to Privacy - A New Equilibrium?*Springer International Publishing, New York, 2014.

personal data, which was one of the fundamental rights and freedoms of natural persons. The Directive was applied to the personal data processing totally or in part by automatic method, and to the processing otherwise than by automatic means of privatedata that outline part of a filing system or were aimed to form part of a filing system.[118] It is important to note that the mainpurpose of Directive 95/46/EC was to guarantee the highest possible level of private data protection and to facilitate the movement of data freely in the EU member states and in practice within the entire European Economic Area. In addition, it seemed vital that the collection and use of private data in the Community had to be done in line with the law of the Member States[119]. Though the EU GDPR[120]relevant as of 2018, and has been introduced astaticstandard of privacy/data protection customary in the member states of the EU. It looks uncertain whether GDPR can lead to legal certainty for both the data subjects and the companies alike because it includes many unclear legal terms, and Member States of the EU are permitted to subject employees data to stringent regulations, thus, I assume, compliance might be maintained. The content of GDPR attempts to make it apparent that it is constructed on the firm standards of individual European countries. It presents that private data amassing with no a permissive law is illegal. The rules of derogation, some of which are very extensive and undetermined, (attempts to) make it obvious, however, that the legislators of the European Union have already come to recognise the related economic concerns/troubles without planning to offer any large-scale protection of the consumers. Regarding Big Data, the phrasing of the regulation in Article 6 b) is: "[…] processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"[121]. In the (possible near) future, it might be seen more

[118]http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML[accessed 11 Dec 2020]

[119]See, for instance:DE HERT, Paul – GUTWRITH, Serge: *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power.* In:CLAES, Erik – Duff, Antony – GUTWRITH, Serge (eds.),: *Privacy and thecriminal law*, Intersentia, Oxford, 2006, 61-104 . orGUTWRITH, Serge – POULLET, Yves –DE HERT, Paul [et.al.]: Reinventing Data Protection? Springer, New York, 2009. (Doi: https://doi.org/10.1007/978-1-4020-9498-9)

[120]REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016: http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE [accessed on 11 Dec2020]

[121]REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016: http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE [accessed on 11 Dec 2020]

simple to make use of Big Data (as a routine) within the company with no successive consent declaration from every employee having to be gained or with no declarations partly invalid or incomplete/imperfect of consent being integrated in employment contracts. Furthermore, it offers the possibility for users/consumers/ to access their data in the future[122]. They might and can claim info from companies that amass data as to what data pertaining to them is stockpiled, and they might have their data altered/modified and transmitted to other providers. Also, the right to be granted with info, the legislatorsof the European Union have reinforced the user's right to be "forgotten" to the result that data placed online can be efficiently obliterated. An additionalpiece of the protection of the consumers is the obligation of the companies to use comprehensibleconditions and expressions to the effect that the individual user knows for what reason and to what extent their data is made use of.[123]As before, though, there is still the decision, which for the most part services have made use of in their general terms and conditions, of acquiring the data subject consent. Though, sooner or later, such consent is assumed to be valid provided that the user is as a minimum 16 years old, which may lead to many clients/customersregistering under a pseudonym/fictitious name or with a falsified date of birth. Eventually, the regulation will codify a high level of the protection of the consumer in the Member States of the EU that is grown weaker by exceptions, but leaves room for data processing companies simultaneously. The creators/lawmakers of this regulation have managed only to a narrow(er) scope to accomplish a rationalequilibrium among the interests of the companies regarding to the usage of big data[124]. Though it also presents some real novelty, for instance, a new category "pseudonymised data" is made known to the public. Dissimilar to data madeabsolutely anonymous, data in this classification lets an unknown user's data be interrelated. Though the data is not assigned to any certainindividual, linking the data hypothetically and supposedly makes it possible for

[122]WISSKIRCHEN, Gerlind –BIACABE, Blandine Thibault – BORMANN, Ulrich, [et. al.]: *Artificial Intelligence and Robotics and Their Impact on the Workplace*. IBA Global Employment Institute, London, April 2017. Available: https://www.ebglaw.com/content/uploads/2017/05/Workshop-4-2017-AI-Workshop-Participant-Materials.pdf[accessed 11 Dec 2020]

[123] See, for example:www.datenschutzbeauftragter-info.de/eu-datenschutzgrundverordnung-das-sind-die-neuerungen [accessed 11 Dec 2020]

[124]See also:VOSS, W. Gregory: *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*. The Business Lawyer, Vol. 72, No. 1, Winter 2016–2017. Available: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2894571_code1740804.pdf?abstractid=2894571&mirid=1 [accessed 11 Dec 2020]

assumptions to be made on the subject of the nom de plume, so such use is legalised/allowed only within stringent restrictions[125]. Thus, the application and gathering of big data may turn out to be trouble-free with no intrusion of privacy. To sum it up, it is also vital to note that a number of the most important improvements of EU law concerning data/privacy that have arisen since the implementation of the Data Protection Directive[126]. These take account of the adoption of the EU's GDPR,[127] the annulment by the Schrems decision of the U.S.–EU Safe Harbor cross-border data-transfer framework,[128] and the subsequent replacement of the Safe Harbor framework with the EU and the USA, Privacy Shield[129]. The "right to delisting," which was created by the 2014 Google Spain decision, also experienced continual improvement.[130][131] Also, the milestone decision in C-507/17 *Google v CNIL*, the Court of Justice holds that there is no obligation under European Union law[132] for Google to be relevant the EU right to be forgotten worldwide.[133] Thisconclusion makes it clear that, whilst the residents of the EU have the legal right to be forgotten, the application of this right stays and limited within the borders of the Union's then 28[134] Member States. though it must be admitted that with the novel

[125]See:www.anwalt.de/rechtstipps/uebersicht-zum-arbeitsrecht-in-japan_056517.html [accessed 11 Dec 2020] and also WISSKIRCHEN –BIACABE– BORMANN [et. al.]: op. cit.

[126]Council Directive 95/46, 1995 O.J. (L 281) 31 (EC)

[127]Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons withRegard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU)

[128]Case C-362/14, Schrems v. Data Prot. Comm'r (Oct. 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362 [accessed Dec 31 2020]

[129]Transatlantic Data Flows: Restoring Trust Through Strong Safeguards, COM (2016) 117 final (Feb. 29, 2016) Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0117&from=EN [accessed Dec 31 2020]

[130]Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccio´n de Datos (AEPD), 2014 E.C.R. 317, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131. [accessed Dec 31 2020]

In this case the term "right to delisting" has been chosen as the specific reference to one of the forms of the "right to be forgotten," as proposed in Voss and Castets-Renard's taxonomy. To get to know more, see:VOSS, W. Gregory – CASTETS-RENARDCeline:*Proposal for an International Taxonomy on the Various Forms of the "Right to Be Forgotten": A Study on the Convergence of Norms*. 14 Colorado Technology Law Journal, Vol. 14, Iss. 2, 2016, 281, 325–27. Available: https://ctlj.colorado.edu/wp-content/uploads/2016/06/v.3-final-Voss-and-Renard-5.24.16.pdf[accessed Dec 31 2020]

[131] See also:VOSS, W. Gregory: op. cit.

[132]General Data Protection Regulation (EU) 2016/679 (GDPR) replacing Directive 95/46/EC (Data Protection Directive)

[133]Judgment of 24 September 2019, *Google Inc v Commision nationale de l'informatique et des libertés* (CNIL), C-507/17, paragraph 64 Available: http://curia.europa.eu/juris/document/document.jsf?docid=218105&doclang=EN [accessed 1 Jan 2021]

[134]Now, of course, it refers to pre-Brexit circumstances.

European standards, data privacy protection has been recognising some major issues needed to be dealt with[135]. Since GDPR (2018)[136], has introduced a standardized data privacy/data protection "model" in the Member States of the EU. Still the legal uncertainty surrounding GDPR has remained for both parties related, companies and consumers alike, owing to a great deal of debates connected to the vagueness of terminalogy[137][138]. Though, the regulation of the contentclarifies that it is grounded on the strict standards of individual EU States[139]. The regulation states that collecting personal data without an unrestrictive rule is forbidden. The derogation rules, some of which are comprehensive and indefinite, make it obvious, nevertheless, that EU lawmakers have already acknowledged the economic difficulties with no intentions to provide any large-scale consumer protection. Regarding big data, the expression of the regulation in Article 6 b) is: "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract[140]". Thus, as we have already seen it, it seems to have been made simpler to use Big Data within the company with no a consequentdeclaration of consent from every employee having to be attained or without partially invalid declarations of consent being included in the employment contract.

Laws on data privacy protection in the USA derive from a conviction, which is different fundamentally. They are not founded on the general supposition that data is confidential, but provide for such data confidentiality only in individual cases, for example, pertaining to health insurance and minors' protection using the Internet[141]. Unlike

[135]LEENES – VAN BRAKEL –GUTWIRTH: op. cit.

[136]REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679[accessed Dec 31 2020]

[137]WISSKIRCHEN –BIACABE– BORMANN [et. al]: op. cit.

[138] See: GUTWIRTH, Serge –LEENES,Ronald –DE HERT,Paul [et. al.] (eds.):*European Data Protection: In Good Health?* Springer, Dordrecht, 2012. (Doi: 10.1007/978-94-007-2903-2)

[139]CUSTERS,Bart –SEARS, Alan M. –DECHESNE, Francien [et. al.]:*EU Personal Data Protection in Policy and Practice*. T.M.C. Asser Press, The Hague, 2019. (Doi: 10.1007/978-94-6265-282-8)

[140]REGULATION (EU) 2016/679https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN[accessed Dec 31 2020]

[141]See: *National Academies of Sciences, Engineering, and Medicine:Evaluating Data Types: A Guide for Decision Makers using Data to Understand the Extent and Spread of COVID-19*.The National Academies Press, Washington DC, 2020. (Doi: https://doi.org/10.17226/25826) Available:

in most European countries, independent data supervisory authority does not exist and no privacy/data protectionrecognized by act of law. The impact of the Patriot Act[142]is also was principally questioned because the PA permits government agencies in the USA an comprehensive authority to accumulate and amass data in particular cases[143]. Thus it places most companies in the most resourceful/favourable economic position achievable; as a consequenc, revisiting the rudimentary/basic regulations in the USA with an approximation of the stricter EU GDPRis likely advisable. With keeping in mind, that liberated and uncomplicated movement of data is crucial.

2.2 Safe harbour and EU-US Privacy Shield:

The major distinctions in the comprehension of the protection of data and the non-existence of options for EU citizens to pursue judicial relief before US courts caused the European Court of Justice to declare the Safe Harbour treaty negotiated between the EU Commission and the US government in 2000 invalid[144][145] The treaty was assumed to permit companies having their registered offices in the European Union to transmitprivate data lawfully to US companies in that certified US companies were declared "safe harbours" for the data from the EU. Though, the level of the protection of the data could not be "equal" or even comparable to the level of the protection of hte data in the EU. Predominantly with reference to the above-mentioned GDPR, the possible harmonization between is the EU and the USA seems impossible, because of the levels of the protection of the data are essentially different. Also, one should expect realistically that the standards of privacy/data protection in the USA will ever be settled in the the standars of the EU (and

https://www.nap.edu/catalog/25826/evaluating-data-types-a-guide-for-decision-makers-using-data[accessed Dec 31 2020]

[142]Public Law 107–56—Oct. 26, 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Usa Patriot Act) Act of 2001

Available: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf [accessed 1 Jan 2021]

[143]https://wizelife.de/themen/wissen/24986/auf-einen-blick-deutscher-und-us-datenschutz-im-vergleich and https://wizelife.de/themen/wissen/24986/auf-einen-blick-deutscher-und-us-datenschutz-im-vergleich [accessed 31 Dec 2020]

[144]ECJ judgment rendered on 6 October 2016 – C-362/14. Available: http://curia.europa.eu/juris/liste.jsf?num=C-362/14[accessed 11 Dec 2020]

[145]See: JONES – KAMINSKI: op. cit.

vice versa)[146]. However, of course, there can be options for data transfer to the US; these may contain approval by the national data protection supervisory authorities of binding corporate rules (BCRs)[147] within an internationally operating company or the standard contractual clauses specified by the EU Commission. Various data protection authorities have currently suspended the approval of BCRs[148]. Additionally, declarations of consent by the data subjects or works agreements, if only employee data are relevant, areappropriate, too. These options, nonetheless, still may mean risks for any corporation. Approvalsmight be rejected, works agreements might not come to pass, and binding corporate rules must be approved by the national data protection authorities and are tough to modify, while courts can reject declarations of consent as inadmissible.

More agreements on data protection may need to be decided sooner or later so as to meet the prerequisite of digitalisation and interconnection of corporations and to create legal certainty. The European Commission and the government of the USA have already acknowledged this "need" as well, and have already brought to a close a successor agreement to the Safe Harbour treaty, the EU-US Privacy Shield.[149] This permits a legal transfer of data across the Atlantic Ocean, the receiving corporations undertaking to comply with the EU data protection rules and to protect the received private data of third parties. The novel regulation provides that the use and storage of private data is authorised only on condition that the use and storage serves the purpose of processing, as it is portrayedby the principle of dedicated use of private data[150]. If an employee is part of the corporation any more, accumulating and keeping/savingprivate data is not

[146]See, for example: STÖCKER, Christian:*Google's gracious controllers.* Available: www.spiegel.de/netzwelt/netzpolitik/datenschutz-in-den-usa-und-europa-a-849114.html[accessed 1 Jan 2021].

[147]Binding corporate rules (BCR) are policies of the protection of data complied by companies established in the European Union for transfers of private data outside the EU within a group of undertakings or enterprises or undertakings. BCR includes the principles of general data protection and rights enforceable to guarantee appropriate and applicable safeguards for data transfers.

[148] See, for more deatils: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en[accessed 31 Dec 2020]

[149]Consult: https://ec.europa.eu/info/sites/info/files/factsheet_eu-us_privacy_shield_en.pdf[accessed 31 Dec 2020] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_euus_privacy_shield_en.pdf and also the Annexes: https://www.ftc.gov/system/files/documents/plain-language/annexes_eu-us_privacy_shield_en1.pdf [accessed 31 Dec 2020]

[150]See:European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461 or http://europa.eu/rapid/press-release_IP-16-2461_de.htm[accessed 31 Dec 2020]

legalized/allowedto any further extent. In opposition to the Safe Harbour treaty, compliance with these rules is rigorously controlled by the authorities in the USA, and breaches are penalised. Furthermore, the data subjects have the rights to be presented information by US corporations, and there will be an objective and independent ombudsperson at the US State Department whom EU citizens concerned can contact. The mass surveillance of EU citizens by US authorities is to be prohibited, except for the common/standard special cases, such as fight against terrorism or, for instance, national safety, and so on. Both parties are assumed to conjointly re-evaluateyearly whether the EU-US Privacy Shield functions properly.[151] The European Commission adopted the new regulation on 12 July 2016 as a sufficient regulation for the monitoring of the standards of the protection of data.[152] Even though the Member States of the European Uniondo not reject the regulation, critics could and possibly will appeal to the European Court of Justice. Their criticism is anchored in the assumption that the level of the protection of the data cannot be realistically compared to the level of the data protection in the EU and that the guaranteessettled and given/offered by the USA, to be exact, that the companies will be controlled, are not satisfactory. In the intervening time, since 1 August 2016, an additionaloption/substitute for transferring data to the USA is accessible along with BCRs and standard contractual clauses: the self-commitment of US companies under the EU-US Privacy Shield. US companies are presumed to be registered (or, basically, they must) with the US Department of Commerce if they desire for transfering data under the EU-US Privacy Shield.[153] As it has been noted in my previous chapters, due to the nature of the definitions of *privacy*, the American and Continental view and understanding of privacy can differ in many ways. The so-called American privacy standards, the First and the Fourth Amendments (sometimes in conflicting with privacy) set a course for a notion, and, when most Americans think of privacy, they have the tendency to visualizethe protection

[151]See: www.heise.de/newsticker/meldung/Privacy-Shield-EU-Kommission-veroeffentlicht-Text-fuer-loechrigen- Datenschutzschild-3120502.html or https://www.heise.de/news/EU-Kommission-verhandelt-zu-neuem-Privacy-Shield-4876922.html [accessed 1 Jan 2021]

[152]See: European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461 or http://europa.eu/rapid/press-release_IP-16-2461_de.htm [accessed 31 Dec 2020]

[153] EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce Available: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [accessed 31 Dec 2020]

ofpersons from the giving out of a certain piece of risky info, or against particularly intrusive information collection[154]. In addition to this,the basic difference could be understood richer in the light of the description of *data privacy* or *information privacy*, I have already discussed, provided by MegLeta Jones and Margot E. Kaminski.

2.3 A (short) comparison of privacy laws: GDPR, CCPA, China and the „Privacy Act of Hungary[155]"

The GDPR[156] and the California Consumer Privacy Act of 2018 ("CCPA") (SB-1121 as amended at the time of this publication) both aim to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share consumer data, whether the information was obtained online or offline. The GDPR, which went into effect on 25 May 2018, is one of the most comprehensive data protection laws in the world to date. Absent a comprehensive federal privacy law in the U.S., the CCPA is considered one of the most significant legislative privacy improvements in the country.In 2018, the CCPA was signed into law and went into effect last. The final draft of the regulation was submitted to the California Attorney General in June 2020. Formerly, the CCPA would be put into force starting July 1, 2020, but as a result of the COVID-19 pandemic[157], the California Office of Administrative Law has 30 working days, plus an additional 60 calendar days, to approve the recent draft[158]. As the Continental version, GDPR, the CCPA's effect is supposed to be world-wide, assumed California's status as the fifth largest global economy. The CCPA has taken effect on 1 January 2020, but some provisions under the CCPA oblige organizations to provide consumers with information concerning the previous 12-month period, and consequently activities to comply with the CCPA might well be required sooner than the effective date. The basic differences of the GDPR and CCPA are relevant, but the these two laws are similar with respect to their definition of certain terminology; for instance, the foundation of supplementary protections for individuals under 16 years of age; and the inclusion of rights to access personal

[154]SOLOVE, 2008: op. cit., 10–11, 106–07, 161–64.

[155]https://www.naih.hu/act-cxii-of-2011---privacy-act--.html [accessed 4 Jan 2021]

[156] Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj [accessed 4 Jan 2021]

[157] Extra attention has been given to certain forms of data, for instance, National Academies of Sciences, Engineering, and Medicine 2020. *Evaluating Data Types:op. cit.*

[158]https://www.securetrust.com/data-privacy-and-the-california-consumer-privacy-act/?gclid=EAIaIQobChMIjbnVxJ-C7gIVBSgYCh2fsgTREAAYAiAAEgJDy_D_BwE

information. Yet, the CCPA differs from the GDPR in some important ways, predominantly concerning the scope of application; the nature and extent of collection limitations; and rules in relation to accountability. As regards the latter, for instance, the GDPR provides for obligations in relation to the appointment of Data Protection Officers[159], the maintenance of a register of processing activities, and the need for Data Protection Impact Assessments[160] in specified conditions. On the other hand, the CCPA does not definitely concentrates on accountability-related obligations, even if such provisions do exist, such as the obligation for companies to train their staffs that deal with requests from consumers. It is also notable that the fundamental legal framework of the CCPA is quite different from the GDPR[161]. A fundamental principle of the GDPR is the prerequisite to have a "legal basis" for all processing of private data. That is absolutely not the case for the CCPA. Additionally, the CCPA disregards from its scope the processing of some categories of private information altogether, for instance, medical data covered by other U.S. legal frameworks, as well as processing of personal information for clinical trials, and personal inforouted by credit reporting agencies. Furthermore, the CCPA emphases on transparency obligations and on provisions that limit selling of personal information, requiring a "Do Not Sell My Personal Information" link to be included by businesses on their homepage[162]. In addition, the CCPA includes specific provisions in relation to data transferred as a consequence of mergers and acquisitions, providing consumers with the right to opt-out if the "third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection.[163]"

[159]Available:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [accessed 4 Jan 2021]

[160] See, for example: CUSTERS –SEARS –DECHESNE[et. al.]: op. cit. or LEENES – VAN BRAKEL –GUTWIRTH: op. cit.

[161]ZETOONY, David: *California Consumer Privacy Act (CCPA) Practical Guide*. Bryan Cave Leighton Paisner, 2020. Available: https://ccpa-info.com/wp-content/uploads/2019/09/bclp-practical-guide-to-the-ccpa.pdf[accessed 4 Jan 2021]

[162] To get more information, visit: https://www.cookiebot.com/en/what-is-ccpa/ [accessed 4 Jan 2021]

[163]Marini Alice, Alexis Kateifides and Joel Bates (DataGuidance) and Gabriela Zanfir-Fortuna, Michelle Bae, Stacey Gray and Gargi Sen (Future of Privacy Forum): Comparing privacy laws: GDPR v. CCPA 2019

DataGuidance provides a suite of privacy resolutions designed to help organisations to monitor regulatory progresses and improvements, mitigate risk and accomplish global compliance. *Future of Privacy Forum* is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, evolving principled data practices in aid of emerging technologies.

In the first ten years of the 21st Century, China's privacy and personal data protection may seem to present a mixed picture. Optimists may be able to argue that there are solid and sound progresses in both legislative initiatives and judicial enforcement. Though, pessimists can effortlessly affirm that this fragmentary approach is far from offering or guaranteeing a systematic and comprehensive protection for privacy and personal data[164]. Owing to the "special" circumstances, for example, state surveillance, privacy and data privacy in China are supposed to be non-existent. However, it does exist, and China regulates differently privacy from the state and privacy from private actors. Consumer data privacy in China is at the pole position of novel regulations issued during the last couple of years to construct a (applicable) legal framework on data protection, up to the Cybersecurity Law. In spite of the influx of data transfers from the West to China, there is a shortage of of legal studies on Chinese data protection rules, the structure of China's approach on this field and its magnitudes and/or concerns.

Initially, it can be said that China followed a pathway similar to the U.S. method[165], though; scholars assume that this direction has been altered and met with the stricter EU rules and regulations on several legal elements, particularly through the Cybersecurity Law and the Personal Information Security Specification[166]. Up to the point that China now has a comprehensive data protection law on its legislative agenda and encourages privacy protection for consumers that sometimes surpasses U.S. rules. Decrypts specificities can be identified concerning data protection in China that can easily make China's voice special with the probability of gain major influence in this field, while Western directions and regulations have been the solitary regulatory power so far. Emmanuel Pernot-Leplay argues that "[t]hese Chinese characteristics, such as the paradoxical – yet parallel – increase of both state surveillance and consumer privacy and the cyber-sovereignty

[164]XUE, Hong: *Privacy and personal data protection in China: An update for the year end 2009*. Computer law and security Review, Vol. 26, Iss. 3, 2010, 284-289. (Doi: https://doi.org/10.1016/j.clsr.2010.01.004)Available:https://www2.cs.duke.edu/courses/common/compsci092/papers/china/xue.pdf [accessed 4 Jan 2021]

[165]PERNOT-LEPLAY,Emmanuel:*EU Influence on Data Privacy Laws: Is the US approach converging with EU model?* Colorado Technology Law Journal,Vol. 18, No. 1, 2019.Available: https://pernot-leplay.com/wp-content/uploads/2020/04/EU-Influence-on-Data-Privacy-Laws.-Is-the-U.S.-Converging-with-the-EU-Model.pdf [accessed 4 Jan 2021]

[166]PERNOT-LEPLAY,Emmanuel:*China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, Penn State Journal of Law & International Affairs, Vol. 8, No. 1, 2020, 49, 49-53. Available:https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1244&context=jlia [accessed 2 Jan 2021]

principle impacting personal data protection, now compose China's approach. This "data privacy with Chinese characteristics" will bear consequences on the country's forthcoming regulations on artificial intelligence and for future policy developments in the European Union and the United States"[167]. In addition, it can be stated that China stresses more on both the significance of the family and the prominence of the state of China and more Western focuses on individual rights, including the right to privacy. Thus, the interpretation and the regulation of privacy seem to include all meanings of the word. But it has been assumed that information ethics in China is in its embryonic stage. Lü Yao-Huai states that privacy can be justified as an instrumental good, rather than an intrinsic good, and he also assumes that the expansion of the protection of privacy will continue to grow in China. One of the reasons is globalization, growing trade relations with and more contact to Western societies. Other pressures and demands can be realized and witnessed by the younger generations, who have been influenced by individual privacy represented by Western cultures. Still, Lü Yao-Huai supposes that these emerging concepts and different models of privacy cannot modify wholeheartedly the distinctive Chinese traditional features of privacy and data privacy.[168]

Hungary is a member state of the EU, where, due to the Communist Era, privacy as such, and privacy as data protection could not bloom for a long time. After two decades the situation finally started to show some progress. The Hungarian National Authority for Data Protection and Freedom of Information is accountable for supervising and shielding the right to the protection of private data and to freedom of information in Hungary. Our accountabilities extend to cover both the state and private sectors. The National Authority for Data Protection and Freedom of Information is regulated by Act CXII of 2011, on Informational Self-determination and Freedom of Information, which was endorsed by the National Assembly on 11 July 2011. The Act is comprehensive in scope, and concerns all data control and data processing activities undertaken in Hungary. The Act defines these activities as those, which relate to the data of a natural person, as well as data in the public interest and data made public on the grounds of being in the public interest. Compared to

[167]PERNOT-LEPLAY, 2020: op. cit., 49, 49-53.

[168]YAO-HUAI, Lü: *Privacy and Data Privacy Issues in Contemporary China*. Ethics and Information Technology, Vol. 7, No. 1, 2005, 7–15. (Doi: 10.1007/s10676-005-0456-y) Available: https://cdn.tc-library.org/Rhizr/Files/4367e301-0301-4e6f-b2d7-f6a54e794a83/042ef109-e363-4179-a284-4e5be354b67f.pdf [accessed 2 Jan 2021]

the former system, the new regulations confer the Authority with broader competency to pursue violations of both informational rights. Particularly, anyone is entitled to request an investigation from the Authority on the grounds of infringement of data protection law. The Authority is entitled to launch an official data protection procedure if it is presumed that the illegal processing of personal data concerns a wide scope of persons; concerns special data, or significantly harms interests or results in the risk of damages[169]. In order to protect data, the Authority is entitled to decide on several actions. Preferably, it may order the correction of inauthentic personal data; or order the blocking, removal or destruction of illegally controlled personal data. In addition, it is possible for the Authority to order notification of the data subject, should the controller have unlawfully refused to do so. Plus, it can order the disclosure of their decision in the interest of data protection or to protect the rights of a greater number of data subjects. Also, it might prohibit the illegal control or processing of the personal data; and prohibit the transfer of the personal data to other countries; Moreover, a fine may be imposed on, with the range from 100,000 HUF to 10,000,000 HUF; The Authority registers data processing undertaken with respect to personal data in a data protection file or registry in order to assist and enable access to information for the data subject. The Authority is authorised to launch a confidentiality review procedure. The Authority provides a data protection audit as a service on request. This audit is considered to provide a high standard of data protection and security relating to data processing operations. The Hungarian legislation has not reached its peak of its compliance between GDPR and Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act"). Notwithstanding this, there seem to be some developments since the GDPR became applicable on 25 May 2018. Unfortunately, the data controllers may not lay back; there are still many uncertainties in connection with the Hungarian data protection regime. On 20 June 2018, the Hungarian Parliament accepted the first, GDPR-induced amendment of the Privacy Act ("Amendment")[170]. The Amendment still awaits publication; it will enter into force on the day after the date of publication, it finally designates the Hungarian National Authority for Data Protection and Freedom of Information ("Authority") as the proficient supervisory authority with respect

[169] https://www.naih.hu/general-information.html [accessed in 9 Nov 2018]

[170] The Amendment covers a narrower range of topics than the draft modification of August 2017.

to the GDPR[171]. However, even before this, the Authority has taken a few steps to improve the compliance with the GDPR. As one of the steps formed and planned, on 25 May 2018, the Authority published an announcement on its website about the standards to be applied from that date. It was a vital step for the Authority to clarify which legal regulations the Authority uses until the harmonization between the Hungarian data protection laws and the GDPR is completed. As a general rule, regarding the direct applicability and the superiority of the GDPR, the Authority aims to apply the provisions of the GDPR in the first place. However, it is also stated that there are some cases when the GDPR overtly make an allowance for national level regulations, for instance, the processing of private data for journalistic, artistic and academic purposes or literary expression, processing in the context of employment, or its provisions sometimes necessitate the Member States to adapt requirements to enforce the more general rules of the GDPR. This can be seen as the scope of where the Authority proposes to apply the Privacy Act and other, relevant legal regulations, for example, laws on public administration and civil procedure. Besides the aforementioned announcement, the Authority created a private data breach reporting system as well, available on the Authority's website on 25 May 2018. Additionally, another system was planned operational for registering data protection officers as well. The Amendment also includes a provision on the imposition of fines. Not surprisingly, the question of fines has been at the centre of interest since the introduction of the GDPR. In particular, because pursuant to Section 12/A. (1) of Act XXXIV of 2004 on the small and medium-sized enterprises ("SME") and the support of their improvement ("SME Act"), the authorities shall give a verbal notice instead of imposing a fine if the SME in question qualifies as a first time offender. According to the earlier interpretation of both the Authority and the Curia (the Hungarian Supreme Court), this provision applies also in data protection cases. Probably due to the public outcry caused by the Draft, the Amendment takes a third path. The Amendment, referring also to Article 58 of the GDPR, orders that

[171]see also: Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR),
Act CXLL of 2011 on exercising autonomy and the freedom of information;
Act V of 2013 on the Civil Code (hereinafter: Ptk.),
Act C of 2012 on the Criminal Code (hereinafter: Btk.),
Act LXVI of 1995 on Public Records, Public Archives, and the Protection of Private Archives,
Act C of 2003 on electronic infocommunication,

the Authority shall first and foremost give a verbal notice to the data controller or processor in the case of first time offences. Based on the above, we can see that the first steps have been taken towards creating legal certainty. However, the Hungarian data protection situation is far from settled, and the belated reactions from the legislator can cause many difficulties in practice. For instance, many data controllers have prepared their GDPR-compliant policies, notifications and records by now. By adopting a new wave of legal regulations, these documents may need to be modified once again, leading to additional costs for the data controllers.

2.4 The European Data Protection Supervisor (EDPS)

The European Data Protection Supervisor (EDPS)[172] is the European Union's independent[173] data protection authority. Its general task is to monitor and safeguard the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals; counsel/recommend EU institutions and bodies on all matters regarding the processing of personal data, on request or on our own initiative. Particularly, EPDS is consulted by the European Commission on proposals for legislation, international agreements, as well as implementing and delegated acts with influence on data protection and privacy. Also, EPD observes novel technology that might have effects on the protection of personal information, in addition, intercedes before the Court of Justice of the EU to provide expertise on interpreting/inferring data protection law. In order to achieve a greater scope of understanding of data protection, it also collaborates with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal information[174]. Regulation (EU) 2018/1725 sets down the rules for data protection in the EU institutions,

[172]https://edps.europa.eu/about-edps_en [accessed 4 Jan 2021]

[173]In the European Union the requirement for DPAs to be independent: Article 16(2) of the Treaty on the Functioning of the EU (TFEU) and Article 8(3) of the EU Charter of Fundamental Rights. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN [accessed 4 Jan 2021]

[174]Other international instruments: OECD Guidelines governing the protection of privacy and transborder flows of personal data (July 2013)https://edps.europa.eu/sites/edp/files/publication/2013-09-09_oecd-privacy-guidelines_en.pdf[accessed 4 Jan 2021]

OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007)https://edps.europa.eu/sites/edp/files/publication/2013-09-09_oecd_guidelines_en.pdf[accessed 4 Jan 2021]

as well as the duties and powers of the Supervisor (Chapter VI), along with the institutional independence of our supervisory authority.

The EDPS has already presented its vision and strategy for 2020-2024 Strategy: "Shaping a Safer Digital Future: a new Strategy for a new decade" to the public[175]. In an interconnected technological world, where data flows and drifts across borders, unity within Europe, and internationally, might be able to support to reinforce the right to data protection and make data work for people across the European Union and beyond its borders. The Strategy of the EDPS centres on three pillars: foresight, action and solidarity to address digital challenges for a safer, fairer and more sustainable future[176]. One of the EDPS' tasks is to intervene/mediate in cases before the Court of Justice of the European Union (CJEU) and the General Court. It is important to note that there are many ways in which the EDPS[177] can be involved in cases before the Court, such as it has the power to refer a matter to the Court; decisions of the EDPS can be tested before the CJEU; and the EDPS may intervene in cases when these are relevant to his major tasks. Numerous decisions of the EDPS have been challenged before the Court, but the cases were dismissed or withdrawn at an early stage.[178] Regulation 45/2001 Article 47(1)(i)[179], which is to be repealed and replaced with a new Regulation which brings it into line with the General Data Protection Regulation, lays down the right of the EDPS to intervene in actions brought before the CJEU. In its orders of 17 March 2005 in the so-called PNR-cases[180], the CJEU decided that the right of the EDPS to intervene extends to all matters concerning the processing of personal data. In fact, this means that the EDPS' right to intervene in court cases is not limited to cases where personal data has been processed by European institutions or bodies, but extends to all matters effecting the protection of

[175] https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf [accessed 3 Jan 2021]

[176] https://edps.europa.eu/press-publications/press-news/news#news_5895 [accessed 3 Jan 2021]

[177] EDPS is the EU's independent data protection authority

[178] See, for instance, Case -T164/09: Available: https://op.europa.eu/hu/publication-detail/-/publication/9fad0b67-d1f7-4fdf-8d15-8317c960d285/language-en [accessed 4 Jan 2021] and T-237/16 Available: https://op.europa.eu/hu/publication-detail/-/publication/91677a28-a4c1-11e6-8401-01aa75ed71a1/language-en [accessed 4 Jan 2021]

[179] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=EN [accessed 4 Jan 2021]

[180] Available: http://curia.europa.eu/juris/document/document.jsf?docid=57549&doclang=en [accessed 4 Jan 2021]

personal data, either on EU or Member State level. Since privacy is a dynamic and elusive notion that changes through litigation and Court decisions, the EDPS thoroughly monitors the case law of the Court of Justice of the European Union and of the European Court of Human Rights. Though, Europe has a noteworthy legal framework the protection of data, developed around EU Directive 95/46/EC and the Charter of Fundamental Rights, the question of whether data the (EU) protection of data with its legal agenda are up for the challenge has been posed. Cutting-edge and innovative technologies raise major concerns/issues concerning the mainconception of the protection of data/privacy. Dropping prices of storage, growing the performance of chips, the fact that technology is getting gradually implanted and global, the convergence and mergers of technologies and other technological progresses are widening the scope and possibilities of applications fast. Society, nonetheless, keeps changing as well, affecting and effecting the privacy and data protection landscape in their totality. Privacy has been announced and declared dead and governments and policy makers/law-makers sometimes have to to manoeuvre between competing and incompatible purposes and objectives.
The protection of data in the EU is at crossroads and the novel challenge are not only drawing attention to and emphasises on the existing flaws or failings and the predicted complications/concerns, but also, more optimistically, the values and the necessity and requirement for well-built and precise data protection practices and rules in the EU, and in the world.

Chapter 3 History of technology and its regulation:

The concept of privacy has a deep and complex relationship with the history of technology. Throughout the evolution of technology, from ancient times to the modern digital/ age, transformations in technology have both facilitated and challenged/tested our aptitudeor capacity to uphold privacy. The technological challenges provided by technology, especially by novel technologies raise heavy burden on the law: on one hand law is expected to support provisions to ensure that the progress of technology does not undermine the public interests. On the other hand, it also seems obligatory that law does not undermine technological advances/changes. Thus, law is supposed to be responsible for the creation of a link between the technological developments and the welfare of the society. The law is supposed to give adequate legal responses in order to fulfil its

obligation. The key of the proper legal answer does not lies in reprimanding novel technologies simply because they do not always fit to the existing regulatory framework or operate close to a borderline of it. The law needs to create systems of regulations, as a kind of level playing fields between the new and "old"/traditional/existing technologies, thus the history of technology and its regulation may come into the picture as well. Obviously, I do not mean that (old/traditional/existing or) novel technologies do not have to comply with basic regulatory requirements in order to secure the public interests, including, for example, privacy concerns. On the contrary, they are supposed to meet the terms in order to be marketable as well. A pinch of historical insight might help us to understand the way how a great variety of emerging technologies, such as,synthetic biology and bio/nanotechnology, are expected to alter society. Coping with the advancement and regulation of these promising technologies is an overwhelming "mission" as the risksexisting may not be understood til the technologies are further developed. Gregory N. Mandel, for instance, suggests aninnovative governance model that attempts to handle the dynamic of emerging novel technology promise versus risk by moving the point of first governance earlier in a technology's development, but allowing the governance structure to evolve after formation. His model aims to turn some of the greatest challenges of managing emerging technologies, for example, scientific uncertainty and the disruption of extant regulatory systems, on their head to create incentives for widespread stakeholder cooperation to produce more proactive, flexible governance[181]. Since policy makers struggle to develop regulatory oversight models for nanotechnologies, there are essential lessons that need to be drawn from previous efforts to administer and regulate other emerging technologies. According to Marchant GE, Sylvester DJ, Abbott KW, there are five such lessons to be named, these are the following: firstly, public confidence and trust in a technology and its regulatory oversight is probably the most important factor for the commercial success of a technology; the second is that regulation should avoid discriminating against particular technologies unless there is a scientifically based rationale for the disparate treatment; the third is that (any) regulatory systems need to be flexible and adaptive to rapidly changing technologies; the fourth, ethical and social concerns of the

[181]MANDEL, Gregory N:*Regulating Emerging Technologies*. Law, Innovation & Technology, Vol. 1, Iss. 1, 2009, 75, (Doi: 10.1080/17579961.2009.11428365)Available: SSRN: https://ssrn.com/abstract=1355674. [accessed 20 Jul 2020]

public about emerging technologies need to be expressly acknowledged and addressed in regulatory oversight; and the last one is that international harmonization of regulation may be beneficial in a rapidly globalizing world[182].

3.1 Technology in the twentieth and the twenty-first century:

To write about recent history is extremely problematic, because of the number of material to deal with and the problem of distinguishing the noteworthy and relevant from the insignificant among key events that have virtually the power of contemporary experience. However, one fact remains clear: despite of the colossal progresses of technology by 1900, the following decades witnessed more advance over many activities than the whole of previously recorded history. The list may go on and on but what might stand out, for example, the aeroplane, the rocket and interplanetary probes, electronics, atomic power, antibiotics, insecticides, and a lot of new materials (some even survived the tests of time, some did not, for instance, asbestos) have all been invented and industrialised to create an unequalled and never seen social situation, jam-packed of possibilities and dangers, which would and could have been virtually unimaginable before the present century. Some of them were actually declared to be only the work of fiction as well.[183][184] In the development of liability in relation to technological progress, for instance, one of the most disturbing and striking examples has been the case of the "magic mineral," and, with

[182]MARCHANT, Gary E. – SYLVESTER Douglas J. – ABBOTT Kenneth W.:*What does the history of technology regulation teach us about nano oversight?*The Journal of Law, Medicine & Ethics,Vol. 37, Iss. 4, 2009, 724-731(doi:10.1111/j.1748-720X.2009.00443.x.) https://pubmed.ncbi.nlm.nih.gov/20122112/[accessed 20 Jul 2020]

[183] See, for example, FOX, Robert: *Technological Change: Methodsand Themes in the Historyof Technology.* New York, Routledge, 1998. and BRAY, Francesca and Arnold Pacey:*Technology in world civilization: a thousand-year history.* Cambridge,MIT PRESS, 2021. Their book is considered to be a milestone in the history of technology with a global view on several case studies. The authors intend to challenge the cocept of technology transfer by introducing the term technological dialogue.

[184] The history of technology is the history of the invention of tools and techniques and is similar to other sides of the history of humanity. Technology can refer to methods ranging from as simple as language and stone tools to the complex genetic engineering and information technology that has arisen even as early as the 19th century, or even earlier depending on the definition. New ideas, notions have enabled people to create innovative things, and conversely, several scientific activities are made possible by technologies which help transportation of both people and goods to destinations they could not previously reach, and by scientific tools/instruments by which scholars could study nature in more detail than our senses can allow. Since much of technology is seen as applied science, technical history is linked to and associated with the history of science. Since technology uses resources, technical history is tightly related to economic history. From those resources, technology produces other resources, including technological artefacts used in everyday life. Technological change affects, and is affected by, a society's cultural traditions. It is a force for economic progress and a means to promote and support economic, political and military power.

no doubts, has not even ended. It was hailed as a novel technology and asbestos was commonly applied in a great variety of industries such as engineering, road construction, rail, power and shipping, predominantly in the UK from the 1940s to the 1970s.

But it is a fact as well that French authorities responsible for inspecting factories pointed out that workers dealt and work with asbestos suffered from respiratory problems, mainly, that of the lungs[185]. Also, one of the royal orders in 1909, Italy, forbade the employment of women and children in factories using asbestos, only some exceptions were made under some conditions[186]. Some decades later, in 1931, one of the statutory orders in the UK[187], Asbestos Industry (Asbestosis) Scheme 1931. No. 344, attempted to further regulate and standardize the asbestos industry. Though, after not too much time it turned out to be that asbestos carry significant health risks, basically an extremely high risk. It is not negligible that asbestos breaks easily into a dust composed of tiny particles that can float in the air and stick to clothes. The fibres can easily be inhaled or swallowed and are able to cause several serious diseases, including cancer and other illnesses, mainly of respiratory in nature, the lungs and chest. What seems even more important to observe that Asbestos-related diseases have long latency periods: characteristically ten to twenty years for asbestosis and anywhere from 20 to 50 years for mesothelioma and lung cancer. Consequently, claims in the UK arising from exposure to asbestos in the post-war years are now rising and are estimated and supposed to continue to rise until about 2020[188]. In the US, an estimated 80% of all companies are assumed to be exposed to asbestos liabilities to some degree and an escalating number are fighting for survival because of this. It can be stated that In Europe, claims have been lower than in the US or the UK, in some cases because of state compensation systems. However, this might change in the future.

---

[185]MARTIN-CASALS, Miquel: *The Development of Liability in Relation to Technological Change*.Cambridge University Press, 2010, 19-20.

[186]FAVILLI, Chiara:*Technological Change in Italy*.In: MARTIN-CASALSop. cit.213.

[187]https://www.legislation.gov.uk/uksro/1931/344/pdfs/uksro_19310344_en.pdf[accessed 23 Jul 2020]

[188]The long-lasting effects of this (novel) technology for the rights of individuals has left its mark as well, since Asbestos-related diseases have long latency periods, and cases keep coming up.

To found out more, one can visit many sites, for instance:

https://www.tbilaw.co.uk/site/asbestos-injuryclaims/?gclid=CjwKCAjwm_P5BRAhEiwAwRzSO36v80oozddEEv6yI7t2bFGwJxhNn1HnKjo7GaE-g1OAF3xIewN4ABoC4ycQAvD_BwE# or
https://www.stephensons.co.uk/site/news_and_events/archivenews/asbestos_legal_risks or
https://www.slatergordon.co.uk/personal-injury-claim/industrial-disease/asbestos-mesothelioma/asbestos-regulations/

Companies that used asbestos in the past can therefore reliably expect a surge in the number of claims they (may) receive and, to the extent that they have not already done so, should consider the measures essential to manage their potential liability[189].Even nowadays it can be stated that Asbestos-related industrial disease claims are still on the increase in countries such as the UK and the US, and could affect a company's survival. But companies are able to manage their potential liability with obtaining country-specific information on asbestos legislation[190]. In addition to the formerly mentioned facts, there are attempts to solve" asphalt issues by testing the Control and Product Acceptance of Asphalt-Treated Cold Recycled Pavements. One of these efforts is the proposal of the National Academies of Sciences, Engineering, and Medicine.[191] It may suggest us that these regulation might have changed even more than I have already assumed by pointing out that asphalt related cases go back to 50 or so decades.

In daring to understand the (main) events of the 20th century with regard to the revolutionary progress of technology, I claim that it will be suitable to distinct the years before 1945 from those that followed. It seems crucial since the years 1900 to 1945 were undoubtedly dominated by the two World Wars, while those since 1945 were preoccupied by and spent on the urgent need to avoid another world war. With no doubt, the dividing line is one of the most outstanding social and technological importances: the detonation of the first atomic bomb[192] at Alamogordo, N.M., in July 1945. The reaction of the world was a shock[193] and the political changes were profound in the 20th century connected to technological capacity and leadership (potential).

James E. McClellan, Harold Dorn argue that "[t]he development and use of the atomic bomb by the USA during World War II marks a watershed in the history of modern science and technology. The reasons are twofold. One, the case dramatically revealed the

[189]https://uk.practicallaw.thomsonreuters.com/01029187?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 [accessed 9 Aug 2020]

[190]https://uk.practicallaw.thomsonreuters.com/01029187?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 [accessed 9 Aug 2020]

[191]National Academies of Sciences, Engineering, and Medicine. *Proposed AASHTO Practice and Tests for Process Control and Product Acceptance of Asphalt-Treated Cold Recycled Pavements*. The NationalAcademies Press, Washington DC, 2020(https://doi.org/10.17226/25971).

[192] See also, https://www.thoughtco.com/search?q=history+of+regulation [accessed 23 Jul 2020]

[193]EDGERTON, David: *The Shock of the Old: Technology and Global History since 1900*. Oxford University Press, Oxford, 2006.

practical potential of cutting-edge science or what could emerge from turning theory directly to useful ends. Second, it demonstrated what might be forthcoming when government supported largescale scientific research and development (R&D) with abundant resources. The novelty of the atomic bomb case—and what it portended for the future of science and technology in the second half of the twentieth century—stemmed from the combination of these two factors: large-scale government initiatives to exploit scientific theory for practical ends. It set a new pattern that changed not only traditional relations between science and government but how we think about applied science in general."[194] The war production of World War II and the years of reconstruction of Europe enabled the United States to rise as a super state, and the rise to its full potential and its glory was sufficiently fast and dramatic. The basis of this fast-pacing progress can be related to the incredible amount of natural resources exploited to guarantee the ongoing increase of productivity through extensive industrialization. The success of the United States in achieving this goal was tested and demonstrated in the two World Wars. Thus, it is not a surprise that the so-called technological leadership was passed from Britain and the nations of Europe to the USA in the course of these wars and after the years of wars. Although it does not mean that innovation ceased to exist and dried out in Europe. Several significant inventions of the 20th century originated there, but without the sign of dominance. But it was the United States that had the capacity to integrate and embrace innovations and take full advantage from them when other countries were incapable of supplying the vital (social or other) resources without which brilliant ground-breaking inventions cannot be converted into a land sliding commercial success. Similarly as the Industrial Revolution in Great Britain, the technological vigour of the United States in the 20th century was revealed less by any particular innovations than by its ability to adopt novel and original ideas from whatever source they might come[195]. Undoubtedly, the two World Wars were themselves the most significant mechanisms of technological as well as political change in the 20th century. The rapid (r)evolution of the airplane is one of the striking examples of this progression, while the introduction of the first prototype of the

[194]MCCLELLAN– DORN: *op. cit.*, 393.

Ebook.available:https://books.google.hu/books?id=YnqLfVRJ3AkC&printsec=frontcover&hl=hu&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [accessed 23 Jul 2020]

[195]https://www.britannica.com/technology/history-of-technology/The-20th-century#ref14881[accessed 23 Jul 2020]

tank in the First World War and of the atomic bomb in the second demonstrate the same signs of response to an urgent military incentive. It has been claimed that World War I was a chemists' war, on the basis of the immense importance of high explosives and poison gas, although it is often called "trench war". In other respects the two wars rushed the development of technology by extending the institutional apparatus for the encouragement and support of innovation by both the state and private industry. This process was dealt with different issues in the world and could go further in some countries than in others, but no major nation could resist wholeheartedly the need to support and coordinate its scientific-technological effort. The wars were thus responsible for speeding the transformation up from "insignificant science," with research still largely restricted to small-scale efforts by a few isolated scientists, to "real science," with the stress on large research teams sponsored by governments and corporations, working collectively on the development and application of new techniques and novel technologies. While the extent of this transformation should not be exaggerated, and recent research has tended to focus on the on-going need for the independent inventor at best in the stimulation of innovation, there could be little doubt that the change in the scale of technological enterprises had extensive and long lasting consequences. It was one of the most historic transformations of the 20th century, for it transformed the quality of industrial and social organization. In the development it secured technology, for the first time in its long history, a position of significance, reputation in social esteem.[196] Also, Daniel R. Headrick states that Today technology has created a world of stunning progress, growing inequalities of wealth and poverty, and imminent threats to the environment all over the world. His book, *Technology: A World History* offers its readers an enlightening source of background to our present moment, a fascinating history of invention around the world. In tracing the rising power of humans over nature through powerful innovations, he compares the progress of technology in different parts of the world, as an attempt to provide a much broader version than can be found in other histories of technology. He offers a fascinating

[196]https://www.britannica.com/technology/history-of-technology/The-20th-century#ref14881 [accessed 23 Jul 2020]

look at the spread of inventions around the world, both as boons for humanity and as weapons of destruction[197].

Also, David Edgerton states that from the books of H.G. Wells to the press releases of NASA, we are crammed with clichés about technology and history. He offers a surprizing new and different way of thinking about the history of technology, radically revising our notions and concepts about the interaction of technology and society (and by implication the regulation of technology as well) in the past and in the present. Since, as he argues, Modern technology is not just a matter of electricity, mass production, aerospace, nuclear power, and the Internet. It also includes the rickshaw, the horse, corrugated iron, cement, DDT, small arms, flat-pack furniture and the refrigerator. *The Shock of the Old* challenges us to view the history of technology in terms of what everyday people have actually used/applied and continue to use around the world, rather than just what was invented. The wide range of technological progress can be seen, for example, if one takes a look at the following list..The US National Academy of Engineering[198], by expert vote, established the following ranking of the most important technological developments of the 20th century: electrification, automobile, airplane, water supply and distribution, electronics, radio and television, mechanized agriculture, computers, telephone, air conditioning and refrigeration, highways, spacecraft, Internet, imaging technology, household appliances, health technology, petroleum and petrochemical technologies, laser and fibre optics, nuclear technology, materials science.

It could also be seen that many highly praised and advertised technologies, from the V-2 rocket to the Concorde jet, have been costly fiascos. On the other hand, corrugated iron emerges as hugely important, a truly global technology. Its cheapness, lightness, ease of use and long life made it a universal material in the poor world in a way it never had been in the wealthy or wealthier part of the world. Edgerton reassesses the significance of such acclaimed inventions as the Pill and IT, and emphasizes the continued importance of

[197]HEADRICK, Daniel R.: Technology – A World History. Oxford University Press, New York, 2009. https://cryptome.org/2013/01/aaron-swartz/019515648X.pdf[accessed 5 May 2019]

[198]The National Academy of Engineering (NAE) is an American nonprofit, non-governmental organization. The National Academy of Engineering is part of the National Academies of Sciences, Engineering, and Medicine, along with the National Academy of Sciences (NAS), the National Academy of Medicine, and the National Research Council. To get more information, visit: https://www.nae.edu/ [accessed 23 Jul 2020]

unheralded technology, demystifying the idea that we live in an era of ever-increasing invention and casting doubt upon the many naïve claims about "the information age[199].

3.2 Technological society and the ever-present dilemma(s) oftechnology:

The overwhelming trust and optimism of 19th-century about the progress of technology has disseminated, and a growing awareness of the technological dilemma(s) challenging the world makes it probable to offer a novel and more realistic assessment of the role of technology in shaping society in recent days. Whatever the responses to modern technology may be, there cannot be doubt that it presents contemporary society with several urging and immediate difficulties that can take the form of a traditional choice of evils, so that it seems appropriate to consider them as constituting a "technological dilemma." This is the dilemma between, on the one hand, the (over)dependence of life in the advanced industrial countries on technology, and, on the other hand, the threat that technology could demolish or alter the quality of life in "modern" society and even jeopardise society itself. Technology thus confronts Western civilization with the need to make a decision, or rather, many consecutive decisions, about how to use the enormous power available (by the progress of technology) to society constructively rather than destructively[200]. The need to control the expansion and progress of technology, and so to solve the dilemma, by regulating its application to creative social objectives, makes it essential to define these objectives while the problems presented by rapid technological development could be resolved.

3.3 The need for the interactions between society and technology and the alleged autonomy of technology

First, it is noticeably recognized that the relationship between technology and society is complex. Also, there is no doubt that any technological incentive may or can, and as a matter of fact, will activate a wide range of social responses, depending on such random variables as differences between human personalities; also, no specific social

[199]EDGERTON, David op. cit.

[200] Although I mostly use dichotomies to present some major points, I am fully aware of the multifaceted and multifocal nature of these complex issues.

situation could be relied upon to produce a determinable technological reaction, put it simply. Thus, one may state that any "theory of invention," is supposed to stay tremendously cautious, and any concept or view of a "philosophy" of the history of technology must allow for a great variety of probable (and promisingly well-based) interpretations. One of the major lessons learnt of the history of technology, indeed, is that it is impossible to offer (any) accurate predictive value. What one can often see in retrospect when one particular artefact or process reached its peak of usefulness and becoming useless while another promised to be a highly successful innovation, but at the moment no such historical observation is accessible or exist and the course of events cannot be determined. In brief, the complexity of human society has not been able to resolving into a simple identification of causes and effects driving historical advance of an event or events in one direction rather than another and any effort to identify technology as an agent of such a process is not acceptable[201]. Secondly, the definition of technology as the systematic study of techniques for creating and doing things makes or offers technology a status as a social phenomenon and thus as one that could not have full autonomy, unaffected by the society in which it exists. It is vital to make what might seem to be such an obvious statement because so much autonomy has been credited to technology, and the element of anguish in interpretations might come from an exaggerated view of the power of technology to determine its own course apart from any form of social control[202]. Of course, it must be acknowledged that once a technological progress, such as the transition from sail to steam power in ships or the introduction of electricity for domestic lighting, is confidently recognised, it is impossible to put a halt to it before the process is thorough. The rally of resources and the arousal of expectations both can create a certain technological momentum that appears to have a tendency to prevent the process from being arrested or ricocheted. Nonetheless, the decisions made about whether to go ahead with a project or to abandon it are indisputably human. In itself, technology is neutral and passive: it was naive for 19th-century optimists to imagine that technology could create paradise on Earth; it looks similarly simplistic for pessimists today to make

[201] https://www.britannica.com/technology/history-of-technology/The-technological-dilemma [accessed 23 Jul 2020]

[202] See, for example, ELLUL, Jacques: *The Technological Society*. (Trans.) John Wilkinson. Knopf,New York, 1964. London: Jonathan Cape, 1965. Rev. ed.: New York: Knopf/Vintage, 1967. with introduction by Robert K. Merton (professor of sociology, Columbia University).

technology itself a scapegoat for human flaws. Thus my assumption and solution I attempt to highlight throughout my dissertation is for the reconciliation between technology (or technologies) and "the human factor" is regulatory in nature but technical in its practicality. To sum up the complex relationship between technology and privacy one may assume that the concept of privacy has been profoundly linked and tied to the history of technology. Technological progresses have both improved (sometimes boosted and worn downor eroded privacy, and society has had to become accustomed to it through intricate legal and ethical frameworks/agenda to create a kind of equilibriumor delicate balance between the benefits of technology and privacy. Though, we can also state that this relationship cannot be portrayed as static, since this dynamic and vibrant liaison has never stopped to advance and keeps on evolving as technology advances further.

"*It is change, continuing change, inevitable change that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be....*" - Isaac Asimov

Chapter 4 Regulation of technology: past and present:

The allocation/division and application of new technologies is habitually escorted byuncertainties and doubts as to their long-term (un)projected-un(anticipated) or unwelcomed impacts, regarding almost all walks of life, including, for instance, law/regulation, privacy or environmental protection and so on. New technologies also pose enquiries (and a considerable amount of concerns) about the restrictions of the law as the line between injurious/damaging and optimistic/constructive effects is recurrently difficult to draw, and even to find. Still, I assume that the necessity to regulate and to revise regulations time after time cannot be questioned, although the way how to do it may differ, due to different norms in combination with cultural differences between countries seem to result in variances in the (practical) enactment, understanding and enforcement, not to mention compliance as well[203]. It seems even more burdensome for scholars to agree on an issue, such as regulation. Ronald Leenes, for instance, states that "[a]nytime a new

[203]Compliance is one of the major topics in the European Union but this dissertation will not go into this topic wholeheartedly, but to scratch its surface is unavoidable.

technology materializes, or when innovators and entrepreneurs come up with a novel way of doing business, calls for regulatory changes can be heard. These voices do not only come from students and Ph.D. students, who by definition still have a lot to learn, but also from developers, engineers, policymakers, and the odd scientist, who may quickly arrive at the conclusion that there is a regulatory disconnect in need of fixing"[204]. As it can be found in the introduction, several people appear to experience the *Flawed LawSyndrome*: the (instantaneous) push for calling regulation or lawobsolete, invalid or flawed (disengaged) and the craving to patch up the nuisances/troubles by concentrating on the law, rather than using other ways to fix the supposed gaps ('Legal Solutionism)"[205]. Visibly, the "other side", the industry possibly willprowelltestas that the law necessary to be (re)formed or improved. Industry characteristically comes up with two claims relating to the framework of regulationin their own field: first, that they are excessively and unreasonablycontrolled and, second, that the rules are unclear/blurred or inexact, two of my major goals are, firstly,to examine why this ambiguity and elusivenessmight and can occur, and secondly, is to relate this uncertainty and ambiguousness to new technologies, such as biometric systems, drones, Artificial Intelligence, and so forth with the purpose to uncover some practical resolutions. The response to make complaints about and object to the framework of the regulation appears to be amechanical/routin reaction (of any sides) whenever a new technology sufaces, rather than investigating the actual state of the art in connection with the technology and the law[206]. A number of scholars assume that the next on the agenda might and could be robotics, almost certainly, right after, drones, biometrics/biometric systems, ÍCT, bio/nanotechnology, and neuroscience-associated technologies, since robotics can be regarded as as a next key field of technological progress that necessitates

[204]BROWNSWORD, Roger: *Rights, Regulation and the Technological Revolution*. Oxford University Press, Oxford, 2008. (Doi: https://doi.org/10.1093/acprof:oso/9780199276806.001.0001)

[205]LEENES, Ronald: *Regulating New Technologies in Times of Change*. In: REINS, Leonie (Ed.): *Regulating New Technologies in Uncertain Times*. Springer, The Hague, 2019, 5-6.(Doi: https://doi.org/10.1007/978-94-6265-279-8_1)

[206] For instance, in the case of robotics, one can learn more info by:LEENES, Ronald – PALMERINI, Erica – KOOPS, Bert-Jaap [et. al.]: *Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues*. In: Law, Innovation and Technology, Vol. 9, Iss. 1, 2017, 1-44. (Doi: 10.1080/17579961.2017.1304921)Available:https://research.tilburguniversity.edu/files/23365230/Regulatory_challenges_of_robotics_some_guidelines_for_addressing_legal_and_ethical_issues.pdf [accessed 26 Aug 2020] or Zsolt Ződi (2018): *Platformok, robotok, jog*: *Új szabályozási kihívások az információs társadalomban*. Budapest: Gondolat.

the attention of regulators.[207][208]What can tie all these forms together is a sense that the technologicalproducts show some level of autonomy in their functioning[209], which gives aninnovative rim to the interaction-communication between humans and technology; and it is thischaracteristic, for example, that makes robotics as a significant field for regulatorsand regulation scholars to study. Also, the questions, posed by Ronald Leenes, Erica Palmerini, Bert-Jaap Koops, Andrea Bertolini, Pericle Salvini and Federica Lucivero seem even more appropriate: "Are our existing normative frameworks adequate to deal with developments in robotics? Can new robotic technologies, particularly if they feature increasing levels of autonomic behaviour, be regulated within existing legal and ethical frameworks, and if not, should existing laws be made more generic so that provisions also encompass robotic technologies, or should we rather aim for sui generis laws for robots? And are fundamental assumptions underlying regulatory frameworks, such as a very generic distinction between 'things' and 'humans', sustainable in the longer term, if (bio)robotic applications are increasingly built into human bodies?[210]. Of course, these are merely some of the more general, but major questions that the advance of robotics raise, though I may add that those questions, with the specifications related to other technologies, also makes sense, for instance: Are the existing normative frameworks satisfactory to deal with expansions in the field of drones? In order to map the main regulatory challenges of robotics, scholars collaborated in the RoboLaw project, which was the first research project completely devoted to the study of law and robotic technologies to obtain funding from the European Commission research framework programs[211]. As one can see the ongoing "project" of regulation never really stops, owing to the fact(s) that, firstly, even if a novel (might be better) regulation is introduced, some will complain with feeling dissatisfied with the outcome of the law. Secondly, due to the unstoppable nature of the progress of technology, regulation may not come as soon and as smoothly as the situation may require. One of the best examples is, with no doubts, is data protection regulation. Though I devote attention to data protection in the dissertation, here, I add that after years of hard and

[207] For example:LEENES – PALMERINI – KOOPS [et. al.]: op. cit., 1-44.

[208] As a matter of fact, the European Parliament, Committee on Legal Affairs drafted its first report with recommendations to the Commission on Civil Law Rules on Robotics on 27 January 2017 (2015/2103(INL)).

[209] The question of aautonomy is one of the major motivators of debates concerning AI, robots, or drones as well.

[210]LEENES – PALMERINI – KOOPS [et. al.]: op. cit.: op. cit., 3-4.

[211]To get to know more, visit:www.robolaw.eu. [accessed 26 Aug 2020]

demanding negotiations, including the diverselaw-makingphases, the European Parliament processed over 4000 amendments to the original Commission proposal for GDPR and new regulation was lastly agreed on[212][213][214]. The GDPR is an extensive, lengthy and some say it to be too complicated law. The reason is, maybe, that it consists of 99 Articles and a 173-section Preamble, though, the complaints about it based on the fact that there are only a few useful and significant summaries. Also, I argue that the division and distinction between privacy law and data protection law is essential. As Gloria González Fuster arguesthe GDPR is a data protection law, and data protection and privacy are not the same thing[215]. A tension created by their entanglement often creates long term debates with no satisfaction on both sides. As I have already stated, regulators, in this case as well, cannot satisfy each and every players of the IT market, for example, the Net moguls of Facebook raised their immediate concerns[216], with Facebook, (and others, like Twitter) Google has been involved in legal struggles with the DPAs even founded on the previous Data Protection Directive 95/46/EC[217]. But the clash of the titans may never end, even if Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealed Directive 95/46/EC GDPR[218], the battle between the DPAs and the giants using, inventing or promoting technology or its rapid progress. Also, it can be seen that GDPR is a Continental "product" of regulation (itself a technology) with relevant shortcomings.

The GDPRin the EU went into effect in May 2018, it has influence on companies, firms, individuals, and (all the) countries in the world. It provided many issues and concerns as well. Meg Leta Jones and Margot E. Kaminski argue that "[it] is long and notoriously complex. A number of helpful and influential practical overviews exist. None

[212]For an outline of the amendments, see https://lobbyplag.eu/map/amendments/libe/ [accessed 26 Aug 2020]

[213] The first COM proposal of the GDPR (2016/679) was published on 25 January 2012, it entered into force on 24 May 2016 and became directly applicable in all EU Member States on 25 May 2018.

[214]HOOFNAGLE– VAN DER SLOOT– ZUIDERVEEN BORGESIUS: op. cit.

[215]See, for example: GONZALEZ FUSTER, Gloriaop. cit.

[216]https://edri.org/our-work/edrigramnumber10-22facebook-doesnt-like-eu-regulation/[accessed 26 Aug 2020]

[217]See, for example: DREYFUSS, Joel: *EU privacy rules may hit Internet giants hard*. Available: https://www.cnbc.com/2016/02/01/eu-privacy-rules-may-hit-internet-giants-hard.html[accessed 26 Aug 2020]

[218]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN[accessed 26 Aug 2020]

of these overviews, however, has squarely taken aim at what we understand to be the most significant hurdles for U.S.-based readers. Understanding the GDPR requires knowing not only what it contains, but how to read it, and a basic understanding of both data protection and broader European law"[219]. Also, they intend to "correct" some shared misunderstandings surrounding the GDPR: that it is not based on individual consent; that it's about privacy, but, rather it is basically about the protection of data; and that it is not predominantly about the rights ofindividuals and control because it turns out to be just as much about risk management and corporate compliance[220]. And, I need to add that compliance, as one of the major issues, is mostly the heart of the debates among EU member states and EU institutions. In addition, Meg Leta Jones and Margot E. Kaminski claim that "[f]irst, the GDPR is based on fundamental rights, which, in Europe, entail protections provided by the state, not just restrictions on the state. Second, data protection in Europe is importantly distinct from privacy and consumer protection laws, which have their own set of rules and regulations that interact with GDPR. Third, the GDPR harmonizes data protection across EU countries, but much is still left to Member States. As such, domestic law and politics remain relevant to understanding the GDPR and European data protection. Fourth, the GDPR is better understood as a process, not a law. To claim to be able to automate GDPR compliance, or provide a clear checklist, is to misrepresent the nature of the law[221]. Also they go as far as to argue that "[d]ata protection is not: (a) a primarily consent-based or notice-and-choice-based regime, or (b) a regime where individuals have absolute control over their data"[222].

Obviously, the Internet is one of data and novel IT innovative technologies, thus its pace is almost beyond understanding. But, the question remains: how can authorities regulate a technology so elusive in nature? The answer has been given several times, one of them is by David R. Johnson and David G. Post, they debate and examine four basic competing models for the governance of the global Net: The first one is that existing territorial sovereigns can merely intend to extend their jurisdiction, and to amend their laws as required, to make a burdensome effort to govern all actions on the Internet that have

[219]JONES – KAMINSKI: op. cit.

[220]JONES – KAMINSKI: op. cit., 1-2.

[221]JONES – KAMINSKI: op. cit.,4-5.

[222]JONES – KAMINSKI: op. cit.,5.

considerable significant impacts on their own citizenry[223]. Second model is that sovereigns decide to enter into multi-lateral international agreements to create and institute new and uniform rules definitely applicable to the "behaviour" on the net. The penultimate one is the foundation is a novel international organization. The role of it is to endeavour to create new rules, and new ways/means of enforcing those rules and of holding those who make the rules accountable to right constituencies. The last one is the 'decentralized emergent law' the idea that actual rules might arise due to the multifaceted and intricate interplay of individual decisions by domain name and IP (Internet Provider) address registries, concerning what circumstances/terms to impose upon possession of an online address, by sysops[224] ,concerning what local rules to adopt, what filters to install, what users to allow to sign on, and with which other systems to connect, and by users as regards to which personal filters to install and which systems to utilize[225]. The last one can be identified as a form of collective action proposed including a voluntary approval of standards based on private law principles. David R. Johnson and David G. Post also posit that 'the technical protocols of the net have in effect created a complex adaptive system that produces a type of order that does not rely on lawyers, court decisions, statutes, or votes'[226].

Regulation might be able to inhibit/obstruct or motivate technological change(s) or even a (full-scale) revolution. This unusual (and often uneasy) relationship does depend on the technology/expertise of regulation, namely, the choice of design and instrument of regulatory policy. I attempt to examine some morsels of the history of regulations over the last three decades, the explanatory power of theories of regulatory politics, the choice of regulatory apparatuses, the assessment of regulatory influences/effects, and the impact of each of these on the innovation/invention and diffusion of technology and, by implication,

[223]This is the way how, for instance Donald Trump imagines the regulation in order not to give too much power away over the US citizens.

[224]A sysop is the person who runs a computer server . In general, a sysop or system operator is one who runs the day-to-day operation of a server and the term suggests a person who is available when the system is.

[225]JOHNSON, David R. – POST, David G.:*And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized*,*emergent Law*. In: KAHIN, Brian - KELLER, James H.: *Coordinating the Internet*. MIT Press, Cambridge MA, 1997.(Doi: https://doi.org/10.7551/mitpress/2170.003.0007) Available online at: www.temple.edu/lawschool/dpost/writings.html#RecentWritingsAlso see:JOHNSON, David R. – POST, David G.: *Law and borders: the rise of law in cyberspace*. Stanford Law Review,Vol. 48, No. 5, 1996,1367. (Doi: https://doi.org/10.2307/1229390) Available: https://www.jstor.org/stable/1229390?origin=crossref&seq=1[accessed 27 Aug 2020]

[226]JOHNSON– POST: op. cit.

of regulation. Ultimately, I venture to conclude with recommendations for the future of regulation and technology in relation to concerns of privacy, with bearing in mind that there are cultural and legal differences to be (re)considered and brought to the surface. Technology and regulation are frequently perceived and depicted as opponents or oppositions. One can observe that technology frequently symbolizes diverse sorts of markets, enterprises, and development, whilst regulation represents government, administration (and its apparatus), and limitations to growth and improvement. Jonathan B. Wiener argues that "[t]he modern regulatory era, beginning in the 1960s, has regularly pitted calls to restrain technological risk through regulation against the competing concern that regulation could unduly hobble new technology and progress. In the 1970s that debate focused on technologies such as nuclear power, supersonic transport, and food additives. Today the debate continues as fears of technologies such as electromagnetic fields, greenhouse gas emissions, and genetically modified foods spark new calls for precautionary regulation[227]. Also, in the 1980s the so-called space technology started to bloom, and in the 1990s[228] technologies using virtual space started their march[229][230]. As a matter of fact I also include telephones/cells, drones biometric systems, robots, AIs, too. Regulation is usually depicted as a single kind of rule or strategy. Jonathan B. Wiener states that "regulation is treated as if it comes in one type and has only one effect on technology, like an engine transmission that can shift into only forward or reverse. In reality, just as there are many different types of technologies[231], one might be able to identify various sorts of regulations, for example, one may list different regulatory apparatuses and mechanisms, such as requirements for technology, performance standards/criteria, taxes, tradable allowances, and disclosure of info, are supposed to have diverse effects on technological progress, and there may be other significant consequences,

[227]WIENER (2004): op. cit., 443.

[228]*The Regulation of Scienceand Technology* (Studies in Regulation), edited by Helen LAWTON-SMITH, offers us a unique set of perspectives on a different regulatory mechanisms set out to achieve this. The contributors use and rely on a large amount of data and analysis to give a critique of political, economic, ethical, technological, and geographical issues connected to the allocation of resources to science and technology, the control and use of the information generated in the context, and the operation of regulatory agencies.

[229] See, for example:KLEMENS, Guy: *The Cell phone: The History and Technology of the Gadget That Changed the World*. McFarland and Company, Inc., Publishers, London, 2010.

[230] To get more on AIs, MALOOF, Mark:*Artificial Intelligence: An Introduction*. Georgetown University, Washington DC, 2017.visit: http://people.cs.georgetown.edu/~maloof/cosc270.f17/cosc270-intro-handout.pdf[accessed 27 Aug 2020]

[231]WIENER (2004): op. cit.,443. see also: BUNCH – HELLEMANS: op. cit., or MCCLELLAN– DORN: *op. cit.*

concerning, for example,issues and concerns related to privacy or/and propety. Thus, a combination of one or two (or even more) is often chosen and formed in order to fill gap of regulation as soon as possible with more or less success till another but vaguely similar (novel) tech set its foot on the market. But, to clarify my purpose again, I do not state that legislators or policy makers are to be blamed, quite the opposite, I mean to emphasize the fact that this difficulty is embedded in the nature of the complex connection between technology and law/regulation. Certainly, if technology is understood in its broad sense, as not just hardware or equipment/tools or cogs or chips, but as any device or system for converting inputs into outputs, for changing the production function, then regulation itself can be considered to be a kind of a technology. If one attempts to define regulation, it can be a set of methods or procedures for changing production functions to produce fewer of some outputs, such as, for instance, air pollution or intrusion of privacy. It seems that regulation is the technology of governance. Not to mention the point that the terminology that scholars examining regulation(s) use to analyze invokes the formerly mentioned technological, for example, 'instrument choice' as in medicine or music, of choosing' 'policy tools' from the ''regulator's toolkit'', and of' 'reinventing government' to accomplish goals more fruitfully. The influence of regulation on technology critically rely on the technology of regulation[232]. Different regulatory strategies can obstruct or accelerate technological transformation or (r)evolution, or (re)form it in many ways, favouring some categories of technology over others[233]. Though his argument is well-based, others may opt for a different approach, for example, Anne Chapman argues that "[i]n recent decades protests have generally been regarded as being about the risks associated with a technology: industry and government portray the public as being concerned about the risks of physical harm, to people or to the environment, posed by a technology. Risk assessment has become the dominant framework within which regulators consider technological developments. However, while people often are concerned about risks, it is apparent from the debates about genetic engineering that risks of physical harm are not the limit of their concerns. Debates have also raised issues about the power of multinationals, the direction of agricultural development, food security, the preservation of biodiversity and how we

[232]See more on the the effect on both: SCHWARTZ, Robert A. – BYRNE, John Aidan – COLANINNO, Antoinette (eds.): *Technology and Regulation: How Are They Driving Our Markets?*Springer, New York, 2009. (DOI 10.1007/978-1-4419-0480-5)

[233]WIENER(2004): op. cit. 443-445.

should be relating to other living organisms. For that reasonit seems apparent that one needs to get free of the narrow confines of risk assessment and extendto an enlarged framework for considering, weighing up and measuring technology in the context of public policy[234]. Also, one may pose the question: Is the kind of regulatory tool important? Does it matter anyway? Yes, it is. It does matter, indeed.[235] The requirements connected to technology are thought to embrace the intention to "force" industry to upgrade or to improve, and might foster the distribution of existing technology throughout the entire sector of industry. But then again, paradoxically, it also has an effect that may dishearten or stagnate innovation of novel technologies by (over)specifying a certain technology and promising or assuring no driving forces or supports for advancing progresses[236]. As soon as constraints are authorised, the actors of that particulararea have even fewer motivations (and reasons) to create anenhanced or superior method. The reason is that the government is characteristically lags behind technology, as weighed against industry, and because regulations nearly always last years to extend and enforce, the ''best technology'' authorised by regulation possibly will be low-grade to the best that industry may perhapsin fact install. To put it plainly without anypurpose to blame either the regulators or the industry/technology, and by implication innovation/innovators and invention/inventors, do not stop to wait for the cavalry of regulatory forces to arrive, though they do arrive with full forces, which is often not so well-thought of. Furthermore, imposing additional requirements on new (re)sources encourages firms and factories to keep older facilities and vehicles in operation longer, retarding the diffusion of novel equipment and making, for example, environmental pollution worse[237]. Plus, we must not forget about the fact that implementing new facilities or purchasing new flotillas of vehicles can be a costly business. Jonathan B. Wiener observes that "[s]ome argue although technology

[234]CHAPMAN, Anne: *Democratizing Technology: Risk, Responsibility and the Regulation of Chemicals*. Earthscan Publications, London, 2007, 2.

[235]WIENER, Jonathan Baert: *Global environmental regulation: instrument choice in legal context*.The Yale Law Journal, Vol. 108, No. 4, Jan. 1999, 677-800. (Doi: https://doi.org/10.2307/797394)Available:https://core.ac.uk/download/pdf/62562074.pdf[accessed 27 Aug 2020]

[236]BREYER, Stephen:*Regulation and its reform*. Harvard University Press, Cambridge, MA, 1982, 105.

Available: https://www.scienzegiuridiche.uniroma1.it/sites/default/files/docenti/dalberti/breyer-regulation-and-its-reform.pdf[accessed 27 Aug 2020]

[237]GRUENSPECHT, Howard K.: *Differentiated Regulation: the Case of Auto Emissions Standards*. American Economic Review, Vol. 72, No. 2, 328.

requirements may be more costly and less innovation-friendly, they are easier to monitor than performance standards. Yet, monitoring the installation of the technology is not the same as monitoring actual environmental performance; and the added costs of performance monitoring are often far outweighed by the benefits of performance standards over technology requirements. Moreover, this debate points out that well-designed performance standards can stimulate innovation in monitoring technologies, by offering greater credit, for example, for better-monitored emissions reductions[238]. Although the latestadvancement of the questions/concerns above might be observed differently by Harry Armstrong and Jen Rae, the argue "[…] regulation has struggled to be more future-facing, largely unequipped to cope with more fluid, fast moving technological development, preferring to let markets decide the direction of travel and intervening later as issues begin to surface. Anticipatory regulation helps reframe regulation as a supportive tool for the responsible development and use of new technologies and business models. New and existing methods are helping regulators do this in three important ways: Firstly, regulators/regulation can better support innovation as it emerges. Secondly, regulators/regulation can drive innovation directly. Lastly, regulators/regulation can respond faster or act pre-emptively to prevent public harm"[239]. Also, they argue that [a]s technologies create new products and services, and disrupt existing competitive advantage in the global market, creating a dynamic and flexible regulatory environment could secure the industries that will drive growth and create jobs.[240] Two primary drivers have transformed the equity markets in recent years: technological advances and regulatory initiatives. How does modern, electronic technology facilitate trading, and to what extent does it present new challenges? How does regulation adjust to the changing structure of the markets, and to what extent is it itself a source of change? What are the new problems and solutions for handling institutional orders? On both sides of the Atlantic, what are the overall impacts of technology and regulation on market quality?[241]There is no doubt the fact that three dominant forces worldwide are able to drive change today in our financial markets: competition, technology and regulation. But

[238]WIENER (1999): op. cit., 490.

[239]ARMSTRONG, Harry –RAE, Jen: *A working model for anticipatory regulation*. A working paper,Nov. 2017. Available: https://www.nesta.org.uk/report/a-working-model-for-anticipatory-regulation-a-working-paper/[accessed 27 Aug 2020]

[240]ARMSTRONG–RAE: op. cit.

[241]SCHWARTZ – BYRNE – COLANINNO: op. cit.

their collective impact on (re)shaping the markets, though they might be regarded independently as necessary or well-meant, is producing stimulating results that are challenging to foresee, difficult and complex to control and not stress-free to comprehend. Extreme market turmoil (with instability) emphasised the basic issues as much attention turns to the applicable and valid regulatory response[242]. Do novel "smart" technologies such as robotics, Artificial Iintelligence, robotics, smart devices/drones, social media, and mechanization/computerization threaten to disrupt the whole fabric of our society?[243] Or does technological improvement/innovation/progress hold the potential to reform/transform/convert our democracies, civic societies and legal/regulatory "attitude", creating ones that are more equal and liable or the opposite? Peter Bloom and Alessandro Sancino, for example, while exploring and examining how technology has or assumes the power to redesign and restructure our civic participation and our privacy, economic and political/legal governance, and by implication, the entire existence of our civilization, go as far as to predict the upcoming clash between a progressive "Techno-democracy" and a regressive "Techno-populism"[244]. Do we need to raise our voices or concerns or does the so-called regulation of technology happeneffortlessly? We live an age of never-ending, multifaceted and disruptive technological innovation, one couldcontemplate on the ideas what, when, and how to structure regulatory intercessions. Manifestly, to answer them have become more and more challenging and for understandable reasons, challenging. Those who even make an effort to regulate repeatedly find themselves in a surrealistic and contradictory position where they believe they are assumed to decide on either rushed action, for example, regulations without crucial facts[245], or reserving to do nothing.

[242]SCHWARTZ, Robert A. – BYRNE, John Aidan – SCHNEE, Gretchen (eds.): *Rethinking Regulatory structure*. Springer, New York, 2013. (Doi: 10.1007/978-1-4614-4373-5)

[243]Though it seems futuristic, many movies and series have already attempted to answer some repercussion of the introduction of a novel technology, such as an AI.One of the best example is *Humans*, which is a science fiction tv series that premiered on Channel 4, and was written by the British team Sam Vincent and Jonathan Brackley, based on the Swedish science fiction drama *Real Humans*, the series focuses on the themes of artificial intelligence and robotics, concentrating on the socio-cultural, and psychological impact of the introduction/invention of anthropomorphic robots called "synths". It includes debates on the right and liability of high-tech AIs, and their legal status as well.

[244]BLOOM, Peter – SANCINO, Alessandro: *Disruptive Democracy: the Clash Between Techno-Populism and Techno-Democracy*. SAGE Publications, London, 2019. (Doi:http://dx.doi.org/10.4135/9781526465658)

[245]As it will be shown later in my chapter on drone technology, in that case even the terminology blurred by the lack of consensus. As far as terminology is concerned, drones mainly refer to aerial vehicles, which can fly with no human operator or without any human assistance. However, for regulatory purposes, it should be admitted that many countries and international organizations have already accepted and formed wide-ranging definitions. In general aviation and space-related phraseology, a "drone" usually related to *any* vehicle that

Predictably, in such a case, caution tends to outshine risk. But, I assume, such caution solely works as a kind of strengthening of the status quo and it looks that it makes it more complicated for new technologies to penetrate the market in time. Though time after time some resolutions surface, one of the answers is offered by Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, they suggest that law-making and regulatory design need to become more proactive, dynamic and responsive.[246] The reformation of the regulatory framework to address escalating and mounting regulatory concerns related to disruptive novel technologies has turned out to be a central issue in the world[247][248]. Setting up a regulatory framework that is assumed to assure the safety of both the users and the public at the same time, whilst supporting and aidind the commercial use and consumers' pleasure and satisfaction of a novel technology does not seem to be an easy and hassle-freemission. Also, the question of how and what to regulate couldintroduce even more questions and concerns.[249]In our day, it looks even more significant, since innovation is faster (in the same way as its development) and the global distribution of that technology is much

---

can operateon multiple surfaces and/or in the air without the assistance ofa human being on board to control it. Also, a small UAS manufacturer has to go through a 3-to-5-year process to get hold of a type certificate, which allows the issuance of a standard airworthiness certificate, the small UAS would be technologically outdated and "old-fashioned" by the time it could complete the certification process. For more information, see: Notice of Proposed Rulemaking: Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9549 (proposed Feb. 23, 2015) [NPRM]. available:

https://www.federalregister.gov/documents/2019/02/13/2019-00758/safe-and-secure-operations-of-small-unmanned-aircraft-systems [accessed 25 Mar 2019]

[246]FENWICK, Mark – KAAL, Wulf A. – VERMEULEN, Erik P. M.: *Regulation Tomorrow: What Happens When Technology Is Faster than the Law*. American University Business Law Review Vol. 6, Iss. 3, 2017, 561-594.

[247]See also: SCHERER, Matthew U.: *Regulating Artificial Intelligence Systems: Risks, Challenges,Competencies, and Strategies*. Harvard Journal of Law and Technology Vol. 29, No. 2, Spring 2016, 353-400. Available: http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf[accessed 4 Dec 2020]orZETZSCHE, Dirk A. – BUCKLEY, Ross P. – BARBERIS, Janos N. [et.al.]: *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*. Fordham Journal of

Corporate and Financial Law Vol. 23, no. 1, 2017, 31-103. Available:https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1450&context=jcfl[accessed 4 Dec 2020]

[248]Anne Chapman, for instance, decided to choose to examine the regulation of chemicals, to see why

the regulatory system was so ill equipped to address the issues raised by endocrine disruption. She was concerned and felt that treating chemicals as isolated entities became the part of the problem, that was why her research turned out to be an investigation into how we think about and publicly assess technologies, taking synthetic chemicals as her prime example. See: CHAPMAN: op. cit.

[249]BUTENKO, Anna – LAROUCHE, Pierre: *Regulation for Innovativeness or Regulation of Innovation*? Law, Innovation and Technology, Vol. 7, Iss. 1, 2015, 52, 72. (Doi: 10.1080/17579961.2015.1052643)

quicker, quicker than ever before.[250] It is not tricky to envisage that such condition do not really support the burdensome work of regulators, thus it is often observed that regulators find it difficult to keep up with the rapid development of innovation/technology[251][252]

Anne Chapman argues that "[i]n recent decades protests have generally been regarded as being about the risks associated with a technology: industry and government portray the public as being concerned about the risks of physical harm, to people or to the environment, posed by a technology. Risk assessment has become the dominant framework within which regulators consider technological developments. However, while people often are concerned about risks, it is apparent from the debates about genetic engineering that risks of physical harm are not the limit of their concerns. Debates have also raised issues about the power of multinationals, the direction of agricultural development, food security, the preservation of biodiversity and how we should be relating to other living organisms. Thus it is apparent that one needs to break out of the narrow confines of risk assessment and widen framework for thinking about and assessing technology in the context of public policy"[253]. Although her argument seems well-formed, and the limits of risk assessment are known by the regulators, risk assessment is still

[250] See, for instance, MCGRATH, Rita:*The Pace of Technology Adoption is Speeding Up*. Harvard Business Review, November 25 2013,Available:https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up[accessed 4 Nov 2018]; or BROWNSWORD, Roger – SOMSEN, Han: *Law, Innovation and Technology:Before We Fast Forward - A Forum for Debate*. Law, Innovation and Technology, Vol. 1, Iss. 1, 2009, 1-73.(Doi: 10.1080/17579961.2009.11428364) To link to this article: https://doi.org/10.1080/17579961.2009.11428364 [accessed 4 Nov 2018]

[251]See MARCHANT, Gary E. – ALLENBY, Braden R. – HERKERT, Joseph R. (Eds.):*The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: the Pacing Problem 3.*Springer, NewYork, 2011 (Doi 10.1007/978-94-007-1356-7) ("Moore's Law notoriously states that the 'functional capacity of ICT products roughly doubles every 18 months', with the same dynamics manifesting in biotechnology, and namely in sequencing human genome. As a result, regulating innovation involves what is called a 'pacing problem' in the academic literature from the US, or the 'challenge of regulatory connection' or 'regulatory disconnection' in European-based scholarship."); Butenko and Larouche, ("The 'pacing problem' generally refers to the situation when technology develops faster than the corresponding regulation, the latter hopelessly falling behind. The metaphor of 'the hare and the turtle' is often brought up as a comparison. As summarized by Marchant and Wallach, 'at the rapid rate of change, emerging technologies leave behind traditional governmental regulatory models and approaches which are plodding along slower today than ever before'."). BUTENKO– LAROUCHE: op. cit.

MARCHANT, Gary E. – WALLACH, Wendell:*Coordinating Technology Governance*. Issues in Science and Technology Vol. 31, No. 4, Summer 2015. Available: https://issues.org/coordinating-technology-governance/ [accessed 11 Nov 2020]

[252]MARCHANT – ALLENBY – HERKERT: op. cit.

[253]CHAPMAN: op. cit., 2.

dominating in the world as I will demonstrate later in the case of the drone regulation provided by the European Union[254]. For example, after the urgent demand by the EU Commission, the Member States of EU and other stakeholders, the *European Aviation Safety Agency* (EASA) set off to come up with proposals for an operation fundamental, proportionate, regulatory framework based on performance and risk for every one of un-manned (UA) ariel aircraft/vehicle establishing three categories with diverse safety requirements, proportionate to the risk: open' (low risk) is a UA operation category; 'specific' (medium risk); 'certified' (high risk).[255] Similarly, in the case of chemicals, Anne Chapman argues that "no formal assessment of risk had to be carried out until the 1990s when, in 1992, the seventh amendment (92/32/EEC) introduced the requirement for an assessment of the risks of new substances. Then, in 1993, Regulation 793/93 set out a procedure for assessing risks from existing substances. In both instances risk assessment was to be carried out by regulators. How they were to carry out the assessment was set out in Directive 93/67/EEC for new substances and Regulation (EC) 1488/94 for existing substances. Both used the same model of risk assessment, consisting of four stages and described with almost identical wording as follows: hazard identification: 'the identification of the adverse effects which a substance has an inherent capacity to cause'; dose (concentration)–response (effect) assessment: 'the estimation of the relationship between dose, or level of exposure to a substance, and the incidence and severity of an effect'; exposure assessment: 'the determination of the emissions, pathways and rates of movement of a substance and its transformation or degradation in order to estimate the concentrations/doses to which human populations or environmental compartments are or may be exposed'; and risk characterization: 'the estimation of the incidence and severity of the adverse effects likely to occur in the human population or environmental compartment due to actual or predicted exposure to a substance'. (Quotations are from the definitions in Article 2 of Directive 93/67/EEC.)"[256] Obviously, risk assessment as a form of pre-stage of

[254]See, for example, Hungary: https://www.uavsystemsinternational.com/drone-laws-by-country/hungary drone-laws/ [accessed 1 Nov 2018] or https://ec.europa.eu/commission/presscorner/detail/en/IP_14_384 [accessed 23 Jan 2019] and https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_14_110 [accessed 25 Jan 2019]

[255]https://www.easa.europa.eu/domains/civil-drones-rpas[accessed 25 Mar 2019] Consider to look intothe following sources for more details: European RPAS Steering Group, Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System, June 2013: http://ec.europa.eu/DocsRoom/documents/10484/attachments/1/translations/[accessed 25 Mar 2019]

[256]CHAPMAN: op. cit., 64-65.

any regulation has not lost its charm even if it has turned out to be a dead-end time after time. To present a form of model regulation, in 1993, Regulation 793/93 set forth a procedure for assessing risks from existing substances. In both instances risk assessment was to be performed by regulators based on Directive 93/67/EEC[257] (laying down the principles (or assessment of risks to man and the environment of substances notified in accordance with Council Directive 67/548/EEC) for new substances and Regulation (EC) 1488/94[258] (laying down the principles for the assessment of risks to man and the environment of existing substances in accordance with Council Regulation (EEC) No 793/93) for existing substances. Admittedly, as a practice, both applied the same model of risk assessment, consisting of four stages and designated with almost identical wording as follows: hazard identification: "the identification of the adverse effects which a substance has an inherent capacity to cause[…]; dose (concentration)–response (effect) assessment: [t]he estimation of the relationship between dose, or level of exposure to a substance, and the incidence and severity of an effect; exposure assessment: the determination of the emissions, pathways and rates of movement of a substance and its transformation or degradation in order to estimate the concentrations/doses to which human populations or environmental compartments are or may be exposed[…]; and risk characterization: [t]he estimation of the incidence and severity of the adverse effects likely to occur in the human population or environmental compartment due to actual or predicted exposure to a substance"[259]. Visibly, these four steps are identical to the four phases of the risk assessment process set forth in a key 1983 US publication on risk assessment (NRC, 1983[260]), demonstrating the influence of the US approach on Europe. It is acknowledged, however, that this model is not always applicable or precise, if it is the case regulators have to assess risks on a case-by-case basis and give a full description and validation of their evaluation in their report to the Commission[261]. The idea and the justification of the necessity of the survival of risk assessment can be related to and supported by Rosario

[257] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31993L0067 [accessed 3 Sep 2020]

[258] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31994R1488 [accessed 3 Sep 2020]

[259] https://www.researchgate.net/publication/286208518_Technical_guidance_document_on_risk_assessment_in_support_of_commission_directive_9367EEC_on_risk_assessment_for_new_notified_substances_and_commission_regulation_EC_No148894_on_risk_assessment_for_ex [accessed 3 Sep 2020] and https://echa.europa.eu/documents/10162/16960216/tgdpart2_2ed_en.pdf[accessed 3 Sep 2020]

[260] https://www.epa.gov/fera/nrc-risk-assessment-paradigm[accessed 30 September 2020]

[261] To get to know more, study:CHAPMAN: op. cit., 64-71.

Girasa, who states that AI is the state-of-the-art technological (r)evolution which keeps transforming the global economy and can be seen as a key part of the "Fourth Industrial Revolution.[262]" The work by Girassa examines and considers the denotation, categoris/varieties, (sub)fields and applications/function of Artificial Intelligence, in addition to the governmental policies and regulations of the USA, ethical and privacy concerns, principally as they connect and affect programs of facial recognition and the Internet-of Things. There is anextensivestudy of prejudice, and favourism, AI's effect on the current and job market in the future, and how AI triggered fake news. From the point of view of technological management, Roger Brownsword's recent book (re)considers the implications of the regulatory burden have been come to life progressively by technological management rather than by rules of law. Posing some relevant questions, I also find applicable, he attempts to highlight the challenges, presented by novel technologies. In an era of smart regulatory technologies, how should we comprehend the environment to be regulated and the nature of its regulatory indications? How does technological management be seated with the Rule of Law and with the traditional ideals of legality, legal consistency/coherence, and respect for freedom, human rights and dignity? What is the future for the rules of criminal law, torts? How are human informational securities to be identified/ classified and protected? Can traditional rules of law endure and persist not only the emergent use of technological management but also a risk management mentality that pervades the collective engagement with new technologies? Even if technological management is effective, is it acceptable? Are we ready for rule by technology?[263] The unmistakable fate of the current regulatory systems/laws, with reference to innovative/novel technologies, is founded on the fact that technological progress is noticeably unstoppable, we might not find a single or a way out for such a multifaceted, intricate and far and wide disputed topic as the regulation of novel technologies without coming across more and more and newer concerns related to privacy applying all meaning of it. But I need to put emphasis on the point that my doomsday mind-set, concerning the regulation of novel tech, where a drone or an IA, for example, is just a fine example besides mobile/cell phones or biometrics, I do not mean to argue that

[262]GIRASA, Rosario: *Artificial Intelligence as a Disruptive Technology - Economic Transformation and Government Regulation*. Palgrave Macmillan, 2020, 70-80. (Doi 10.1007/978-3-030-35975-1)

[263]BROWNSWORD, Roger: *Law, Technology and Society: Re-imagining the Regulatory Environment*. Routledge, New York, 2019. (Doi: https://doi.org/10.4324/9781351128186)

law makers are not up to their task, on the contrary. What I really endeavour to highlight is the fact that legal regulations and laws are destined to lag behind because of the inherent nature of the relationship between technology and law. Thus, I might opt for a revisionist[264] regulatory system in place of the existing perfectionist one. In order to avoid being misinterpreted, I state that a revisionist mode to cope with6reconsiderationregulation of novel technologies may not try to construct flawless system of laws, since the liaison between technology and law can predict a constant requirement for review, as opposed to this, a perfectionist law-maker feels the need and the urge to create a "perfect" laws and regulatory systems in order to assume to fulfil the traditional/classical ideology based on legal certainty and continuity. Obviously, my stand does not mean that we do not need legal certainty and continuity, but as for the tech related laws concerning privacy, I firmly believe that they are required to be revised time after time with bearing in mind their further consideration with regards to the pace of technology and the need to protect personality rights. As for the proof of my argument, or at least, one part of it, I endeavour to demonstrate how hectic/chaotic, for instance, the regulation of drones throughout the world is, including UK, the USA, Italy, Spain, Hungary, and to join to those, for example, Stuart Casey-Maslen, who gives the impression to have come to recognize that Pandora's Box has been unlocked, and so far as the regulations are concerned, I assume it will remain open/unlocked, since I argue that closing it forever by a "perfect" regulatory system cannot be an aim, as it seems the case now. With a perfectionist attitude, we may face a situation characterized by Craig McCracken,[265] in his cartoons the Powerpuff Girls, Blossom, Bubbles and Buttercup were created by Professor Utonium in an attempt to create the "perfect little girl" using a mixture of "sugar, spice, and everything nice". However, he accidentally added a mysterious substance called "Chemical X" into the mixture, creating three girls and granting all three superpowers including wingless flight, super strength, superhuman speed, near invulnerability, x-ray vision, superhuman senses, red heat vision, pink-green-and-blue energy projection, invisibility, and control over lightning and fire. It appears to me that the similarity to perfectionists, by implication, is striking. If we aim to construct "perfect little laws" to regulate/legalise novel technology, we have to ruminate

[264]Through my chapters, I intend to use the expressions, such as revision, revisionist, and perfectionist, as my own coinage/tecnicus terminus as I have defined.

[265]The Powerpuff Girls is an American superhero animated television series created by animator Craig McCracken.

on “chemical x” as a fine representation of technological progress and its future. Its unavoidable and forseeable presence guarantees us that our laws will not be perfect, that is the reason for allowing for a revisionist standpoint, and regarding (new) technology related laws and regulatory systems. The implied risks of privacy under the circumstances described may not allow for passivity, since the developing techs pose a considerable amount of legal challenges without even slowing down for a second.[266]

To get a better scope and understanding of the intricate relation between regulation/law and technology and their effect on each other, we should have knowledge of the work of Susan Brenner*: In Law in an Era of "Smart" Technology.* It sounds practical to analyse whether law ought to be technologically impartial/neutral, or it ought to progress as human relationships withtechnology become more advanced. In her work, Susan Brenner analyses the many-sided and evolving interactions/collaborations between technology and law and endeavours to provide a methodical, systematic andcomprehensive account of the law in technology at the beginning of the 21st century. Brenner draws upon contemporary technological growth/advances, evaluating how emerging novel technologies may be able tomodify how humans cooperate with each other and with their milieu[267]. She analyzes the advancement of technology as shifting from one of "use" to one of "interaction," and assumes that this transactionor substitution entails that we need to (re)conceptualize our approach toregulations, which were originallyintended to prevent the "misuse" of “older” technologies. As technologies continue to expand over the next several decades, Brenner states that the laws directed between human and technological relationships oughtto stay neutral. She gives explanation how older technologies are reliant on human performance, but new "smart" technology will be absolutely automated. She prophesizes that this can/will eventuallyset in motion, as she explains it, the ultimate “evolution” in our relationship with technology: the fusion of human physiology and technology.[268]Also, Brenner offers us anin depth, historically-anchoured explanation as to why our traditional relationship (or rather liasion) with technology is developing/materializing and why at equivalent/parallel shift in the law is impending and

[266]MENDEL, Gregory N.:*Regulating Emerging Technologies*.Law, Innovation and Technology, Vol. 9, Iss. 1, 2017. (Doi: https://doi.org/10.1080/17579961.2009.11428365)

[267]BRENNER, Susan: *Law in an Era of "Smart" Technology*. Oxford University Press, New York, 2007. (Doi:10.1093/acprof:oso/9780195333480.001.0001)

[268]BRENNER: op. cit.

indispensable. Moreover, analysing the same or rather similar challenges of the law created by the progress of technology, Emilie Cloatre and Martyn Pickersgill suppose that the relationships between knowledge, technologies, and legal processes are at the core of the constitution of contemporary societies. As such, they have come to provide the focus for a variety of academic projects, across interdisciplinary legal studies and the social sciences. The domains of medical law and ethics, intellectual property law, environmental law, civil law and criminal law are just some of those within which the pervasive place and "impact" of techno-science is instantaneouslynoticeable. Simultaneously, social scientists investigating the making of technology and expertise, above all, scholars working within the tradition of science and technology studies, recurrentlycross-examine how regulation and legal processes, and the making of knowledge and technologies, are combined in multifaceted ways that come to shape and define each other. They endeavour chart the important interface between studies of law, science/technology and society, as explored from the perspectives of socio-legal studies and the increasingly influential field of science and technology studies. Also, their book brings together scholars from both areas to interrogate the joint roles of law and science in the construction and stabilization of socio-technical networks, objects, and standards, as well as their place in the production of contemporary social realities and subjectivities.[269] Moreover, other experts, for instance, Sheila Jasanoff, argue that concerns/disputes spawned by the hasty pace of progresses in science and technology fill the courts. Asanoff ask how we should deal with frozen embryos and leaky implants, dangerous chemicals, DNA fingerprints, and genetically engineered animals? Sheila Jasanoff also suggests that the demesne of the law, to which overwhelmed people search for answers, is occasionally at a loss, constrained by its own assumptions/rules and practices[270]. She attempts to expose American law's time-honoured involvement in constructing, propagating, and perpetuating a selection of myths about science and technology. In addition to this, she also examines in detail how two powerful American institutions, both seekers after truth, interact with each other. Looking at cases involving product liability, medical malpractice, toxic torts, genetic engineering, and life

[269] CLOATRE, Emilie – PICKERSGILL, Martyn (Eds.):*Knowledge, Technology and Law*. Routledge, New York, 2015. (Doi: https://doi.org/10.4324/9780203797600)

[270]JASANOFF, Sheila:*Science at the Bar: Law, Science, and Technology in America*. Harvard, University Press, London, 1997. (Doi: https://doi.org/10.2307/j.ctvjz822j) Available: https://monoskop.org/images/a/ae/Jasanoff_Sheila_Science_at_the_Bar_Law_Science_and_Technology_in_America_Twentieth_Century.pdf [accessed 29 September 2020]

and death, Jasanoff argues that the courts do not simply depend on scientific findings for guidance, in reality, they can influence the production of science and technology at many different levels. Thus, it might be reasonable to suppose that research is conducted and interpreted to answer legal questions. Experts are selected to be credible on the witness stand. Products are redesigned to reduce the risk of lawsuits. At the same time the courts emerge here as democratizing agents in disputes over the control and deployment of new technologies, advancing and sustaining a public dialogue about the limits of expertise. Jasanoff endeavours to show how positivistic views of science and the law often prevent courts from recognising their full potential as centers for a progressive critique of science and technology[271]. While we attempt to consider the effect of the expansion/progress or the evolution of technology, one is flooded by intricate and challenging/problematic contemporary issues. The 21th century triggered a chain reaction with quite a few (re)vibrations with reference to privacy related issues. Since privacy can be identified as one of the most pressing issues/concernslinked to technology in total, IT and digital media. We can state that what individualsactuallyare concerned about when they protest and object that privacy has been violated is not the act of sharing technology or information itself, most people recognize that this is fundamental and has become ordinary to social life, but the wrongful, improper, and most decisively illegal use of technology. One of the best examples can be found in connection with info-technology in Helen Nissenbaum's book, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Arguing that privacy concerns should not be limited exclusively to concern about control over personal information, she counters that "information ought to be distributed and protected according to norms governing distinct social contexts whether it be workplace, health care, schools, or among family and friends. She warns that basic distinctions between public and private, informing many current privacy policies, in fact obscure mo than they clarify. In truth, contemporary information systems should alarm us only when they function without regard for social norms and values, and thereby weaken the fabric of social life."[272] What one can really observe here is none other than an increasing social demand for a kind of "norm based" (legal) regulatory system in order to give a rise to a novel type of protective

[271]JASANOFF:op. cit.

[272]NISSENBAUM, Helen: *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, 2010.(Doi: https://doi.org/10.1515/9780804772891)

system.As a consequence, the above mentioned argument may bring us closer to complex questions, such as, should law be technologically neutral, or should it evolve as human relationships with technology become more advanced? As Susan Brenner suggests that he transformation of the society cannot really be stopped, but one might search for “privacy friendly” resolutions.[273]

Since technologies keep on advancing without a stop over upcoming several decades; Brenner give the impressions that the laws directed between human and technological relationships must stay neutral. She clarifies the difference between “old” and “novel/modern” technology and their “association/link” to human factors, such as reliance on human execution/, and she also assumes that elder technologies hinge onthe implementation of human beings, but new "smart" technology are and will be utterlymechanized or ultimately programmed. This will ,in the long run,produce, as she explains, the eventualevolution in our link to technology: the synthesis of human physiology and technology, in addition, she also insists on historically-groundedness, concerning the the uneasy relationship and interrelatedness between us and technology, which as a consequence, seems to require the (impending and obligatory)“transformation.” of law as well[274]

Information/communication technologies (ICTs) play a progressively significant role in modern society. The digital insurgency in the last two decades has had an effect onnearly every aspect of humanlife; its impact might be and can be uncovered on numerous domains, such as, healthcare, education and so on. Endre Győző Szabó, Katinka Bojnár and Péter Búzás state that ICTs are hereall through thelifetime of aperson, from birth until the unavoidable end, and, of course, in various cases, even after death[275]. Correspondingly, Susan Brenner argues that the historical roots of this issue cannot be denied, and advancement can be observed and characterized/clasified in a mixture of

[273] MENDEL: op. cit.

[274] BRENNER: op. cit.

[275]One of the interesting and popular I have not dealt with is privacy after death, to get a wider picture of the topic, see, for example: Schubauer Petra: A személyes adatok személyiségi jogi védelme, különös tekintettel a halál utáni védelem egyes kérdéseire – PhD értekezés, 2021 https://ajk.kre.hu/images/doc2021/doktori/dr_Schubauer_Petra_PhD_2021_ (final.pdf) [accessed 11 Sept 2023]

ways.[276] Nevertheless, progress not only makes everyday life easier, it also offesr an opportunity for the related actor, stakeholders of the public and the private sector to scrutinize the lives and activities of millions of individuals by amassing and exploring/examining an unparalleled, unprecedentedquantity of information. The more people bank onnovel technologies, the more exposed/unprotected and delicate their human dignity and privacy can become. The use of ICTs has already brought up novel challenges (unavoidably) for lawmakers to set up legal and institutional agenda for data/privacy protection. The technology, evidently, could be used to serve the interests of the individuals, though this resolution is habituallybehind schedule: the apt use repeatedly drops behind the plausible abusive application of ICTs. For these reasons, public institutions and legistlators shall implement the relevant novel laws and take all the required measures to make answers available for the concerns/alarms hoisted by the use of ICTs.[277] The above mentioned author triad examine the privacy/data protection aspects of five applications of modern technology: geolocation, fingerprint-based biometric identification, social networks, remotely piloted aerial systems and search engines. Also, they target to present how certain, widely applied ICTs affect the privacy of the individuals concerned, and what measures might be necessary to protect the individual to avoid the potential risks arising from the use of such technologies. The other objective of their analysis is to introduce regulations, good practices and case-law with which legislators and key actors take action against abuses.[278] Although, among many others, Gregory N. Mendel assumes that almost allemerging technologies, including bio/nanotechnology and synthetic biology, can convert society. Mamaging the progress/evolution and regulation of these promising technologies is a difficult task as the risks presented will not be relized or recognized til the technologies are further progressed. Mendel proposes aninnovative governance model that seeks outto administer/supervise the dynamic of emerging technology promise versus risk by moving the point of first governance earlier in a technology's progress and growth, but enabling the governance structure to progress after

[276]BRENNER: op. cit.

[277]SZABÓ Endre Győző – BOJNÁR Katinka – BUZÁS Péter: *Új globális technológiák kihívásai a magyar jogban/Challeges created by Modern Technologies in Hungarian Law*. In: TÓTH András. (Ed.): *Technológia jog: új globális technológiák jogi kihívásai*. Patrócinium Kiadó, Budapest, 2016, 52-53. Available: http://www.kre.hu/ajk/images/doc/Uj_technologia_jog_kotet.pdf[accessed 10 Oct 2018]

[278]Later on, my intention is to examine some of the analitical thoghts of these authors, concerning regulations and practice SZABÓ – BOJNÁR – BUZÁS: op. cit., 52-53.

formation. His model aims to address some of the greatest challenges of managing emerging technologies, such as scientific uncertainty and the disruption of extant regulatory systems.[279] By means of key events to illustrate major concerns, Schwabach, Aaron examines such significant legal battles as A&M Records v. Napster[280] and Apple Computer v. Franklin Computer[281], letting us to take a a look into stories of trade secrets, music theft, and industrial espionage. He also states that since information technology develops rapidly and the Internet's global influence and stretch reinforces, it is getting more problematic and challenging to define rules to regulate it[282]. Governments have already attempted, for countless motives and reasons, to constrain and control (or "regulate") Internet content but have not managed to do so, to some extent because the international nature of the Internet makes enforcement challenging and problematic.[283] Although his book, *Internet and theLaw: Technology, Society, and Compromises* was published in 2006, his prediction seems valid now, and the debate surrounding the Net is still going on concerning privacy/personality rights and its influence as well.[284][285]

"Things do change. The only question is that since things are deteriorating so quickly, will society and man's habit change quickly enough?" – Isaac Asimov

[279]MENDEL: op. cit.

[280]https://onlinelaw.wustl.edu/blog/case-study-am-records-inc-v-napster-inc/[accessed 10 Oct 2018]

[281]https://law.justia.com/cases/federal/district-courts/FSupp/545/812/1432138/[accessed 10 Oct 2018]

[282] LESSIG, Lawrence: *Code and Other Laws of Cyberspace*. Basic Books, New York, 1999. and LESSIG, Lawrence:*Code: version 2.0.*Basic Books,New York, 2006.

[283]SCHWABACH, Aaron: *Internet and the Law: Technology, Society, and Compromises*. ABC-CLIO, Oxford, 2006.

[284] See, for example: How Countries Are Regulating Internet Content: https://web.archive.org/web/20160103124414/https://www.isoc.org/inet97/proceedings/B1/B1_3.HTM

Or https://iccwbo.org/publication/the-impact-of-internet-content-regulation/[accessed 10 Oct 2018]

[285] See, also: ZIMMER, Michael – Kinder-Kurlanda, Katharina:*Internet Research Ethics For The Social Age: New Challenges, Cases, And Contexts*. Peter Lang Media and Communication, New York, 2017.(Doi: https://doi.org/10.3726/b11077)

Chapter 5 AI: dawn of the human factor: basics and definition(s)[286][287].

The first challenge one needs to face is the definition of AIs because even the terms "artificial intelligence" and "intelligent human behaviour" are not well-defined, however. Artificial intelligence designates the work processes of machines that would necessitate intelligence if performed by humans. The term "artificial intelligence" thus means "investigating intelligent problem-solving behaviour and creating intelligent computer systems"[288] To go even deeper, we need to consider the fact that, at least, two kinds of artificial intelligence can be identified, the so-called *weak artificial intelligence* when the computer is simply an instrument forstudying or probing cognitive processes, and the computer simulates intelligence. The other one is called *strong or general artificial intelligence*, when the processes in the computer are intellectual, self-learning processes. Computers can comprehend by means of the rightsoftware/programming and are able to optimise their own behaviour onthe basis of their former behaviour and their experience.[289] This comprises automatic networking with other machines/devices, which leads to a dramaticscaling effect. It is also central to note that according to European commission "[a]rtificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.[290]" .Artificial intelligence and related technologies are altering, forming and reforming both the law and the legal profession. Particularly, technological

[286]This chapter is based on: SIMÓ, Ferenc Zoltán. *Preliminary Observations on AI Regulation*. Mesterséges Intelligencia 3: 1 pp. 33-59. , 27. (2021)

[287]To Get to know more about the future of robot laws, the code of AI and the probable interaction/relation/communication between the behaviour of AI and laws, see, for example: ZŐDI, Zsolt*What Will Robot Laws Look Like? The Code of AI and Human Laws*.Acta Univ. Sapientiae, Legal Studies, 8, 2 253–268. (2019)

[288]See: http://wirtschaftslexikon.gabler.de/Archiv/74650/kuenstliche-intelligenz-ki-v12.html [accessed 19 Dec 2020]

[289]See, for exaple: https://www.machinedesign.com/markets/robotics/article/21835139/whats-the-difference-between-weak-and-strong-ai or https://www.internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learning-policy-paper/?gclid=Cj0KCQiA5vb [accessed 19 Dec 2020]

[290]Communication from the Commission too the European Parliament, The European Council, the Council, The European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe Brussels, 25.4.2018 COM(2018) 237 final

Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN [accessed 19 Dec 2020]

progresses in fields ranging from machine learning to more cutting-edge robots, including sensors (with hyper sensitivity), virtual realities, algorithms, biometrics[291], drones, self-driving cars, and more sophisticated "human-like" robots are creating different/novel and formerly unimagined challenges for regulators[292]. Among many others, AI[293][294], drones, biometric systems and their disruptive capabilities present a conspicuous example for the ability to pose a disruptive potential and regulatory challenges related to such disruption in the existing regulatory framework. AI seems an even more complicated issue because national and international law do not presently recognize Al as a subject of law, Al does not have legal personality and as such cannot be held personally liable for damages[295]. It must be admitted that AI might be able to do much good, including by making products

[291]See, for instance, a recent study on the subject: National Academies of Sciences, Engineering, and Medicine. Life-Cycle Decisions for Biomedical Data: The Challenge of Forecasting Costs. Washington, DC: The National Academies Press. (2020) (Doi: https://doi.org/10.17226/25639).

[292] One of the best and up-to-date (though bulky) examples: a three-volume research conducted by the National Academies of Sciences, Engineering, and Medicine

National Academies of Sciences, Engineering, and Medicine. Airports and Unmanned Aircraft Systems, Volume 1: Managing and Engaging Stakeholders on UAS in the Vicinity of Airports. Washington, DC: The National Academies Press. (2020) (Doi: https://doi.org/10.17226/25599).

National Academies of Sciences, Engineering, and Medicine. Airports and Unmanned Aircraft Systems, Volume 2: Incorporating UAS into Airport Infrastructure Planning Guidebook. Washington, DC: The National Academies Press.(2020) (Doi: https://doi.org/10.17226/25606).

National Academies of Sciences, Engineering, and Medicine. Airports and Unmanned Aircraft Systems, Volume 3: Potential Use of UAS by Airport Operators. Washington, DC: The National Academies Press. (2020)(Doi: https://doi.org/10.17226/25607).

[293]Some of the legal problems and concerns have already been brought up movie makers / writers. For example, *A.I. Artificial Intelligence* (also known as *A.I.*) is a 2001 American science fiction drama film directed by Steven Spielberg. The screenplay by Spielberg and screen story by Ian Watson were loosely based on the 1969 short story "Super toys Last All Summer Long" by Brian Aldiss. The movie also carries a hint of "The Adventures of Pinocchio, *Le avventure di Pinocchio*, is a novel for children by Italian author Carlo Collodi, written in Pescia, his work can be seen as an early example of an AI. It is about the mischievous adventures of an animated marionette named Pinocchio and his father, a poor woodcarver named Geppetto.It was originally published in a serial form as *La storia di un burattino*) in one of the earliest Italian weekly magazines for children, starting from 7 July 1881.

All kinds of concerns and issues are brought up by the creators, including the rights of AIs, the regulation on their production, liability for "wrong-doing," privacy issues, and so on.

[294]The European Association for Artificial Intelligence EurAI (formerly ECCAI) was established in July 1982 as a representative body for the European Artificial Intelligence community. Its aim is to promote the study, research and application of Artificial Intelligence in Europe. The next European Conference on AI (ECAI 2020) will take place in Santiago de Compostella. The conference was originally scheduled for June but due to the COVID19 situation it will take place at the end of August and the first week of September. The theme of the conference is "Paving the way towards Human-Centric AI"

For more information, visit: https://www.eurai.org/

[295]PEARL, Tracy Hresko: *Fast & Furious: The Misregulation of Driverless Cars.* New York University Annual Survey of American Law, Vol. 73, Iss. 1, 2017, 19-72. Available: https://ttu-ir.tdl.org/bitstream/handle/2346/73420/Fast%20%26%20Furious%2073%20NYU%20Ann%20Sur%20Am%20L%2019.pdf?sequence=1&isAllowed=y [accessed 21 Dec 2020]

and processes safer, it can raise concerns as well by doing harm. The harm may be both physical and immaterial. The might be as follows, safety and health of individuals, including loss of life, damage to property, intrusion of privacy, limitations to the right of freedom of expression, human dignity, or even discrimination, and can be in connection with a great variety of risks or/and threats[296]. Evolving combinations of artificial intelligence, big data, and the applications have already been paid substantial attention concerning privacy/confidentiality and other ethical issues. Scholars feel the need to address comprehend these issues systematically and find mechanisms of addressing them that include stakeholders, civil society, to guarantee and safeguard that the benefit(s) of these novel technologies outweigh their disadvantages, or negative impacts. Information and communication technologies (ICTs) have long been documented and realized as having significant impacts on social, legal and economic arenas. As a consequence, they often seen as factors that cannot exist without regulatory supervision and, in addition, they call for ethical and social evaluation. Presently, one can observe two intertwining progresses that have the potential to add significantly and critically to the benefits of ICTs but that can also have undesirable effects on ethics and human rights. One of them is an accelerated rate of production and collection of big data, and the other one is novel ways of analysing and using this data. These two have been able to cloud other impacts, such as privacy concerns, not related to data protection. There are several ethical and human/personality rights issues/concerns, such as privacy, loss of employment, consent, identity, dual use, trust, power asymmetries, justice fairness, inequality, autonomy/agency discrimination, security, inclusion and so on[297].Artificial intelligence (AI) and big data analytics are the key technological drivers of what we call "smart information systems" (SIS). Examples of such intelligent sociotechnical systems abound, Google's search engine, Google Translate, Amazon's recommendation system, Amazon's Alexa home assistant, Facebook's likes, smartphones with GPS tracking, predictive policing systems, automated share dealing, healthcare and surgery robots, applications for personal fitness and training, virtual and augmented reality, and many others, ranging from social network

[296]See the works by Isaac Asimov. He has already presented some major issues, concerning robots and AIs.

[297]STAHL, Bernd Carsten – WRIGHT, David: *Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation.* IEEESecurity and Privacy, May/June 2018, Vol. 16, Iss. 3, 26-33. (Doi: 10.1109/MSP.2018.2701164) Available: https://ieeexplore.ieee.org/document/8395078[accessed 21 Dec 2020]

data analysis for advertising to traffic data prediction for energy conservation[298].WhenStahl, Bernd Carsten Stahl and David. Wright have coined the term SIS to point to a novel progress, the technologies elaborated on have a long history, as do some of the ethical questions they can be related to, such as privacy and data protection. A lot of the SIS use personal data, thus protecting such data is therefore an essential step to avoid rising concerns. Many of the newcharacteristics of GDPR[299]openly address the impact of SIS. Most of the new the novel features relevant to SIS are breach notifications, hefty financial penalties, data protection impact assessments,[300] privacy by design,[301] and the so-called *right to be forgotten*[302]. Thus, a regulatory framework is supposed to focus on how to minimise the numerous risks of potential harm, particularly, the most noteworthy ones. The main risks associated with the usage of AI concern the application of rules/regulations intended to protect fundamental rights, including personal data and privacy protection and non-discrimination), as well as safety and those concerns/issues related to and dealing with liability. Nowadays, the question of, what an AI is, is often asked by both experts and fans as well. Modern Information Technologies and the dawn of machines/mechanisms power-driven by artificial intelligence (AI) have already had a great influence on the world, including almost all walks of life in the 21st century[303]. Workstations, computers, CPUs, algorithms and software make simpler everyday tasks, and it is difficult to envision how most of our life could be succeeded without them. Nevertheless, is it also unmanageable to imagine how most process steps or stages could be accomplished without the human factor? The famous name behind the idea of AI is

[298]STAHL – WRIGHT: op. cit.

[299]Available:https://gdpr-info.eu/[accessed 19 Dec 2020]

[300]"Privacy Impact Assessment (PIA) Good Practice," CNIL, 2015. Available: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf[accessed 19 Dec 2020]

[301]Privacy by Design Strong Privacy Protection – Now, and Well into the Future A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners. Information Commissioner's Office,2008. Available: https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf[accessed 21 Dec 2020]

[302]Available: https://gdpr-info.eu/[accessed 19 Dec 2020]

[303] See, for instance, ANDERSON, Janna – RAINIE, Lee – LUCHSINGER, Alex: *Artificial Intelligence and the Future of Humans*. Pew Research Center, December 2018, Available: https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/ [accessed 19 Dec 2020]

John McCarthy[304], who began his groundbreaking research on this subject in 1955 and his assumption was that each and every aspect of learning and other domains of intelligence can be described so precisely and accurately that they can be computer-generated or simulated by a machine. Since 1948, McCarthy has been doing researching on artificial intelligence. The term, IA, was actually used by McCarthy in 1955 in a research application written with the legendary computer scientists Claude Shannon, Marvin Minsky and Nathaniel Rochester. The basic assumption of the scientists: "Every aspect of learning and other characteristics of intelligence can in principle be described so precisely that a machine can simulate it." From 1965 to 1980, McCarthy led the Artificial Intelligence Laboratory at Stanford University. Three years later, in 1958, McCarthy developed the programming language Lisp, an acronym for List Processing; it refers to the structure of the source code of programs written in Lisp, which consists basically of lists. Joseph Weizenbaum programmed his legendary program Eliza in Lisp. Written questions are answered by the software, using natural language, which is considered to be a breakthrough or a revolutionary leap in computer-assisted language processing.[305]The regulation of artificial intelligence can be seen as the expansion of public sector policies and laws for stimulating and regulating artificial intelligence (AI);[306][307] it is therefore related to the broader regulation of algorithms. The regulatory and policy landscape for AI is an emerging issue in jurisdictions globally, including in the European Union.[308][309] Regulation is considered necessary to both encourage AI and manage

[304]LISCHKA, Konrad – MCCARTHY, John: *Der Vater der Rechner-Cloud ist tot*. Spiegel Online vom 25.10.2011. Available: www.spiegel.de/netzwelt/web/john-mccarthy-der-vater-der-rechner-cloud-ist-tot-a-793795.html [accessed 14 Dec 2020]

[305]See: LISCHKA – MCCARTHY: op. cit.

[306]BERRYHILL, Jamie –HEANG, Kévin Kok – CLOGHER, Rob – MCBRIDE, Keegan:*Hello, World: Artificial Intelligence and its Use in the Public Sector*. OECD Working Papers on Public Governance, No. 36, 2019. Available:

https://oecd-opsi.org/wp-content/uploads/2019/11/AI-Report-Online.pdf [accessed 19 Dec 2020]

[307]BARFIELD, Woodrow – PAGALLO, Ugo: *Research handbook on the law of artificial intelligence*. Edward Elgar Publishing, Cheltenham, 2018.

[308]Law Library of Congress (U.S.). Global Legal Research Directorate, issuing body. *Regulation of artificial intelligence in selected jurisdictions*. LCCN 2019668143 Available: https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf[accessed 19 Dec 2020]

[309]*Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*. European Commission, Directorate-General for Justice, Brussels, 2020.

Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0064&from=en [accessed 19 Dec 2020]

associated risks[310][311] Regulation of AI through mechanisms such as review boards can also be seen as social means to approach the AI control problem[312].Some of the possible solutions can be find in an article, titled*Solutions to address AI's anticipated negative impacts* by Janna Anderson and Lee Rainie. They assume that, as a result of their canvassing offered solutions to the troublesome future produced by AI can be the following: first, improving collaboration across borders and stakeholder groups; second, developing policies to assure that development of AI will be directed at augmenting humans and the common good; and third, shifting the priorities of economic, political and education systems to empower individuals to stay ahead in 'the race with the robots'[313]."

5.1 Regulation of AI in the European Union: Europe as a leader in trustworthy Artificial Intelligence[314]

Europe has everything it needs to become a world leader in Artificial Intelligence (AI) systems that can be safely used and applied. It has outstanding research centres, secure digital systems and a strong position in robotics as well as competitive manufacturing and services sectors, covering almost all walks of life imaginable. The so-called White Paper presented today, presented by the Commission envisions a framework for reliable Artificial Intelligence, based on quality and trust. In partnership with the private and the public sector, the target is to mobilise resources and to create the proper and reasonable drives to accelerate deployment of AI, including by smaller and medium-sized enterprises. This European Union intends to work with its Member States and the

[310]BUITEN, Miriam C.: *Towards Intelligent Regulation of Artificial Intelligence*.European Journal of Risk Regulation, Vol. 10, No. 1, 2019, 41–59. (Doi:10.1017/err.2019.8)

Available:https://www.cambridge.org/core/services/aop-cambridge-core/content/view/AF1AD1940B70DB88D2B24202EE933F1B/S1867299X19000084a.pdf/towards_intelligent_regulation_of_artificial_intelligence.pdf[accessed 19 Dec 2020]

[311]WIRTZ, Bernd W. – WEYERER, Jan C. – Geyer, Carolin: *Artificial Intelligence and the Public Sector—Applications and Challenges*. International Journal of Public Administration, Vol. 42, Iss. 7, 2019, 596-615. (DOI:10.1080/01900692.2018.1498103)Available: https://www.tandfonline.com/doi/abs/10.1080/01900692.2018.1498103 [accessed 19 Dec 2020]

[312]SOTALA, Kaj – YAMPOLSKIY, Roman V: *Responses to catastrophic AGI risk: a survey*.Physica Scripta, Vol. 90, No.1, 2014. (Doi: 10.1088/0031-8949/90/1/018001) Available: https://iopscience.iop.org/article/10.1088/0031-8949/90/1/018001/pdf[accessed 19 Dec 2020]

[313] Available: https://www.pewresearch.org/internet/2018/12/10/solutions-to-address-ais-anticipated-negative-impacts/ [accessed 19 Dec 2020]

[314]Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence:https://ec.europa.eu/digital-single-market/en/artificial-intelligence[accessed 19 Dec 2020]

research community, to promote, attract and keep talents. Since AI systems can be and are intricate and bear noteworthy risks in certain contexts, such as privacy issues and concerns. Thus, building trust is vital. Clear rules need to address high-risk AI systems without putting too much burden on less risky ones. As always, there are strict EU rules for consumer protection, to address unfair commercial practices and to protect personal data and privacy, are still to be applied. As for high-risk cases, such as in health, policing, privacy, or transport, AI systems are supposed to be transparent, traceable and guarantee human oversight/inaccuracy. As for lower risk AI applications, the Commission envisages a voluntary labelling scheme if they apply higher standards. All AI applications are welcome in the European market as long as they comply with EU rules[315]. AS customary in the EU, risk analyses must be done in advance in a company in order to protect employees when they work with robots. Furthermore, the so-called Machinery Directive sets a minimum standard/requirement that all machine products in Europe must meet. The Directive also provides for a manufacturer's risk assessment for any machine. The term machinery is defined as: an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts, at least one of which moves that are joined together for a specific application. Thereforerobots are "machinery" for the purposes of the Directive. The machinery might not be operated till a safety briefing concerning the individual workplace of the employee working with the machinery has taken place. It is also suggested to regulate the use of the systems by establishing policies. If technical hitches with the system happen, these incongruities must also be included by the manufacturer of the machinery in its risk assessment.[316]

[315]*White Paper: On Artificial Intelligence - A European approach to excellence and trust.* For more information, visit: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf[accessed 2 Sep 2020]

[316]*DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)* Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0042&from=HU [accessed 2 Sep 2020]

5.2 The White paper[317]

In 2017, the European Parliament issued a Resolution calling on the Commission to come up with "ground-breaking" resolutions centred on civil law that could reply (successfully) to the prompt current development of robotics and AI. The Resolution, with an idea or intention of aiming for the preparation of new tort law concentrating on robots, proposes that a new definition of robot should be prepared. Responding to the Resolution, Paweł Księżak and Sylwia Wojtczak has prepared a study, which is made up of a legal-cognitive-linguistic analysis. It draws three conclusions: the first conclusion is that the definitional method is not the best approach to determining the scope of the regulation of robotics and AI. The second one is that the Resolution is flawed by supposing that a new civil law solution should turn on differentiating between AI and robots and that robot should be treated as central in defining the scope of the regulation. Lastly, that any new norms should be deep-seated in the concept of AI and not, as suggested and offered by the Resolution, in the concept of robot[318]. According to the European Commission, and the rapid development and progress of Artificial Intelligence cannot be denied. It will have the potential to alter or even revolutionize our lives by improving healthcare, for instance, by making diagnosis more precise, allowing enhanced methods of prevention of illnesses, increasing the efficiency of production systems through predictive maintenance, or by improving the efficiency of other sectors, such as agriculture, environmental protection, or the security sector, and this list may go on. Simultaneously, The EC argues that Artificial Intelligence (AI) involves numerous potential risks, such as opaque decision-making, gender-based and/or bias or other kinds of discrimination, intrusion in our private lives or, this novel technology can be used for criminal purposes as well. Since global competition has never been so competitive, a firm European approach is required, with bearing in mind the European strategy for AI presented in April 2018[319]. A working definition can be, though it may be simple that AI can be defined as a collection of technologies that combine data, algorithms and computing power. Progresses in computing and the growing

[317]commission-white-paper-artificial-intelligence-feb2020_en

[318]KSIĘŻAK, Paweł – WOJTCZAK, Sylwia: *AI versus robot: in search of a domain for the new European civil law*. Law, Innovation and Technology, Vol. 12,Iss. 2,2020, 297-317,(Doi: 10.1080/17579961.2020.1815404)

[319]AI for Europe, COM/2018/237 final

Available: https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF[accessed 2 Sep 2020]

availability of data are therefore strategic drivers of the recent expansion of AI. Europe has the potential to combine its technological and industrial assets with a high-grade digital infrastructure and a regulatory framework constructed on its fundamental values and principles to turn into a global leader in innovation in the data economy and its applications as set forth in the European data strategy[320]. The White Paper, presented in 2020, offers policy alternatives in order to facilitate a dependable and safe improvement of AI in Europe, with respect to the (core) values and rights of EU citizens. The main building blocks of this White Paper are: "The policy framework setting out measures to align efforts at European, national and regional level. In partnership between the private and the public sector, the aim of the framework is to mobilize resources to achieve an *ecosystem of excellence* along the entire value chain, starting in research and innovation, and to create the right incentives to accelerate the adoption of solutions based on AI, including by small and medium-sized enterprises (SMEs). The key elements of a future regulatory framework for AI in Europe that will create a unique *ecosystem of trust*. To do so, it must ensure compliance with EU rules, including the rules protecting fundamental rights and consumers' rights, in particular for AI systems operated in the EU that pose a high risk. Building an ecosystem of trust is a policy objective in itself, and should give citizens the confidence to take up AI applications and give companies and public organisations the legal certainty to innovate using AI. The Commission strongly supports a human-centric approach based on the Communication on Building Trust in Human-Centric AI8 and will also take into account the input obtained during the piloting phase of the Ethics Guidelines prepared by the High-Level Expert Group on AI"[321]. Representing the European Commission President Ursula von der Leyen announced the plan[322] at a press conference with the goal is to promote "trust, not fear." The plan also includes measures to update the European Union's 2018 AI strategy[323] and pump billions into Research and

[320]*Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.*COM(2020) 66 final

Available:https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf[accessed 2 Sep 2020]

[321]commission-white-paper-artificial-intelligence-feb2020_en 2-3. [accessed 2 Sep 2020]

[322]*Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence*. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273 [accessed 2 Sep 2020]

[323]RABESANDRATANA, Tania: *With €1.5 billion for artificial intelligence research, Europe pins hopes on ethics*. Science, Apr 25, 2018. https://www.sciencemag.org/news/2018/04/15-billion-artificial-intelligence-research-europe-pins-hopes-ethics [accessed 2 Sep 2020]

Development over the next decade[324]. It can be seen that the EU attempts to come up with a solid and all-inclusive regulatory framework, with no doubts on the probabilities of threats and risks as well. Thus, it not a surprise that The commission requests binding rules for "high-risk"[325] uses of AI in sectors like health care, transport, or criminal justice. Accordingly, the criteria to determine/define risk may include considerations such as whether it could be harmful to someone, by an AI driven car or a medical device/tool, for instance, or whether a person has little say in whether they are affected by an AI's decision, such as when it is used in job recruitment or policing. For high-risk scenarios, the commission intends to put a stop to indecipherable "black box" AIs by demanding human oversight. The rules needs to govern the large data sets used in training AI systems, safeguarding and guaranteeing that they are legally acquired, traceable to their source, and sufficiently broad to train the system. The liability for an AI system's actions is supposed to be dealt with by the law, from both the users' sides and the manufacturers' or designers' sides as well. As for the high-risk applications, they have to be presented to be compliant with the rules/regulations before being installed in the European Union. The commission also proposes to offer a "trustworthy AI" certification, to inspire voluntary compliance in low-risk uses. Although EU countries such as Germany has revealed plans to set upand install these systems, officials say they often violate EU privacy laws, including special rules for police work.[326]I argue that the new AI strategy is not merely about regulation. The commission may be able to produce an "action plan" for incorporating AI into public services such as public transport and health care, and even more. The commission is calling for more R&D, including AI "excellence and testing centres" and a new industrial partnership for AI that could invest billions. Alongside its AI plan, the commission also drawn a separate strategy to encourage data sharing, in part to backing up the development of AI.

[324]*Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence*.https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273 [accessed 2 Sep 2020]

[325]The EU sticks to its risk-based solutin here as well as in the case of drones.

[326]GRÜLL, Philipp: *Germany's plans for automatic facial recognition meet fierce criticism*. https://www.euractiv.com/section/data-protection/news/german-ministers-plan-to-expand-automatic-facial-recognition-meets-fierce-criticism/ [accessed 2 Sep 2020]

5.3 Report No. A9-0186/2020 presented by the European Parliament:

The Report observes the necessity of the mutual goal of European Union for a regulatory framework for the progress and expansion, distribution and use of artificial intelligence, robotics and associated/interrelated technologies ('regulatory framework for AI') should allow citizens to share the benefits drawn from their potential, while protecting citizens from the potential risks of such technologies and upholding and supporting the reliability of such technologies in the European Union and elsewhere; that framework should be built on Union law and values and guided by the principles of transparency, fairness, accountability and responsibility, understanding and in accordance with the core values of the European Union.

This regulatory framework is of vital importance in order to avoid the disintegration of the Internal Market, which may result from conflicting and different national legislation. The common regulatory framework can help nurture much needed investment, improve data infrastructure and support research. Also it should consist of common legal obligations and ethical principles as set out in the proposal for a Regulation. Still, it should be established and be consistent with the improved regulation guidelines. The Union has a strict legal framework in place to guarantee and to safeguard, inter alia, the protection of personal data and privacy and non-discrimination, to support and encourage gender equality, environmental protection and consumers' rights; whereas such a legal framework consisting of an extensive body of horizontal and sectoral legislation , as well as the existing rules on product safety and liability, will continue to apply concerning artificial intelligence, robotics and related technologies, though certain adjustments of specific legal instruments may be necessary to reflect the digital transformation and address new challenges posed by the use of artificial intelligence. The report also states that there are (major) concerns that the recent European Union legal framework, including the consumer law and employment and social acquis, data protection legislation, product safety and market surveillance legislation, as well as antidiscrimination legislation may no longer be suitable for purpose to effectively challenge and confront the risks created by artificial intelligence, robotics and related technologies. And, in addition to amendments to current legislation, legal and ethical inquiries with regard to AI technologies ought to be addressed through an effective, comprehensive and future-proof regulatory framework of

European Union law reflecting the Union's principles and values as preserved and protected in the Treaties and the Charter of Fundamental Rights that ought to avoid over-regulation, by only closing existing legal gaps, and increase legal certainty/decrease legal uncertainty for businesses and citizens alike, namely by including mandatory measures to prevent practices that would undoubtedly undermine fundamental rights[327]. As it is suggested by and can be drawn from this report as well, the existing EU regulatory framework for AI seems to struggle with not having the nature of being "common" (for the purpose of EU harmonization processes) and with being unfit to face the challenges presented by AI. Needless to say, I assume that can be applied to any novel technologies by implication.

5.4 The key issues of regulation: Can we have a "realistic" basis of regulation?

The term *issue* refers to a certain matter of disagreement or conflict which is situated in the public sphere and which gives way to a call for regulatory action. We need and can differentiate the key issues for policy and regulation in relation to two dimensions. The first one is: do they deal with public or private concerns? The other one is: do they have a positive or negative "trend" or direction, enclosed in terms of possible benefits or harm? A short introduction of the grounds on which the novel technologies, including AI, the Internet, drones and so on, are problematized can be given, as follows, issues/concerns of public or private concern (either relating to benefits or harms), the protection of public order and the security of the state, attaining benefits for the public domain in terms of information flow, access, diversity and public participation. 1. Preventing harm to society, especially by way of harm to children/young people from undesirable content. 2. Protecting individual rights to reputation. 3. Preventing wrongdoing to individuals. 4. Avoiding harm to individuals from violent or perverted content. 5. Protecting propertyrights in communication and information. There is no doubt about the fact that the rapid progress and expansion of AI is set to transform all walks of life, there may not be any segments of society remaining untouched or undisturbed. As a general-purpose

[327] Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL))
Available: https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.pdf [accessed 29 Dec 2020]

technology, its constant development and application will speed up innovation across all dimensions of human enterprise. These changes can both offer remarkable progresses to public welfare and we must not forget that they can create unparalleled public risk as well. Thus, it has been and will be crucial to attempt to minimize that risk, plus, it is vital to comprehend how the progress and application of AI is presently being ruled and overseen.

Remodelling or (re)forming the regulatory framework to address accumulating and growing regulatory issues/concerns related to (disruptive or/novel) technologies comes to be more and more essential. Planning or developing a regulatory framework that guarantees the protection of users and the public, while aiding the commercial use and consumer enjoyment of disruptive innovation seems even more complex and complicate.[328] This appears "factual" in contemporary settings, where innovation is faster and the global distribution of that technology is much faster.[329]

5.5 AI regulation US[330]

The government of the USA has attempted to takeseveral projects to address the growing concern of AI's relationship to national security and its regulation. One of them is the "foundation" of the Defense Innovation Board launched in 2016 with a renewable 2-year mandate whose mission, partly, is to give the Secretary of Defense and other related government officials with advice and recommendations to address future challenges in technology and capabilities[331].

In 2019, President Trump signed Executive Order 13859 introducing a relatively new era, the American AI Initiative, the national starategy of USA concerning AI.

[328]BUTENKO– LAROUCHE: op. cit.

[329]MCGRATH: op. cit. and DESILVER, Drew: *Chart of the Week: The Ever-Accelerating Rate of Technology Adoption*. Pew Research Center report, 2014. available: https://www.pewresearch.org/fact-tank/2014/03/14/chart-of-the-week-the-ever-accelerating-rate-of-technology-adoption/ [accessed 3 Sep 2020]

[330]https://www.whitehouse.gov/ai/ [accessed 2 Sep 2020]

[331]DEFENSE INNOVATION BOARD, https://innovation.defense.gov/and PELLERIN, Cheryl:*Defense Innovation Board Makes Interim Recommendations*, DEPARTMENT OF DEFENSE NEWS (Oct. 5, 2016), https://dod.defense.gov/News/Article/Article/965196/defense-innovation-board-makes-interimrecommendations/. or *Ten Commandments of Software*, DEFENSE INNOVATION BOARD (April 20,2018),https://media.defense.gov/2018/Apr/22/2001906836/1/1/0/DEFENSEINNOVATIONBOARD_TEN_COMMANDMENTS_OF_SOFTWARE_2018.04.20.PDF [accessed 2 Sep 2020]

Theapproach is a concertedendeavour to promote and protect national technology of AI and innovation. The Initiative puts into practice a government strategy in unison and engagement with the private sector, academia, and the public and international partners in agreement with it. It directs the Federal government to pursue five pillars for progressing AI: first, finance AI research and development, the next is to give a free rein to AI resources, third is to remove obstacles to AI improvement/novelty, the penultimate is to school and instruct an AI-ready personnel/labour force, and the last is to aid an international milieu that is encouraging of American AI innovation and its liable/accountable use (with a particular attempt on transparency). The USA is also compassionate to AI technology to support the work of the Federal government more efficientlyin its own services and assignments/tasks in trustworthy and reliable ways. In February 2020, the American Artificial Intelligence Initiative was release by the White House: Year One Annual Report. In the year since the AI Executive Order was signed, the Administration called for record amounts of AI Research and Development investment, led the expansionand progress of the first international statement on AI Principles, issued the first-ever strategy for engagement in AI technical standards (and measures), published the first-ever reporting of government-wide non-defense Artificial Intellignce Research and Developmentexpenditure, and released the first-ever AI regulatory document for the reliableexpansion/progress, testing, use/operation, and adoption of AI technologies[332][333].

5.6 AI and Regulation[334]

Regulation is regularly characterized/portrayed as "the sustained and focused attempt to alter the behaviour of others according to standards or goals, with the intention of producing a broadly identified outcome"[335][336]For a regulatory regime to be effective

[332]Available:*Maintaining American Leadership in Artificial Intelligence*. Federal Register,Vol. 84, No. 31, 2019.https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf[accessed 2 Sep 2020]

[333]https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/available: https://www.whitehouse.gov/ai/[accessed 2 Sep 2020]

[334]One of the latest views on the subject presented in the form of a case study by LEENDERS, Gijs: *The Regulation of Artificial Intelligence — A Case Study of the Partnership on AI*.
https://becominghuman.ai/the-regulation-of-artificial-intelligence-a-case-study-of-the-partnership-on-ai-c1c22526c19f [accessed 4 Dec 2020]

[335]BROWNSWORD, Roger: *From Erewhon to AlphaGo: For the sake of human dignity, should we destroy the machines?* Law, Innovation and Technology, Vol. 9, Iss. 1, 2017, 117-153. (Doi: https://doi.org/10.1080/17579961.2017.1303927) and BROWNSWORD –SOMSEN:*op. cit.*

(and efficient), it has to have (or, at least it should have) a clear (even plain) working definition of what it regulates. Disappointingly, one can findvarious different definitions of AI circulating among experts in the field.[337][338]If one goes deeper i to finding one it discovers that the non-technical definition that is leading and common in the literature on AI policy is that an AI is any digital tool or system that is capable of performing tasks that, if performed by a human, would be said to require intelligence.[339][340] A fundamental implication of this definition is that AI is a technology assuming general purpose, the combination of intelligence with computing properties has the prospect to enhanceand raise productivity across all industries by accelerating invention/innovation (and by implication, research and development).[341] The recurring importance of AI is sthrengthened by the evolution and the fruition of a extensive range of machine learning (ML) techniques. These techniques are used to generate/construct digital systems (or sometimes structures) that are capable of improving"[....] their performance on a given task over time through experience."[342] A mixture of cheaper and better and upgraded computer processing power, access to mammoth and organised training data-sets, and algorithmic innovation has permitted machine learning academics, experts and professionals to make key innovations in several (relevant) domains commonly presupposed to be the most important, vital elements of AI.[343][344]

[336]MOSES, Lyria Bennett: *How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target*. Law, Innovation and Technology, Vol. 5, Iss. 1, 2013, 1-20, (Doi: 10.5235/17579961.5.1.1) [accessed 4 Dec 2020]

[337]SCHERER:op. cit.

[338] For more information on AI and updates, consult, for example, this website:

https://nikolanews.ndnsocial.com.hk/the-regulation-of-artificial-intelligence%E2%80%8A-%E2%80%8Aa-case-study-of-the-partnership-on-ai/[accessed 4 Dec 2020]

[339]BRUNDAGE, Miles. – AVIN, Shahar. – CLARK, JACK [et al.]:*The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, 2018. (Doi: https://doi.org/10.17863/CAM.22520) Available:

https://www.repository.cam.ac.uk/bitstream/handle/1810/275332/1802.07228.pdf?sequence=1&isAllowed=y [accessed 4 Dec 2020]

[340]SCHERER: op. cit.

[341]BRUNDAGE, Miles – BRYSON, Joanna: *Smart Policies for Artificial Intelligence*. 2016. Available: https://arxiv.org/pdf/1608.08196.pdf [accessed 4 Dec 2020]

[342]BRUNDAGE – AVIN – CLARK [et al.]: op. cit.

[343]BRUNDAGE – BRYSON: op. cit.

The risk to public welfare springs from two different forms of AI. The AI literature categorises existing and up-to-date ML techniques as "narrow AI", consisting of greatly specialized statistical models that have been trained to match or surpass performance at a human level at a specific task, in a specifically and precisely well-defined environment[345]. The progress and use of narrow AI is coupled with substantial risks concerning personal privacy, bias, inequality and prompt computerisation/robotics[346][347]. One of the foremost concerns is undeniablyattached to the above mentioned personal privacy, which can be said to be greatly linked to novel/innovativetechnology, too. Yet, misgivings/issues/concerns even fearswere produced/created and sensationalized by the media. Also one can point to the media for the (great) expectations of AI regularly concerning Artificial General Intelligence (AGI). By definition, AGI refers to a system that equals or surpasses human level performance at any task across multiple domains, non-dependent of its training milieu.

Though there is no apparent progress "line" toward AGI right now, a survey of AI researchers/experts provides a 10% chance of such AI being developed by 2024, and a 50% chance of it being developed by 2050.[348][349] AGI presentsd public welfare risks on a diverse order of magnitude, including geopolitical security concerns, labour market displacements and severe economic inequality and unfairness. Several researchers even identify an existential risk to the survival of our species, if we are unable to

[344]CALO, Ryan: *Artificial Intelligence Policy: A Primer and Roadmap*.*UC Davis Law Review*, Vol. 51, Iss. 2, 2017.(Doi:http://dx.doi.org/10.2139/ssrn.3015350)Available: https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Calo.pdf [accessed 4 Dec 2020]

[345]CAMPOLO, Alex – SANFILIPPO, Madelyn –WHITAKKER, Meredith – CRAWFORD, Kate: *AI Now 2017 Report*. AI Now Institute, New York, 2017. Available: https://ainowinstitute.org/AI_Now_2017_Report.pdf [accessed 5 Dec 2020]

[346]BRUNDAGE – AVIN – CLARK [et al.]: op. cit.

[347]To get to know more on limiting technology: MULLIGAN, Christina M:,*Perfect Enforcement of Law: When toLimit and When to Use Technology*.Richmond Journal of Law and Technology, Vol. 14, Iss. 4, 2008.

Available:https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1295&context=jolt [accessed 4 Dec 2020]

[348]GRACE, Katja – SALVATIER, John – DAFOE, Allan – ZHANG, Baobao – EVANS, Owain: *When Will AI Exceed Human Performance? Evidence from AI Experts.* Future of Humanity Institute, UK and AI Impacts, Berkeley, USA (2017) Available: https://arxiv.org/abs/1705.08807[accessed 4 Dec 2020]

[349] Centre for the Governance of AI, Future of Humanity Institute, Oxford University. BOSTROM,Nick– DAFOE, Allan – FLYNN, Carrick: *Policy Desiderata in the Development of SuperintelligentAI*. Future of HumanityInstitute,2017.Available:http://governance40.com/wpcontent/uploads/2018/12/aipolicy.pdf[accessed 5 Dec 2020]

control/regulate or bring into line an AGI with our values/principles.[350] Others, for instance, Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang and Owain Evans, while analysing the possible impacts and progresses in artificial intelligence (AI), they predict that AI will transform modern life by remodelling transportation, health, science, finance, and the military, and we may add regulation[351] and privacy as well. In order to adapt public policy/regulation, it seems essential for us to better anticipate these progresses. They report their findings from a large survey of machine learning researchers on their beliefs about progress in AI. These searchers predict that "AI will outperform humans in many activities in the next ten years, such as translating languages (by 2024), writing high-school essays (by 2026), driving a truck (by 2027), working in retail (by 2031), writing a bestselling book (by 2049), and working as a surgeon (by 2053). Researchers believe there is a 50% chance of AI outperforming humans in all tasks in 45 years and of automating all human jobs in 120 years, with Asian respondents expecting these dates much sooner than North Americans. These results will inform discussion amongst researchers and policymakers about anticipating and managing trends in AI"[352].

5.7 AI and Self-Regulation[353]

This dissertation presents the argument that the development and use of AI presents exceptional/exclusive regulatory challenges, and that the panorama of AGI can produce a competitive dynamic that prioritizes the fast expansion and progress of AI over the safe "maturity" of AI (technology). This dynamic affects the corporations developing AI technology, and the countries tasked with regulating them. Traditional regulatory solutions seem ill-suited to the task of minimizing public risk while sustaining innovation. Self-regulation can be identified as an alternative form of governance where an industry designs/creates and puts in force new rules, standards and ethics for themselves, often in

[350]BOSTROM– DAFOE– FLYNN: op. cit.

[351] See: CALO, Ryan:*Robotics and the lessons of cyberlaw*. California Law Review, Vol. 103, No. 3, 2015, 513. (Doi: http://dx.doi.org/10.2139/ssrn.2402972)

[352]GRACE, Katja – SALVATIER, John – DAFOE, Allan – ZHANG, Baobao – EVANS, Owain: *Viewpoint: When Will AI Exceed Human Performance? Evidence from AI Experts*.Journal of Artificial Intelligence Research, Vol. 62, 2018, 729-754. (Doi: https://doi.org/10.1613/jair.1.11222)

[353]LEENDERS:op. cit.

"areas where government rules are lacking"[354]. I hypothesize that a self-regulatory system has the prospect to be an effective and practical answer to the unique regulatory challenges of AI, and could assist and allow the AI industry to prevail over the competitive dynamic that incentivises AI progress/expansion haste over security or protection.

Chapter 6 Drones in all forms: definitions, regulation and their clouded future.[355]

6.1 Outline on drones and their "definition(s)":

When I first started to study new technologies, such as drones, and their "troublesome relation" to privacy related (legal) concernsand related issues, I really felt somewhatlike Alice, as she wondered into another land, now a kind of strange techno-land, tumbling down another rabbit hole. I soon realized that in this world, as in Alice's wonderland, here the laws, including the laws of physics, do not apply as they do as a rule. This bizarre terrain seems chaotic, so does the relation between technology and privacy (not to mention the regulation of the first. As a consequence, we may perhaps even feel after tumbling down that we need or era supposed to realize bit by bit how deep the concerns are in connection with drones. In this case, it appears similar to an unexploredand unfamiliar territory or, at least, one can identify legal areas with no real or realistic resolutions or answers offered for lessening or reducing those concerns. At the present time, we could also state thatthe moment when we examine novel techs, such as drones, for instance, that we are witnessing anexpansion of their use into the civilian and humanitarian domain. One cannot or should not disagree with the fact that drones, for example, are all the time more used for goals as diverse as news gathering, aerial inspection of oil refinery flare stacks, mapping of the certain terrains, crop spraying or search and rescue operations (with visibly more and more success and efficiency).

[354]HAUFLER, Virginia: *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy*. Carnegie Endowment for International Peace, Washington, D.C., 2001, 8-10.

[355]This chapter is based on: SIMÓ Ferenc Zoltán. *Drones and Privacy-Related Issues/Concerns: Alice inTechno-Land.* ACTA UNIVERSITATIS SAPIENTIAE LEGAL STUDIES 8 : 1 pp. 89-105., 17 p. (2019) and SIMÓ, Ferenc Zoltán. *Privacy in Context: Info-tech based society and the revolutionary effects ofdrones/phones/biometrics*JURA 25: 2 pp. 458-469. , 12 p. (2019)

The civil use of drones is becoming or one can go as far as to state that it is a reality in the European Union (one can win a civilian drone in the Hungarian version of *the Wheel of Fortune/Szerencsekerék,* fro example) and in the US. The revolution of the drones may be seen as a new technological revolution with numerous(side-) effects with reference toroughly all walks of life. Proliferation of the next generation of "recreational" drones illustrates how drones will be sold as any other consumer item with no real difference. The cultural perception of the technology is shifting and keeps changing, as drones are increasingly being used for humanitarian activities, on one hand, but they can also tightly and resolutely be positioned in the widespread (known) modes of postmodern governance on the other hand. In addition to postmodern governanca, I presuppose that the arguments and enquiries/topics suggested and introduced by Timothy M. Ravich[356]come into viewas fairly relevant, since he brings up with the idea that within the "IoTs," hardly anyexisting(and trendy) subjects more than "drones" encapsulate "informatics," freely defined as the study of the application of computer technology to accomplish any information and data/facts and "lore" in business, legal, and social processes , for instance, one considers Facebook, political polling, and medical records storage and so on.

The given chapter offers to make an effort to provide a (moderately) brief intro to the concept of drones, and some technologies that can incorporate with and their current commercial potentials and applications. I go on to explore the legal issues/concerns and regulations on drones' usage alongside with providing a comparative regulatory frameworks of different jurisdictions. The concluding section deals with the possible balance between drone usage and policy/law making.

When we need to consider the effect of the expansion or the (r)evolution of technology, one is flooded by intricate and (above all) challengingand problematical contemporary issues. The 21st century triggered a chain response(even feedbacks) with quite a few (re)vibrations in relation to privacy related issues. Since privacy can be one of the most urgent issues that various academicssupposes can be associated with

[356]Assistant Professor, University of Central Florida, College of Health and Public Affairs, Department of Legal Studies. The author, a Florida Bar Board Certified Aviation Lawyer, presented aspects of this article by invitation at the 2015 Law + Informatics Symposium on Digital Evidence at the Northern Kentucky University Salmon P. Chase College of Law.

technology[357]. For this reason, it appears, that oneis able to state that what personsactuallytake into account when they make a complaint and object that (their) privacy has been defied/violated is not the act of sharing technology or info itself, most individuals are able to cope with that this seemscrucial and critical and has been converted intocommonplace to social life, but the unlawful, offensive, and most unfalteringly illegal use of technology.

Drones, as they have known in our time, are said to symbolize and signify a substantial/extensve progress in technology in robotics and the private/civil application of drones has set in motion trending in media most recently. The use of unmanned aircraft such as drones is not a newidea and the origins of the concept could be traced back to the 19th century, when in 1896, the first pilotless steam-powered aircraft recorded a powered flight lasting over a minute. Drones have a lengthy history and they have been with us for a long time their "(r)evolution" commenced long time ago, and it seems that it is one of the most progressive techs which ought not to be considered to be historically stoppable or preventable. Consequently, it looks crucial to mention the fact that more than fifty five years ago, in July 1963, the 4028th Strategic Reconnaissance Weather Wing, equipped with U-2 strategic reconnaissance aircraft, set off flying global missions from Davis-Monthan air-base. The event, of course, is strongly connected to the Cuban Missile Crisis in 1963, the 4080th Strategic Reconnaissance Wing at Laughlin AFB, Texas, relocated to the base and assumed (full) responsibility for all U-2 operations, focusing on long-range strategic reconnaissance and intelligence collection. As a Strategic Air Command (SAC) unit, the 4080th was re-designated afterwards the 100th Strategic Reconnaissance Wing and also acquired Lockheed DC-130 Hercules aircraft for launch and control of Firebee reconnaissance drones that were the precursors of contemporary unmanned aerial systems[358].

[357] See, for instance, HAMBLING: op. cit..orSTUART, Casey-Maslen: *Pandora's box? Drone strikes under jus ad bellum, jus in bello, and international human rights law*. In: International Review of the Red Cross, Vol. 94 No. 886 Summer, 2012.

[358]For more information onearly unmanned aircraft, drones and their "brief" history, see: KEANE, John F. – CARR, Stephen S.: *A Brief History of Early Unmanned Aircraft***.** In.: Johns Hopkins APL Technical Digest, Vol. 32, No 3., 2013, 558-571 available: http://www.jhuapl.edu/techdigest/TD/td3203/32_03-Keane.pdf[accessed 25 Mar 2019]

The revolution of the drones may as well be seen as an innovative, "modern" technological revolution with various(side-)effects in relation to, more or less, every sector of our life. Abundance of the next generation of "recreational" (civil) drones presents how drones will be sold and marketed as any other ordinary consumer article or single piece. The cultural awarenessand sensitivity of the technology is evolving and keeps being altered, as drones are growingly being used for many different purposes, such as, humanitarian reason/activity, on one hand, but they can also strongly and determinedly be positioned in the prevailing (recognized) modes of postmodern governance on the other hand.

The term "drone" is the colloquial language of all sorts of aircrafts[359], which are operated without a (human) pilot on board, and their auxiliary components, such as a control station, if relevant. In addition to "drone", other phrases/expressions and acronyms are also used in anextensivevariety of scientific publications and documents related to regulation(s). As we can observe one can find more and more definitions to describe "drones," which I suppose is due to the rapidly changing technology of the drones and the response of the society to the concerns related to them. The widespread and ordinary examples are Unmanned Aerial Vehicles (UAV), Unmanned Aircraft (UA), Pilotless Aircraft and Unmanned Aircraft System (UAS)[360]. Though one may find out surprisingly that those terms in theory seem the same, but diverse authorities dealing with aviation have their own preference[361]. For instance, the International Civil Aviation Organization (ICAO) applies the "pilotless aircraft", but the US Federal Aviation Administration (FAA) and the European Aviation Safety Agency (EASA) make use of the term "UAS". As expected, it can be stated that the terms UAV, UA and Pilotless Aircraft refer to *an aircraft* which is operated without a (human) pilot on board. With reference to UAS, one possibly will include that the additional word "system" refers to the *ancillary components* (control station, command and control date link, and so on.) as opposed to the aircraft component.

[359] Of course, there are several types of aircrafts, including aeroplanes with fixed wings, airships (lighter than air) and helicopters (rotary wing).

[360] ZAVRSNIKop. cit.

[361] Whether a drone was an "airplane" as a matter of law, subject to regulatory enforcement by the Federal Aviation Administration, or a "model airplane" subject to mere policies issued by aviation regulators was largely unresolved until the decision of Huerta v. Pirker. SeeHuerta v. Pirker, CP-217, Board's Decisional Order No. EA-5730 (Nat'l Transp. Safety Bd. Decisions (N.T.S.B.) Nov. 18, 2014), available athttp://www.ntsb.gov/legal/alj/OnODocuments/Aviation/5730.pdf [accessed 25 Mar 2019]

Within the range of drones, one seems to settle with two main modalities, they can be described as: drones remotely piloted from another place (Remotely Piloted Aircraft System (RPAS)), or programmed and fully autonomous drones[362]. But drones could be the combination of the two of abovementioned major modalities. Therefore, in order not to be confused, I intend to use the term "drone" as an over-arching concept to include all applicable modalities and components, and also refers to those acronyms insofar as (any) existing laws and regulations apply any specific ones. Nowadays it seems relevant to notice that drones can appear in various shapes and sizes and could be operated/controlled by individuals for recreational/sport or commercial purposes. Unlike traditional vehicles, such as helicopters and hot-air balloons, drones are capable of flying at lower altitudes combined with data capturing potentials of smart (computing) devices. And, of course, drones also differ from the traditional aircrafts, as they are mainly economical to operate and accessible to a wider range of population without any difficulties.Yet, as far as terminology is concerned, drones chiefly refer to aerial vehicles, which can fly without a human operator or without human assistance. However, for regulatory purposes, it must be admitted that different countries and international organizations have already come up with wide-ranging definitions. In general aviation and space-related phraseology, a "drone" usually refers to *any* vehicle that can operateon multiple surfaces and/or in the air withouta human being on board to control it. And, as matter of fact, we may go even further in this respect, because, as a as far as their varieties are concerned, they can vary in size, shape, form, speed, and a host of numerous other characteristics/aspects, despite the fact that some jurisdictions catalogue/label and regulate them by weight. A drone could vary from a model aircraft / toy in a store or a large sized aircraft sent in a war zone[363].

While it can be safely stated that most of the other terminologies describe drones as Unmanned Aerial Vehicles ('UAVs'), Model Aircrafts, Unmanned Aerial Systems/ Unmanned Aircraft Systems ('UAS'),

[362]ICAO. (2011). Unmanned Aircraft Systems (UAS), Cir. 328, Glossary. Retrieved from https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf [accessed 25 Mar 2019]

[363]For more information: KREPS: op. cit.or ZAVRSNIK op. cit.

6.2 All forms: Unmanned Aerial Vehicles ('UAVs'), Model Aircrafts and Unmanned Aerial Systems ('UAS').

A UAV refer to a power driven aircraft that is designed to fly with no human operator on board. The International Civil Aviation Organization (the "ICAO"), liable to codification and regulation of airways, categorize drones as UAVs. It has also coined an exclusive term defining them as Remote Piloted Aircraft Systems (the "RPAS")[364]. According to the ICAO Circular on Unmanned Aircraft Systems, 2011 an RPAS as '[a] set of configurable elements consistingof a remotely-piloted aircraft, its associated remotepilot station(s), the required command and controllinks and any other system elements as may berequired, at any point during flight operation.'[365]It is of primary importance to note that the term "remote pilot" is a keyconcept here as it (visibly) emphasizes the fact thatthe system is not always unmanned and alwayshas a pilot in command liable for the flight,[366] which could also be controlled eitherby on-board computers or remotely piloted on/from the ground. Hence, RPAS fit in to the wider category of Unmanned AircraftSystems. The ICAO has had anRPAS Panel, as well, which has the objective to produce standards for unmanned aircraft to ICAO's GoverningCouncil ('GC') by the end of 2018.[367]

Model Aircrafts' are defined as aircrafts, which are mechanically driven or launched into flight for recreational purposes and are not designed to carry persons or living creatures. According to FAA Modernization and Reform Act, 2010, a drone may be equated with a "model aircraft" if it weighs less than 55 pounds and is operated in compliance with certain safety guidelines such as flying within the operator's line-of-sight, below 400 feet, and providing prior notice to air traffic control operators if flying within a 5 mile radius of an airport.[368] Since model aircraft are by and large distinguished or identified as being aimed only for recreational purposes (for example, entertainments),

[364]KREPS op. cit.

[365]ICAO Circular 328-AN/190.

[366] Council of the European Union. Towards a European Strategy for the development of civil applications of Remotely Piloted Aircraft Systems external (RPAS), Working Paper (13438/12), September 6, 2012.

[367]https://www.ainonline.com/aviation-news/aerospace/2015-01-06/icao-panel-will-recommend-first-uav-standards-2018 [accessed 25 Mar 2019]

[368]https://www.faa.gov/uas/publications/model_aircraft_ operators/ [accessed 23 Mar 2019]

they are not covered under the scope of any international regulations, and are utterly and absolutely governed/regulated by applicable national regulations, if any.

The term 'UAS', though defined in the same way, is broader in its ambit and includes: the aircraft; the control system(s) on the ground; the control data link(s); other support equipment.While these definitions are centred on the technology and operation of drones, the military journals may come up with varied definitions based on their applications or usage. For instance, the *US Department of Defence Dictionary of Military and Associated Terms* gives us a different definition for UAVs, thus, they are said to be:"a powered, aerial vehicle that does not carry a humanoperator, uses aerodynamic forces to provide vehicle-lift, can fly autonomously or be piloted remotely, canbe disposable (as non-essential) or recoverable, and can holdand transport a lethalor non-lethal consignment. Though ballistic or semi-ballistic vehicles,cruise missiles and artillery projectiles are notconsidered unmanned aerial vehicles".[369]For this reason, anchored in the above mentioned classifications/characterizations, we may perhaps roughly consider drones to be unmanned aircrafts/ships guided/directed/controlled by remote controls used for different purposes/functions/aims. The (simple) fact that they could be operated/controlled without a person (ör a human being) on board, lets them be designed smaller, making them less disruptive from the conventional aircrafts.[370]Also, a drone can also beequipped (potentially) with various other apparatuses/devices/tools such as Global Positioning System ('GPS'), cameras of numerous sorts, CPU, workstations and other related systems and so on. The (moderately) user friendly nature of drones has opened ways many for their uses in commercial and civilian/domestic areas. One of the studies by the Association for Unmanned Vehicles Systems International (AUVSI) offers estimation on the "influence" of drone production, since it states that drone industry in the United States of America is able and ready to provide up to over 100,000 new jobs and add $82 billion in the economic activity between 2015 and 2025.[371] Drones, consequently, are "figure" of technical advancements/innovations that have tapped the doors to an unreservedly and completelynew-fangled market, exploding the market with unforseen potential(s). At the

[369]http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2385448 [accessed 25 Mar 2019]

[370]http://www.academia.edu/11845032/Privacy_law_implications_of_the_use_of_drones_for_security_and_justice_purposes [accessed 24 Mar 2019]

[371]http://www.auvsi.org/auvsiresources/economicreport [accessed 25 Mar 2019]

moment the reality is that there are unlimited civil applications for drones with no doubts about that, and the potentials seem to develop and hauled up at even higher rates as the technology progresses/becomes or evolvesto be a productbeing easier to get to (or by) the public. As a reaction to this exceptional/unparalled intensification and increase in the numbers in production, the FAA has come to a decision to augment, even boost regulation and supervision of drone operation for not only commercial operators but recreational (civil users/operators) users as well. As a start December in 2015, the FAA initiateda quantity of changes with reference to the obligations and constraints for every bit of recreational drone operator, from then on operators are required to register.[372][373]

6.3 The revolutionary applications of drones nowadays:

Drones have massive amount applications which have grown to beperceptible[374]. They could be used for the quick/immediate delivery of donated organs, thus avoiding the expense of hiring air transport or having to handle traffic in that way potentially saving more lives.[375] They can be used for enhancing agricultural effectiveness/proficiency by identifying factors such as moisture content and nutrient soil availability. Remote sensing through drones can be of significant use in disaster-prone areas like pinpointing and fighting fires[376] or detection of theft and pilferage of goods meant for public utilization, or in detection of LPG gas leaks which can save several lives and resources.[377] Drones also find application in law enforcement agencies, aiding and contributing to border patrolling, though; concerning its cost efficiency have been questioned by a lot, evidently, pertaining to the "enterprise" on the US-Mexico border,[378] which seems to be a never-ending project for any administration in US. Nevertheless, with developing/evolving technologies such

[372]Press Release, FED. AVIATION ADMIN., FAA Announces Small UAS Registration Rule (Dec. 14, 2015) https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856 [accessed 25 Mar 2019]

[373]https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856 [accessed 24 Mar 2019]

[374] See, for example, some Hungarian scholars on the application of drones as well: Békési Bertold. és Seres József: Drónok alkalmazásának lehetőségei REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK 32. évfolyam (2020) 3. szám 5–19.

[375]http://www.content/501388/drones-maysoon-used-organ.html [accessed 25 Mar 2019]

[376]http://www.businessinsider.in/The-fire-in-Alberta-doubledin-size-on-Saturday-and-firefighters-are-using-drones-to-fightit/articleshow/52170421.cms [accessed 25 Mar 2019]

[377]https://www.businessinsider.in/Now-a-drone-that-detects-LPG-gas-leak-and-delivers-emergency-medical-kits/articleshow/48467531.cms [accessed 26 Mar 2019]

[378]https://www.foxnews.com/us/federal-report-says-border-patrols-drone-program-doesnt-fly [accessed 25 Mar 2019]

concerns (and reassurances as well) can be overcome and indisputable advantages such as being (moderately) unnoticeable/untraceable may be able to give support to prevent human and drug trafficking, pinpointing and reacting to border violations and in monitoring otherwise inaccessible terrain[379]. Visiblyone can argue that the core issue in this case is the degree of autonomy that is to the non-human parts/moduls/components. With the rapid progress of drones, it may possibly benoticeable that quite a lot of sorts of drones have been in operation with autonomous functionality, to the extent that collisions can be avoided and are prevented, and, also, some are capable of executing general instructions. While regulations have normally not addressed this aspect, the circular released with the latest FAA regulations in June 2016, has allowed autonomous operation, but within certain limits.[380] However, it does not even offer resolutions or answers to regulate larger (size) drones as in the case of a drone taxi or it having only non-pilot human passengers. At the same time as it stays in a legal grey arena, this field is supposed to proceed along the lines of self-driven cars. At the moment, it can also be stated that we are witnessing a rapid progress of the use of drones into the civilian and humanitarian domain. Also, it can be admitted that more and more drones, for example, are used for objectives as diverse as news gathering, aerial inspection and even surveillance, charting of the jagged or inaccessible and remote terrains, crop spraying or search and rescue operations. The civil use of drones has become a (harsh) reality in the European Union and in the US. From our point of view, I assume, it does not really matter whether one considers the revolution of the drones as a novel technological innovation/revolution/evolution or phenomenon or only as a sixty year-old one, the fact stays put, the effects of this technology have started off to be detectablewith reference to and pertaining topractically all walks of life. As a result, the assembly and invetion of the next generation of “recreational” drones demonstrates and points up to how drones will be marketed as a consumer item without differentiation concerning its risk management.

[379]HAMBLING:op. cit.

[380]https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_107-2.pdf [accessed 25 Mar 2019]

6.4 Applications of civilian drones, security and privacy concerns: including unauthorized surveillance, data aggregation/ mass collection, potential security hazards, and hacking.

Countless books, articles, pamphlets, and commentaries ache and yell for reforms, for the most part for restrictions/constraints in law and policy to upholdand boost defences against the erosion of privacy attributable tothe ever-growing ranks of technology-based systems practices. It looks noteworthy to point out that Hillary B. Farber informs us on the fact that only some years ago one may have seen a small object flying above our head without any ideas what it could be. These days, basically, it is a view with no shock or surprise to see drones flying around our neighbourhood skies. Also, she reveals that in 2015 hobbyists, recreational users, and commercial businesses purchased unmanned aerial vehicles, commonly referred to as drones, in record-breaking numbers[381]. The Federal Aviation Administration (FAA) calculates/predicts that there will be (more than) seven million drones populating our skies by 2020.[382]As well as, the Federal Aviation Administration ("FAA") admits plainly that its traditional processes for guaranteeing the safety of airplanes and helicopters are inapt for the mounting number of small drones, which onemay perhapsinclude, growing even smaller: "[T]he FAA's current processes for issuing airworthiness . . . certificates were designed to be used for manned aircraft and do not take into account the considerations associated with civil small UAS [Unmanned Aircraft Systems] . . . .[383]" [O]btaining a type certificate and a standard airworthiness certificate . . . currently takes about 3 to 5 years . . . . [I]t is not practically feasible for many small UAS manufacturers to go through the certification process required of manned aircraft. This is because small UAS technology is rapidly evolving at this time, and consequently, if a small UAS manufacturer goes through a 3-to-5-year process to get hold of a type certificate, which allows the issuance of a standard airworthiness certificate, the

[381]FARBER, Hillary B.*: Keep out the efficacy of trespass, nuisance and privacy torts as applied to drones.*Georgia State University Law Review Vol. 33, No. 2, 2017,1-2.Available: https://core.ac.uk/download/pdf/233916802.pdf[accessed 5 Nov 2020]

[382]https://www.faa.gov/data_research/aviation/aerospace_forecasts/ FED. AVIATION ADMIN. FAA AEROSPACE FORECAST 31 (2016). [accessed 22 Mar 2019]

[383]Notice of Proposed Rulemaking: Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9549 (proposed Feb. 23, 2015) [*NPRM*]. available: https://www.federalregister.gov/documents/2019/02/13/2019-00758/safe-and-secure-operations-of-small-unmanned-aircraft-systems [accessed 25 Mar 2019]

small UAS would be technologically outdated by the time it completed the certification process"[384]. It is growingly declared that remotely piloted aircrafts (RPAs) have the potential to pose a serious threat to citizens' privacy, since they are capable of intruding on any person's or a business's (private) conducts either with (criminal) intent, as it can be said in the case of planned/deliberate surveillance, or unintentionally or by coincidence in the course of other activities, such as aerial photography, traffic monitoring or search and rescue. Since RPAs have grown to be more economical and even more capable/adept, and, evidently, this progress or procedure has not even reduced speed or held back, and so as the instruments they are able to carry have developed into more tuned/sensitive. Hence, these techno-gadgets can supply governments, companies/firms and customers/individuals/civilians/persons alike with the money-spinningpotentialand capacity to observe and gather information on almost anybody, potentially without their knowledge or consent. One of the main concerns relating to drones is that they could be used to record images of other people without their consent. Drones can take video cameras on a regular basis to allow the remote pilot to fly them. Thus, images can be recorded and techs could be used to kit out drones such as high-power (and high quality) zoom, microphones and a multitude of sensors as well as GPS systems recording the location of persons filmed[385]. The visible absence of adequate safeguards and regulations with respect to the use of drones has raised several (major) issues. These can be related to concerns such as government overreach, data aggregation and invasion of privacy in public. It is of the essence that these concerns are recognized and concentrated on professionally by sufficient regulatory decisions.

It is renowned that drones can be exploited (without any difficulty) for mass surveillance. In context of new/innovative techs, it is merely meant to endeavour to reform our daily lives, with the rationale of having more detailed records about those lives.[386] On the authority of national security and terrorism, surveillance devices/apparatuses even kits

[384]Notice of Proposed Rulemaking: Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9549 (proposed Feb. 23, 2015) [*NPRM*]. available: https://www.federalregister.gov/documents/2019/02/13/2019-00758/safe-and-secure-operations-of-small-unmanned-aircraft-systems [accessed 25 Mar 2019]

[385]European Parliamentary Research Service, Civil drones in the European Union, October 2015: http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571305/EPRS_BRI(2015)571305_EN.pdf [accessed 25 Mar 2019]

[386]https://harvardlawreview.org/2013/05/the-dangers-of-surveillance/ [accessed 25 Mar 2019]

are employed to "hunt down" and profile the citizens by the state as well and private agencies[387]. On account of their design and size, drones can manoeuvre and function without being spotted, letting the operator/controller observe people without their awareness. For instance, there are drones with high-techand sophisticated cameras that can be used to track people and vehicles from altitudes as high as 20,000 feet.[388]Ultra-modern drones are able to bear equipment with which Wi-Fi codes can be broken, text messages and mobile phone conversations intercepted or and interrupted even without the awareness of either the communication/service provider or the user.[389] Drones equipped with advancedhigh-techs can gain access to and penetrate test networks and amass unencoded data and even set up fake access points. Though it may perhaps be argued that the compilation of data/facts about persons as such does not (necessarily) violate one's privacy interests, extensive (and comprihensive)collection/set of data possibly will be argued to be able to get to a level of privacy intrusion.Both data mining and aggregation refer to the method of matching different data sets to deduce to learn novel things and make (valuable) predictions about the data subjects.[390] Aside from observation, drones accumulate large amounts of personal/private data, which are of crucial importance for individual privacy. Post collection, the aggregation of drone-collected data with other private information such as the details of bank account, phone number, biometrics and so on attained from other resources can lead to a unique privacy infringement beyond the sheer collection of those individual data sets[391] Other illustrious privacy related concerns pertaining to drones can be hacking, since each and every computer source or a connected one, such a drone, are also apt to getting compromised. There have been earlier cases where even the high-tech drones on patrol duty have been compromised. Thus, there is a need to warrant that ampleand satisfactory measures must be taken to uphold high encryption standards for the data stocked up on the drones and strict sentence and penalties are supposed to be prescribed for unauthorized hacking of drones. There are more and more potential security hazards can be named, since the opening up of national skies for the private and domestic use of UAVs

[387]ZAVRSNIK op. cit.

[388]https://www.eff.org/deeplinks/2012/01/drones-are-watching-you [accessed 25 Mar 2019]

[389]https://www.eff.org/issues/surveillance-drones [accessed 26 Mar 2019]

[390]http://www.dbta.com/Editorial/Trends-and-Applications/What-is-Data-Analysis-and-Data-Mining-73503.aspx [accessed 25 Mar 2019]

[391]CUDD – NAVINop. cit.

allows for the risks of potential accidents caused by impacts, collisions, failures of battery failures, failure and/or error of navigational control and so on. The operation of UAVs notably differs from that of the conventional aircrafts. The traditional air traffic control system issues a command for the pilot by radio and the pilot thereby avoids the collision. Thus, the relevant human factor can directly interfere in order to prevent incidents.

6.5 Drone regulation highlights: United States of America: General Rules for Flying a Drone in the United States of America:[392]

At this instant, the domestic use of drones is at a relatively early stage. Manyof the countries all around the world do not provide for exclusive regulations to administrate (and overse) their operations. Only a handful of countries such as United States of America, France, and Germany have methodically set up and designedto address various concerns involved with UAVs and have decided on orchestrating comprehensive legislations to regulate their applications. In accordance with the U.S. national aviation authority, the U.S. Federal Aviation Authority (FAA), flying a drone is legal in the U.S., though one is supposed to be aware of and compliant with the drone regulations listed below before doing so. For instance, there are some special travel concerns and issues when you travel to the United States of America and are set to to take your drone, the FAA lists these special considerations for foreigners who wish for flyimg drones, they must register their drone with the FAA using the FAADroneZone portal. If drones used for fun/recreational purposes, they must follow the rules for recreational / hobbyist flying as it is listed, but if drones are flown and operated for work that can complicates the matter, since operators must get a certificate from the FAA and follow the rules for flying as listed. When one travels domestically in the U.S. with his/her drone, travelling is allowed with your drone by the U.S. Transportation Security Administration (TSA), but drones must be brought in carry-on luggage only. A drone is not allowed to be packed in checked luggage.[393] Here I intend to illustrate the most fundamental (and essential) rules to be familiar with for flying a drone in the USA. But one is supposed to take into account the fact laws relate the drones can and will vary in each state in the United States;thus, one is recommended to look for assistance on the website of the state one i ntends to fly a droneas well.

[392] https://uavcoach.com/drone-laws-in-united-states-of-america/ [accessed 25 Mar 2019]

[393] https://uavcoach.com/drone-laws-in-united-states-of-america/ [accessed 25 Mar 2019]

Recreational/Hobbyist Rules are the following; there are some "musts" fly for hobby or recreation only without side jobs or in-kind work, register your UAV with the FAA on the FAADroneZone website, and fly within visual line-of-sight. follow community-based safety guidelines/protocols and fly within the programming of a nationwide community-based organization (CBO) like the AMA, fly a drone under 55 lbs. unless certified by a community-based organization, never fly near other aircraft, report to the airport and air traffic control tower prior to flying within 5 miles of an airport, and, of course, never fly near emergency response efforts. For commercial purposes the "musts" are the following; hold a Remote Pilot Certificate issued by the FAA to fly commercially, register your UAV with the FAA on the FAADroneZone website, Your UAV must weigh less than 55 pounds, including payload, at takeoff, fly in Class G airspace, keep your UAV within visual line-of-sight, fly at or below 400 feet, during daylight or civil twilight and at or under 100 mph. One must give way to manned aircraft, and cannot fly directly over people or from a moving vehicle, unless in a sparsely populated area. And, in addition, there are Certification Requirements for Flying a Drone in the United States of America, thus in order to fly a drone for commercial purposes in the U.S. you must obtain a Remote Pilot Certificate from the FAA. But one ought not to be shocked to learn that law on technologies, including drones, could be diverse from one state to another, as we have seen it before. The United State of America rules the drones industry, which unmistakably means the dominance over manufacturing and usage. According to the Federal Aviation Administration (FAA)'s report, the number of drones is estimated to cross 7 million by 2020, with recreational drones accounting for 4.3 million units.[394] As a result, to stay abreast of the accelerating pace of UAVs' usage, the FAA and the particular states have provided for an excess of legislations for their regulation. In 2012, the USA Congress with an endeavour to address the safety concerns and to provide for uniformity all the way through the national airspace passed the FAA Modernization and Reform Act, 2012. The act calls for the FAA to "developa comprehensive plan to safely accelerate theintegration of civil unmanned aircraft systemsinto the national airspace system."[395] It goes on to declare that a 'model aircraft' which can be a drone, must not weigh more than 55 pounds;

[394] http://www.govtech.com/public-safety/Drone-Sales-Could-Reach-7-Million-by-2020-FAA-Says.html [accessed 25 Mar 2019]

[395] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2357657 [accessed 25 Mar 2019]

and, must be within the visual line of sight ('VLoS') of the operator; and must be used solitarily for recreational or hobby purposes. Model aircrafts are covered by Federal Aviation Regulation ('FAR') 101 which came into force in August 29, 2016.37 Now, it can be stated that any federal, state or local agency intending to operate a drone in national airspace must have a certificate of authorization from the FAA, whereas the commercial use of drones is allowed in accordance with FAA regulations and guidelines for private commercial use and the state-specific guidelines. In addition, FAA has already decided to implement plans to create test ranges and designating specific airspace throughout the country to be used to operate drone flights to develop better certification and air traffic standards.[396] "Even some of the simplest toy drones sold at stores are equipped with powerful high definition cameras. Perhaps it was just a matter of time before headlines such as "Neighbors Complain of Drones Flying over Backyards" appeared in newspapers across the nation[397]. Brian Farkas States that "[i]n the old system of British common law, courts enforced the notion of "ad coelum et ad inferos," literally meaning "to the heavens and to hell." This meant that a property owner had rights to everything above his land and everything under it. This concept has mostly disappeared from American courts, now that common electrical wires and pipes run under our homes, and aircraft fly above them"[398].

Legislation has not completely been up-to-date with new drone technology, though. The Federal Aviation Administration has passed regulations with the expressed intent of "minimiz[ing] risks to other aircraft and people and property on the ground." But, one thing can be observed concerning these guidelines or/and regulations, these "endeavours" mainly exempt hobby and recreational flying, which might be the very thing what your neighbour is doing[399]. Of course, the answers for these concerns have come by the form(s) of novel(and sometimes innovative) state or federal laws, and they have become part of the mixture. Many states are still researching and studying the matter in readiness to pass

[396] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2357657 [accessed 25 Mar 2019]

[397] Visit, for instance, Tara Evans, Neighbors Complain of Drones Flying over Winter Park Back Yards, WKMG Orlando, (May 7, 2015), https://www.clickorlando.com/news/2015/05/07/neighbors-complain-of-drones-flying-over-winter-park-back-yards/ [accessed 5 Nov 2020]

[398] https://www.nolo.com/legal-encyclopedia/what-do-when-your-neighbor-has-drone.html [accessed 5 Nov 2020]

[399] https://www.faa.gov/search/?omni=MainSearch&q=drone[accessed 5 Nov 2020]

legislation[400], and some states have already decided to pass it. There are states where these issues are solved differently, for instance, several states have exercised their police forces to confront reported use of UAS to intrude personal privacy rights.In Florida, and for example, *Criminal Code Section 934.50* forbids using drones for surveillance in violation of another person's reasonable expectation of privacy[401]. In another state, Arkansas, *AR Code Section 5-60-103* prohibits flying drones to invade privacy and commit video voyeurism[402]. In California, *Civil Code Section 1708.8* forbids the using drones to record another person without consent and this state forbids entering the airspace of an individual to capture an image or recording of that individual engaging in a private, personal, or familial activity lacking permission[403]. And Nevada law (*NRS 193.130*) outlaws weapons on drones[404]. The laws come from state rights to safeguard public health, safety, and welfare[405]" Under anti-paparazzi rules, Florida, for instance, prohibits the use of a drone to capture an image of privately owned property or the owner, tenant, or occupant of such property without consent if a reasonable expectation of privacy exists[406] Flying a drone to commit "peeping tom" activities in Mississippi is a felony[407]. Virginia requires law enforcement agencies to get hold of a warrant before using a drone for any purpose, except in limited circumstances[408409].

[400]See, for example: https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx [accessed 5 Nov 2020]

[401]http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0900-0999/0934/Sections/0934.50.html [accessed 5 Nov 2020]

[402]https://law.justia.com/codes/arkansas/2015/title-5/subtitle-6/chapter-60/subchapter-1/section-5-60-103/ [accessed 5 Nov 2020]

[403]https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1708.8.&lawCode=CIV [accessed 5 Nov 2020]

[404]https://www.leg.state.nv.us/NRS/NRS-193.html#NRS193Sec130 [accessed 5 Nov 2020]

[405] National Academies of Sciences, Engineering, and Medicine. Evolving Law on Airport Implications by Unmanned Aerial Systems. The National Academies Press, Washington DC, 2017, 40-41.Available: https://doi.org/10.17226/24932[accessed 5 Nov 2020].

[406]https://www.flsenate.gov/Laws/Statutes/2013/934.50 and https://casetext.com/statute/florida-statutes/title-xlvii-criminal-procedure-and-corrections/chapter-934-security-of-communications-surveillance/section93450-searches-and-seizureusingdrone/analysis?PHONE_NUMBER_GROUP=C&citingPage=1&sort=relevance [accessed 5 Nov 2020]

[407]https://law.justia.com/codes/mississippi/2013/title-97/chapter-29/in-general/section-97-29-61/ [accessed 5 Nov 2020]

[408]https://law.lis.virginia.gov/vacode/title19.2/chapter5/section19.2-60.1/ [accessed 5 Nov 2020]

6.6 The European Union

The framework for privacy/data protection legislation has already been provided in the European Union. The Charter for Fundamental Rights of the EU institutes, principally, the rights to respect private and family life, home and communications (Article 7) and addresses the protection of personal data (Article 8).[410]As a kind of first step, these rights are implemented through the EU Data Protection Directive 95/46/EC. The UK Human Rights Act 1998 and the European Convention on Human Rights also currently apply to the operation of surveillance drones. As far as the terminology of 'unmanned aircraft' is concerned, it can be a massive aircraft comparable to a manned aircraft in size and feature, but, of course it may well be a miniature consumer electronics aircraft. These days, the use of the smaller, even more sophisticate ones are being used in the Europe Union (EU), but, the (satisfactory) regulatory framework has not appeared yet, having only a presentation of a fragmented feature without being capable of fulfilling its main regulatory function. Fundamentally, in most cases, national safety rules can be applied, but the rules applicable look different from one member states to another in the EU, and, what is even more challenging is the fact that several key safeguards have not been addressed (so far) in a structured/coherent way. Some scholars have been coming up with concerns posing rational questions aching for clarification for the legal status of drones, but it is not unexpected in this field that a large numbers of answers might be found to enlighten us, for instance, about civilian drones. Thus, the question w*hat a civil drone is* could be answered and classified in a different way in accordance with the interpretations of different authorities. One of the memos of the European Commission has already made an attempt to respond to some repeatedly asked demanding questions concerning drones. The European Commission supposes that the term drone is used to portray any type of aircraft that is automated/computerized or programmed and can function with no pilot on board. In accordance with this authority, there are two types of drones. "Remotely Piloted Aviation Systems (RPAS), in short a drone where the aircraft is controlled by a human pilot from a

[409]National Academies of Sciences, Engineering, and Medicine 2017. Evolving Law on Airport Implications by Unmanned Aerial Systems. Washington, DC: The National Academies Press. https://doi.org/10.17226/24932.

[410] European RPAS Steering Group, Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System, June 2013:

http://ec.europa.eu/DocsRoom/documents/10484/attachments/1/translations/ [accessed 25 Mar 2019]

distant location. This means that there is always a pilot in control, even if remotely. These are the only types of drones that can be authorised presently, and under the new framework, for use in EU airspace. Unmanned drones, these are drones which are automatically programmed without being piloted (piloted by a human being present), even remotely. These are not yet authorised for use, either by ICAO or under EU rules."[411] Also, It is could be acknowledged that the term "civil" drones is used to cover those RPAS that are used for civil purposes such as delivering mail or examining an oil platform out at sea. Over time, civil drones have a great potential to perform various tasks, including jobs which are dirty, dull or dangerous for people. As for the usage of the civil drones, the European Commission declares that they have already been used to take over wearisome or sometimes hazardous/risky tasks which could be more efficiently or securely be performed by a technological instrument. In Europe, drones are being used for safety inspections of infrastructure, such as rail tracks, dams, dykes or power grids and other infrastructural facilities. There are some novel endeavours for regulating drones, one of them is the Notice of proposed Amendment (NPA) Unmanned aircraft system operations in the open and specific category and its Impact Assessment. On demand by the European Commission, Member States and other stakeholders, the Agency began to develop proposals for an operation centric, proportionate, risk- and performance-based regulatory framework for all unmanned aircraft (UA) establishing three categories with different safety requirements, proportionate to the risk: "open" (low risk) is a UA category for operation that, considering the risks involved, does not require a prior authorisation by the competent authority before the operation takes place; "specific" (medium risk) is a UA operation category that, taking into consideration the risks involved, needs an authorisation by the competent authority before the operation takes place and takes into account the mitigation processes identified in an operational risk assessment, except for certain standard scenarios where a declaration by the operator is adequate; "certified" (high risk) is a UA operation category that, considering the risks involved, requires the certification of the UAS, a licensed remote pilot and an operator approved by the competent authority, to certify an appropriate level of safety. After the publication of an Advance-NPA 2015-10 in July 2015, a Technical Opinion in December 2015, a "Prototype"regulation was drafted for the "open" and

[411] http://europa.eu/rapid/press-release_IP-14-384_en.htm [accessed 23 Jan 2019] and http://europa.eu/rapid/press-release_STATEMENT-14-110_en.htm [accessed 25 Jan 2019]

”specific” categories. In August 2016 the ‘Prototype’ regulation was published proposing actual rules providing the necessary clarity, notably on what are the responsibilities of the Member States and what is the flexibility offered to them. One must note the fact that a significant number of comments has been received and together with the significant inputs provided by an expert group have been taken into account to further develop the regulation text leading to the publication of an NPA. An impact assessment details analysis of several potential options considered. The analysis benefited also from feedback provided by stakeholders. The NPA has taken into consideration the developments in the international arena e.g. work done in the International Civil Aviation Organisation (ICAO); in the Joint Authorities for the Rulemaking of Unmanned Systems (JARUS) and of course in the USA (Federal Aviation Administration- FAA). The proposal grants a framework to safely operate drones while allowing this industry to have the chance to remain responsive and agile, to innovate and continue to grow. The risk posed to people on the ground and to other aircraft as well as privacy, security and data protection issues created by such drones are taken into consideration as well. The proposed regulation defines and classifies the technical and operational requirements for the drones. Technical requirements refer for instance to the remote identification of drones. Operational requirements refer among others to geofencing; a system that ensures the drones does not enter a prohibited zone. The proposal also addresses the pilots’ qualifications. Furthermore, drone operators will have to register themselves, except when they operate drones lighter than 250g. One can only admit that this proposal is ready for breaking new grounds by combining Product legislation and Aviation legislation. Indeed, design requirements for small drones will be implemented by using the legislation relative to making products available on the market (the well-known CE marking). The standard CE mark is be accompanied by the identification of the class of the drone (from C0 to C4) and by a do’s and don’ts leaflet that shall be found in all drone boxes. Based on the drone class an operator shall know in which area he or she can operate it and what competence is required for the operation. As it can be seen the proposal allows a high degree of flexibility for EASA Member States; they shallbe capable of defining zones in their territory where either drones operations are prohibited or restricted (for example to protect sensitive areas), or where certain requirements are alleviated. It is worth noting the fact that in order to operate drones with (be as it may evidently or regulatory) posing higher risks, the requirements hall be defined

an operational risk assessment that an operator needs to comply before flying (or operating) the drone.It is worth noticing that the proposal also attempts to provide special alleviations for people flying model aircraft which are also drones to recognize the good safety records in aero modelling identifying three options: Firstly, Member States may issue a special authorisation to model clubs and associations defining deviations from the UAS regulation; Secondly, Operations can be conducted in specific zones designated by Member States; or, thirdly, rations can be conducted in the open category according the operational limitations defined for one of the Subcategory (A3) EASA will submit a final Opinion to the European Commission at the end of 2017 which will take into account the feedback received to this proposal. With the adoption of the revision of Regulation 216/2008 *on common rules in the field of civil aviation and establishing a European Aviation Safety Agency* foreseen for mid-2018, the European Union will become competent to regulate civil operations of all kind of drones. To put it in practice, obviously, this means that national regulations ruling today's civil operations of drones lighter than 150 kg will be progressively replaced in 2019 and 2020 by new European legislations. The EU regulatory framework will cover all type of existing and future drone operations, fostering the development of innovative applications and the creation of a European market for unmanned aircraft services. While aiming mainly at making sure safe operations of drones, the European regulatory framework will also assist the enforcement of citizen's privacy rights and contribute to address security issues and environmental concerns in the benefit of the EU citizens. It will in addition enable the deployment of an Unmanned Traffic Management System, the U-Space, to support the development of drone operations in low-level airspace, beyond visual line of sight and congested areas.

Similarly to the USA, the EU has (made) an effort(or rather got a challenge) to provide for comprehensive set of regulations for regulating drones operation. The European Aviation Safety Agency (the 'EASA') in December, 2015 released the following notes titled: *"Introduction of Regulatory Frameworkfor the Operation of Unmanned Aircraft" and"Proposed Concept of Operations for Drones",* with reference to the regulation relating to the use and operation of drones.[412]

[412]https://www.easa.europa.eu/easa-and-you/civil-drones-rpas [accessed 25 Mar 2019]

The purpose of these “memos” is to recommend feedback for the members of EASA and other stakeholders such as companies/manufacturers and operators of regulatory framework for operation of drones. Anchored in the nature and purpose, the notes divide drones in the above mentioned classifications/categories. As regardsto the privacy/data protection implications and effects, the European Union has released a report on the assessement and evaluation of the ramifications of drones[413]. Nonetheless, one needs to acknowledge that detailed/comprehensive and in depth provisions are supposed to be outlined by the Eropean Union, the EASA notes grants and make transparency a possibility in terms of the objective of the proposed law and the rights and duties of the stakeholders. Till the final EASA rule is issued and made public, the EASA has delegated interim rulemaking for the regulation of Drones to its Member States, which have promulgated national regulations alike. National authorities are draw on (or utilizing) more use of drones in rescue operations or disaster relief actions, for instance, to overfly flooded/swamped areas and sectors or to give arial support to the fighting of forest or building fires. Other sectors can also be mentioned such as; drones operators can back precision farming through more effective and apt application of fertilizer, compost or insecticide. What one may possibly be able to envisage is that sooner or later drones could make it achievable to improve more efficient wind turbines and produce "greener" electricity, or to accomplish coverage of telecommunications in a money-spinning way. At the opposite side of the scale, engineers keep on working on miniaturization of drones (which can make them even more profitable and marketable), for example, micro drones which could be applied and manoeuvred to tackle gas or chemical leaks, or which could be programmed to act like bees to pollinate plants The zone is growinghastily with industries indicating their interest in adapting drones to execute specific/qualified services for which there is a market.[414] It looks realistic and logical, though, to note that the rules covering drones have been set at UN level, by the International Civil Aviation Organisation (ICAO), the UN body dealing with civil aviation. It permits drones operations (RPAS) on condition that a national authority gives a explicit authorization, for example, authorising the use of drones in a non-segregated airspace (this means that the same airspace also used by

[413] http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/519221/IPOL_IDA(2015)519221_EN.pdf [accessed 25 Mar 2019]

[414] http://europa.eu/rapid/press-release_IP-14-384_en.htm&http://europa.eu/rapid/press-release_STATEMENT-14-110_en.htm [accessed 19 Apr 2019]

"manned," human piloted air traffic). Such authorisations are routinely and naturally restricted/controlled to specific operations under specific circumstances to avoid security/safety hazards. Some of the member states in the European Union, such as Sweden, France, Denmark, Italy, Germany, Czech Republic, Lithuania and the UK have adopted legislation for simple operations by light RPAS, to avoid this case-by-case authorization process.[415]

Still, one setback appears to be unmistakable that national authorizations do not benefit from mutual recognition and do not allow for European wide activities, either to produce or to operate drones. The authorisation procedures do not provide a rational framework as well, with the required legal protections/precautions in connection to concerns about safety, security, privacy, liability to be built in. These nuisances might point to another constant issue related to the EU Member States' progress connected to the "desired" harmonization procedure advocated by many. The European Commission raises its concerns and endeavours to alarm the member states since drones have already started to appear in our skies but there are no clear general rules, at national or at European level, which put in place the obligatory safety measures protect thesafety, security and privacy of people. Moreover, operational and technical rules are also supposed to be further improved in order toguarantee that civil drones can fly like 'normal' air traffic and be integrated among 'normallypiloted' aircraft in non-segregated airspace without affecting the safety and the operationof the whole aviation system.It looks obvious that mastering civil drones (RPAS) technology is the key to the future competitiveness of the European aeronautics industry - on some approximations in the next 10years it could be worth 10% of the aviation market.The impact of drones and their countless applications on the economy could potentially becompared to the development of the internet in the nineties. It means that the safedevelopment of the European market for drones is crucial step towards building theaviation market of the future.[416]According to the memo of the European Commission, the Communication on opening the market for RPAS is an invitation to all stakeholders to build together a policy framework for the development of a competitive

[415] I intend to devote a subchapter analyze some of the above mentioned countries in order to highlight the differences in contrast to other attempts.

[416]http://europa.eu/rapid/press-release_IP-14-384_en.htm&http://europa.eu/rapid/press release_STATEMENT-14-110_en.htm [accessed 19 Apr 2019]

drones market as well as rules that will tackle all citizens' concerns. This policy framework will concern civil rules and commercial operations, in line with EU competence. It does not discourse military applications, for obvious reasons.The proposal would cover the 5 basic aspects (a-e): First, strict EU wide rules on safety, second is protect citizens' fundamental rights, the third is to have tough(er) controls to ensure security, fourth guarantee third party liability and insurance, and the last one is to support market development and European industries.

6.7 Strict EU wide rules on Safety:

One can admit that security/protection is thecentral objective of EU aviation guiding principle, or, as a minimum, it is assumed to be in the centre of the agenda. The integration of RPAS will be supposed to be based on the principle that all operations will have acomparable level of safety in contrast to ordinary/standar, manned, aviation. The regulatory framework would first centre on areas where technologies are advanced and where there is appropriate confidence on the basis of actual lessons learnt and/or adapted. Building on developing expertise and the improvement of the permitting technologies, regulatory measures will be introduced gradually and more multifaceted/intricate and multi-layered RPAS operations will be progressively permitted. The European Aviation Safety Agency is best positioned to develop such common rules which must be compatible with ICAO standards.

Protect citizens' fundamental rights:

Drone operations must (or as far as I can see, are supposed to) respect the Charter of Fundamental Rights of the EU, including the respect for the right to private and family life, and the protection of personal data. Flexibility, discretion, (relatively) low costs (depending on their sophistication or precision) and ever more sophisticated sensors are some of the characteristics that make RPAS unique tools for effective and discrete/undercover surveillance and monitoring missions. But the increased use of RPAS together with the capacity to store ever accumulating amounts of data on the ground might be likely to promote ethical, privacy/data protection issues and concerns. The Commission endeavour to assess how to guarantee that RPAS applications comply with the applicable rules and regulations of data/privacy protection. Privacy requires unceasing monitoring and

observation by the "proficient," "expert" authorities as well as the national data protection supervisory authorities.

Tough controls to ensure Security:

RPAS are not supposed to be immune to potential unlawful actions and might potentially be used as weapons. Terrorists, criminals or rogue states could use their own RPAS, could jam the navigation or communication system signals of other RPAS or hijack ground control stations. Security aspects are vital when developing the necessary information streams to manage 4D trajectories in the future air traffic management system. As this information needs to be shared in real time by all aviation stakeholders to optimize the performance of the system, the security dimension becomes all the more important. Security aspects therefore are essential elements of the future air traffic management system, of which RPAS will become an integral part.[417] The identified security requirements will then require to be interpreted into legal obligations for everyapplicable player, like service provider for air navigation, RPAS operator or telecom service provider, under the oversight of the competent authorities at the national or European levels.

Guarantee third party liability and insurance:

The recent third-party insurance system has been established frequently in terms of manned aircraft. The Commission will assess the need to amend the existing rules for RPAS specificities and the way to promote the expansion of an efficient insurance market where fees correspond to the real financial risk projected on the basis of assimilated evidence through incidents and accident reporting.

Support market development and European industries:

The Commission aids the emergence of a RPAS market and the competitiveness of the associated industrial sectors making use of EU instruments such as the Horizon 2020 and COSME programmes. It will support the development of RPAS applications and the associatedand linked techs, inspire and encourage user-driven innovation, and promote the formation of cross sectorial industrial value chains, apt support infrastructures and clusters. The Commission identifies policy opportunities to promote the utilization of this

[417] http://europa.eu/rapid/press-release_IP-14-384_en.htm&http://europa.eu/rapid/press release_STATEMENT-14-110_en.htm [accessed 19 Apr 2019]

innovative technology. For example, RPAS might assume an important role in Copernicus, the EU's Earth Observation Programme, where they could successfully complement space-borne and onsite sensors for some monitoring and surveillance services.[418]

6.8 Drones in the United Kingdom:

I have decided to devote a subchapter to Britain, since it looks observable that the imminent challenges presented by the Brexit "paradox" must be affecting every walk of live. Though we could observe Brexit as a grim reality of the EU, it appears fair not to exclude Britain as a key actor in the market, to get hold of a clearer picture of drones and their regulations; UK presents us a quite nice illustration how deep this difficulty or dilemma can go with no exaggeration. Consequently, I aim to outline current regulations for the use of recreational and commercial drones in the UK. I also intend to highlight the latest policy development in the UK and worldwide, as well as emerging technological and regulatory issues connected to drone integration or "assimilation" into domestic airspace. The Civil Aviation Authority (CAA) is the independent statutory authority liable for regulating civil aircraft, including (among many things) drones. Applicable legislation is contained primarily in the Civil Aviation Act 1982 and the Air Navigation Order 2016, with detailed guidance set out in the CAA's Unmanned Aircraft System Operations in UK Airspace – Guidance (CAP 722). What we can easily identify is that drone policy and relevant legislation can be mainly said to be the liability of the Department for Transport (DfT) and the CAA. It is also fair to state that the Government does not (really) has an (or any) official policy or strategy on drones this is unmistakably an area where policy is moving fast.[419] In 2016 the DfT consulted on proposals to fill any gaps in drone regulation. The result was published in July 2017, with a number of initiatives, such as registration, training and "geo-fencing" to be taken forward in different ways.[420]

[418] http://europa.eu/rapid/press-release_IP-14-384_en.htm&http://europa.eu/rapid/press release_STATEMENT-14-110_en.htm [accessed 19 Apr 2019]

[419] Let us not forget the fact that is a global problem realised in many countries, as I have already outlined in the case of Hungary.

[420] HAYLEN, Andrew – BUTCHER, Loise: *Civilian drones*. Briefing Paper Number CBP 7734, 3. available: http://researchbriefings.files.parliament.uk/documents/CBP-7734/CBP-7734.pdf [accessed 9 Jan 2019]

It is important to observe that Adrew Haylen and Louise Butcher argue that "[....] achieving the full and safe integration of drones into non-segregated airspace is the underlying policy objective of Government. To achieve this requires technology, which is not yet fully developed, for sensing and avoiding air traffic under all possible scenarios."[421]They also claim that, in the intervening time policy and regulation is expected to focus on drone system reliability, and enforcement, as well as training and qualification standards for drone pilots and operators.[422][423] Although wemay well ponder upon the legal "tools" to be effective, since it might seem easy to starve for regulations but how to create a relevant and effective regulatory system of drone matters may prove to be more tricky as far as the current developments seem to suggest. Andrew Haylen and Butcher Loise argues that many experts view the use of the term 'drone' as inaccurate and ambiguous/deceptive, as it fails to capture/define either their purpose or degree of technological sophistication. Though, for the purposes of their paper, the term drone is used with no better alternative. What are universally or commonly known as drones, but also referred to as remotely piloted aircraft systems (RPAS), Small Unmanned Aircraft (SUA), or unmanned aerial vehicles (UAVs) – come in a variety of shapes and sizes,[424] ranging from small hand-held types up to large aircraft.[425]

Drones have been emerging beyond the confines of the military and are now used in a wide range of industries, such as, precision agriculture; inspection of public facilities; safety (including inspecting high, dangerous structures such as oil rigs); mapping; aerial photography (including by the news media); and filming and by police and security forces for, among other things, search and rescue operations, border patrols and general surveillance.[426]

[421]HAYLEN – BUTCHERop. cit. 3.

[422]HAYLEN – BUTCHERop. cit. 3.

[423]I intend to examine the regulatons currently launched in the Eu, the USA, and some common law countries as well, in connection wirh technology related topics, such as Internet regulations.

[424]In order to obtain more information, one should consult the following: House of Lords European Union Committee, Civilian Use of Drones in the EU (Seventh Report of Session 2014-15), HL Paper 122, 5 March 2015, Table 1, p.12

[425]Civil Aviation Authority (CAA) Flying Drones - Guidance on the safety rules [accessed 22 Feb 2018]

[426]Statewatch, *Back from the Battlefield – Domestic Drones in the UK*, May 2014 https://www.caa.co.uk/Consumers/Unmanned-aircraft-and-drones/ [accessed 22 Feb 2018] also in April 2015 UPS announced its participation in a study for the use of UAVs for humanitarian disaster relief operations,

In the UK alone, there are now almost 2,500 permissions for commercial drone operations.[427]

6.9 Italy and Hungary: New Drone Regulations:

In accordance with Italy's national aviation authority, the Italian Civil Aviation Authority (ENAC), flying a drone is legal in Italy;however we recommend being aware of and compliant with the drone regulations listed General Rules for Flying a Drone in Italy, since one may find some characteristically Italian rules related to drones.

One can find many rules and regulationswith reference to drones, but the most significant and vital rules to know for flying a drone in Italy as follow: Drones must be identified by a plate showing the identification of the system and of the operator. An identical plate shall be installed also on the remote ground pilot station. As of the 1st of July 2016, besides plates required by the Art 8.1, all drones that let the transmission of data in real time must be equipped with an Electronic Identification Device. Also, drone pilots must maintain a direct line of sight with their drone during operations, and the drones may not be flown at night. In addition, drones are not permitted to fly over people or crowds, including sports events, concerts, and other large events. There is a special/additional regulation for (civil) recreational drones or drones used for commercial purpose(s), in view of the fact that drones being flown for recreational purposes may well not fly more than 70 meters (230 feet) above the ground, and drones being flown for commercial purposes may not fly more than 150 meters (492 feet) above the ground. Plus, drones may not be flown within 5 kilometers (6.8 miles) of any airport or airfield. Commercial drone pilots conducting low-risk operations must submit a statement of compliance with specific requirements to ENAC along with a 94 Euro processing fee. For higher risk operations commercial drone pilots must obtain training and operating certificate as well as a health certificate. Learn more about the requirements for commercial operations on the ENAC website[428].

---

see: *UPS press notice, "UPS Brings Technology and Logistics Expertise to Study of Drone Use in HumanitarianResponse*", 21 April 2015.

[427]CAA, Approved SUA operators, as at 17 February 2017

[428]https://uavcoach.com/drone-laws-in-italy/ [accessed 31 Oct 2018]

Nonetheless, it is not unexpected for us that another, slightly diverse, interpretation of Italian drone laws can be found on the website of UAV systems international.[429] On this site, it is declared, of course, that drone use is permitted in Italy, but the regulations/rules are very strict weighed againstthe regulations of numerous countries, and there are several drone laws that require to be considered and followed when one flies a drone in Italy. Operators must make it certain that they follow the appropriate drone laws when flying in Italy. You shall not fly your drone over people or large crowds, this rule is taken seriously, and there are numerous reports online of individuals being arrested and having their drones seized within minutes of take-off when trying to fly them around tourist attractions with loads of people close by.

While using a drone, one shall respect others privacy when one flies a drone and must fly during daylight hours and only fly in good weather conditions. Your drone ought not to fly/be flown in/over sensitive areas including government or military facilities because the use of drones or camera drones in these areas are prohibited. You may not fly your drone higher than 230 feet and further than 650 feet horizontally or out of visual line of sight, whichever is first. Additionally, one should not control your drone using goggles such as the DJI Goggles unless you have somebody else alongside you visually watching the drone all the time. To fly over some places requires permission, thus you may not carry dangerous goods on your drone and may not fly your drone over beaches (during summertime), national parks, urban areas, infrastructures, railways, highways, or industrial plants without prior permission

Of course one also can find supplementary rules, they are the following: You must stay at least 5km away from airports and must only fly your drone during daylight. As for the weight of drones is concerned, a drone must weigh under 25 kg, and one must keep the drone 50m away from persons/property not under the control of the drone operator. Furthermore, you must carry third-party insurance if you will be using your drone for commercial use.[430] Drone use is permitted in Hungary, but there are several drone laws that

[429] https://www.uavsystemsinternational.com/drone-laws-by-country/italy-drone-laws/ [accessed 31 Oct 2018]

[430] https://www.uavsystemsinternational.com/drone-laws-by-country/italy-drone-laws/ [accessed 31 Oct 2018]

require to be followed when flying in the country[431]. Operators must ensure that they follow the following drone laws when flying in Hungary[432], one shall not fly the drone over people or large crowds and shall respect others privacy when flying your drone. Also, one is not supposed to fly your drone over airports or in areas where aircraft are operating and drones are assumed to be flown during daylight hours and only in good/fair weather conditions. Any drones era not permitted to fly in sensitive/protected areas including government or military facilities. And lastly, the use of drones or camera drones in these areas is prohibited. The rules and regulations on unmanned aircraft systems (drones) in Hungary are aligning with international trends, and have been tightened by an amendment to Act CXXXVI of 2016 on the Amendment of Act XCVII of 1995 on the Aviation (the "Act"). The new rules were in force as of 31 December 2016. However, most of the details are to be regulated in an upcoming government decree, and lawmakers are also expected to cover data protection aspects. For example, the Act does not differentiate between toy machines and heavier ones. Effective data protection regulations, according to this issue's importance in the world, are still to come in Hungary.[433] Also, the condition for the legal operation of a drone: operators shall be aware of the airspace, territories and restricted areas where they shall not enter with their drones. These areas may vary from time to time, they can be different types, such as, accidents, entourages of protected persons, protected objects or territories, for instance, filming locations. The aviation authority intends to create a mobile phone application to inform drone operators and the public on airspace closure. As for as liability insurance is concerned, in order to protect operators and third parties, operators shall have liability insurance regarding the aviation activity performed with their device. The insurance shall, at least, cover the following amounts of compensation for damage caused by the drone: below 2 kg takeoff mass: up to HUF 3,000,000 (approx. EUR 10,000) ;Between 2 kg and 10 kg: up to HUF 5,000,000 (approx. EUR 17,000) ;And above 10 kg: up to HUF 10,000,000 (approx. EUR 33,340).The

[431]See, for instance: Tóth László.: Tájékoztató a pilóta nélküli légijármű-rendszerek (UAS) frekvenciahasználatáról és engedélyezési kérdéseiről. Nemzeti Média- és Hírközlési Hatóság, 2018https://nmhh.hu/dokumentum/193162/UAV_tajekoztato.pdf[accessed 11 Sept 2023]

[432]https://www.uavsystemsinternational.com/drone-laws-by-country/hungary-drone-laws/ [accessed 1 Nov 2018] On these website there is a warning, and we are informed that drone laws are constantly changing. To stay up to date on the latest drone laws changes, one should sign up for an account to receive drone law notifications.

[433]http://www.cms-lawnow.com/ealerts/2017/02/hungary-new-drone-regulations[accessed 1 Nov 2018]

government decree is expected to enter into force on 2018. It may ease the strict rules of the Act, red tape and unrealistic requirements with more detailed provisions. The draft provides that not every drone shall be registered, but each category of drone falls under the obligation of completing an e-course on aviation. The toy drones less than 250 grams are not regulated under the scope of the regulation. The decree attempts divide the drones into three plus one categories. According to the latest amendment of the upcoming government decree, the weight of the drones shall be applied on the takeoff mass. Except for toy drones, devices may not fly above 130 meters from ground and more than 500 meters away from the operator who must maintain continuous and direct visual contact without the use of supporting tools throughout the entire duration of the flight[434]. Although it seems similar to the EU regulations on drones[435], Hungary has an supplementary, 4th, category, in the first category for drones below 2 kg, the operator shall perform the minimum requirements, such as visibility and passing online training, but in the second category, the operator shall register the drone and have an operating license issued by the aviation authority after attending training and passing theoretical and practical exams. For drones between 2 and 25 kg, liability insurance is not obligatory. For devices above 25 kg in the third category, the operator shall have a qualified professional license, after the device has passed the airworthiness test. In this case, the operator shall keep an (electronic) logbook, and shall conclude liability insurance for the aviation activity. The fourth, extra, additional category, drones of over 150 kg in weight, falls within the competence of the European Aviation Safety Agency. With the imminent government decree, inhabited areas will reach a special position among restricted areas. The operator may use the device there if conforming with specific visibility requirements for drones and operators. The devices may not be operated within an altitude of 30 meters above private property without consent. According to the draft, specific rules will apply on drone operation for sports and private purposes. Drones may approach residential buildings not closer than 100 meters. Drones can approach individuals not involved in the aviation closer than 30 meters only upon their prior written

[434]https://www.uavsystemsinternational.com/drone-laws-by-country/hungary-drone-laws/ [accessed 1 Nov 2018]

[435]There are some new attempts for regulating drones, one of the most recent developments on drones is *the Notice of proposedAmendment (NPA) Unmanned aircraft system operations in the open and specific category and its Impact Assessment*.

consent. The drones shall have such paint and built-in lighting, and operators shall wear such clothing like safety vests, which ensure their visibility in daylight as well[436].

6.10 The latest development on drone regulation: 2020.[437]

As it could be foreseen, from July 2020, national rules will be replaced by a common EU regulation. The purpose of this reform is to create a harmonised drone market in Europe with the highest level of safety[438], which one might add is in sync with the attempts of harmonisation by the EU, covering almost all walks of life. In fact, it means that once a drone pilot has received an authorisation from its state of registry, he or she will be allowed to freely circulate in the European Union. To obtain more information about the new EU wide rules and regulations on drones are accessible in details on the website of the European Aviation Safety Agency[439][440][441]. The endeavour of the EU regulatory framework is to cover every type of existing and supposedly future drone operations, encouraging the growth of high-tech/modern applications and the creation of a European market for unmanned aircraft services. It might be seen as a kind of nurturing environment for market based and friendly regulated drone services, While targeting primarily at certifying and guaranteeing safe operations of drones, the European regulatory framework will try to assist and promote the enforcement of citizen's privacy rights and contribute/support to address security concerns and environmental issues in the benefit of the EU citizens. Additionally, it will in enable the distribution of an Unmanned Traffic Management System, the U-Space, to support and sustain the progress of drone operations

[436] https://www.uavsystemsinternational.com/drone-laws-by-country/hungary-drone-laws /[accessed 1 Nov 2018]

[437] https://dronerules.eu/en/professional/eu_regulations_updates [Accessed 24 Jun 2020]

[438] AMC & GM to Commission Implementing Regulation (EU) 2019-947 - Issue 1 Related ED Decision ED Decision 2019/021/RExplanatory Note [pdf] Explanatory note to ED Decision 2019/021/R

[439] https://www.easa.europa.eu/domains/civil-drones-rpas [Accessed 24 Jun 2020]

[440] For more information, one can also turn to: Flying a Drone - do's and don'tsProposed consumer information – 2018[pdf] and Safe operation of drones in EuropeUpdate on EASA's activities - April 2018 [Accessed 24 Jun]

[441] See also: Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 - Unmanned Aircraft Systems and Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 - Unmanned Aircraft SystemsEasy Access Rules: Unmanned Aircraft Systems (Regulation (EU) 2019/947 and Regulation (EU) 2019/945)

in low-level airspace, beyond visual line of sight and blocked areas. The European regulatory framework will be based on the following principles: a risk-based and proportionate approach and a shared responsibilities between the European Union and its Member States, and as it has been debated (and I have already outlined it), there should be three different categories, namely, based on the risks involved, open category, specific category and the last is certified category.

A risk-based and proportionate approach:

The (relatively new) framework will present three categories of operations (open, specific and certified) consistent with the level of risks involved. In order to get a clearer view of the targeted subjects of the regulation, a different regulatory method will be implemented for each category. Low-risk operations ("open" category) will not require any authorization, but will be subject to strict operational limitations. As for medium risk operations, operators will have to oblige an authorization from the national aviation authority on the basis of a standardized risk assessment or a specific scenario (specific category). Lastly, for the high risk operations, classical aviation rules will apply (certified category).

A sharing of responsibilities between the EU and the Member States:

In order to achieve the necessary flexibility considered necessary by the Member States of European Union, every state will be allowed to delineate "zones" to restrict the access of certain portions of their airspace or in contrast ease the conditions there. By doing so, national "characters" and specificities will be addressed (and applied) at the most applicable and appropriate level. It also seems important that registration and authorizations will also be dealt with and executed at national level on the basis on common rules. By the end of the year 2020, the European Commission will adopt two regulations covering unmanned aircraft operations in the Open and Specific categories. The first regulation will define rules and procedures for the operation of unmanned aircraft. The second one will define the technical specification applicable to the drones authorized to be operated under the open category. The basis of these regulations will be the Opinion

01/2018[442] published by EASA, the European Aviation Safety Agency on the 6 February 2018.

The categories implemented: open, specific, and certified category.

It is vital to realize the "open" category is considered to be the least risky of the three operations, thus this category will not require prior authorizations or pilot license. Still, the operations are limited to: in visual line of sight (VLOS), below 120 m altitude and performed with a privately built drone or a drone compliant with the technical requirements defined in the regulation. To demonstrate this compliance drones that can be operated in the open category need to have a class identification label. Plus, additional operational restrictions and limitations apply to each class of drone, particularly concerning the distance that must be maintained between the drone and non-involved persons. When the planned operation surpasses the restrictions of the "open" category, the operator ought to consider operating under the "specific" category (medium risk), as it is the operator's duty to modify it based on its intended operation. Due to risk assessment, only high-risk operations require compliance to classical aviation rules under the "certified" category, as if it were operated in controlled airspace. Operations concerning drones of more than 25 kg and/or operated beyond visual line of sight will characteristically are considered to get the "specific" category label. Before starting an operation in the specific category, operators must either perform a risk assessment, using a standardized method, the SORA[443][444]. It is provided by EASA[445], and helps the definition of mitigation measures or verifies whether they can comply with a specific scenario defined by EASA or the national aviation authority. On that basis they will be able to obtain an authorization from the national aviation authority. There might be some cases a simple declaration may be enough. The authorization or the specific scenario will outline the authorized operation and the applicable mitigation measures, for instance, the technical requirements of drones, pilot competence, or licenses and so on. The "certified" category, assuming high risk, involves

[442]https://www.easa.europa.eu/document-library/opinions/opinion-012018 [Accessed 24 Jun]

[443]SORA (Specific Operations Risk Assessment) is a multi-stage process of risk assessment aiming at risk analysis of certain unmanned aircraft operations, as well as defining necessary mitigations and robustness levels.

[444]To obtain more information on SORA, visit: https://www.eurocockpit.be/positions-publications/specific-operations-risk-assessment-sora [Accessed 24 Jun 2020]

[445]To get more information, see: https://www.easa.europa.eu /[Accessed 24 Jun 2020]

operations including “large” drones in controlled airspaces. Rules applicable to the “certified” category will be the same as for manned aviation: drones must be certified for their airworthiness, pilots shall be licensed, and safety oversight will be performed by the relevant National Aviation Authorities and EASA. But there should be some amendments related to existing regulations, on which EASA is presently working on. The specific features of the high-risk UA operations are the following: the approval of design, production and maintenance organisations; air operator certificates of air operator; UA operations, licences of personnel.

Chapter 7 Future of novel techs such as biometrics and drones:

Regardless of the security benefits these novel and innovative technologies afford society, however, their wide-ranging application also involves and observably leads to severe issues, including technological challenges, disputes and concerns related to privacy. Various forms of identification, such as driving licenses, passports, and other identity cards, are increasingly being combined with biometric info, and it can stated as well that the use of them will be spread to other sectors as well. As a result, I presuppose that this perceptiblerichness of private info will entail more advanced measures connected to data/privacy protection, encryption technologies, and other safeguarding measures, both to support their approval, recognition and use by the civilian population and to keep this critical info from falling into the wrong hands. The multifaceted and itricate relationship between biometric data and drones concerning privacy and their regulation entails and leads to quite a few important ethical, legal, and practical considerations and concerns. Some of these aspects related to the liason between biometrics and drones are the following: data collection, mass surveillance,data storage and security.Thus, one might admit, there might be no doubts, the “bond” between biometric data and drones pertaining to privacy and regulation is comprehensive and requires a delicate balance.

A so-called equilibrium is needed between innovation and the protection of individuals' rights. Effective regulations should address consent, data storage, data sharing, biases, and transparency to ensure responsible and ethical use of biometric data in drone operations as well. Furthermore, international collaboration may be indispensable to create

consistent regulations across borders, given the global nature of drone technology and data flow.

Still, it should not be neglected that biometric data possibly will be used by governments in loads of ways. Critics such as the American Civil Liberties Union (ACLU) are overwhelmingly concerned that such power could easily be abused for unethical, corrupt and unlawful purposes. While biometric technologies have highly developed with a velocity unprecedented, they are still given to technological deficiency or limitations, such as computer errors, “cog in the wheels” and glitches, which might and are able to misidentify individuals, discloseor reveal sensitive or critical private data, and lead to other privacy-related concerns/issues.Also, there are concerns connected to surveillance and its uneasy relation to Civil Liberties, the use of drones for biometric data collection can infringe on civil liberties, including the right to privacy, freedom of movement, and freedom from unwarranted/unjustifiable surveillance by any governments/administrations or agencies related to them. No one really denies that striking and achieving a balance between security and individual rights is a significant challenge. Nowadays, concerns that most often brought up are connected to the potential for "mission creep," where drones primarily deployed for specific purposes, such as search and rescue or monitoring critical infrastructure, are repurpose for broader surveillance or law enforcement activities.

As far as I can distinguish we have to admit there are quite a fewextra issues readymaterializeand come into sight world-widely, first and foremost related to privacy and third-party liability, to improve integration and perhaps as radically or extensively, the public perception of novel technologies, such as drones. The regulatory framework applicable for drones is multilateral, and my doctoralthesis has only endeavoured to draw attention to some linkedapplicable aspects of privacy/private data protection law, aviation law. The so-called drone acts are not even close to being concluded, let alone effective, but to lay them to rest looks too early, as they can be observed as new born babies with no relevant experience, in their toothing period. The legal and institutional framework of privacy/data protection does not always seem ready to face innovative challenges offered and readily presented by the use or applications of novel technologies, such as drones, for example. Regulatory “enterprises”(to go where no-one has ever gone before) may differ, as the FAA regulations categorise/clasify drones by size and shape, the EASA regulations opt for more *risk*-based categories, and the EU regulations are focused on licenses and

certifications. But I venture to state that one fact stays, novel/innovative techs, such as drones, need to be regulated at a srict level and their regulations are needed to be revised time after time to catch up with the latest developments happening, without exaggeration, on a weekly basis.Navigating the evolving landscape of biometric data amassing by drones necessitates nonstop-constant adaptation of regulations, ethics, and technologies. It also dictates a commitment to transparency, accountability, and the protection of individual rights to guarantee that the integration of biometric data and drones provides and supplies the greater good while minimizing potential harms and wrong-doings.We need to keep in mind the emerging biometric technologies as well, for example, *Heart Rate and Gait Analysis*, when drones equipped and kitted out with sophisticated and advanced sensors can potentially accumulate biometric data beyond facial recognition, including heart rate or gait analysis. One may be well awere of the fact that this introduces novel privacy concerns and issues as more intimate physiological and behavioural data can be attained and acquired.Also the collection of DNA and Genetic Data should be reconsidered as well, since;researchers are getting closer to a phase when drones may have the capability to accumulate genetic information from individuals through various means, such as hair or skin samples. The ethical implications and regulations surrounding the gathering /accumulating and use of genetic data are complex and evolving.

7.1 Then and now: laws on first and second generation biometric systems[446]

Respected and well-versed legal scholars, for instance, Tamás Klein András Tóth, Péterfalvi Attila and Révész Balázs who are experienced in technology and its latest achievements discuss and examine, biometrics, biometric systems, phones, and drones independently as if they were not aware of the fact that most devices mentioned can interplay/communicate with each other or can even cooperate to achieve and execute complex tasks. This might be explained by the fat that covering one of the devices is a tremendous amount of research. Also, it may appear that scholars keep forgetting that

[446]This chapter is based on: SIMÓ, Ferenc Zoltán. *Thenand now: Laws on first and second generationbiometricsystems*. PRO FUTURO - A JÖVŐ NEMZEDÉKEK JOGA 9 : 3 pp. 78-90. , 13 p. (2019)

scientists workday and night to invent and develop novel technologies/prototypes and trial products. Although their work is comprehensive, fine-tuned and refined, Tamás Klein and Adrás Tóth[447] do not discuss (comprehensively) the so-called second generation biometrics. It could sound as a work of science fiction, but, in actual fact, it is reality. One of the best examples may be telephones, as we have been calling them for decades without being aware of the fact of their progress, but (smart) phones, to be honest, are no longer "*simple*" caller and receiver devices, but complicated computers, cameras (contributing to the extinction of "mere" cameras), data bases, and calculators (to name some) as well. They can also beconnected by other phones and other devices (for example drones) using biometrics. Thus, even if I examine them in separate chapters, I incline to bear in mind that they should be dealt with caution, since those technological devices can be interconnected or even controlled by an Artificial Intelligence, which now is a barefact and not a chapter in a piece of literature any more. In due course, I propose to focus on the examination of normative regulation with an emphasis on the legal reaction evoked by new/innovative techs.

7.2 An Introduction: Application(s) of Biometric Technology and Preliminary observations on biometrics:

Biometric characteristics havebeen used for a long time to recognize /identify/categorize known/identified or unknown/unidentified persons. Biometric systems are unlike the former use of unique or distinctive human features/characteristics in that these dayssystemsare capable of buildin up and amassing the unique and persistent/distinctive characteristics for computerized/automatic wvaluations and comparisons. Biometric systems are fairly novel, theirexpansion set off only some decades ago. But these highly complex systems and their functioning are mostly understood by only experts. And, in the meantime, one cannot and should deny that biometric systems have been set up and broke new ground for (exceptionally and extremely) large-scale implementations, meeting a societal requirement and "wish" for more security and able/professional cooperation. Principally, it is well-known that these systems have been

[447]KLEIN – TÓTH: op. cit. The authors focus on two aspect of novel innovations, "disruptive" and "unknown" innovations, but they mostly center their attention on legal challenges in connection with technological innovations and related issues such as data protection, robots, cyber law and drones.

installed by the governments primarily focused on third country nationals, for example, on foreigners, such as asylum seekers or applicants for visas. Launching systems, such as Eurodac and VIS, were proposed to investigate/observe criminals by SIS and SIS II. Also, biometric systems have steadily been expanding to the European Union and Member State nationals, for instance, the introduction in 2004 of the biometric ePassport in the Union Member States without reflective public responds or disputes then. Furthermore, the rationale of these systems has been formulated or, if the original purposes were limited, the purposes and access to the databases were in quite a lot of cases extended (and delayed), as in the case of VIS. Additionally, biometric systems have been and are still impending in every one's day to day life in the private sector, on occasion at a young age, for instance, for access control in schools, which possibly willhoist even more privacy concerns than ever before, though the purpose or objective of the previously mentioned example looks understandable and plain. To smooth the progress of the debate about the use of biometric systems, including an analysis of its legal aspects, a "*plain*" understanding of the functioning of biometric systems (at least, for the legal and public sector) and of their main features, including of some more technical aspects as well, is supposed to be mandatory but, as it can be seen, is often absent. But, it seems that biometrics have captured the attention of private and legal sector, and the debate, regarding privacy concerns has started to heat up around the globe. Or, as Els J. Kindt makes a note of it, the results could be offered by a biometric system are for each use and application different and, it should be admitted that they are not "*plug and play*" and, since these systems are chieflyanchored in measurements and statistical methods, with (noticeable and understandable) standard errors (being inherent or even inbuilt intentionally), these considerations must be taken into account,too.[448]Besides, with taking into account that because of the intra-class and interclass variability of the characteristics measured, the comparison can never be100 %[449], even though the technology has been developing in haste without holding back in the horizon, thus wrepossibly will state that biometric systems remain "inherently fallible". With no doubts, this fact may lead us to our privacy concerns too, since we need therefore to recognize that biometric systems are because of the rates of the error(s) not suitable or

[448]KINDT, Els J.:*Privacy and Data Protection Issues of Biometric Applications – A Comparative Legal Analysis*. Springer, Dordrecht, 2013. (https://doi.org/10.1007/978-94-007-7522-0)https://link.springer.com/content/pdf/10.1007/978-94-007-7522-0.pdf [accessed 10 Sep 2019].

[449]Though I do not aim to state that there is the slightest chance to guarantee a system with 100% infallibility.

apt to offer 100 % security or convenience and that the efficiency for this reason is sometimes questionable, though I can also state that 100% accuracy is only a fairy tale and could not realisticly be achieved by any systems according to the present state of nowledge. And, of course, the accuracy which can be attained with biometric systems therefore remains (highly) conditional or uncertain[450].

7.3 Privacy and biometric technology:

One can find and ever-growing list of major concerns demonstrating/signifying the wearisome relation between novel techs and privacy. There is no doubt, and it looks apparent and evident that it may derive from two facts that were recognized and admitted a long time ago, first the unstoppable nature of (high) tech expansion/progress and the subjective nature of the concept of privacy, and as the clash of titans, these two are at a constant adjustment and readjustment to "live together" in peace (though, they sometimes seem to have at each other's throats), or rather in a status quo.[451] Jane E. Kinley declares that "[p]rivacy is a subjective, and therefore, elusive, concept. Invoking it can create unlimited opportunities for mischief and genuine damage to public welfare. Ignoring it can undercut the individual's right to determine what his or her identity and destiny will be"[452]. Considering the illusiveness of the concept of privacy and the ever-changing, fast-pacing nature of technology together may offer us some insights in order to come up with a "relationship" or a "*cooperation*" that might actually work without creating more and more concerns. Doubtless, it is not far-fetching to assert that technology, let alone "*novel*" technology and its concept are as elusive as the concept of privacy[453]. And, of course, there may not be any hope for anybody to come up with a unified definition of both. As far as biometric systems are concerned, it looks that the (re)definition of the notion of them is a

[450]The following issues related might be addressed in separate (sub)chapters of my dissertation: Biometric Data, Data Protection and the Right to Privacy, Biometric Data and the Concept of Personal Data, The Emergence of the Data Protection Legislation and the Concept of Personal Data, Are Biometric Data Personal Data? Are Biometric Data 'Sensitive Personal Data'?

[451]See, for example: WRIGHT, David – DE HERT, Paul (eds.):*Enforcing privacy – Regulatory, Legal and Technological Approaches*. Springer, New York, 2016. (Doi: https://doi.org/10.1007/978-3-319-25047-2) https://link.springer.com/content/pdf/10.1007%2F978-3-319-25047-2.pdf [accessed 17 Oct 2019]

[452]KINLEY, Jane E.:*Introduction.* In: ANGLIM op. cit., xxvi.

[453]See, JIANG, Richard – AL-MAADEED, Somaya – BOURIDANE, Ahmed – CROOKES, Danny – BEGHDADI, Azeddine (eds.):*Biometric Security and Privacy – Opportunities & Challenges in The Big Data Era*. Springer, New York, 2017. (https://doi.org/10.1007/978-3-319-47301-7) https://link.springer.com/content/pdf/10.1007%2F978-3-319-47301-7.pdf [accessed 25 Aug 2019]

project in progress. Some scientist, for example, Joseph N. Pato and Lynette I. Millett declare that "[v]irtually every discussion of the social implications of biometricsbegins with privacy, and for good reason. Biometric information is part ofan individual's identity (in the colloquial sense of the term), and a loss ofcontrol over that information can threaten autonomy and liberty. In thinking about these concerns, context is crucial. There is no onesize-fits-all set of rules to ensure that a biometric system adequately protectsprivacy[454]. They also argue, to support my point, that it will be essential instead to formulate policies for specificsituations and to (re)evaluate them time after time. But even this way, success cannot be guaranteed. Though Biometric technologies do not unavoidably threaten privacy, these technologies might be unbiased or neutral in that regard or they may perhaps even enrich privacy. Theresult rests on the choices each and every society makes with having a short-term or a long-term aftermath, too. Privacy links various constitutional norms in legal cultures of the world. For instance, In the USA, in the public sector, the failure of the administration to safeguard personalinformation can involve due process, its abuse of information can suppressfree speech, and its failure to have an adequate basis for obtaining information can challenge protections against unreasonable search andseizure as well as self-incrimination[455]. Thus, the complexity of privacy in connection with technology in different legal cultures may arise. *Kyllo v. United States:*[456]*The* recent Supreme Court decision that throws light on privacy and biometrics is *Kyllo v. United States*. Federal AgentWilliam Elliott suspected that marijuana was being grown in the home of Danny Kyllo, but he did not have the probable cause essential to get asearch warrant. Consequently, Agent Elliott sat in a car in the street nextto Kyllo's home and used a thermal imager to scan the residence. Theimager detected infrared radiation coming from Kyllo's house. The observed pattern revealed that parts of the house were hotter than the rest of thehouse and the neighboring homes. Agent Elliott decided that Kyllowas using

[454]PATO, Joseph N. –MILLETT,Lynette I.(Eds.), National Research Council:*Biometric Recognition: Challenges and Opportunities.*National Academies Press, Washington DC, 2010, 100-101. (Doi: https://doi.org/10.17226/12720) Available:http://nap.edu/12720 [accessed 25 Aug 2019]

[455]See, for instance, a recent decision of the U.S Supreme Court that can relate to the connection of biometrics and privacy rights. While the case does not directly concern biometrics, some of its potential implications for that field are noted. Consider the Supreme Court's 2004 decision in *Hiibel v. Sixth Judicial District Court*. Full text of the case available:https://www.lexisnexis.com/community/casebrief/p/casebrief-hiibel-v-sixth-judicial-dist-court [accessed 16 Sep 2020].

[456]KYLLO v. UNITED STATESCERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUITNo. 99-8508. Argued February 20, 200l-Decided June 11,2001. Available: https://supreme.justia.com/cases/federal/us/533/27/ [accessed 16 Sep 2020].

halide lights to grow marijuana. Using this and other information,Elliott acquired a warrant for a search. Once he was inside Kyllo's home, federal agents found more than a hundred marijuana plants. Kyllo, whowas ultimately convicted of manufacturing marijuana, appealed on theground that using a thermal imager without probable cause constituted anunreasonable search under the 4th Amendment. The Supreme Court,in another 5-4 decision, agreed with Kyllo. Two major lessons for biometrics may surface from *Kyllo*. The first lesson is that as a technology progresses and becomes widespread, our (private) zone or sphere ofconstitutionally guaranteed privacy seems to wane and dwindle. The Court of the United States recognizes, moreover, that the society's expectations of privacy set the baseline for lawsgoverning searches. In *California v. Ciraolo*,[457]the Court, inupholding aerial surveillance of a fenced backyard, explicitly said that"in an age where private and commercial flight in the public airways isroutine, it is unreasonable to expect" that one's backyard is private.[458] In*Kyllo* the implication of the Court was that if thermal imagers had been in common useits decision would have been different. Therefore, it can be supposed if the day comes when a biometric device that analyzes voices is able to function from a hundred feet or soand extend its range into a private home, and if use of that device turns out to bewidespread product sold by the thousands, the Fourth Amendment will have little application.If the first lesson offers a boost for biometrics, the second lesson doesthe opposite. All nine justices in *Kyllo* expressed concern about futuretechnologies that invade on privacy. The majority intended to step in now;the opposition desired to let the legislatures have the first crack at controllingfuture developments. On this question, the nine justices on the SupremeCourt are representative of a wide range of public opinion. The abilityof the government to use biometrics in order to track people's movementsaround their neighborhood or even inside their own homes will raise alarms for those concerned aboutprivacy and government intrusion. Publicagreement and approval, so vital and unavoidable, is likely to be missing unless the application of biometricsis highly justifiable and sensibly restricted[459].

[457]https://supreme.justia.com/cases/federal/us/476/207/ [accessed 16 Sep 2020].

[458]476 U.S., at 215.https://supreme.justia.com/cases/federal/us/476/207/ [accessed 16 Sep 2020]

[459]PATO – MILLETT op .cit. 100-101.

7.4 Short history of biometrics:

In our time technology is recognized across the world as an integral component of social transformation (and challange), and, by implication, it is also linkedto (a kind) of progress[460]. Furthermore, it is progressively more approved and agreed that technology cannot be understood outside its social context. Historians, and chiefly historians of technology, have come to make a distinction between the roles that cultural, political, and economic values have played in shaping technological improvement/novelty/innovation, as well as the role that technological innovation has played in formative/determining values. Such a "*contextual*" appreciation of technology is part of a larger endeavour to understand and control the interactions of technology and law as well. For this reason, a better understanding of our technological past can offer us and contribute to the practical end of revealing/exposing technology. The twentieth century witnessed a historic change and transformation in the relationship between science and society. In the so-called trench war, World War I, scientists were recruited and died in the trenches. In World War II they were excused as national treasures and committed to the utmost secrecy, and they united behind their country's war effort, and, of course, they devoted their lives to the "*cause*". The explanation of the change is not hard to find, since governments were ready to consider and recognize that theoretical research could produce practical progress in industry, agriculture, medicine and almost all walks of life, but having been in a hurry, they hardly pondered upon, and never imagined that one day, in the post-war future, the Pandora's box they had opened would not be able to be shut. It was not realized that without progressive legal attempts to regulate novel technologies, it would become the source of serious (legal) concerns. Their belief was firmly strengthened by improvements such as the discovery of antibiotics and the application of nuclear physics to the production of atomic arsenals. Science became so identified with practical profit and benefits and that the dependence of technology on science is universally supposed to be an eternal affiliation and a solitary enterprise.[461] Thus, science and technology, research and development, all four are seen to

[460]Though, the idea that technology is a progress is questioned time after time.

[461]See, for example: STUART, Casey-Maslen:*Pandora's box? Drone strikes under jus ad bellum, jus in bello, and international human rights law*.International Review of the Red Cross, Vol. 94 No. 886 Summer, 2012, 597 – 625 (https://doi.org/10.1017/S1816383113000118) .Available: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/D9D63CB248435F211105B052E3AB55EA/S1816383113000118a.pdf/pandoras_box_dro

be as inseparable as twins. The conviction in the pairing of science and technology is now petrified in the dictionary definition of technology as applied science. When we talk about technology, we usually think about novelty and the future. For many decades now the term "technology" has been closely linked with *invention* (the creation of a new idea) and *innovation* (the first use of a new idea). Talk about technology centres on research and development, patents and the early stages of use, for which the term *diffusion* is used. The timelines of technological history, and they abound, are based on dates of invention and innovation.[462] The most important twentieth-century technologies are often abridged to the following some examples: flight (1903), nuclear power (1945), contraception (1955), and the well-known Internet (1965)[463]. It[464]is frequently told that change is taking place at an ever increase speed, and that the new is increasingly influential, and, in addition, technology is always faster than the reaction to its influence on the society. Also, it is supposed that societies are really slow to adapt to novel technologies, and the list of novelties is expanding, by now it consists of many, such as biometrics, drones, smart phones, and so on. However, before the reign of technology and its progress, it was admitted that some parts of our body could be used to identify our unique selves, thus the ides does not seem novel at all. Since prints of hand, foot and finger have been used in ancient times due to their unique characteristics. Since it is not my primary aim is to create a timeline, I mention only a handful of them with no intention to give a full account. The Babylonian King Hammurabi (1792–1750 BC) is known to have enacted one of the first written codes of law in the world in clay tablets. The kings of Babylon were allegedly using an imprint of their right hands in the clay tables in order to authenticate the tables[465]. Among other things, in *Babylonia*, fingerprints were also used in business transactions that

ne strikes under jus ad bellum jus in bello and international human rights law.pdf[accessed 17 Oct 2019]or MCGUIRE, James E. – TUCHANSKA, Barbara:*Science Unfettered – A Philosophical Study in Sociohistorical Ontology*. Ohio University Press, Athens, 2000.

[462]See, for instance, KENDALL, Diana: *Sociology in our times*. Wadswort, Belmont, 2003. orKLEIN – TÓTH: *op. cit.*

[463]*See* CUMO, Christopher: *Science and technology in 20th-century American life*. Greenwood Press, London, 2007. *or*CHANNELL, David F.:*A History of Technoscience Erasing the Boundaries between Science and Technology*. Routledge, London, 2017. (https://doi.org/10.4324/9781315268897).

[464]HEADRICK: *op. cit.*

[465] See ASHBOURN, J.: *The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies. Background paper for the Institute of Prospective Technological Studies*. DG JRC – Seville, Commission, January 2005, 4, ('Ashbourn, Social Implications of Scale Implementation of Biometrics, 2005'), http://www.statewatch.org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf[accessed 9 Jan 2019].

were recorded on clay tablets. It is also a well-known fact that Chinese use fingerprints and handprints as marks of authenticity for at least 2,000 years. In ancient *China*, fingerprints were customarily pressed in clay tablets and clay seals. Documents from the Tang dynasty in China (618–907) referred to the use of fingerprints and handprints on contracts[466]. These examples can be seen as the earliest attempts to "*identify*" or "*verify*" the identity of an individual, and I include them in order to draw attention to the fact that though the "*idea*" of improving identification started long ago, it seems that we did not have the time to "*prepare*" for the revolution of technology, which might have begun for the most part in the nineteenth and the early twentieth century.

7.5 Introduction to biometric systems

Although a non-professional might have some information on what biometrics or biometric systems can or couldsignify, not a soul is expected to be an expert on these systems other than pros (and no-one has the time to follow up the progress), even if people use them more and more often with having prior knowledge on them. As a result, for the rationale of my study, I make an effort to highlight some basics of biometrics or biometric systems.

A biometric system measures one or more physical or behavioural characteristics, including fingerprint, palm print, face, iris, retina[467], ear, voice, signature, gait, hand vein, odour, or the DNA[468] info of aperson to establish/determine or verify one's identity. These characteristics are referred to by diverse terms such as traits, indicators, identifiers, or modalities The capability to identify individuals uniquely/individually and to relate personal attributes, forexample, name, nationality, to an individual, has always been essential to the fabric of human society. Humans use body characteristics by and large such as face, voice, and bear other contextual information, such as position and outfits) to

[466]FARELO, A.: *A History of Fingerprints*, Interpol, April 2009, 2. Available: http://www.interpol.int/Public/Forensic/fingerprints/History/BriefHistoricOutline.pdf [accessed 9 Jan 2019].

[467]The Eugenics Wars: The Rise and Fall of Khan Noonien Singh is a two volume set of novels written by Greg Cox and they were published in 2001 and 2002 and it is about the life of the fictional Star Trek character Khan Noonien Singh, appeared in the Star Trek movie Star Trek II: The Wrath of Khan premired in 1982. Even in these pieces of science fiction, a .biometric system (retina/iris scan) is used to confirm authorization for Admiral KIRK James T. -COX, Greg:*The Eugenics Wars – The Rise and Fall of Khan Noonien Singh*.Pocket Books, New York, 2002.

[468] DNA refers to deoxyribonucleic acid, which contains the genetic information necessary for the development and functioning of living organisms.

recognize one another. The set of attributes connected to a person constitutes their identity. In the beginning of civilization, people lived in small communities where individuals could easily recognize each other, and stranger among them was easily recognizable. Yet, an explosion in population growth accompanied by improved and more flexible mobility in modern society has demanded the development of sophisticated identity management systems that could efficiently record, maintain, and eliminate personal identities of individuals. Identity management plays a significant role in several applications. Examples of such applications can or could include regulating international border crossings, limiting physical access to key civilian and military facilities such as, nuclear plants or airports, controlling logical access to collective resources and information, performing remote financial transactions, or distributing social welfare benefits. The spread of web-based services, for instance, online banking and transactions, and the deployment of decentralized customer service centres, for instance, credit cards have shown the way to the risk of identity theft[469]. I also add that it looks vital that the term *biometrics* is often criticized by experts on this field, for example, Anil K. Jain, Arun A. Ross and Karthik Nandakumar argue that the term *biometric recognition* is possibly more appropriate than *biometrics* because the latter has been historically used in the field of statistics to refer to the analysis of biological (particularly medical) data[470]. In order to clarify the importance of biometrics, first we need to turn to the origin of the term, Thus, the term *biometrics* derives from the ancient Greek *bios* = "*life*" and *metron* = "*measure*." Biometrics refers to the entire class of technologies and techniques to uniquely identify humans. Although biometric technology has diverse applications, the most crucial purpose of it is to provide a more secure alternative to the traditional access-control systems used to protect personal or corporate assets. Biometric systems apply facial images, fingerprints, iris and/or voice in a computerized way to identify or to confirm (identity) claims of persons. It is completed on the basis of the automated measurement and analysis of their biological, such as fingerprints, face and iris, and even ear[471], or behavioural, such as signature and voice,

[469]Identity theft or identity fraud occurs when a person usurps the identity of another individual or claims a false identity in order to access resources or services to which he is not entitled.

[470]JAIN, Anil K. – ROSS, Arun A. – NANDAKUMAR, Karthik:*Introduction to Biometrics*. Springer, New York, 2011,1–3.(https://doi.org/10.1007/978-0-387-77326-1)
https://link.springer.com/content/pdf/10.1007%2F978-0-387-77326-1.pdf[accessed 20 Jun 2019].

[471] Using the ear as a biometric modality is a newcomer in the fields of biometric recognition techniques. There are relatively not many ongoing researches within this topic, in which most of them deals with

characteristics. Biometric technology has been used for some time in civil applications on a small scale for access control purposes to places which require an enhanced/advanced security, such as to military and nuclear facilities or bank vaults, but is now gaining increased interest from governments and the private sector as well.

While a heated debate has come up about whether conventional biometric technology can offer society any noteworthy advantages over other forms of identification, and whether it represents a (considerable amount of) threat to privacy, technology is progressing fast. Moreover, it is striking to see how politicians and the public are still discussing fingerprinting and iris scan, while scientists and engineers have already started testing futuristic (though realistic) solutions. These are the so-called *second generation biometrics*, which include multimodal biometrics, behavioural biometrics, dynamic face recognition, EEG and ECG biometrics, remote iris recognition, and other, still more astounding, applications, is a reality which promises to turn over any current ethical standard about human identification. Robots which are capable of identifying their makers/masters, CCTV which is able to "*sense*" intentions, voice responders which have the ability to evaluate/analyse emotions: to be frank, these are only some applications in progress to be developed further.

Knowing all this, it possibly will be unmistakable that legal certainty has cropped up, but, there is no consensus but legal uncertainty on various aspects of its use.[472]At this time, biometric technologies play a crucial role in security, immigration and border control policies of the Union, above all, in large-scale systems, such as Eurodac, VIS. Before looking at the different well-known (and celebrated) methods, a review of why at all bother using the ear as a biometric will be examined. To make a biometric characteristic practical, the following seven properties described by must be valid to some degree[473]: First, *universality*, it means that very person should have the biometric characteristic. Second, u*niqueness*, no two persons ought to be the same in terms of the biometric characteristic.

investigating unused methods in order to improve the performance. Therefore there is yet no well-established fully automated ear recognition system.

[472]See STRANDBURG, Katherine – STAN RAICU, Daniela (eds.):*Privacy and Technologies of Identity – A Cross-Disciplinary Conversation*. Springer, New York, 2006. (Doi: https://doi.org/10.1007/0-387-28222-X) https://link.springer.com/content/pdf/10.1007%2F0-387-28222-X.pdf [accessed 10 Sep 2019].

[473]JAIN, Anil K. – ROSS, Arun A. – PRABHAKAR, S.: *An introduction to biometric recognition*. IEEE Transactions on Circuits and Systems for Video Technology, 2004/1, 4–20. (https://doi.org/10.1109/TCSVT.2003.818349).

Third, p*ermanence*: the biometric characteristic should be invariant over time. Fourth, *collectability*, of course, it implies that the biometric characteristic should be measurable with some (practical) sensing device. The fifth one is p*erformance*, referring to the fact that the technology applied should have a certain accuracy, speed, and robustness (often associated with validity). Last but one is a*cceptability*, this property refers to the notion that the particular user population and the public in general should have no (serious) objections to the measuring/collection of the biometric, and last but not least, c*ircumvention*, which entails that the technology should be ease of use of a substitute.

With the ever-increasing concerns on security breaches and transaction fraud, highly reliable and convenient personal verification and identification technologies are more and more indispensable in our social activities and national services. Biometrics, used to recognize the identity of an individual, are gaining ever-growing popularity in an extensive range of governmental, military, forensic, and commercial security applications.[474]

Additionally, biometrics is used chiefly for authentication and identification by governments, employers, and a range of service providers. Data collection is effortlesslyand simplydone and does not have need of cooperation or awareness of the target. Government agencies, particularly law enforcement agencies, are the largest data collectors. It is also well-known that the government of the United States operates and preserves some of the largest biometric identification systems around the globe. The Department of Homeland Security (DHS) upholds and sustains an automated biometric identification system (IDENT). IDENT maintains a database of more than 126 million records and conducts about 250,000 biometric transactions, averaging 10 seconds or less per transaction, each and every day.[475] The DHS Biometric Optical Surveillance System (BOSS) executes and completes real-time facial recognition and has the capability of capturing iris data from a target 10 meters away even while the individual is on the go. Since biometric technology has swollen, the capacity to store and disseminate the collected

[474]See STRANDBURG – STAN RAICU:op. cit.

[475]TAYLOR, Mark:*Genetic data and the law – A critical perspective on privacy protection*. Cambridge University Press, Cambridge, 2012. (https://doi.org/10.1017/CBO9780511910128)or CAMPISI, Patrizio (eds.):*Security and Privacy in Biometrics*. Springer, New York, 2013. (https://doi.org/10.1007/978-1-4471-5230-9) https://link.springer.com/book/10.1007/978-1-4471-5230-9[accessed 5 May 2019]

data has increased radicallyand extensivelly. Most local and national law enforcement agencies seek to make the communication between their diverse databases flawless/faultless and responses to inquiries fast and precise. The ability to combine/assimilate/integrate and store information from various different databases has spectacularly increased the value of biometric data to organizations. However, it also has radically increased the risks that come with amassing and maintaining it. Privacy advocates expressed their great concern(s) about the use of biometrics in law enforcement. With the combined use of surveillance tools such as facial recognition technology, many fear that the United States is entering a regime of pervasive, large-scale surveillance. The application of biometrics does entail various and serious privacy risks, including identity theft, “function creep”, and government surveillance. There is greater safety and convenience in using biometrics rather than older forms of personal recognition. In some cases, biometrics may be used to replace or supplement the existing technology. In other cases, biometrics is the only viable approach given the circumstances. Biometrics is better than traditional recognition in several different cases. In some applications, it either replaces or supplements/augments existing technologies; in others, biometrics is the only sensible approach to personal recognition. As the infrastructure for dependable automatic personal recognition goes on to be developed along with the ability to associate an identity with other personal behaviour, privacy advocates articulate increasing concern that this information might violate individual privacy rights. A human physiological or behavioural trait might be a biometric characteristic if it meets the following criteria: first, the trait must be universal, which simply means that each person has the characteristic and second distinctive, thus the characteristic is unique for each person. Thirdly, the trait must be permanent, which basically means that the characteristic ought to be adequately invariant; that is, it must match the criterion over a certain period of time, and last but not least, it needs to be collectible, meaning that the characteristic ought to be quantitatively measurable). Virtually, it means that a functioning biometric system must reach satisfactory(or tolerable) levels of performance, satisfactoriness/tolerability, and circumvention. But, it looks central/critical as well that it must also be satisfactorily strong and is capable of resisting a great variety of fraudulent methods and attacks. A biometric system uses pattern recognition to recognize a particular person based on a specific physical or behavioural characteristic possessed by a particular person. Depending on the

application context, a biometric system typically operates in one of two modes: verification mode or identification mode. In the verification mode, the system confirms the person's identity by comparing the captured biometric characteristic with the individual's biometric template, which is stored in the system database. In line with Christopher Puniskis, there are some major concerns, biometrics raises several concerns: The first one is unintentional(or unplanned) functional scope. He presumes that it can easily happen because biometric identifiers are biological in origin; it appears very probable that collectors possibly will pick up extra, addedprivate information from the biometric measurements. The second might be unintended application scope. The supposition is that strong biometric identifiers such as fingerprints make an allowance for(almost certainly) unwanted and unnecessary identifications. The last one is covert recognition. A biometric sample, such as a person's face, may and could be retrieved without the target person knowing or realizing it[476]. Of course, it leads the conclusion that any individuals who intend to keep their anonymity could have their privacy rights violated by biometric recognition[477]. He also argues that prevention is also achievable, thus, abuse of biometric information (or its derivatives) can be prevented or mitigated through the application of a number of methods:"1. Government legislation and regulation. The EU has adopted legislation against sharing biometric identifiers and personal information. 2. Assurance of self-regulation. A group of biometric vendors could join to agree to be bound by ethical guidelines in their operations. 3. Autonomous enforcement by independent regulatory organizations, such as a central biometrics agency."[478] Of course, several institutions have been established in order to assume better understanding and promote novel tech, such as biometrics. Thus, the introduction of some is of primary importance for our purpose.

[476]For example, a drone can be easily used to achieve "relative invisibility" to get close enough to a target person without being revealed or discovered. I have already discussed some of the issues and concerns, concerning drones and privacy issues in Privacy in Context: Info-tech based society and the revolutionary effects of drones/phones/biometrics.

[477]ANGLIMop. cit., 46–47.

[478]ANGLIM, op. cit., 46–48.

7.6 Biometric Center for Excellence (BCOE) and Biometric Optical Surveillance System (BOSS):

The Biometric Center for Excellence was set upand launched in 2007 by the Science and Technology Branch of the Federal Bureau of Investigation to review, advance, and spread out the use of novel/innovative and enhanced biometric technologies, potentials, criterions/standards, and policies, for integration into operations. Its mission by and large is to add force to criminal investigative potential and enhance national security to a greater potential. Coming from a need to advance and manage the growing biometric activities and priorities of the FBI more efficiently, the BCOE[479] is vitally a consortium of the services and expertise of three divisions, the Criminal Justice Information Division, Laboratory Division, and Operational Technology Division, intended to prop up collaboration, progress and support info sharing and advance the adoption of optimal biometric and identity resolutions. This "alliance" aids to abolish a major challenge the capability gap by providing obtainable/accessible biometric capabilities while assessing future needs (and requirements). Outside the FBI, habitually, the centre works with the Office of the Director of National Intelligence, Department of Homeland Security, Department of Defense, and Department of Justice, in addition to other law enforcement agencies and national security communities. The BCOE aids and sponsors researches/studies, evaluates techs, develops training, establishes standards, and certifies biometric products as well. The BCOE addresses privacy and procedural and policy issues related to the use of biometric systems while working in compliance with privacy laws, policies, and regulations. One of the systems aches for mentioning is BOSS, Biometric Optical Surveillance System.[480] It is a system with the capacity to distinguishand identify faces and match them with personal identification info. Government agencies and federal, state, and local law enforcement developed BOSS to amass, tostore up and utilize this data legally, as needed. Government agencies, chiefly public safety agencies, are major collectors of data. The administration of the USA operates some of the largest biometric identification systems all around the globe. The Department of Homeland Security (DHS) maintains automated biometric identification stems (IDENT) that have a database of more

[479]PUNISKIS, Michael J.:*Biometric Center of Excellence (BCOE)*. In: ANGLIM op. cit., 42–43.

[480]ANGLIMop. cit., 44–45.

than 126 million records and conducts 250,000 biometric transactions per day averaging 10 seconds or less per transaction. BOSS can execute and complete real-time facial recognition and also capture the iris data from 10 meters away while a person is in motion[481]. Even though, especially American citizens have a great expectation of privacy, this right, as in the EU, is (with authorization, officially) balanced against the needs public for safety and national security. Private info is stored, correlated, and shared among law enforcement agencies with the purpose of guaranteeing and assuring public safety, but this use might involve some trade-offs/substitutions in terms of privacy. Cyber-tampering is an existing risk based on how much and how often this information is used and protected. Inadequate security could allow criminals (or actors with no authorization or consent) to access this information (even from great distances) and allow private identification info to be (critically) compromised. Plus, these considerations, the aggregation and accumulation of data from several different sources can pose a serious privacy threat. The theft of biometric information could aid criminal access to bank accounts and credit cards, and, for instance, there can be a danger of data creep, where information willingly provided to one law enforcement agency may possibly be transferred without (any) permission to another government agency, then linked with other data or applied to a new and unauthorized purpose (even with or without being recognized). Simultaneously, the unfettered scope of data amassing/collection, sharing, linking and connecting, and storing could invite misuse. Law enforcement officials are aware of the risks involved in the usage of BOSS. They trust that the government surveillance is necessary in these instances and requires support. As I have formerly mentioned, there are quite a few concerns are supposed to be addressed/considered and many of them have come to the surface by the insurgency of new/innovative techs, Shaunté Chácon poses and attempts to answer a sternquery when he asks: "*How should BOSS be regulated so that the legitimate privacy rights of U.S. citizens are not violated?*"[482] He states that one of the proposals is to limit access to BOSS as much as possible. Two policies are indispensable to provide adequate parameters for BOSS. First, facial recognition databases are supposed toor must use images of known terrorists and convicted felons (exclusively). Driving license photos and other images of innocent

[481]PUNISKIop. cit., 42–43.

[482]CHÁCO, Shaunté:*(BOSS)* In: ANGLIMop. cit., 45.

people should never be included in a facial recognition database without the knowledge and consent of the public. Second, access to databases should be limited and monitored[483].

As far as Europe and the European Union are concerned, we can see that the situation may seem a bit "grievous." Although Europe has a significant legal data protection framework, built up around and really started with EU Directive 95/46/EC and the Charter of Fundamental Rights, the question of whether data protection and its legal framework are "in good health/condition" is being posed ever more. Evidently, since the application of the General Data Protection Regulation (GDPR).Directive (EU) 2016/680 of the European Parliament of the Council of 27 April 2016 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, and repealing Council Framework Decision 2008/977/JHA[484] has started. Advanced technologies raise fundamental issues regarding key concepts of data protection. Falling storage prices, increasing chips performance, the fact that technology is becoming increasingly embedded and ubiquitous, the convergence of technologies and other technological developments are broadening the scope and possibilities of applications rapidly. Society however, is also changing, affecting thescenery and setting of data/privacy. The "demand" for free or liberated services, security, convenience, governance, for example, changes/modifications (even if they seem slight or insignificant) the mind-sets of all the stakeholders involved. Privacy is being proclaimed dead or at least worthy of dying by the captains of industry; governments and policy makers have to manoeuvre between competing and incompatible aims; and citizens and customers are considered to be indifferent.

7.7 Multi-biometrics[485]A brief Introduction:

As I have argued, it can be reaffirmed that systems of personal recognition are (typically and habitually) based on individual biometric traits, such as, face, iris and fingerprint, have been the focal point of my investigationhitherto. Most of these biometric

[483]CHÁCO, Shaunté:*(BOSS)* In: ANGLIMop. cit., 43–45.

[484]https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN [accessed 9 Jan 2019].

[485]JAIN – ROSS – NANDAKUMAR [2011] op. cit.

systems could be categorized/classified or characterized as uni-biometric systems for the reason that they are dependent on a single biometric source for recognition. Any piece of evidence that can be autonomously used to recognize a person is called a *source* of biometric information. One of the topics that appears to be more and more often discussed is whether uni-biometric systems have got or have not got some constraints/restrictions need to be considered for various reasons. One of the raison d'être is what if the biometric source becomes undependable/untrustworthyon account of some technical error (with no human error behind it), for instance, sensor or software failure/malfunction, poor quality of specific biometric trait of the user, or intentional manipulation? Besides, high-security applications and extensive civilian identification systems set rigorous accuracy requirements/modus operandi (to be followed and applied) that cannot be met by existing uni-biometric systems. Multi-biometric systems on the other hand seem more than capable of handling the previously mentioned obligations or trems/conditions. By definition multi-biometric systems of personal recognition are systems that combine and gather evidence from multiple sources of biometric information in order to determine, identify or verify the identity of an individual. For instance, face and iris traits, or fingerprints from all ten fingers of an individual, might be used in concert to determine the identity of the person with reasonably high precision or accuracy. As it is argued over and over again, multi-biometric systems are capable of triumph over several limitations/shortcomings of uni-biometric systems because the diverse (and altered) biometric sources commonly balance for the inbuilt or inherent limitations of one another. Therefore, multi-biometric systems are commonly supposed to be more reliable and accurate than uni-biometric systems, as well as offer wider population coverage[486]. The process of consolidating the information/data or evidence obtained by multiple biometric sources is known as information fusion. In order to improve precision, the so-called accuracy improvement, which is the prime impetus for applying multi-biometric systems, occurs as a result of (at least) two (main) reasons. To start with, the fusion of multiple biometric sources successfully increases the dimensionality of the feature space and reduces the overlap between the feature distributions of different individuals, or put it differently, I presume that a combination or mixture of multiple biometric sources is observedmore distinctive/unique (capable of identification or verification)to an individual than a single

[486] See also: JIANG – AL-MAADEED – BOURIDANE – CROOKES – BEGHDADIop. cit.

biometric sample. The second reason is that noise, imprecision/uncertainty, vagueness or natural drift, might be caused by factors like aging or an accident, in a subset of the biometric sources can be compensated by the discriminatory information given by the remaining sources. Thus, availability of multiple biometric sources provides redundancy and fault-tolerance in the sense that the recognition system continues to operate even when certain biometric acquisition modules fail[487][488].

Regardless of the security benefits these technologies offer, their all-embracing application involves and obviously leads to serious issues as well, including technological challenges, disputes and concerns for individual citizens' rights of privacy. Copious forms of identification, such as driving licenses, passports, and other identity cards, are increasingly being combined with biometric information, and one can go as far as to state as well that the use of them will be spread to other sectors too. Consequently, I suppose that this noticeable prosperity of private/individual information will lead to more advanced data protection measures, encryption technologies, and other safeguarding measures, both to encourage their acceptance and use by the civilian population and to keep this critical information from falling into the wrong hands. Still, it cannot be overseen that biometric systems (and data) may be used by governments in many ways. Critics such as the American Civil Liberties Union (ACLU) are genuinely and severely concerned that such power might be effortlessly abused for unethical, unlawful purposes. While biometric technologies have advanced in haste, they are still given to technological deficiency or limitations, such as computer errors, "*cog in the wheels*" and glitches, which can misidentify individuals, leak sensitive or critical personal data, and lead to other privacy-related issues. Oher solutions might be that privacy concerns ought to be dealt with when a biometric distribution is being implemented. For instance, in addressing the question of whetherto store biometric data as processed references or in source samples orimages,

[487]JAIN– ROSS – NANDAKUMAR (2011.): op. cit., 211.

[488]The contribution of the following works seem vital, too: CAMPISI: op. cit.This text/reference highlights the latest secured and privacy-compliant techniques in automatized/computerized recognition of humans. Presenting viewpoints from an international selection of experts in the relevant field, the comprehensive coverage spans both theory and practical implementations, taking into consideration all ethical and legal issues and concerns. Its topics are unique with focusing on new and innovative methods/approaches and new architectures for uni/multimodal template protection; studies signal processing techniques in the encrypted domain, security and privacy leakage assessment, and aspects of standardization.

which approach best, protects privacy may need to be considered. The same can be stated of the choice between local or centralized storage of biometric data, with bearing in mind that it is a choice that has major security and privacy implications. And, in addition, the most relevant and essential might be that the application of biometric systems needs be well-defined and restricted at the outset of aprogram, by legislation when appropriate.

Chapter 8 Privacy tort and the civil procedure: international perspective

8.1 The Privacy Torts: past, present and future

As I have already endeavoured to point out in my previous chapters, the concept of privacy is multi-layered, elusive and it keeps changing. Thus, it is not a surprise that there is no single time-honoured nominate tort intended to protect privacy. In 1972, long before the enactment of the Human Rights Act 1998, the Younger Committee[489] decided to consider the protection of privacy and it observed and came up with the comprehensive interpretation of privacy as the state of being left alone, free from any kind of human interference. Though, the Committee also recognised and acknowledged some elements within that definition which it considered to be of equal importance, such as protection from physical harm and restraint, freedom from direction and the peaceful enjoyment of one's surroundings. Also, there are numerous ways in which these aspects of the privacy of individuals may possibly be protected by the law of tort. For instance, the torts of nuisance and trespass protect several aspects of privacy with regard to land, trespass to the person protects from bodily intrusion, and defamation protects individuals from having untrue details of their lives made public. As I have already stated that there is no single longstanding nominate tort envisioned to protect privacy, the observation and conclusion of the Committee seems long-lasting enough to be relevant and valid, since it concludes that "[….] if the concept of privacy were to be embodied into a right: its adaptation to the dominant pressures of life in society would require so many exceptions that it would lose

[489]DWORKIN, Gerald: *The Younger Committee Report on Privacy*. The Modern Law Review, Vol. 36, No. 4, Jul.,1973,399406.Available:https://www.jstor.org/stable/pdf/1093890.pdf?refreqid=excelsior%3Aa62403ddf72ee8a8182e4316e98d464b[accessed 5 Jan 2021]

all coherence and hence any valid meaning.[490][491] By 1990, the Calcutt Committee on Privacy and Related Matters[492] endeavoured to outline a potential statutory tort of infringement of privacy concerning explicitly the publication of personal information, which Committee defined roughly to include: those aspects of an individual's personal life which (any) reasonable members of society would respect as being such that an individual is usually entitled to keep them to himself/herself, whether or not they are regarding his/her mind or body, to his/her home, to his/her family, to other personal relationships, or to his/her correspondence or documents[493][494]. One of the most influential sources of privacy as a part of American legal culture was the famous article titled *The Right to Privacy* in the 1890 Harvard Law Review. It was written by Samuel D. Warren and Louis D. Brandeis, this article was inspired by the rise of newspapers, photography, and other (novel) technologies (at the time) with the probability (and risks) to expose people's images/photos and personal information to the public. Warren and Brandeis compared privacy to the law of defamation, to physical property rights, to intellectual property, and to the law of contract.Their major concern, it is vital to note, was with publicity given to sensitive personal information/data, undesirable and embarrassing scrutiny of private life by the press and public. Privacy as considered by Warren and Brandeis did not deal with matters that were of legitimate public or general interest. And publication of facts by the individual concerned, or with that person's consent, deprived of that person's right to privacy in that information.Later on, another major discussion or debate started, when in 1960, eminent legal scholar William L. Prosser recognized and documented how privacy as a legal concept had come to constitute four distinct torts. To be precise, a person whose privacy has been invaded could sue the invader for damages. These torts still exist today, and are

[490]DWORKIN: op. cit.

[491]HARPWOOD, Vivienne: *Modern tort law*. Routledge-Cavendish, New York. 2009. 470-471. (Doi: https://doi.org/10.4324/9780203868812)

[492]*Calcutt Report*. Available: https://api.parliament.uk/historic-hansard/commons/1990/jun/21/calcutt-report [accessed 5 Jan 2021]

[493]*Calcutt Report*. Available: https://api.parliament.uk/historic-hansard/commons/1990/jun/21/calcutt-report [accessed 5 Jan 2021]

[494]CALCUTT, David QC: *Review of Press Self-Regulation*: *Presented to the Parliament by the Secretary of State for the Department of National Heritage*. HMSO, London, 1993. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/271963/2135.pdf [accessed 5 Jan 2021]

formed as four separate branches[495]:intrusion upon seclusion or solitude, or into private affairs;public disclosure of embarrassing private facts;publicity which places a person in a false light in the public eye; andappropriation of name or likeness.

The privacy torts are often forgotten or deliberately ignored by some privacy advocates, although concerns, surrounding them in a high-tech era have been growing for decades. Litigation is debatably far superior to administrative regulation as a means to protect privacy whereas preserving innovation. And as the U.S. Department of Commerce said in a July, 2000 memorandum to the European Commission, "The right to recover damages for invasion of personal privacy is well established under U.S. common law." The starting point has been and still is that English law does not recognize general tort of invasion of privacy. Since the Human Rights Act 1998, courts have constantly held that they do recognize privacy as a 'fundamental value' of English law. Nonetheless, it has been unmistakably stated that recognition of an underlying value differs from recognition of a legal principle which might be applied in concrete situations.[496] An underlying value is not of necessity a protected interest. It is fairly well-known and well- documented that controversy has centred on the commanding injunctive remedies available to protect privacy, and particularly the element of secrecy involved with 'super-injunctions'. At the same time, however, evidence of illegal violations of personal privacy, mainly, on the part of the press, and the continuing complications of restraining online publications, have already created a novel impetus in order to make an effort to achieve a "liable" press. Of course, it can be argued that this may or will be a counterpoint to the developments towards improved freedom of expression that are evident, for instance, in defamation reform, and come up with the question of how far it is probable to control the press with no compromising its independence.Christopher T Anglim argues that "while 'The Right to Privacy' was a significant piece of legal literature, privacy law in the United States was slow in developing—many judges were sceptical of claims of psychological damage resulting from invasions of one's privacy. Without being able to make explicit physical claims as to harm, plaintiffs in tort actions could not recover damages"[497].

[495]To obtain more information, consult: https://lawshelf.com/shortvideoscontentview/the-torts-of-invasion-of-privacy/ or https://www.stimmel-law.com/en/articles/legal-right-privacy[accessed 5 Jan 2021]

[496]Lord HOFFMANN, *Wainwright v Home Office* [2004] 2 AC 406, at [31]

[497]ANGLIM, Christopher T.:*Privacy Rightsin the Digital Age*. Greyhouse Publising Inc., 2018, 431.

The current state of privacy tort cannot be described more precisely as it is responded to a *New York Times* editorial criticising the result in Roberson, a member of the majority voting not to be acquainted with the novel cause of action took the uncommon step of writing a law review article that wanted to justify the court's holding. Judge Denis O'Brien insisted that: "It is quite unattainable to define with anything like precision what the right of privacy is or what its limitations are, or how or when the right is invaded or infringed, or what remedy can be applied if any.[498][499][500] The history of the tort has already proved later that courts and critics/observers/reporters should have paid more attention to these issues/concerns. The value of privacy in reality embraces a variety of interests, and it might well be that not every one of them values the sort of protection that tort law can efficiently (and successfully) provide. Furthermore, the failure of the courts to cultivate the kinds of rules that can signal to potential defendants what kinds of behaviour may be tortious and standards that juries can reasonably relate has been a main cause of the confusion in which the privacy tort now finds itself. The difficulty in using the common-law litigation process to define and demarcate private and public spheres in an ethical/principled/moral way has demonstrated to be a far greater challenge than Warren and Brandeis ever imagined[501]. Also, tort law is repeatedly seen as a tool for protecting privacy. But then again tort law can also reduce and weaken privacy, by pressuring defendants to gather sensitive information about people, to install comprehensive surveillance, and to disclose information. And this stress has grown, since technology makes surveillance and other information gathering more probable and cost effective and

[498]O'BRIEN, Denis: The Right of Privacy. Columbia Law Review, Vol. 2, No. 7, Nov. 1902, 437.(Doi: https://doi.org/10.2307/1109924)
Available:https://www.jstor.org/stable/pdf/1109924.pdf?refreqid=excelsior%3Aaa912ae10059838a82fa715770ddc96f[accessed 5 Jan 2021]

[499]To get to know more about the attempts to define privacy, see, for instance:MOREHAM, Nicole:*Privacy in the Common Law: A Doctrinal and Theoretical Analysis*.Law Quarterly Review, Vol. 121, 2005, 628.; WACKS, Raymond: *Personal Information: Privacy and the Law*. Clarendon Press, Oxford, 1989; and SOLOVE, 2008: op. cit.

[500]SOLOVE, Daniel J.: *I've Got Nothing to Hide' and Other Misunderstandings of Privacy.*San Diego Law Review, Vol. 44, 2007. Available: https://ssrn.com/abstract=998565 or GWU Law School Public Law ResearchPaper,No.289.https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications [accessed 7 Jan 2021]

[501]BRÜGGEMEIER, Gert –COLOMBI CIACCHI, Aurelia –O'CALLAGHAN, Patrick (Eds.):*Personality Rights in European Tort Law*. Cambridge University Press, Cambridge, 2010, 69-72. (DOI: https://doi.org/10.1017/CBO9780511676161)

thus more likely to be seen as part of defendants' duty to take "reasonable care.[502]" Still, Tamás Fézer observes that "[e]ven if we stay in the world of private law, no legal systems are alike when it comes to determine and interpret the institutions of tort liability. Social, cultural significances and economy of the examined country and legal system strongly put a remarkable influence on how tort law evolved and interpreted there[…]", and he goes on to state that "[t]ort law is a very dynamically evolving area of private law and in many European Union Members States, beyond the relatively constant nature of civil codes, new cases, technological development and questions arisen from new social connections provoke new approaches and certain reinterpretation of well know statute law principles.[503]" However, Danielle Keats Citronstates that "[…] courts have too often rigidly interpreted the four privacy torts. Prosser's conceptualization of privacy interests worth protecting is too narrow to accommodate the privacy interests implicated by networked technologies. As a result, the privacy torts often cannot properly redress contemporary privacy injuries"[504]. Novel technologies makes conceptualization of privacy interests more difficult, since the progress of high-tech never ceases, still the regulation and protection of these personality rights must be guaranteed. Considering progressive technologies influential to any walks of life the Internet of Things may lead the world. It has unbelievable possibilities to make society better and improved society by offering colossal amounts of rich sensory data for analytics and other countless practices. Still, there are also numerous unforeseen and latent risks and even threats that could be noticeable as the Internet of Thingsthrives. These unexpected and concealed risks may include privacy violations and security risks. Alexander. H. Tran warns us: "[s]ociety has reached a technological milestone requiring the special attention of the law, as we have entered a digital era where every device and every physical object surrounding us can be connected to the Internet. Soon, every human experience and physical sensation will be recorded and transmitted across the Internet for a variety of purposes. The growing

[502]VOLOKH, Eugene: *Tort Law vs, Privacy*. Columbia Law Review, Vol. 114, No. 4, 2014, 879-880. Available:https://columbialawreview.org/wp-content/uploads/2016/04/May-2014-7ArticleVolokh.pdf[accessed 5 Jan 2021]

[503]FÉZER Tamás: *Comparative Tort Law: E-Learning textbook*. (E-book), Debrecen2013.

[504]CITRON,Danielle Keats: *Mainstreaming Privacy Torts*. California Law Review, Vol. 98, 1805-1806. Available:https://29qish1lqx5q2k5d7b491joo-wpengine.netdna-ssl.com/wp-content/uploads/2014/10/Citron.FINAL_.pdf[accessed 7 Jan 2021]

presence of theIoT should motivate the legal community to prepare for this exciting, yet frightening digital frontier and the privacy challenges that will accompany its arrival"[505].

8.2 Privacy law and the intrusion of privacy[506]:

When we consider the factors contributing to the intrusion of privacy, in fact, we may state that numerous things done in public places would not be seen or considered private, although, it seems even privacy laws leave a considerable amount of gray zone as to what may be considered "public". The Fourth Amendment of the U.S. Constitution[507] protects against searches that violate or disturb the reasonable expectation of privacy of a person, which may or can be defined (roughly) as something for which society as a whole would consider or think legitimate. The 1967 Supreme Court case *Katz v. United States*[508]held that the government may not record a conversation made from a public phone booth (with the glass door shut), even if the recording device is on the outside since the individual calling somebody has a reasonable expectation of privacy. Other places or areas where one has a reasonable expectation of privacy is within one's home; a post office (if closed to the public); and most post sent or received through the U.S. a Postal Service, especially, in the U.S. to name only a few examples. One may have a much more restricted or narrower expectation of privacy when a person is out in public places, for example, parks or plazas, offices. An invasion of one's privacy could raise one of the following claims in tort law: intrusion of Solitude[509], appropriation of Name or Likeness, Public Disclosure of Private Facts False Light. In America, for example, most U.S. jurisdictions allow civil lawsuits for the claim of invasion of privacy, the specifics of which are mainly regulated by state laws.

---

[505]TRAN, Alexander. H.:*The Internet of Things and Potential Remedies in Privacy Tort Law*. Columbia Journal of Law and Social Problems,Vol. 50, Iss. 2, Winter 2017, 297-298. Available: http://jlsp.law.columbia.edu/wp-content/uploads/sites/8/2017/03/50-Tran.pdf [accessed 7 Jan 2021]

[506]See more: https://criminal.findlaw.com/criminal-rights/is-there-a-difference-between-confidentiality-and-privacy.htmland https://injury.findlaw.com/torts-and-personal-injuries/invasion-of-privacy.html [accessed 6 Jan 2021]

[507]Available: https://www.law.cornell.edu/constitution/fourth_amendment[accessed 6 Jan 2021]

[508]Available: https://www.oyez.org/cases/1967/35[accessed 6 Jan 2021]

[509]HARTSHORNE, John: *The need for an intrusion upon seclusion privacy tort within English law*. Common Law World Review, Vol. 46, No. 4, 2017,287–305. (Doi: https://doi.org/10.1177/1473779517739798) Available:https://leicester.figshare.com/articles/journal_contribution/The_need_for_an_intrusion_upon_seclusion_privacy_tort_within_English_law/10229567[accessed 7 Jan 2021]

8.3 Reasonable Expectation of Privacy and Intrusion of Solitude:

Let us suppose that a person goes to walk in the park and unintentionally leave or drop his or her personal letter containing full of private information on a public park bench, and that letter is found and read by somebody else. Even though the sharing of this information damages his or her reputation/status or causes other harm, it is not a violation of your privacy. That requires a "reasonable expectation of privacy", which would apply if the letter was not left out in public. The reasonable expectation of privacy is an element of privacy law that regulates and defines in which places and in which activities a person has a legal right to privacy. Sometimes mentioned as the "right to be left alone," a person's reasonable expectation of privacy means that someone who unreasonably and seriously compromises another's interest in keeping her affairs from being known can be held liable for that exposure or intrusion. Though we also need to bear in mind that an expectation of privacy is far from absolute, it needs also be "reasonable." In this case it means that the disclosure or discovery of a private matter must have happened when the plaintiff was in a place or situation in which the average person would be offended at being intruded upon. Below I attempt to give a few examples of places or activities where a reasonable expectation of privacy might exist. Here, I simply debate expectations of privacy only with regard to those cases where a private citizen compromises the privacy, solitude or seclusion of another private citizen. Expectation of Privacy in the Home may be one of the clearest examples of a place where there may be a reasonable expectation of privacy. A person does not have to be the owner for the law to protect that expectation; tenants who rent a flat also have a protected right to privacy. Furthermore, invasion of privacy does not merely mean that somebody physically goes in a place where a person has a reasonable expectation of privacy[510]. It can also occur if somebody uses electronic equipment to observe or record what somebody is doing in his or her home. Let's say you accidentally leave a personal letter containing private information on a public park bench, and that letter is picked up and read by someone else. Even if the sharing of this information damages your reputation or causes other harm, it is not a violation of your privacy. That requires a "reasonable expectation of privacy", which would apply if the letter was not left out in

[510]RICHARDS, Neil M.:*The Limits of Tort Privacy*. Journal of Telecommunications and HighTechnology Law, Vol. 9, 2011, 29. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1862264[accessed 7 Jan 2021]

public. An invasion of privacy happens when there is an intrusion upon your reasonable expectation to be left by yourself. There are four main types of invasion of privacy claims. The four main categories of invasion of privacy claims are the following: intrusion of solitude, appropriation of name or likeness, public disclosure of private facts, false light. The following information explores these types of claims and the basics of invasion of privacy law in general.

One can describe solitude as a situation, state or a condition of being alone (physically or sometimes psychologically, often by choice or preference.Intruding upon another's solitude or private affairs is subject to liability if the intrusion is considered extremely offensive to a reasonable person. It is important to note that his tort is often associated with "peeping Toms,[511]" when somebody unlawfully (or criminally) intercepts private phone calls, or “peeping” through somebody's private records. Also, it is interesting that taking photographs of somebody in public would not be considered to be intrusion of privacy; but, using a long-range camera or a drone to take photos of somebody inside their home would absolutely qualify. If somebody makes a few unwelcomed or unwanted telephone calls might not constitute to a privacy invasion, but calling repeatedly after being asked or warned to stop would.

8.4 Appropriation of Name or Likeness and Public Disclosure of Private Facts:

Claimants may make a claim for damages if an individual (or company) uses their name or likeness for benefit without their permission. The case is generally a business using a celebrity's name or likeness in an advertisement. Some states even limit this type of privacy tort to commercial uses. But there is another way, when a private investigator who impersonates somebody else to get confidential information has invaded that person's privacy. The recognition of this tort is like a property right; in other words, a person's name and likeness is considered as that person's property. For celebrities, this is often referred to as "right of publicity".

[511]See,for instance: California’s “Peeping Tom” Laws. https://www.shouselaw.com/ca/defense/laws/peeping-tom-laws/

Public Disclosure of Private Facts is a type of invasion of privacy claim that must be evaluated (and often balanced) against the First Amendment's protection of free speech.[512][513] Unlike defamation (libel or slander), truth of the disclosed information does not stand as a defence. If an individual publicly discloses truthful information that is not of public concern and which a reasonable person would find offensive if made public, they could be liable for damages.The notion of tort privacy offered by Warren, Brandeis and Prosser sits at the core of American considerations and comprehensions of privacy law. Deeply embedded in protection of confidential/private info against unwanted/unsolicited/unwelcomedcompilation/amassing, use, and disclosure, tort privacy protects against emotional (and/or psychological)"injury", and was bound for by design against disclosures of true/factual, embarrassing facts by the media. Neil M. Richards states that as envisioned and regarded by Warren and Brandeis and interpreted by Prosser; tort privacy seems a weak tool for dealing with difficulties and complications of privacy and character/reputation in the age of rapidly progressing technologies. Tort privacy, specifically the disclosure tort, has from its start been in clash with First Amendment values. And when First Amendment values and tort privacy conflict, First Amendment values ought to triumph practically every time. Thus, disclosure tort holds limited usefulness and efficacy in the automated and technological milieu, but privacy in the age of IT and social media needs novel/innovative approaches and new legal tools. These approaches or methods can take either an extensive look at tort privacy, together with novel (and different) torts and new theories of injury beyond emotional harm, or they can include fresh proposals and ideas of privacy altogether, such as confidentiality law[514].

8.5 False Light:

A false light claim bears the similarity to a defamation claim in that it permits an individual to sue for the public release of information that is misleading or puts that person in a "false light", but, it is not false in principle[515][516]. The basic and vital difference is that

[512]Available:https://www.law.cornell.edu/wex/first_amendment [accessed 6 Jan 2021]

[513]ABDO, Alex: *Why Rely on the Fourth Amendment To Do the Work of the First?* Yale LawJournal Forum, Vol. 127, 2017. Available:https://www.yalelawjournal.org/pdf/Abdo_e3en3agt.pdf [accessed 7 Jan 2021]

[514]RICHARDS: op. cit, 357-358.

[515]See: FINCH, Emily – FAFINSKI, Stefan: *Tort Law*. Pearson Education Limited, London, 2017, 199-221.

defamation claims only apply to the public broadcasting of false information and as with defamation, sometimes protections bestowed First Amendment triumph. In general, a false light claim must enclose the following elements: (1) the defendant made a publication about the claimant; (2) it was done with reckless neglect; (3) it positioned the plaintiff in a false light; and (4) it would be highly offensive or embarrassing to a reasonable person[517] .

8.6 Personality rights and privacy in Hungary: the Fundamental Law of Hungary, the Hungarian Act on Civil Code and the Hungarian Civil Procedure.

The Hungarian lawyer has the Code of the Hungarian Civil Procedure, and for him or her civil procedure is the subject matter of that code. Though, an English or a French lawyer would nearly sure to recognise and comprehend as a civil kind of proceedings regulated by that code and standard as such in Hungary. Though it does not mean at all that the understanding of all three of what civil is are all-embracing. Probably, the English one may see it as the widest in context, while the French and the Hungarian may see it very differently, due to differences in legal culture, history and so on[518]. Treating and guaranteeing certain personality rights in Hungary are ensured with the assistance of the Fundamental Law of Hungary, the Hungarian Act on Civil Code and the Hungarian Civil Procedure. Constitutional privacy embraces the right of the individual not to have certain private information gathered, preserved, or disseminated by the government or by implication, any other authorities. Constitutional law and other acts as well and consequently restrict intrusions into certain/relevant areas (concerned and/or related) or communications. The Hungarian Constitution or as it is commonly known now, the Fundamental Law of Hungary affirms the commitment of Hungary and assures the protection of the rights of persons in the National Avowal section by stating that "human existence is based on human dignity and [....] that individual freedom can only be complete

[516]See: MCKENNA, Bruce A: *False Light: Invasion of Privacy?*Tulsa Law Review, Vol. 15, Issue. 1, 2013, 113.Available: https://core.ac.uk/download/pdf/232683176.pdf or https://digitalcommons.law.utulsa.edu/tlr/vol15/iss1/7[accessed 6 Jan 2021]

[517]See more: https://criminal.findlaw.com/criminal-rights/is-there-a-difference-between-confidentiality-and-privacy.htmland https://injury.findlaw.com/torts-and-personal-injuries/invasion-of-privacy.html

[accessed 6 Jan 2021]

[518]See: JOLOWICZ, John Anthony: *On civil procedure*. Cambridge University Press, Cambridge, 2000. (Doi: https://doi.org/10.1017/CBO9780511549540)

in cooperation with others. Also, more regulation can be found in the Hungarian Civil Code Act V of 2013[519], part three: rights relating to personality (Title XI). Under the title, General Provisions and certain rights relating to personality, one can find the necessary protection of rights relating to personality. Section 2:42 (1) assures us that everyone is entitled to freely practice his or her personality rights within the framework of the law and within and with respect to the rights of others, and to not be impeded in exercising such right by others. It also states, as it is similarly can be seen in the Fundamental Law of Hungary that (2) Human dignity and the related personality rights must be respected by all. Personality rights are protected under this Act. Also, (3) Personality rights shall not be considered violated by any conduct if the person affected has given prior consent thereto. And in addition, in Section 2:43 specifies personality rights and observes that those on the subsequent list, particularly, shall be construed as violation of personality rights: any violation of life, bodily integrity or health; any violation of personal liberty or privacy, including trespassing;discrimination; any breach of integrity, defamation; any violation of the right to protection of privacy and personal data;any violation of the right to a name;any breach of the right to facial likeness and recorded voice.[520] In order to the Hungarian perspective on Civil law and Civil Procedure, I highlight some changes made in the second decade of the twenty first century, effecting both civil law and civil procedure with having lasting influence on the legal "attitude" towards privacy torts.

In 2014, Hungary adopted a new Civil Code, which effects the protection of personality rights in two ways. First, lawmakers changed the text of the Civil Code in order to match new jurisprudence. Second, the new Code introduced the institution of restitution instead of non-pecuniary damages. The latter change is relevant in that in cases where personality rights have been violated, claimants can now request monetary compensation without having to prove that the violation caused damage. Thus, a finding of a violation of personality rights on its own constitutes grounds for entitlement to restitution.The purpose of restitution, which now takes the place of non-pecuniary damages, is primarily to ensure that the injured party receives compensation for the violation of his/her rights. The Civil

[519]See: FÉZER Tamás: *Re-CivilLaw in Hungary*. Studia Prawnicze, Rozprawy i Materiały / Studies in Law: Research Materials, Vol. 15, No. 2, 2014, 73–92. Available: https://sp.ka.edu.pl/numery/studia-prawnicze-rim-2014-2.pdf[accessed 6 Jan 2021]

[520]Act of V on the Civil Code/Polgári törvénykönyvről. 2013.évi. V. törvény. 2:43. §

Code presumes that injury has been suffered as a result of the violation of the injured party's rights, thus injury itself need not be proven. This change came in response to problems in both the legislation and jurisprudence regarding the difficulty of proving the existence of non-pecuniary damage. In contrast to non-pecuniary damages, to claim restitution the plaintiff need not prove that s/he has suffered any disadvantage as a result of the violation. In the case of a wrongful violation, the injured party will always have a right to some amount of restitution. The amount of restitution that is set by the court depends on evidentiary elements and the judgment of the tribunal. It seems vital to note that as far as restitution is concerned, there are (some) guarantees in Section 2:52. Any person whose rights concerning personality had been violated/dishonoured shall be entitled to restitution for any non-material violation endured. With regard to the conditions/terms for the obligation of payment of restitution, such as the definition of the person liable for the restitution payable and the cases of exemptions, the rules on liability for damages shall be applied, with the provision that except for the fact of the infringement no other harm has to be confirmed for entitlement to restitution. The court shall determine the amount of restitution in one (total) sum, taking into consideration the seriousness and/or magnitude of the intrusion, whether it was committed on one or more occasions, the degree of liability, the impact of the intrusion upon the aggrieved party and his milieu.For the purpose of my examination, it seem essential to define Civil procedure, which can be said to be the body of law that specifies the rules and standards that courts shall follow when adjudicating civil lawsuits (as opposed to procedures in criminal law matters). These rules govern how a lawsuit or case may be commenced; what type of service of process (if any) is required; the sorts of pleadings or statements of case, motions or applications, and orders allowed in civil cases; the timing and conduct/manner of statements/evidence and discovery or disclosure/exposé; the conduct of trials; the process for judgment; a variety of available remedies; and how the courts and clerks are obliged to function.[521] Privacy/personality rights have been regulated even further, since Hungarian Civil Procedure concerning certain personality rights can be found in chapter XXXVIII,

[521]It should be noted that as far as Civil Judicial Procedures and Remedies are concerned, the US state department reports in its *2018 Human Rights Report* "By law individuals or organizations may seek civil remedies for human rights violations through domestic courts. Individuals or organizations who have exhausted domestic legal remedies regarding violations of the European Convention on Human Rights allegedly committed by the state may appeal to the European Court of Human Rights (ECHR) for redress". https://www.state.gov/documents/organization/289381.pdf[accessed Apr 10 2019]

designate as “actions brought for the enforcement of certain personality rights. It also sets up the so-called Common rules, which is Section 493, titled Actions brought for the enforcement of personality rights. To create and develop a clarified and specified system, for the purposes of this chapter, it identifies certain actions can be brought for enforcing the right of a person, or privacy rights. Those are the following: an action brought for the enforcement of personality rights shall mean an action for press correction, an action brought for the enforcement of the right to the protection of image and recorded voice, or an action brought for asserting personality rights related to belonging to a community. In addition, as far as the application of the general rules are concerned, the Act states in Section 494 the provisions of this Act shall apply in actions brought for the enforcement of personality rights, as regulated in this Chapter, with the derogations specified in this Chapter. The first one, the Act deals with, is an action brought for press correction in Section 495, where mandatory preliminary procedure with a press organ can be found. In this case, the first discussed is the request for the publication of a corrective statement, which shall be in reference to the Act on the freedom of the press and the general media content. The form of the corrective statement is in writing and the time period given is a thirty day term of preclusion after the publication of the disputed publication from the editorial office of the press product or from the news agency (hereinafter jointly “press organ”) by the person or organization concerned. The prejudicial publication and the false or misrepresented statements of fact shall be specified in the request, as well as the actual facts, if its publication is also requested. It is also clarified that a corrective statement be published and received in writing and in due time shall not be denied, except the correction was demanded by a person other than the person entitled[522]. In addition, .it must be observed that the statement of claim shall be submitted within fifteen days after the last day of the obligation to publish; an application for excuse might be filed in case of failure to meet this official dead line. There are formal criteria for the statement of claim, which shall include the corrective statement requested, including its explicit content, the harmful publication and the false or distorted/misused/misrepresented statements of fact, as well as the actual/authentic facts, if their publication is requested by the plaintiff, and the presentation of the facts demonstrating that the plaintiff requested the defendant to publish

[522]Act CXXX of 2016 on the Code of Civil Procedure (as in force on 1 July 2018)

the correction within the statutory time limit. Additionally, the following shall be attached to the statement of claim: a certificate confirming that the plaintiff requested the defendant to publish the correction within the statutory time limit, and, if it is available, the press product containing the contested publication.

The above mentioned press correction does not seem as important for the purpose of my examination, but the actions brought for enforcing the right to the protection of image and recorded voice of a person are closely related to the technology, such as drones, biometrics and others, and their related legal concerns I intend to deal with. Therefore, I assume that the discussion of the mandatory preliminary procedure for remedying the violation of law can take as closer to an understanding needed. If an image or voice recording is made of a person without his consent/permission, or an image or voice recording of a person made with or without his consent/permission is used without his permission, he could request the producer or user, by a written request in which he sets a time limit (with dead line) in days and which is sent within a term of preclusion of thirty days calculated from the date of becoming aware of the making or use of the image or voice recording, to cease the violation of law, provide proper contentment, and provide appropriate publicity for doing so at its own expenditure, stop the damaging situation, restore the situation existing prior to the violation, and destroy the thing produced through the violation of law or deprive it of its unlawful character. The harmful/damaging image or voice recording, the time and manner of use, if any, the time of becoming aware of the situation, and the sanction wanted against the infringing party shall be specified in the request for remedy. It is also crucial to observe that there is no request for remedy shall be submitted if three months have passed after the time of making or using the image or voice recording. Also, the realization of the request for remedy received in writing and within the time limit shall not be denied, unless it was not submitted by the person entitled, the request is with no contain the information required, or the reliability of statements made in the request can be disproven at once or directly. In case of an action brought, there are additional attachments, the following “items/documents/material evidence” shall be attached to the statement of claim: certification that the remedy was requested by the

plaintiff within the statutory time limit, the image or voice recording, and documentary or physical evidence, if available, in accordance with the form used, if any[523].

[523]Act CXXX of 2016 on the Code of Civil Procedure (as in force on 1 July 2018)

Conclusion:

All through my dissertation, I have intended to point out that one of the possible sources of misperception and sense of chaos is the fact that regulation is typically portrayed as a single kind of rule or strategy envisioned with one and only purpose: regulating the regulated. Also, the idea that regulation can be treated as one kind with only a solitary effect on technology may and can contribute to their burdensome liaison and link, with no visible intention turn it to a peaceful coexistence or a partnership. Regulation has the capability of being able to constrain/obstruct or stimulate technological change(s) or even an all-front revolution. This "strange" liaison does rest on the technology/expertise of regulation, namely, the choice of design and instrument of regulatory policy. I have attempted to examine some fragments and notions of the history of regulations over the last three decades preferably, the explanatory power of theories of regulatory politics, the choice of regulatory apparatuses, the assessment of regulatory influences/effects, and the effect of some of these on the innovation/invention and transmission of technology and, by implication, of regulation at different levels. I have examined the development and progress of novel, and emerging technologies, such as AIs, biometrics and drones, that pose a considerable amount of threat to longstanding institution(s), such as privacy, with bearing in mind the existence of other fast pacing technologies as well. Eventually, I have ventured to conclude with recommendations for the future of regulation of technology and its uneasy relation to privacy with bearing in mind that cultural and legal differences can be (re)measured and reflected on. Furthermore, I intended to consider the fact in my dissertation that technology and regulation are recurrently distinguished/observed and depicted as opponents or oppositions fighting as rivals. Since technology often embodies diversevarieties of markets, enterprises/ventures, and progression, while regulation exemplifies government/administration, bureaucracy (and its apparatuses), and restrictions to growth and development. Rapid technology progresses have fundamentally transformed the way we all live, work and spend our free time, and the legal profession is absolutely not exempt from the impact of these changes. In order to improve the assistance of their clients, and to have a better position on the competing legal market, it is vital for lawyers, regulators, law-makers to comprehend and recognize the ethical, functional, legal, and

business consequences of novel technologies on their respective practices and in the world in general as well.

I have attempted to find some answers all through my dissertation concerning the following questions:

Is there a need for modification in the context of personality protection, which may be justified by the diverse nature of individual technologies?

Yes, there may be a need for modification in the context of personality protection, which can be justified by the diverse nature of individual technologies.The need for modification in the context of personality protection may come from the rapid progresses/improvement and diverse nature of technology in the world today. As novel (innovative) technologies emerge and evolve, they often bring novel challenges/issues and risks/concerns to the protection of privacy. There are some key points to consider:

1. Data Privacy Concerns: With the proliferation of digital platforms[524], social media, and IoT devices, there is an increasing amount of personal data being collected, stored, and analyzed. Protecting individuals' privacy and ensuring that their personality traits, preferences, and behaviours are not misused or exploited has already become critical issues, nuisances in almost every Western society I have examined.

2. AI and Machine Learning: The advancement of artificial intelligence (AI) and machine learning technologies has enabled the development of sophisticated algorithms that are able to analyze gigantic amounts of data and, with no doubts, make accurate predictions about individuals' personalities and behaviours. Though one can also state to have positive applications, even advantages, it may raise concerns and alarm societies about potential misuse or unethical profiling.

3. Biometric Data and Identity: Biometric data, such as fingerprints or facial recognition, is all the time more used for identification and authentication purposes. The protection of this

[524]To be uptodate on the regulations related to platforms, see: Zsolt Ződi. *Characteristics of the European Platform Regulation Platform Law and User Protection*. Public Governance, Administration and Finances Law Review Vol. 7. No. 1. (2022) • 91–108

data has already turned to vital to prevent phenomena, such as, identity theft or unauthorized access to personal information.

4. Internet of Things (IoT): The interconnected nature of IoT devices can lead to the collection of personal data from various sources (for instance, AI commanded drones). Ensuring the security and privacy of such data has grown to be critical to safeguard privacy and prevent potential abuses/intrusions.

5. Legislative and Regulatory Challenges: The diversity of technological applications often outpaces/overtakes the progress of adequate laws and regulations to protect privacy and personality rights. Governments and policymakers need to stay proactive in updating and adapting legal frameworks to address emerging challenges/concerns.

6. Transparency and Informed Consent: Individuals need to be aware of how their data is being collected, used, and shared. Transparent data practices and obtaining informed consent from users are crucial to maintain trust and respect privacy rights as well.

7. Ethical Use of Data: Organizations collecting and analyzing personality-related data ought to hold on to ethical guidelines and principles. This includes ensuring data is anonymized whenever possible, avoiding discriminatory practices, and using the data for legitimate and transparent purposes.

8. Education and Awareness: Increasing public awareness about the risks and challenges associated with personality protection in the digital age is vital. Empowering individuals with knowledge about data privacy practices and cybersecurity can help them take more control over their personal information.

In conclusion, the diverse nature of individual technologies necessitates ongoing vigilance and adaptation to protect privacy. A multi-faceted approach, combining technological progressions, legal frameworks, ethical considerations/notions, and public awareness, is critical to guarantee a (delicate) balance between technological progress and safeguarding privacy.

Taking into account that typically administrative law is the first to respond to new technologies, the question arises as to what legislative attitudes can be inferred for civil courts.

It can be observed that the legislative attitudes primarily characterize the response to new technologies in the field of administrative law. Nevertheless, this approach can also serve as inspiration/insight for civil courts. The civil courts, dealing with civil law matters, can also recognize the possibilities/opportunities and impacts of new technologies in their legal system.New technologies such as automated systems (AIs and drones, for instance), can be beneficial in a great variety of areas/sectors for the functioning of courts and the efficiency of legal proceedings. Learning from legislative attitudes can help civil courts become acquainted with (also, up-to-date on) and understand these novel technological developments, and their application can accelerate, simplify/shorten, or develop legal procedures.Nevertheless, it is vital to consider legal principles cautiously, data/privacy protection, and fair procedures when introducing technological progress. In adopting legislative attitudes, civil courts must develop appropriate regulatory frameworks that ensure the ethical and fair implementation of new technologies.

In addition, legislative attitudes can provide important perspectives for civil courts regarding the analysis of legal literature and precedent cases related to the application of novel technologies. Administrative law often anticipates and explores new legal challenges/concerns, while in civil law; these challenges might arise at a later stage. By adopting legislative attitudes, civil courts can keep track of such forecasts and prepare for upcoming challenges. Also, the application of legislative attitudes in civil courts can also foster innovation and the development of legal technology.Taken as a whole, legislative attitude can hold significant importance for civil courts in the application of new technologies.

What regulatory trends of novel technologies have emerged in response to the growing issues of privacy protection?

Many regulatory trends have emerged in response to the growing issues/concerns of privacy protection, particularly concerning novel technologies. These trends were driven by the growing/escalating use of technologies like drones, artificial intelligence, big data analytics, Internet of Things (IoT), biometrics, and other innovative and rapidly changing

applications. Since technology and regulations are constantly evolving, it seems essential to consult up-to-date sources for the latest developments. There are some notable regulatory approaches:

1. Strengthening Data Protection Laws: Many countries have been revising or implementing new data protection laws to provide individuals with greater control over their personal information. The General Data Protection Regulation (GDPR) in Europe is one of the most significant and recent examples, setting a high standard for data protection globally, even as a prime example.

2. Enhanced Consent Mechanisms: Regulations focus on obtaining informed and explicit consent from individuals before collecting and processing their personal data. This trend aims to make sure that users have a clear understanding of how their data will be used.

3. Data Minimization and Purpose Limitation: To reduce privacy risks, regulations encouraged organizations to collect only the minimum amount of data necessary for a specific purpose and not use it for unrelated activities.

4. Algorithmic Transparency and Explainability: With the increased use of AI and machine learning algorithms, there was a push for regulations that required organizations to provide explanations for automated decisions that affect individuals.

5. Privacy by Design: Privacy considerations were required to be integrated into the design of technologies from the outset, ensuring that privacy protection was an integral part of the development process.

6, Biometric Data Regulation: Given the sensitivity of biometric information, some regions have been introducing specific regulations to govern its collection, use, and storage.

7. IoT Security and Privacy Guidelines: The proliferation of IoT devices has raised concerns/issues about data security and privacy. Regulatory trends included guidelines and standards to ensure IoT devices have appropriate security measures and data protection protocols.

8. Data Breach Notification: Many regulations mandated organizations to notify individuals and authorities promptly in the event of a data breach that could compromise their privacy.

9. Cross-Border Data Transfers: Regulations were addressing the challenges of cross-border data transfers, aiming to ensure that data is adequately protected when moving between jurisdictions.

10. Increased Regulatory Enforcement and Fines: Regulators have been becoming more vigilant in enforcing privacy regulations and imposing significant fines for non-compliance, signalling a stronger commitment to privacy protection.

11. Artificial Intelligence (AI) Ethics and Governance: As AI applications become more pervasive, there is a growing focus and attention on the ethical use of AI and guaranteeing that AI systems do not perpetuate bias or infringe on individual rights. It can also be seen that some jurisdictions are exploring AI-specific regulations to address these concerns/issues specifically related to privacy protection.

12. Privacy in Healthcare Technologies: With the rise of telemedicine, health apps, and wearable devices, there is a heightened emphasis and attention paid on privacy and security regulations for healthcare technologies, given the sensitivity of health data.

13. Regulating Social Media and Big Tech: Some regions have started exploring regulations to address the privacy concerns related to the vast collection and use of personal data by social media platforms and big tech companies, especially great number of cases can be seen in the USA.

14. Data Protection Impact Assessments (DPIAs): Increasingly, organizations are required to conduct DPIAs to assess the privacy risks associated with their data processing activities, especially when deploying novel technologies.

15. Privacy and Autonomous Vehicles: As self-driving cars and autonomous vehicles become more prevalent, regulators are addressing privacy and security concerns related to accountability, and the data generated and collected by these vehicles.

16. Cybersecurity and Privacy: Regulations are increasingly emphasizing the importance of robust cybersecurity measures to protect personal data from unauthorized access and data breaches.

16. Consumer Privacy Control: Some regulations are focusing on empowering individuals with greater control over their personal data, including the ability to access, modify, or delete their data held by organizations.

Though we need to note that the regulatory landscape is dynamic, and new trends have emerged beyond the scope of my dissertation. In order to keep up with novel concerns related to the dynamic relationship between privacy (and its protection), it seems that one is supposed to embrace a multidisciplinary mindset.

References:

BOOKS AND ARTICLES:

ABDO, Alex: *Why Rely on the Fourth Amendment To Do the Work of the First?* Yale Law Journal Forum, Vol. 127, 2017. Available: https://www.yalelawjournal.org/pdf/Abdo_e3en3agt.pdf [accessed 7 Jan 2021]

AIELLO, J.R.: *Human Spatial Behavior*, In: D. Stokols and I. Altman (Eds.): *Handbook of Environmental Psychology*. John Wiley & Sons, New York, 1987, 359-504.

AIELLO, J. R. and THOMPSON, D. E., and Baum, A: *The symbiotic relationship between social psychology and environmental psychology: Implications from crowding, personal space, and intimacy regulation research*. In: HARVEY, J. H. (Ed.): *Cognition, social behavior and the environment*. Hillsdale, New Jersey: Lawrence Erlbaum Associates, 1981, 423-438;

ALTMAN, Irwin: *A Conceptual Analysis*.Environment and Behavior, Vol. 8, Iss 1, 1976. (https://doi.org/10.1177/001391657600800102)

ALTMAN, Irwin: *The environment and social behavior*.Brooks/Cole, Monterey, 1976.

ALTMAN, Irwin– CHEMERS, Martin M.:*Culture and environment*. Brooks/Cole, Monterey,1980.

ANGLIM, Christopher T.: *Privacy Rightsin the Digital Age*. Greyhouse Publising Inc., 2018.

ANDERSON, Janna – RAINIE, Lee – LUCHSINGER, Alex: *Artificial Intelligenceand the Future of Humans*. Pew Research Center, December 2018, Available: https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/[accessed 19 Dec 2020]

ASHBOURN, J.:*The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies. Background paper for the Institute of Prospective Technological Studies*. DG JRC – Seville, Commission, January 2005, 4, (‘Ashbourn, Social Implications of Scale Implementation of Biometrics,

2005’).http://www.statewatch.org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf[accessed 9 Jan 2019]

AUSTIN, Sarat: *Whither privacy: an introduction*. In: *A world without privacy: what law can and should do?* Cambridge University Press, New York, 2015.

BADII, Atta, EINIGMathieu andTIEMANN, Marco [et. al.]:*Visual context identification for privacy-respecting video analytics*. Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on. IEEE, 2012. (Doi:10.1109/MMSP.2012.6343470)

BARBEY, Gilles:*L’appropriation des espaces du logement: Tentative de cadrage théorique*. In:KOROSEC-SERFATY, Perla. (Ed.):*Actes de la 3ème Conférence Internationale de Psychologie de l’Espace Construit Strasbourg, France*. Université de Strasbourg Press, *Strasbourg*, 1976.

BARFIELD, Woodrow – PAGALLO, Ugo: *Research handbook on the law of artificial intelligence*. Edward Elgar Publishing, Cheltenham, 2018.

BATTEN, Donna (Ed.): *Gale Encyclopaedia of American Law*. Gale Cengage Learning, New York, 2010, 176.

BEANEY, William M.: *The Right to Privacy and American Law*. Law and Contemporary Problems, Vol. 31, No. 2, Privacy, *1966* Spring, 253-271.Available:https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3107&context=lcp [accessed 16 Jan 2021]

BERRYHILL, Jamie –HEANG, Kévin Kok – CLOGHER, Rob – MCBRIDE, Keegan:*Hello, World: Artificial Intelligence and its Use in the Public Sector*. OECD Working Papers on Public Governance, No. 36, 2019. Available:https://oecd-opsi.org/wp-content/uploads/2019/11/AI-Report-Online.pdf [accessed 19 Dec 2020]

Békési Bertold. és Seres József: *Drónok alkalmazásának lehetőségei*. REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK 32. évfolyam (2020) 3. szám 5–19.

BLOOM, Peter – SANCINO, Alessandro: *Disruptive Democracy: the Clash Between Techno-Populism and Techno-Democracy*. SAGE Publications, London, 2019. (Doi:http://dx.doi.org/10.4135/9781526465658)

BOSTROM,Nick – DAFOE, Allan – FLYNN, Carrick: *Policy Desiderata in the Development of SuperintelligentAI*. Future of Humanity Institute, 2017. Available: http://governance40.com/wp-content/uploads/2018/12/aipolicy.pdf[accessed 5 Dec 2020]

BRAY, Francesca and Arnold Pacey:*Technology in world civilization:a thousand-year history*.Cambridge,MIT PRESS, 2021.

BRENNER, Susan: *Law in an Era of "Smart" Technology*. Oxford University Press, New York, 2007. (Doi:10.1093/acprof:oso/9780195333480.001.0001)

BREYER, Stephen:*Regulation and its reform*. Harvard University Press, Cambridge, MA, 1982.Available:https://www.scienzegiuridiche.uniroma1.it/sites/default/files/docenti/dalberti/breyer-regulation-and-its-reform.pdf[accessed 27 Aug 2020]

BROWNSWORD, Roger: *From Erewhon to AlphaGo: For the sake of human dignity, should we destroy the machines?* Law, Innovation and Technology, Vol. 9, Iss. 1, 2017, 117-153. (Doi: https://doi.org/10.1080/17579961.2017.1303927)

BROWNSWORD, Roger: *Law, Technology and Society: Re-imagining the Regulatory Environment*. Routledge, New York, 2019. (Doi: https://doi.org/10.4324/9781351128186)

BROWNSWORD, Roger: *Rights, Regulation and the Technological Revolution*. Oxford University Press, Oxford, 2008. (Doi: https://doi.org/10.1093/acprof:oso/9780199276806.001.0001)

BROWNSWORD, Roger – SOMSEN, Han: *Law, Innovation and Technology:Before We Fast Forward - A Forum for Debate*. Law, Innovation and Technology, Vol. 1, Iss. 1, 2009, 1-73.(Doi: 10.1080/17579961.2009.11428364) Available: https://doi.org/10.1080/17579961.2009.11428364 [accessed 4 Nov 2018]

BROWNSWORD, Roger – SOMSEN, Han: *Innovation and Technology: Before We Fast Forward — AForum for Debate*. Law, Innovation and Technology. Vol. 1, Iss. 1, 2009, 1–73. (Doi: https://doi.org/10.1080/17579961.2009.11428364)

BRÜGGEMEIER, Gert – COLOMBI CIACCHI, Aurelia – O'CALLAGHAN, Patrick (Eds.):*Personality Rights in European Tort Law*. Cambridge University Press, Cambridge, 2010. (DOI: https://doi.org/10.1017/CBO9780511676161)

BRUNDAGE, Miles. – AVIN, Shahar. – CLARK, JACK [et al.]:*The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, 2018. (Doi: https://doi.org/10.17863/CAM.22520) Available:

https://www.repository.cam.ac.uk/bitstream/handle/1810/275332/1802.07228.pdf?sequence=1&isAllowed=y[accessed 4 Dec 2020]

BRUNDAGE, Miles – BRYSON, Joanna: *Smart Policies for Artificial Intelligence*. 2016 Available: https://arxiv.org/pdf/1608.08196.pdf [accessed 4 Dec 2020]

BUITEN, Miriam C.: *Towards Intelligent Regulation of Artificial Intelligence*.European Journal of Risk Regulation, Vol. 10, No. 1, 2019, 41-59. (Doi:10.1017/err.2019.8)

https://www.cambridge.org/core/services/aop-cambridge-core/content/view/AF1AD1940B70DB88D2B24202EE933F1B/S1867299X19000084a.pdf/towards_intelligent_regulation_of_artificial_intelligence.pdf[accessed 19 Dec 2020]

BUNCH, Bryan H. – HELLEMANS, Alexander: *The History of Science and Technology: A Browser's Guide to the Great Discoveries, Inventions, and the People Who Made Them from the Dawn of Time to Today*. Houghton Mifflin Harcourt,Boston, 2004.

BUTENKO, Anna – LAROUCHE, Pierre: *Regulation for Innovativeness or Regulation of Innovation*? Law, Innovation and Technology, Vol. 7, Iss. 1, 2015. (Doi: 10.1080/17579961.2015.1052643)

CALCUTT, David QC: *Review of Press Self-Regulation*: *Presented to the Parliament by the Secretary of State for the Department of National Heritage*. HMSO, London, 1993. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/271963/2135.pdf [accessed 5 Jan 2021]

CALO, Ryan: *Artificial Intelligence Policy: A Primer and Roadmap*.*UC Davis Law Review*, Vol. 51, Iss. 2, 2017, 399-435. (Doi: http://dx.doi.org/10.2139/ssrn.3015350) Available at: https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_Calo.pdf [accessed 4 Dec 2020]

CALO, Ryan:*Robotics and the lessons of cyberlaw*. California Law Review, Vol. 103, No. 3, 2015, 513-563. (Doi: http://dx.doi.org/10.2139/ssrn.2402972)

CAMPISI, Patrizio (eds.):*Security and Privacy in Biometrics.* Springer, New York, 2013. (https://doi.org/10.1007/978-1-4471-5230-9) https://link.springer.com/book/10.1007/978-1-4471-5230-9[accessed 5 May 2019]

CAMPISI, Patrizio: *Security and Privacy in Biometrics: Towards a Holistic Approach.* In: CAMPISI, Patrizio (Ed.):*Security and Privacy in Biometrics*. New York, Springer, 2013.

CAMPOLO, Alex – SANFILIPPO, Madelyn –WHITAKKER, Meredith – CRAWFORD, Kate: *AI Now 2017 Report*. AI Now Institute, New York, 2017. Available: https://ainowinstitute.org/AI_Now_2017_Report.pdf [accessed 5 Dec 2020]

CAVOUKIAN, Ann:*Privacy Engineering: Proactively Embedding Privacy, by Design.* Information and Privacy Commissioner, Ontario, 2014.avilable: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-priv-engineering.pdf [accessed 1 Sep 2020]

CHANNELL, David F.:*A History of Technoscience Erasing the Boundaries between Science and Technology.* Routledge, London, 2017. (https://doi.org/10.4324/9781315268897)

CHAPMAN, Anne: *Democratizing Technology: Risk, Responsibility and the Regulation of Chemicals*. Earthscan Publications, London, 2007.

CHO, Hyunghoon – IPPOLITO, Daphne– YU, Yun William: *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs.* Available:https://arxiv.org/pdf/2003.11511v2.pdf[accessed 17 Sep 2020]

CITRON,Danielle Keats: *Mainstreaming Privacy Torts*. California Law Review, Vol. 98, 1805-1852. Available: https://29qish1lqx5q2k5d7b491joo-wpengine.netdna-ssl.com/wp-content/uploads/2014/10/Citron.FINAL_.pdf[accessed 7 Jan 2021]

CLOATRE, Emilie – PICKERSGILL, Martyn (Eds.):*Knowledge, Technology and Law*. Routledge, New York, 2015. (Doi: https://doi.org/10.4324/9780203797600)

CUDD, Ann E. – NAVIN, Mark C. (Ed.): *Core Concepts and Contemporary Issues in Privacy*. Springer International Publishing, (AMINTAPHIL: The Philosophical Foundations

of Law and Justice 8), 2018. https://doi.org/10.1007/978-3-319-74639-5_1 [accessed 9 Jan 2019]

CUMO, Christopher:*Science and technology in 20th-century American life*. Greenwood Press, London, 2007.

CUSTERS,Bart –SEARS, Alan M. –DECHESNE, Francien [et. al.]:*EU Personal Data Protection in Policy and Practice*. T.M.C. Asser Press, The Hague, 2019. (Doi: 10.1007/978-94-6265-282-8)

DWORK, Cynthia – MCSHERRY, Frank – NISSIM, Kobbi [et. al.]:*Calibrating Noise to Sensitivity in Private Data Analysis*. In: HALEVI, Shai – RABIN, Tal (eds.): *Theory of Cryptography. Lecture Notes in Computer Science*, Vol. 3876, Springer, Berlin, Heidelberg,2006, 265-284. (https://doi.org/10.1007/11681878_14) Available:https://people.csail.mit.edu/asmith/PS/sensitivity-tcc-final.pdf[accessed 17 Sep 2020]

DE HERT, Paul – GUTWRITH, Serge: *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power.*In:CLAES, Erik – Duff, Antony – GUTWRITH, Serge (eds.),: *Privacy and thecriminal law*, Intersentia, Oxford, 2006.

DWORKIN, Gerald: *The Younger Committee Report on Privacy*. The Modern Law Review, Vol. 36, No. 4, Jul., 1973, 399-406. Available: https://www.jstor.org/stable/pdf/1093890.pdf?refreqid=excelsior%3Aa62403ddf72ee8a8182e4316e98d464b [accessed 5 Jan 2021]

EDGERTON, David: *The Shock of the Old: Technology and Global History since 1900*. Oxford University Press, Oxford, 2006.

ELLUL, Jacques: *The Technological Society*. (Trans.) John Wilkinson. Knopf,New York, 1964. London: Jonathan Cape, 1965. Rev. ed.: New York: Knopf/Vintage, 1967. with introduction by Robert K. Merton (professor of sociology, Columbia University).

FARBER, Hillary B.*: Keep out the efficacy of trespass, nuisance and privacy torts as applied to drones.*Georgia State University Law Review Vol. 33, No. 2, 2017, 359-409. Available: https://core.ac.uk/download/pdf/233916802.pdf[accessed 5 Nov 2020]

FARELO, A.: *A History of Fingerprints*, Interpol, April 2009. Available: http://www.interpol.int/Public/Forensic/fingerprints/History/BriefHistoricOutline.pdf[accessed 9 Jan 2019]

FAVILLI, Chiara:*Technological Change in Italy*.In: MARTIN-CASALSop. cit.

FEIGENBAUM, Joan –FREEDMAN, Michael J.– SANDER, Tomas [et. al.]: *Privacy Engineering for Digital Rights Management Systems*.(ACM Workshop on Security and Privacy in Digital Rights Management)Associated with ACM Communication and Computer Security, Philadelphia, 2001. available: http://www.cs.yale.edu/homes/jf/FFSS-DRM2001.pdf[accessed 13 Oct 2020]

FENWICK, Mark – KAAL, Wulf A. – VERMEULEN, Erik P. M.: *Regulation Tomorrow: What Happens When Technology Is Faster than the Law*. American University Business Law Review Vol. 6, Iss. 3, 2017, 561-594. Available: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=https://www.google.hu/&httpsredir=1&article=1028&context=aublr[accessed 25 Mar 2019]

FÉZER Tamás: *Comparative Tort Law: E-Learning textbook*. (E-book), Debrecen2013.

FÉZER Tamás: *Re-CivilLaw in Hungary*. Studia Prawnicze, Rozprawy i Materiały / Studies in Law: Research Materials, Vol. 15, No. 2, 2014, 73–92. Available: https://sp.ka.edu.pl/numery/studia-prawnicze-rim-2014-2.pdf [accessed 6 Jan 2021]

FINCH, Emily – FAFINSKI, Stefan: *Tort Law*. Pearson Education Limited, London, 2017.

FLORIDI, Luciano (eds.): *Protection of Information and the Right to Privacy - A New Equilibrium?*Springer International Publishing, New York, 2014. (Doi: 10.1007/978-3-319-05720-0)

FOX, Robert: *Technological Change: Methodsand Themes in the Historyof Technology*. New York, Routledge, 1998.

FREITAS, Pedro Miguel –COELHO MOREIRA, Teresa –ANDRADE, Francisco: *Data Protection and Biometric Data: European Union Legislation.* In: JIAN, Richard –AL-MAADEED,Somaya–BOURIDANE, Ahmed [et. al.] (Eds.): *Biometric Security and Privacy Opportunities & Challenges in The Big Data Era*. Springer, New York, 2017.

GIRASA, Rosario: *Artificial Intelligence as a Disruptive Technology - Economic Transformation and Government Regulation*. Palgrave Macmillan, 2020. (Doi: 10.1007/978-3-030-35975-1)

GONZALEZ FUSTER, Gloria: *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer, New York, 2014. (DOI 10.1007/978-3-319-05023-2)

GONZALEZ FUSTER, Gloria– GUTWIRTH, Serge:*Opening up personal data protection: A conceptual controversy*. Computer Law and Security Review, Vol. 29, Iss. 5, October 2013, 531–539.

GRACE, Katja – SALVATIER, John – DAFOE, Allan [et. al.]: *Viewpoint: When Will AI Exceed Human Performance? Evidence from AI Experts.*Journal of Artificial Intelligence Research, Vol. 62, 2018, 729-754. (Doi: https://doi.org/10.1613/jair.1.11222)

GRACE, Katja – SALVATIER, John – DAFOE, Allan [et. al.]: *When Will AI Exceed Human Performance? Evidence from AI Experts.* Future of Humanity Institute, UK and AI Impacts, Berkeley, USA (2017) Available: https://arxiv.org/abs/1705.08807[accessed 4 Dec 2020]

GRUENSPECHT, Howard K.: *Differentiated Regulation: the Case of Auto Emissions Standards*. American Economic Review, Vol. 72, No. 2, 1982, 328-331.

GUTWIRTH, Serge – DE HERT, Paul:*Privacy, data protection and law enforcement. Opacity of the individual and transparency of power*.In:CLAES, Erik – DUFF, Antony– GUTWIRTH, Serge (eds.):*Privacy and the criminal law*.Intersentia,Antwerp/Oxford, 2006. (ISBN 90 5095 545 2) Available:https://works.bepress.com/serge_gutwirth/5/ [accessed 10 Sep 2020]

GUTWIRTH, Serge –LEENES,Ronald –DE HERT,Paul [et. al.] (eds.):*European Data Protection: In Good Health?* Springer, Dordrecht, 2012. (Doi: 10.1007/978-94-007-2903-2)

GUTWRITH, Serge – POULLET, Yves –DE HERT, Paul [et.al.]: Reinventing Data Protection? Springer, New York, 2009. (Doi: https://doi.org/10.1007/978-1-4020-9498-9)

HAMBLING, David: *Swarm Troopers: How Small Drones Will Conquer the World*. Archangel Ink Publishing, Venice, Florida, 2016.

HARPWOOD, Vivienne:*Modern tort law*. Routledge-Cavendish, New York. 2009. (Doi: https://doi.org/10.4324/9780203868812)

HARTSHORNE, John: *The need for an intrusion upon seclusion privacy tort within English law*. Common Law World Review,Vol. 46, No. 4, 2017,287–305. (Doi: https://doi.org/10.1177/1473779517739798) Available: https://leicester.figshare.com/articles/journal_contribution/The_need_for_an_intrusion_upon_seclusion_privacy_tort_within_English_law/10229567[accessed 7 Jan 2021]

HAUFLER, Virginia: *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy*. Carnegie Endowment for International Peace, Washington, D.C., 2001.

HEADRICK, Daniel R.:*Technology – A World History.* Oxford University Press, New York, 2009 https://cryptome.org/2013/01/aaron-swartz/019515648X.pdf[accessed 5 May 2019].

HENDRICKS, Even– HAYDEN, Trudy –NOVIK, Jack D.: *Your right to privacy: a basic guide to legal rights in an information society*. Southern Illinois University Press, Carbondale, Edwardsville, 1990.

HIJMANS, Hielke: *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*. Springer, New York, 2016. (Doi: 10.1007/978-3-319-34090-6)

HOOFNAGLE, Chris Jay– VAN DER SLOOT, Bart – ZUIDERVEEN BORGESIUS, Frederik: *The European Union general data protection regulation: what it is and what it means*. Information and Communications Technology Law, Vol. 28, Iss. 1, 2019, 65-98. (DOI: 10.1080/13600834.2019.1573501) Available: https://www.tandfonline.com/doi/pdf/10.1080/13600834.2019.1573501?needAccess=true[accessed 26 Aug 2020]

INNESS, Julia C.: *Privacy, Intimacy and Isolation*. Qxford University Press, Oxford, 1992.

JAIN, Anil K. – ROSS, Arun A. – NANDAKUMAR, Karthik:*Introduction to Biometrics*. Springer, New York, 2011, 1–3. (https://doi.org/10.1007/978-0-387-77326-1) https://link.springer.com/content/pdf/10.1007%2F978-0-387-77326-1.pdf[accessed 20 Jun 2019]

JAIN, Anil K. – ROSS, Arun A. – PRABHAKAR, S.:*An introduction to biometric recognition*. IEEE Transactions on Circuits and Systems for Video Technology, 2004/1, 4–20. (https://doi.org/10.1109/TCSVT.2003.818349)

JASANOFF, Sheila:*Science at the Bar: Law, Science, and Technology in America*. Harvard, University Press, London, 1997. (Doi: https://doi.org/10.2307/j.ctvjz822j) Available: https://monoskop.org/images/a/ae/Jasanoff_Sheila_Science_at_the_Bar_Law_Science_and_Technology_in_America_Twentieth_Century.pdf [accessed 29 September 2020]

JIANG, Richard – AL-MAADEED, Somaya – BOURIDANE, Ahmed – CROOKES, Danny – BEGHDADI, Azeddine (eds.):*Biometric Security and Privacy – Opportunities & Challenges in The Big Data Era*. Springer, New York, 2017. (https://doi.org/10.1007/978-3-319-47301-7) Available:https://link.springer.com/content/pdf/10.1007%2F978-3-319-47301-7.pdf [accessed 25 Aug 2019]

JOHNSON, David R. – POST, David G.:*And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized,emergent Law*. In: KAHIN, Brian - KELLER, James H.: *Coordinating the Internet*. MIT Press, Cambridge MA, 1997.(Doi: https://doi.org/10.7551/mitpress/2170.003.0007) Available online at: www.temple.edu/lawschool/dpost/writings.html#RecentWritings[accessed 27 Aug 2020]

JOHNSON, David R. – POST, David G.: *Law and borders: the rise of law in cyberspace*. Stanford Law Review,Vol. 48, No. 5, 1996. (Doi: https://doi.org/10.2307/1229390) Available: https://www.jstor.org/stable/1229390?origin=crossref&seq=1[accessed 27 Aug 2020]

JOLOWICZ, John Anthony: *On civil procedure*. Cambridge University Press, Cambridge, 2000. (Doi: https://doi.org/10.1017/CBO9780511549540)

JONES, Meg Leta– KAMINSKI, Margot E.:*An American's guide to the GDPR.* Forthcoming in Denver Law Review, Vol. 98, No. 1, 2020, 20-33. Available: https://ssrn.com/abstract=3620198[accessed 26 Aug 2020]

KEANE, John F. – CARR, Stephen S.: *A Brief History of Early Unmanned Aircraft***.** In.: Johns Hopkins APL Technical Digest, Vol. 32, No 3., 2013, 558-571. Available: http://www.jhuapl.edu/techdigest/TD/td3203/32_03-Keane.pdf[accessed 25 Mar 2019]

KENDALL, Diana:*Sociology in our times.* Wadswort, Belmont, 2003.

KENYON, Andrew T. – RICHARDSON, Megan (Eds.): *New dimensions in privacy law: international and comparative perspective*. Cambridge University Press, New York, 2006.

KINDT, Els J.:*Privacy and Data Protection Issues of Biometric Applications – A Comparative Legal Analysis*. Springer, Dordrecht, 2013. (https://doi.org/10.1007/978-94-007-7522-0)https://link.springer.com/content/pdf/10.1007/978-94-007-7522-0.pdf [accessed 10 Sep 2019]

Admiral KIRK James T. -COX, Greg:*The Eugenics Wars – The Rise and Fall of Khan Noonien Singh*.Pocket Books, New York, 2002.

KITCHIN, Rob: *Big Data, new epistemologies and paradigm shifts*. Big Data and Society, Vol. 1, No. 1, 2014, 1-12. (Doi: https://doi.org/10.1177/2053951714528481) Available: https://journals.sagepub.com/doi/pdf/10.1177/2053951714528481[accessed 17 Aug 2020]

KLEIN Tamás – TÓTH András (eds.):*Technológiai jog-Robotjog-Cyberjog.* Wolters Kluwer, Budapest, 2018.

KLEMENS, Guy: *The Cell phone: The History and Technology of the Gadget That Changed the World*. McFarland and Company, Inc., Publishers, London, 2010.

KLITOU, Demetrius:*Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*. (Information Technology and Law Series (25)), Springer, New York, 2014. (Doi: https://doi.org/10.1007/978-94-6265-026-8_2)

KOROSEC-SERFATY, Perla. (Ed.):*Appropriation of space.* In: SERFATY-GARZON, Perla: *Proceedings of the third International Architectural Psychology Conference*.Louis Pasteur University, Strasbourg, 1976.

KREPS, Sarah Elizabeth: *Drones: what everyone needs to know*. Oxford University Press, New York, 2016.

KSIĘŻAK, Paweł – WOJTCZAK, Sylwia: *AI versus robot: in search of a domain for the new European civil law*. Law, Innovation and Technology, Vol. 12, Iss. 2,2020, 297-317,(Doi: 10.1080/17579961.2020.1815404)

LEENES, Ronald: *Regulating New Technologies in Times of Change*. In: REINS, Leonie (Ed.): *Regulating New Technologies in Uncertain Times*. Springer, The Hague, 2019.(Doi: https://doi.org/10.1007/978-94-6265-279-8_1)

LEENES, Ronald – PALMERINI, Erica –KOOPS, Bert-Jaap [et. al.]: *Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues*. In: Law, Innovation and Technology, Vol. 9, Iss. 1, 2017, 1-44. (Doi: 10.1080/17579961.2017.1304921)Available:https://research.tilburguniversity.edu/files/23365230/Regulatory_challenges_of_robotics_some_guidelines_for_addressing_legal_and_ethical_issues.pdf [accessed 26 Aug 2020]

LEENES,Ronald– Van BRAKEL,Rosamunde – GUTWIRTH,Serge [et.al.] (Eds.): *Data Protection and Privacy: (In)visibilities and Infrastructures.* Springer,New York, 2017. (Doi: 10.1007/978-3-319-50796-5)

LESSIG, Lawrence:*Code: version 2.0.*Basic Books,New York, 2006.

LESSIG, Lawrence: *Code and Other Laws of Cyberspace*. Basic Books, New York, 1999.

LISCHKA, Konrad – MCCARTHY, John: *Der Vater der Rechner-Cloud ist tot*. Spiegel Online vom 25.10.2011. Available: www.spiegel.de/netzwelt/web/john-mccarthy-der-vater-der-rechner-cloud-ist-tot-a-793795.html [accessed 14 Dec 2020]

MALOOF, Mark: *Artificial Intelligence: An Introduction*. Georgetown University, Washington DC, 2017.http://people.cs.georgetown.edu/~maloof/cosc270.f17/cosc270-intro-handout.pdf[accessed 27 Aug 2020]

MANDEL, Gregory N:*Regulating Emerging Technologies.* Law, Innovation and Technology, Vol. 1, Iss. 1, 2009, 75-92, (Doi: 10.1080/17579961.2009.11428365) Available: https://ssrn.com/abstract=1355674. [accessed 20 Jul 2020]

MARCHANT, Gary E. – ALLENBY, Braden R. – HERKERT, Joseph R. (Eds.):*The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: the Pacing Problem 3.*Springer, NewYork, 2011 (Doi 10.1007/978-94-007-1356-7)

MARCHANT, Gary E. – SYLVESTER Douglas J. – ABBOTT Kenneth W:*What does the history of technology regulation teach us about nano oversight?*The Journal of Law, Medicine and

Ethics,Vol. 37, Iss. 4, 2009, 724-731(doi:10.1111/j.1748-720X.2009.00443.x.) https://pubmed.ncbi.nlm.nih.gov/20122112/[accessed 20 Jul 2020]

MARCHANT, Gary E. – WALLACH, Wendell:*Coordinating Technology Governance*. Issues in Science and Technology Vol. 31, No. 4, Summer 2015. Available: https://issues.org/coordinating-technology-governance/ [accessed 11 Nov 2020]

MARGULIS, Steven. T.:*Conceptions of privacy: current status and next steps*. Journal of Social Issues, Vol. 33, No.: 3, 1977, 5-21. (Doi: https://doi.org/10.1111/j.1540-4560.1977.tb01879.x)

MARTIN-CASALS, Miquel:*The Development of Liability in Relation to Technological Change*.Cambridge University Press, 2010.

MCCLELLAN, James E. – DORN, Harold: *Science and Technology in World History*. Johns Hopkins University Press, Baltimore, 2006. Available: https://books.google.hu/books?id=YnqLfVRJ3AkC&printsec=frontcover&hl=hu&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [accessed 23 Jul 2020]

MCGRATH, Rita:*The Pace of Technology Adoption is Speeding Up*. Harvard Business Review, November 25 2013,Available:https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up[accessed 4 Nov 2018]

MCGUIRE, James E. – TUCHANSKA, Barbara:*Science Unfettered – A Philosophical Study in Sociohistorical Ontology*. Ohio University Press, Athens, 2000.

MCKENNA, Bruce A: *False Light: Invasion of Privacy?*Tulsa Law Review, Vol. 15, Iss. 1, 2013.Available: https://core.ac.uk/download/pdf/232683176.pdf or https://digitalcommons.law.utulsa.edu/tlr/vol15/iss1/7[accessed 6 Jan 2021]

MENDEL, Gregory N.:*Regulating Emerging Technologies*.Law, Innovation and Technology, Vol. 9, Iss. 1, 2017. (Doi: https://doi.org/10.1080/17579961.2009.11428365)

MILL, John Stuart (Ed.): *Utilitarianism, On Liberty, Essay on Bentham: together with selected writings of Jeremy Bentham and John Austin*.Collins, London, 1962.

MOREHAM, Nicole:*Privacy in the Common Law: A Doctrinal and Theoretical Analysis*. Law Quarterly Review, Vol. 121, 2005, 628-656.

MOSES, Lyria Bennett: *How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target*. Law, Innovation and Technology, Vol. 5, Iss. 1, 2013, 1-20, (Doi: 10.5235/17579961.5.1.1) [accessed 4 Dec 2020]

MULLIGAN, Christina M:,*Perfect Enforcement of Law: When toLimit and When to Use Technology*.Richmond Journal of Law and Technology, Vol. 14, Iss. 4, 2008, 1-49.https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1295&context=jolt [accessed 4 Dec 2020]

NISSENBAUM, Helen: *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, Stanford, 2010.(Doi: https://doi.org/10.1515/9780804772891)

O'BRIEN, Denis: The Right of Privacy. Columbia Law Review, Vol. 2, No. 7, Nov. 1902, 437-448.(Doi: https://doi.org/10.2307/1109924) Available: https://www.jstor.org/stable/pdf/1109924.pdf?refreqid=excelsior%3Aaa912ae10059838a82fa715770ddc96f[accessed 5 Jan 2021]

PATO, Joseph N. –MILLETT,Lynette I.(Eds.), National Research Council:*Biometric Recognition: Challenges and Opportunities.*National Academies Press, Washington DC, 2010. (Doi: https://doi.org/10.17226/12720) Available:http://nap.edu/12720 [accessed 25 Aug 2019]

PEARL, Tracy Hresko: *Fast & Furious: The Misregulation of Driverless Cars.* New York University Annual Survey of American Law, Vol. 73, Iss. 1, 2017, 19-72. Available: https://ttu-ir.tdl.org/bitstream/handle/2346/73420/Fast%20%26%20Furious%2073%20NYU%20Ann%20Sur%20Am%20L%2019.pdf?sequence=1&isAllowed=y[accessed 21 Dec 2020]

PERNOT-LEPLAY,Emmanuel:*China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, Penn State Journal of Law & International Affairs, Vol. 8, No. 1, 2020. Available:https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1244&context=jlia [accessed 2 Jan 2021]

PERNOT-LEPLAY,Emmanuel:*EU Influence on Data Privacy Laws: Is the US approach converging with EU model?* Colorado Technology Law Journal,Vol. 18, No. 1,

2019.Available: https://pernot-leplay.com/wp-content/uploads/2020/04/EU-Influence-on-Data-Privacy-Laws.-Is-the-U.S.-Converging-with-the-EU-Model.pdf [accessed 4 Jan 2021]

PÉTERFALVI Attila–RÉVÉSZBalázs –BÚZÁS Péter (Eds.): *Magyarázat a GDPR-ról*. Wolters Kluwer, Budapest, 2018.

POSSER, William L: '*Privacy*'. California Law Review, Vol. 48, No. 3, 1960, 383-423. (Doi: https://doi.org/10.2307/3478805)

PROSHANSKY, Harold M.:*The City and Self-Identity*. Environment and Behavior, Vol 10, Iss. 2, 1978, 147-169. (Doi: 10.1177/0013916578102002),available: http://eab.sagepub.com/content/10/2/147 [accessed 7 Oct 2020]

RABESANDRATANA, Tania: *With €1.5 billion for artificial intelligence research, Europe pins hopes on ethics*. Science, Apr 25, 2018. https://www.sciencemag.org/news/2018/04/15-billion-artificial-intelligence-research-europe-pins-hopes-ethics [accessed 2 Sep 2020]

RICHARDS, Neil M.: *The Limits of Tort Privacy*. Journal of Telecommunications and High Technology Law, Vol. 9, 2011, 357-384. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1862264[accessed 7 Jan 2021]

RODRIGUES, Rowena – PAPAKONSTANTINOU, Vagelis (Eds.): *Privacy and Data Protection Seals*. T.M.C. Asser Press /Springer, London, 2018. (Doi: 10.1007/978-94-6265-228-6)

SCHERER, Matthew. U.: *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies and Strategies*. Harvard Journal of Law and Technology, Vol. 29, No. 2, Spring 2016, 353–400. Available: http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf[accessed 4 Dec 2020]

SCHOEMAN, Ferdinand David: *Privacy and social freedom*. Cambridge University Press, Cambridge, 1992. (Doi: https://doi.org/10.1017/CBO9780511527401)

SCHWABACH, Aaron: *Internet and the Law: Technology, Society, and Compromises*. ABC-CLIO, Oxford, 2006.

SCHWART, Paul M.: *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*.Stanford Law Review, Vol. 52, No. 5, 2000, 1559-1572. (Doi: https://doi.org/10.2307/1229521)

SCHWARTZ, Robert A. – BYRNE, John Aidan – COLANINNO, Antoinette (eds.): *Technology and Regulation: How Are They Driving Our Markets?*Springer, New York, 2009. (DOI 10.1007/978-1-4419-0480-5)

SCHWARTZ, Robert A. – BYRNE, John Aidan – SCHNEE, Gretchen (eds.): *Rethinking Regulatory structure*. Springer, New York, 2013. (Doi: 10.1007/978-1-4614-4373-5)

SHANNON, ClaudeElwood:*Communication theory of secrecy systems*. Bell system technical journal, Vol. 28, No. 4, 1949, 656–715. (Doi: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x) Available: https://www.cs.virginia.edu/~evans/greatworks/shannon1949.pdf [accessed 17 Sep 2020]

SIMÓ, Ferenc Zoltán. *Drones and Privacy-Related Issues/Concerns: Alice inTechno-Land.* ACTA UNIVERSITATIS SAPIENTIAE LEGAL STUDIES 8 : 1 pp. 89-105. , 17 p. (2019)

SIMÓ, Ferenc Zoltán. *Preliminary Observations on AI Regulation*. Mesterséges Intelligencia 3 : 1 pp. 33-59. , 27 p. (2021)

SIMÓ, Ferenc Zoltán. *Privacy in Context: Info-tech based society and the revolutionary effects ofdrones/phones/biometrics*JURA 25 : 2 pp. 458-469. , 12 p. (2019)

SIMÓ, Ferenc Zoltán. *Thenand now: Laws on first and second generationbiometricsystems*. PRO FUTURO - A JÖVŐ NEMZEDÉKEK JOGA 9 : 3 pp. 78-90. , 13 p. (2019)

SIMÓ, Ferenc Zoltán. Right to life in Hungary and in the EU: the ever-troublesome issue of abortion KÜLÖNLEGES BÁNÁSMÓD 2020 : 4 pp. 83-90. , 1 p. (2020)

SOLOVE, Daniel J.: *I've Got Nothing to Hide' and Other Misunderstandings of Privacy.*San Diego Law Review, Vol. 44, 2007. Available:https://ssrn.com/abstract=998565GWU Law School Public Law Research Paper, No. 289. Available: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications [accessed 7 Jan 2021]

SCHUBAUER Petra: A személyes adatok személyiségi jogi védelme, különös tekintettel a halál utáni védelem egyes kérdéseire – PhD értekezés, 2021 - https://ajk.kre.hu/images/doc2021/doktori/dr_Schubauer_Petra_PhD_2021_ (final.pdf). [accessed 11 Sept 2023]

SOLOVE, Daniel J: *Understanding Privacy*.Harvard University Press, London, 2008.

SÓLYOM László: *A személyiségi jogok elmélete.*Közgazdasági ég Jogi Kiadó, Budapest, 1983.

SOMA, John. T.– RYNERSON, Stephen D. – KITAEV, Erica: *Privacy Law in a nutshell*. West Academic Publishing, West, 2014.

Sommer, Robert: *Personal Space: The Behavioural Basis of Design*. Prentice-Hall, New Jersey.1969.

SOTALA, Kaj – YAMPOLSKIY, Roman V: *Responses to catastrophic AGI risk: a survey*.Physica Scripta, Vol. 90, No.1, 2014, 1-33. (Doi: 10.1088/0031-8949/90/1/018001) Available: https://iopscience.iop.org/article/10.1088/0031-8949/90/1/018001/pdf[accessed 19 Dec 2020]

SPIEKERMANN, Sarah and CRANOR, Lorrie Faith. *Engineering Privacy*. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS,*Transactions on Software Engineering*,. Volume 35. No. 1. 67 - 82. 10.1109/TSE.2008.88. 2009.

STAHL, Bernd Carsten – WRIGHT, David: *Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation.* IEEESecurity and Privacy, May/June 2018, Vol. 16, Iss. 3, 26-33. (Doi: 10.1109/MSP.2018.2701164) Available: https://ieeexplore.ieee.org/document/8395078[accessed 21 Dec 2020]

STAPLES, William G: *Encyclopedia of privacy*.Greenwood Press, London, 2007.

STEG, Linda – DE GROOT, Judit I. M.:*Environmental Psychology:An introduction*. John Wiley & Sons Ltd, Chichester, West Sussex, 2019.(Doi:10.1002/9781119241072)Available:http://www.wiley.com/go/permissions[accessed 7 Oct 2020]

STRANDBURG, Katherine – STAN RAICU, Daniela (eds.):*Privacy and Technologies of Identity – A Cross-Disciplinary Conversation*. Springer, New York, 2006. (Doi: https://doi.org/10.1007/0-387-28222-X)

https://link.springer.com/content/pdf/10.1007%2F0-387-28222-X.pdf [accessed 10 Sep 2019]

STUART, Casey-Maslen:*Pandora's box? Drone strikes under jus ad bellum, jus in bello, and international human rights law*. International Review of the Red Cross, Vol. 94 No. 886 Summer, 2012, 597 – 625 (https://doi.org/10.1017/S1816383113000118).Available: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/D9D63CB248435F211105B052E3AB55EA/S1816383113000118a.pdf/pandoras_box_drone_strikes_under_jus_ad_bellum_jus_in_bello_and_international_human_rights_law.pdf[accessed 17 Oct 2019]

SUNDSTROM, Eric–TOWN, Jerri. P.– RICE, Robert. W. [et. al.]:*Office noise, satisfaction and performance*. Environment and Behavior, Vol. 26, Iss. 2, 1994, 195–222. (Doi: https://doi.org/10.1177/0013916594026002O4)

SWEENEY, Latanya:*k-anonymity: A model for protecting privacy*. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10, No. 05, 2002, 557–570 available: https://epic.org/privacy/reidentification/Sweeney_Article.pdf[accessed 17 Sep 2020]

SZABÓ, Endre Győző – BOJNÁR Katinka – BUZÁS Péter: *Új globális technológiák kihívásai a magyar jogban/Challeges created by Modern Technologies in Hungarian Law*. In: TÓTH András. (Ed.):*Technológia jog: új globális technológiák jogi kihívásai*. Patrócinium Kiadó, Budapest, 2016, 51-97. Available: http://www.kre.hu/ajk/images/doc/Uj_technologia_jog_kotet.pdf[accessed 10 Oct 2018]

SZABÓ Máté Dávid: *Kisérlet a privacy fogalmának meghatározására*. Információs társadalom, Vol. 5, No. 2, 2005, 44-54. Available: http://epa.niif.hu/01900/01963/00013/pdf/infotars_2005_05_02_044-054.pdf [accessed 30 Sep 2020]

SZÉKELY Iván: *Central and Eastern Europe: Starting from Scratch*. In: FLORINI, Ann (Ed.): *The Right to Know: Transparency for an Open World*. Columbia University Press, New York, 2007.

SZÉKELYIván:*Freedom of Information versus Privacy: Friends or Foes?* In: GUTWIRTH, Serge – POULLET, Yves – DE HERT, Paul – DE TERWANGNE, Cécile – NOUWT, Sjaak (Eds.): *Reinventing Data Protection?* Springer, Dordrecht, London, 2009.

TAYLOR, Mark:*Genetic data and the law – A critical perspective on privacy protection*. Cambridge University Press, Cambridge, 2012. (https://doi.org/10.1017/CBO9780511910128)

TÓTH, László: Tájékoztató a pilóta nélküli légijármű-rendszerek (UAS) frekvenciahasználatáról és engedélyezési kérdéseiről. Nemzeti Média- és Hírközlési Hatóság, 2018.https://nmhh.hu/dokumentum/193162/UAV_tajekoztato.pdf

TRAN, Alexander. H.:*The Internet of Things and Potential Remedies in Privacy Tort Law*. Columbia Journal of Law and Social Problems,Vol. 50, Iss. 2, Winter 2017, 263-298.Available: http://jlsp.law.columbia.edu/wp-content/uploads/sites/8/2017/03/50-Tran.pdf [accessed 7 Jan 2021]

VOIGT, Paul – VON DEM BUSSCHE, Axel: *The EU General Data Protection Regulation (GDPR):A Practical Guide*.Springer International Publishing AG, Cham, 2017. (Doi: 10.1007/978-3-319-57959-7)

VOLOKH, Eugene:*Tort Law vs, Privacy*. Columbia Law Review, Vol. 114, No. 4, 2014, Available: https://columbialawreview.org/wp-content/uploads/2016/04/May-2014-7-Article-Volokh.pdf[accessed 5 Jan 2021]

VOLOKH, Eugene– SCHWART, Paul M.: *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*. Stanford Law ReviewVol. 52, No. 5, 2000, 1049-1124. (Doi: https://doi.org/10.2307/1229510)

VOSS, W. Gregory: *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*. The Business Lawyer, Vol. 72, No. 1, Winter 2016–2017, 221-233. Available: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2894571_code1740804.pdf?abstractid=2894571&mirid=1 [accessed 11 Dec 2020]

VOSS, W. Gregory – CASTETS-RENARDCeline:*Proposal for an International Taxonomy on the Various Forms of the "Right to Be Forgotten": A Study on the Convergence of Norms*.

14 Colorado Technology Law Journal, Vol. 14, Iss. 2, 2016, 281-343. Available: https://ctlj.colorado.edu/wp-content/uploads/2016/06/v.3-final-Voss-and-Renard-5.24.16.pdf[accessed Dec 31 2020]

WACKS, Raymond: *Personal Information: Privacy and the Law*. Clarendon Press, Oxford, 1989.

WARREN, Samuel D.– BRANDEIS, Louis D.: *The Right to Privacy*. Harvard Law Review, Vol. 4, No. 5, 1890, 193-220. Available: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf[accessed 19 Apr 2019]

WIENER, Jonathan Baert: *Global environmental regulation: instrument choice in legal context*.The Yale Law Journal, Vol. 108, No. 4, Jan. 1999, 677-800. (Doi: https://doi.org/10.2307/797394)Available:https://core.ac.uk/download/pdf/62562074.pdf[accessed 27 Aug 2020]

WIENER, Jonathan B.:*The regulation of technology, and the technology of regulation*. Technology in Society, Vol. 26, Iss. 2-3, 2004, 483-500. (Doi: https://doi.org/10.1016/j.techsoc.2004.01.033) Available: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1960&context=faculty_scholarship[accessed 17 Aug 2020]

WIRTZ, Bernd W. – WEYERER, Jan C. – Geyer, Carolin: *Artificial Intelligence and the Public Sector—Applications and Challenges*. International Journal of Public Administration, Vol. 42, Iss. 7, 2019, 596-615. (DOI: 10.1080/01900692.2018.1498103) Available: https://www.tandfonline.com/doi/abs/10.1080/01900692.2018.1498103 [accessed 19 Dec 2020]

WISSKIRCHEN, Gerlind –BIACABE, Blandine Thibault – BORMANN, Ulrich, [et. al.]: *Artificial Intelligence and Robotics and Their Impact on the Workplace*. IBA Global Employment Institute, London, April 2017. Available: https://www.ebglaw.com/content/uploads/2017/05/Workshop-4-2017-AI-Workshop-Participant-Materials.pdf[accessed 11 Dec 2020]

WOODWARD,John D. Jr.:*The law and use of biometrics*. (Doi: https://doi.org/10.1007/978-0-387-71041-9_18) In: JAIN, Anil K. – FLYNN, Patrick – ROSS, Arun A. (Eds.): *Handbook of Biometrics*. Springer, New York, 2008.

WRIGHT, David – DE HERT, Paul (eds.):*Enforcing privacy – Regulatory, Legal and Technological Approaches*. Springer, New York, 2016. (Doi: https://doi.org/10.1007/978-3-319-25047-2) Available: https://link.springer.com/content/pdf/10.1007%2F978-3-319-25047-2.pdf [accessed 17 Oct 2019]

XUE, Hong: *Privacy and personal data protection in China: An update for the year end 2009*. Computer law and security Review, Vol. 26, Iss. 3, 2010, 284-289. (Doi: https://doi.org/10.1016/j.clsr.2010.01.004)Available:https://www2.cs.duke.edu/courses/common/compsci092/papers/china/xue.pdf [accessed 4 Jan 2021]

YAO-HUAI, Lü: *Privacy and Data Privacy Issues in Contemporary China*. Ethics and Information Technology, Vol. 7, No. 1, 2005, 7-15. (Doi: 10.1007/s10676-005-0456-y) Available: https://cdn.tc-library.org/Rhizr/Files/4367e301-0301-4e6f-b2d7-f6a54e794a83/042ef109-e363-4179-a284-4e5be354b67f.pdf [accessed 2 Jan 2021]

ZAVRSNIK, Aleš (Ed.): *Drones and Unmanned Aerial Systems Legal and Social Implications for Security and Surveillance*. Springer International Publishing, Switzerland, 2016.

ZETZSCHE, Dirk A. – BUCKLEY, Ross P. – BARBERIS, Janos N. [et. al.]: *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*. Fordham Journal ofCorporate and Financial Law Vol. 23, No. 1, 2017, 31-103. Available:https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1450&context=jcfl[accessed 4 Dec 2020]

ZETOONY, David: *California Consumer Privacy Act (CCPA) Practical Guide*. Bryan Cave Leighton Paisner, 2020. https://ccpa-info.com/wp-content/uploads/2019/09/bclp-practical-guide-to-the-ccpa.pdf[accessed 4 Jan 2021]

ZIMMER, Michael – Kinder-Kurlanda, Katharina:*Internet Research Ethics For The Social Age: New Challenges, Cases, And Contexts*. Peter Lang Media and Communication, New York, 2017.(Doi: https://doi.org/10.3726/b11077)

ZŐDI, Zsolt:*Characteristics of the European Platform Regulation Platform Law and User Protection.*Public Governance, Administration and Finances Law Review Vol. 7. No. 1. 2022.

ZŐDI, Zsolt: *Jog és Jogtudomány a Big Data korában*. Állam- és Jogtudomány, 2017/1. sz.

ZŐDI, Zsolt: *„Platformok, robotok, jog" Új szabályozási kihívások az információs társadalomban.* Budapest: Gondolat. 2018.

ZŐDI, Zsolt: *Law and Legal Science in the Age of Big Data*. INTERSECTIONS. EAST EUROPEAN JOURNAL OF SOCIETY AND POLITICS, 3 (2). 20

ZŐDI, Zsolt: *What Will Robot Laws Look Like? The Code of AI and Human Laws*.Acta Univ. Sapientiae, Legal Studies, 8, 2. 2019.

OTHER SOURCES:

ACTS AND REGULATIONS

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 - Unmanned Aircraft Systems and Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 - Unmanned Aircraft SystemsEasy Access Rules: Unmanned Aircraft Systems (Regulation (EU) 2019/947 and Regulation (EU) 2019/945)

https://www.easa.europa.eu/document-library/opinions/opinion-012018[Accessed 24 Jun] and https://www.easa.europa.eu/[Accessed 24 Jun 2020]

AMC & GM to Commission Implementing Regulation (EU) 2019-947 - Issue 1 Related ED Decision and ED Decision 2019/021/RExplanatory Note [pdf] Explanatory note to ED Decision 2019/021/Rhttps://www.easa.europa.eu/domains/civil-drones-rpas[Accessed 24 Jun 2020]

5 U.S.C. 552a Privacy Act of 1974 :https://www.law.cornell.edu/uscode/text/5/552a [accessed 15 Feb 2018]

Hessisches Datenschutzgesetz [HDSG] [Data Protection Act of the German Federal State of Hessen], Sept. 30 1970, v 7.10.1970 GVB1, Hesse I § 625 (Ger.).

Datalag (1973:289) [Data Act] (Swed.).https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN [accessed 9 Jan 2019] and https://www.schoenherr.eu/publications/publication-detail/amendments-to-the-hungarian-data-protection-act/ [accessed 9 Jan 2019]

Framework for Demonstrable GDPR Compliance: A mapping of the Nymity's Privacy Management Accountability Framework. Available:https://info.nymity.com/hubfs/Landing%20Pages/GDPR%20Toolkit/Accountability_Roadmap_for_Demonstrable_GDPR_Compliance.pdf [accessed 10 Sep 2020]

Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, available https://eur-

lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en [hereinafter *Data Protection Directive*] [accessed 19 Apr 2019]

The US. CONSTITUTION: FOURTH AMENDMENT https://www.law.cornell.edu/constitution/fourth_amendment [accessed 9 Sep 2020]

Convention Art.8; Charter Arts. 7,8. https://www.echr.coe.int/Documents/Convention_Eng.pdfand https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data [accessed 9 Sep 2020]

Corrigendum to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. and Art. 5. Principles for the processing of personal data. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016: http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE[accessed on 11 Dec 2020]

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML[accessed 11 Dec 2020]

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016: http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE [accessed on 11 Dec2020]

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016: http://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE [accessed on 11 Dec 2020]

www.datenschutzbeauftragter-info.de/eu-datenschutzgrundverordnung-das-sind-die-neuerungen [accessed 11 Dec 2020]

Council Directive 95/46, 1995 O.J. (L 281) 31 (EC)

Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons withRegard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU)

General Data Protection Regulation (EU) 2016/679 (GDPR) replacing Directive 95/46/EC (Data Protection Directive)

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679[accessed Dec 31 2020]

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN[accessed Dec 31 2020]

Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR),

In the European Union the requirement for DPAs to be independent: Article 16(2) of the Treaty on the Functioning of the EU (TFEU) and Article 8(3) of the EU Charter of Fundamental Rights. Available:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN [accessed 4 Jan 2021]

DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL *of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)*https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32006L0042&from=HU [accessed 2 Sep 2020]

Article 6(3) TEU states

Act of V on the Civil Code/Polgári törvénykönyvről. 2013.évi. V. törvény. 2:43. §

Act CXLL of 2011 on exercising autonomy and the freedom of information;

Act V of 2013 on the Civil Code

Act C of 2012 on the Criminal Code

Act LXVI of 1995 on Public Records, Public Archives, and the Protection of Private Archives,

Act C of 2003 on electronic infocommunication,

Act of V on the Civil Code/Polgári törvénykönyvről. 2013.évi. V. törvény. 2:43. §

Act CXXX of 2016 on the Code of Civil Procedure (as in force on 1 July 2018)

WORKING PAPERS AND PROPOSALS/REPORTS:

ARMSTRONG, Harry –RAE, Jen: *A working model for anticipatory regulation*. A working paper,Nov. 2017. Available: https://www.nesta.org.uk/report/a-working-model-for-anticipatory-regulation-a-working-paper/[accessed 27 Aug 2020]

BENTHAM, Jeremy: *Panopticon or the Inspection House*. Letter V (1787), *available:*https://cryptome.org/cartome/panopticon2.htm [accessed 19 Apr 2019]

European Data Protection Supervisor– Annual Report 2015. Publications Office of the European Union, Luxembourg, 2016. Available:https://data.europa.eu/euodp/hu/data/dataset/european-data-protection-supervisor-annual-report-2015[accessed 27 Aug 2020]

HAYLEN, Andrew – BUTCHER, Loise: *Civilian drones*. Briefing Paper Number CBP 7734.

http://researchbriefings.files.parliament.uk/documents/CBP-7734/CBP-7734.pdf [accessed 9 Jan 2019]

Calcutt Report. Available: https://api.parliament.uk/historic-hansard/commons/1990/jun/21/calcutt-report [accessed 5 Jan 2021]

Transatlantic Data Flows: Restoring Trust Through Strong Safeguards, COM (2016) 117 final (Feb. 29,2016) Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0117&from=EN [accessed Dec 31 2020]

European Parliament, Committee on Legal Affairs drafted its first report with recommendations to the Commission on Civil Law Rules on Robotics on 27 January 2017 (2015/2103(INL)).www.robolaw.eu. [accessed 26 Aug 2020]

The first COM proposal of the GDPR (2016/679) was published on 25 January 2012, it entered into force on 24 May 2016 and became directly applicable in all EU Member States on 25 May 2018.https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN[accessed 26 Aug 2020]

Communication from the Commission too the European Parliament, The European Council, the Council, The European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe Brussels, 25.4.2018 COM(2018)237 finalhttps://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN [accessed 19 Dec 2020]

Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics. European Commission, Directorate-General for Justice, Brussels, 2020.https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0064&from=en [accessed 19 Dec 2020] and https://gdpr-info.eu/[accessed 19 Dec 2020]

"Privacy Impact Assessment (PIA) Good Practice," CNIL, 2015. Available: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf[accessed 19 Dec 2020]

Privacy by Design Strong Privacy Protection – Now, and Well into the Future A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners. Information Commissioner's Office,2008https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf[accessed 21 Dec 2020]

AI for Europe, COM/2018/237 final.

https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF[accessed 2 Sep 2020]

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.COM(2020) 66 finalhttps://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf[accessed 2 Sep 2020]

White Paper: On Artificial Intelligence - A European approach to excellence and trust. available: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf[accessed 2 Sept 2020] and https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en [accessed 15 Sept 2023]

Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273 [accessed 2 Sep 2020]

Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL))https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.pdf [accessed 29 Dec 2020]

DESILVER, Drew: *Chart of the Week: The Ever-Accelerating Rate of Technology Adoption*. Pew Research Center report, 2014. available: https://www.pewresearch.org/fact-tank/2014/03/14/chart-of-the-week-the-ever-accelerating-rate-of-technology-adoption/ [accessed 3 Sep 2020]

DEFENSE INNOVATION BOARD, https://innovation.defense.gov/and PELLERIN, Cheryl:*Defense Innovation Board Makes Interim Recommendations*, DEPARTMENT OF DEFENSE NEWS (Oct. 5, 2016), https://dod.defense.gov/News/Article/Article/965196/defense-innovation-board-makes-interimrecommendations/.

Ten Commandments of Software, DEFENSE INNOVATION BOARD (April 20, 2018), https://media.defense.gov/2018/Apr/22/2001906836/-1/-1/0/DEFENSEINNOVATIONBOARD_TEN_COMMANDMENTS_OF_SOFTWARE_2018.04.20.PDF [accessed 2 Sep 2020]

ICAO Circular 328-AN/190.

Council of the European Union. Towards a European Strategy for the development of civil applications of Remotely Piloted Aircraft Systems external (RPAS), Working Paper (13438/12), September 6, 2012.Council of the European Union.

https://www.ainonline.com/aviation-news/aerospace/2015-01-06/icao-panel-will-recommend-first-uav-standards-2018 [accessed 25 Mar 2019]

Notice of Proposed Rulemaking: Operation and Certification of Small Unmanned AircraftSystems, 80 Fed. Reg. 9544, 9549 (proposed Feb. 23, 2015) [*NPRM*]. https://www.federalregister.gov/documents/2019/02/13/2019-00758/safe-and-secure-operations-of-small-unmanned-aircraft-systems [accessed 25 Mar 2019]

Notice of Proposed Rulemaking: Operation and Certification of Small Unmanned AircraftSystems, 80 Fed. Reg. 9544, 9549 (proposed Feb. 23, 2015) [*NPRM*]. available:https://www.federalregister.gov/documents/2019/02/13/2019-00758/safe-and-secure-operations-of-small-unmanned-aircraft-systems [accessed 25 Mar 2019]

European Parliamentary Research Service, Civil drones in the European Union, October 2015:http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571305/EPRS_BRI(2015)571305_EN.pdf [accessed 25 Mar 2019]

European RPAS Steering Group, Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System, June 2013:http://ec.europa.eu/DocsRoom/documents/10484/attachments/1/translations/ [accessed 25 Mar 2019]

US state department reports in its *2018 Human Rights Report*https://www.state.gov/documents/organization/289381.pdf[accessed Apr 10 2019]

House of Lords European Union Committee, Civilian Use of Drones in the EU (Seventh Report of Session 2014-15), HL Paper 122, 5 March 2015, Table 1, p.12

SORA (Specific Operations Risk Assessment) https://www.eurocockpit.be/positions-publications/specific-operations-risk-assessment-sora[Accessed 24 Jun 2020]

ADMINISTRATIVE GUIDEBOOKS/GUIDES:

National Academies of Sciences, Engineering, and Medicine. *Proposed AASHTO Practice and Tests for Process Control and Product Acceptance of Asphalt-Treated Cold Recycled Pavements*. The NationalAcademies Press, Washington DC, 2020(https://doi.org/10.17226/25971).

National Academies of Sciences, Engineering, and Medicine. Life-Cycle Decisions for Biomedical Data: The Challenge of Forecasting Costs. Washington, DC: The National Academies Press. (2020) (Doi: https://doi.org/10.17226/25639).

National Academies of Sciences, Engineering, and Medicine. Airports and Unmanned Aircraft Systems, Volume 1: Managing and Engaging Stakeholders on UAS in the Vicinity of Airports. Washington, DC: The National Academies Press. (2020) (Doi: https://doi.org/10.17226/25599).

National Academies of Sciences, Engineering, and Medicine. Airports and Unmanned Aircraft Systems, Volume 2: Incorporating UAS into Airport Infrastructure Planning Guidebook. Washington, DC: The National Academies Press.(2020) (Doi: https://doi.org/10.17226/25606).

National Academies of Sciences, Engineering, and Medicine. Airports and Unmanned Aircraft Systems, Volume 3: Potential Use of UAS by Airport Operators. Washington, DC: The National Academies Press. (2020) (Doi: https://doi.org/10.17226/25607).

https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_107-2.pdf [accessed 25 Mar 2019]

National Academies of Sciences, Engineering, and Medicine. Evolving Law on Airport Implications by Unmanned Aerial Systems. The National Academies Press, Washington DC, 2017, 40-41 Available: https://doi.org/10.17226/24932[accessed 5 Nov 2020]

Handbook on European non-discrimination law. 2018:https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf [accessed 10 Sep 2020]

Evaluating Data Types: A Guide for Decision Makers using Data to Understand the Extent and Spread of COVID-19.The National Academies Press, Washington DC, 2020. (Doi: https://doi.org/10.17226/25826) Available: https://www.nap.edu/catalog/25826/evaluating-data-types-a-guide-for-decision-makers-using-data[accessed 4 Jan 2021]

Maintaining American Leadership in Artificial Intelligence. Federal Register, Vol. 84, No. 31, 2019, 3967-3972.https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf[accessed 2 Sep 2020]

EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. Available: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf [accessed 9 Sep 2020]

Privacy & biometrics building a conceptual foundation. NSTC, Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics. Tech rep, September 2006. Available: https://www.hsdl.org/?view&did=463913[accessed 10 Sep 2020]

Marini Alice, Alexis Kateifides and Joel Bates (DataGuidance) and Gabriela Zanfir-Fortuna, Michelle Bae, Stacey Gray and Gargi Sen (Future of Privacy Forum): Comparing privacy laws: GDPR v. CCPA 2019https://www.naih.hu/general-information.html [accessed in 9 Nov 2018]

OECD Guidelines governing the protection of privacy and transborder flows of personal data (July 2013)https://edps.europa.eu/sites/edp/files/publication/2013-09-09_oecd-privacy-guidelines_en.pdf[accessed 4 Jan 2021]

OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007)https://edps.europa.eu/sites/edp/files/publication/2013-09-09_oecd_guidelines_en.pdf[accessed 4 Jan 2021]

TECHNICAL GUIDANCE ON RISK ASSESESMENT : DIRECTIVE 9367 EEC https://www.researchgate.net/publication/286208518_Technical_guidance_document_on_risk_assessment_in_support_of_commission_directive_9367EEC_on_risk_assessment_for_new_notified_substances_and_commission_regulation_EC_No148894_on_risk_assessment_for_ex [accessed 3 Sep 2020]

Law Library of Congress (U.S.). Global Legal Research Directorate, issuing body. *Regulation of artificial intelligence in selected jurisdictions*. LCCN 2019668143 Available: https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf[accessed 19 Dec 2020]

Available: https://www.pewresearch.org/internet/2018/12/10/solutions-to-address-ais-anticipated-negative-impacts/ [accessed 19 Dec 2020]

Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence:https://ec.europa.eu/digital-single-market/en/artificial-intelligence[accessed 19 Dec 2020]

ICAO. (2011). Unmanned Aircraft Systems (UAS), Cir. 328, Glossary. Retrieved from

https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf [accessed 25 Mar 2019]

CASE STUDIES AND CASES:

Lord HOFFMANN, *Wainwright v Home Office* [2004] 2 AC 406, at [31]

LEENDERS, Gijs: *The Regulation of Artificial Intelligence — A Case Study of the Partnership on AI.*https://becominghuman.ai/the-regulation-of-artificial-intelligence-a-case-study-of-the-partnership-on-ai-c1c22526c19f [accessed 4 Dec 2020]

Entick v. Carrington(1765) 19 St Tr 1029

Katz v. U.S., 389 U.S. 347 (1967).

https://www.law.cornell.edu/supremecourt/text/389/347 [accessed 9 Sep 2020]

Kyllo v. United States, 533 U.S. 27 (2001) and Carpenter v. United States, No. 16-402, 585 U.S. (2018) Available: https://supreme.justia.com/cases/federal/us/585/16-402/case.pdf [accessed 9 Sep 2020]

Case C-362/14, Schrems v. Data Prot. Comm'r (Oct. 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362 [accessed Dec 31 2020]

Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccio´n de Datos (AEPD), 2014 E.C.R. 317, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131. [accessed Dec 31 2020]

Judgment of 24 September 2019, *Google Inc v Commision nationale de l'informatique et des libertés* (CNIL), C-507/17, paragraph 64 Available:

http://curia.europa.eu/juris/document/document.jsf?docid=218105&doclang=EN [accessed 1 Jan 2021]

ECJ judgment rendered on 6 October 2016 – C-362/14. Available: http://curia.europa.eu/juris/liste.jsf?num=C-362/14[accessed 11 Dec 2020]

Case -T164/09: Available: https://op.europa.eu/hu/publication-detail/-/publication/9fad0b67-d1f7-4fdf-8d15-8317c960d285/language-en [accessed 4 Jan 2021]

T-237/16 Available: https://op.europa.eu/hu/publication-detail/-/publication/91677a28-a4c1-11e6-8401-01aa75ed71a1/language-en [accessed 4 Jan 2021]

Hiibel v. Sixth Judicial District Court. Supreme Court's 2004 decision Full text of the case available:https://www.lexisnexis.com/community/casebrief/p/casebrief-hiibel-v-sixth-judicial-dist-court [accessed 16 Sep 2020].

KYLLO v. UNITED STATESCERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUITNo. 99-8508. Argued February 20, 200l-Decided June 11,2001. Available: https://supreme.justia.com/cases/federal/us/533/27/ [accessed 16 Sep 2020].

476 U.S., at 215.https://supreme.justia.com/cases/federal/us/476/207/ [accessed 16 Sep 2020] and https://supreme.justia.com/cases/federal/us/476/207/ [accessed 16 Sep 2020].

Huerta v. Pirker, CP-217, Board's Decisional Order No. EA-5730 (Nat'l Transp. Safety Bd. Decisions (N.T.S.B.) Nov. 18, 2014), available athttp://www.ntsb.gov/legal/alj/OnODocuments/Aviation/5730.pdf [accessed 25 Mar 2019]

NET SOURCES:

DREYFUSS, Joel: *EU privacy rules may hit Internet giants hard*. Available: https://www.cnbc.com/2016/02/01/eu-privacy-rules-may-hit-internet-giants-hard.html[accessed 26 Aug 2020]

GRÜLL, Philipp: *Germany's plans for automatic facial recognition meet fierce criticism*. https://www.euractiv.com/section/data-protection/news/german-ministers-plan-to-expand-automatic-facial-recognition-meets-fierce-criticism/ [accessed 2 Sep 2020]

STÖCKER, Christian:*Google's gracious controllers.* Available: www.spiegel.de/netzwelt/netzpolitik/datenschutz-in-den-usa-und-europa-a-849114.html[accessed 1 Jan 2021]

Tara Evans, Neighbors Complain of Drones Flying over Winter Park Back Yards, WKMG Orlando, (May 7, 2015), https://www.clickorlando.com/news/2015/05/07/neighbors-complain-of-drones-flying-over-winter-park-back-yards/ [accessed 5 Nov 2020]

https://edri.org/our-work/edrigramnumber10-22facebook-doesnt-like-eu-regulation/[accessed 26 Aug 2020]

https://www.snia.org/sites/default/files/Hibbard_DSI_2015_Privacy-vs-Data-Protection-v2-revision.pdf[accessed 7 Oct 2020]

https://www.research.uci.edu/compliance/human-research-protections/researchers/privacy-and-confidentiality.html[accessed 7 Oct 2020]

https://criminal.findlaw.com/criminal-rights/is-there-a-difference-between-confidentiality-and-privacy.html[accessed 7 Oct 2020]

https://edps.europa.eu/data-protection/data-protection_en#Privacy[accessed 7 Oct 2020]

https://www.certpro.in/hipaa-compliance-certification/?gclid=CjwKCAjw0On8BRAgEiwAincsHCAV_y4fZ3see-w9aoJndw83vZtvkkerxzPZ-nxSsd_mZv5jtrqCThoCCG0QAvD_BwE[accessed 7 Oct 2020]

https://www.certpro.in/hipaa-compliancecertification/?gclid=CjwKCAjw0On8BRAgEiwAincsHCAV_y4fZ3see-w9aoJndw83vZtvkkerxzPZ-nxSsd_mZv5jtrqCThoCCG0QAvD_BwE[accessed 7 Oct 2020]

https://www.research.uci.edu/compliance/human-research-protections/researchers/privacy-and-confidentiality.html[accessed 7 Oct 2020]

https://www.psychceu.com/ethics/psychgoodtherapy_index.asp[accessed 7 Oct 2020]

https://www.psychceu.com/ethics/psychgoodtherapy_index.asp[accessed 7 Oct 2020]

https://www.pszich.u-szeged.hu/etika/fogadalom-szovegek/?lang=eng[accessed 7 Oct 2020]

https://data.europa.eu/euodp/hu/data/dataset/european-data-protection-supervisor-annual-report-2015[accessed 1 Sep 2020]

https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf[accessed 1 Sep 2020]

https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [accessed 17 Aug 2020]

www.anwalt.de/rechtstipps/uebersicht-zum-arbeitsrecht-in-japan_056517.html [accessed 11 Dec 2020]

https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf [accessed 1 Jan 2021]

https://wizelife.de/themen/wissen/24986/auf-einen-blick-deutscher-und-us-datenschutz-im-vergleich and https://wizelife.de/themen/wissen/24986/auf-einen-blick-deutscher-und-us-datenschutz-im-vergleich [accessed 31 Dec 2020]

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en[accessed 31 Dec 2020]

https://ec.europa.eu/info/sites/info/files/factsheet_eu-us_privacy_shield_en.pdf[accessed 31 Dec 2020]

http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_euus_privacy_shield_en.pdf and

https://www.ftc.gov/system/files/documents/plain-language/annexes_eu-us_privacy_shield_en1.pdf [accessed 31 Dec 2020]

European Commission: EU-U.S. Privacy Shield: stronger protection for transatlantic data flows. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461 or

http://europa.eu/rapid/press-release_IP-16-2461_de.htm[accessed 31 Dec 2020]

www.heise.de/newsticker/meldung/Privacy-Shield-EU-Kommission-veroeffentlicht-Text-fuer-loechrigen- Datenschutzschild-3120502.html

https://www.heise.de/news/EU-Kommission-verhandelt-zu-neuem-Privacy-Shield-4876922.html [accessed 1 Jan 2021]

http://europa.eu/rapid/press-release_IP-16-2461_de.htm [accessed 31 Dec 2020]

EU-U.S. Privacy Shield Framework Principles: the U.S. Department of Commerce Available:https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg[accessed 31 Dec 2020]

https://www.naih.hu/act-cxii-of-2011---privacy-act--.html [accessed 4 Jan 2021]

https://eur-lex.europa.eu/eli/reg/2016/679/oj [accessed 4 Jan 2021]

https://www.securetrust.com/data-privacy-and-the-california-consumer-privacy-act/?gclid=EAIaIQobChMIjbnVxJ-C7gIVBSgYCh2fsgTREAAYAiAAEgJDy_D_BwE

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [accessed 4 Jan 2021]

https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf [accessed 3 Jan 2021]

https://edps.europa.eu/press-publications/press-news/news#news_5895[accessed 3 Jan 2021]

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=EN [accessed 4 Jan 2021]

http://curia.europa.eu/juris/document/document.jsf?docid=57549&doclang=en [accessed 4 Jan 2021]

https://www.britannica.com/technology/history-of-technology/The-20th-century#ref14881[accessed 23 Jul 2020]

https://www.legislation.gov.uk/uksro/1931/344/pdfs/uksro_19310344_en.pdf[accessed 23 Jul 2020]

https://www.tbilaw.co.uk/site/asbestos-injuryclaims/?gclid=CjwKCAjwm_P5BRAhEiwAwRzSO36v80oozddEEv6yI7t2bFGwJxhNn1HnKjo7GaE-g1OAF3xIewN4ABoC4ycQAvD_BwE

https://www.stephensons.co.uk/site/news_and_events/archivenews/asbestos_legal_risks

https://www.slatergordon.co.uk/personal-injury-claim/industrial-disease/asbestos-mesothelioma/asbestos-regulations/

https://uk.practicallaw.thomsonreuters.com/01029187?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 [accessed 9 Aug 2020]

https://uk.practicallaw.thomsonreuters.com/01029187?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 [accessed 9 Aug 2020]

https://www.thoughtco.com/search?q=history+of+regulation [accessed 23 Jul 2020]

https://www.britannica.com/technology/history-of-technology/The-20th-century#ref14881 [accessed 23 Jul 2020]

https://www.britannica.com/technology/history-of-technology/The-technological-dilemma [accessed 23 Jul 2020]

https://lobbyplag.eu/map/amendments/libe/ [accessed 26 Aug 2020]

https://edps.europa.eu/about-edps_en [accessed 4 Jan 2021]

https://www.federalregister.gov/documents/2019/02/13/2019-00758/safe-and-secure-operations-of-small-unmanned-aircraft-systems [accessed 25 Mar 2019]

https://www.uavsystemsinternational.com/drone-laws-by-country/hungary drone-laws/ [accessed 1 Nov 2018]

https://ec.europa.eu/commission/presscorner/detail/en/IP_14_384 [accessed 23 Jan 2019]

https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_14_110 [accessed 25 Jan 2019]

https://www.easa.europa.eu/domains/civil-drones-rpas[accessed 25 Mar 2019]

http://ec.europa.eu/DocsRoom/documents/10484/attachments/1/translations/[accessed 25 Mar 2019]

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31993L0067 [accessed 3 Sep 2020]

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31994R1488 [accessed 3 Sep 2020]

https://echa.europa.eu/documents/10162/16960216/tgdpart2_2ed_en.pdf[accessed 3 Sep 2020]

https://www.epa.gov/fera/nrc-risk-assessment-paradigm[accessed 30 September 2020]

https://onlinelaw.wustl.edu/blog/case-study-am-records-inc-v-napster-inc/[accessed 10 Oct 2018]

https://law.justia.com/cases/federal/district-courts/FSupp/545/812/1432138/[accessed 10 Oct 2018]

How Countries Are Regulating Internet Content: https://web.archive.org/web/20160103124414/https://www.isoc.org/inet97/proceedings/B1/B1_3.HTM

https://iccwbo.org/publication/the-impact-of-internet-content-regulation/[accessed 10 Oct 2018]

http://wirtschaftslexikon.gabler.de/Archiv/74650/kuenstliche-intelligenz-ki-v12.html [accessed:19 Dec 2020]

https://www.machinedesign.com/markets/robotics/article/21835139/whats-the-difference-between-weak-and-strong-ai

https://www.internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learning-policy-paper/?gclid=Cj0KCQiA5vb [accessed 19 Dec 2020] https://www.eurai.org/%20/[accessed 19 Dec 2020]

https://gdpr-info.eu/[accessed 19 Dec 2020]

https://www.whitehouse.gov/ai/ [accessed 2 Sep 2020]

https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/available: https://www.whitehouse.gov/ai/[accessed 2 Sep 2020]

https://www.faa.gov/uas/publications/model_aircraft_ operators/ [accessed 23 Mar 2019]

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2385448 [accessed 25 Mar 2019]

http://www.academia.edu/11845032/Privacy_law_implications_of_the_use_of_drones_for_security_and_justice_purposes [accessed 24 Mar 2019]

http://www.auvsi.org/auvsiresources/economicreport [accessed 25 Mar 2019]

Press Release, FED. AVIATION ADMIN., FAA Announces Small UAS Registration Rule (Dec. 14, 2015) https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856 [accessed 25 Mar 2019]

https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19856 [accessed 24 Mar 2019]

http://www.content/501388/drones-maysoon-used-organ.html [accessed 25 Mar 2019]

http://www.businessinsider.in/The-fire-in-Alberta-doubledin-size-on-Saturday-and-firefighters-are-using-drones-to-fightit/articleshow/52170421.cms [accessed 25 Mar 2019]

https://www.businessinsider.in/Now-a-drone-that-detects-LPG-gas-leak-and-delivers-emergency-medical-kits/articleshow/48467531.cms [accessed 26 Mar 2019]

https://www.foxnews.com/us/federal-report-says-border-patrols-drone-program-doesnt-fly [accessed 25 Mar 2019]

https://www.faa.gov/data_research/aviation/aerospace_forecasts/ FED. AVIATION ADMIN. FAA AEROSPACE FORECAST 31 (2016). [accessed 22 Mar 2019]

https://harvardlawreview.org/2013/05/the-dangers-of-surveillance/ [accessed 25 Mar 2019]

https://www.eff.org/deeplinks/2012/01/drones-are-watching-you [accessed 25 Mar 2019]

https://www.eff.org/issues/surveillance-drones [accessed 26 Mar 2019]

http://www.dbta.com/Editorial/Trends-and-Applications/What-is-Data-Analysis-and-Data-Mining-73503.aspx [accessed 25 Mar 2019]

https://uavcoach.com/drone-laws-in-united-states-of-america/ [accessed 25 Mar 2019]

https://uavcoach.com/drone-laws-in-united-states-of-america/ [accessed 25 Mar 2019]

http://www.govtech.com/public-safety/Drone-Sales-Could-Reach-7-Million-by-2020-FAA-Says.html [accessed 25 Mar 2019]

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2357657 [accessed 25 Mar 2019]

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2357657 [accessed 25 Mar 2019]

https://www.nolo.com/legal-encyclopedia/what-do-when-your-neighbor-has-drone.html[accessed 5 Nov 2020]

https://www.faa.gov/search/?omni=MainSearch&q=drone[accessed 5 Nov 2020]

https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx [accessed 5 Nov 2020]

http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0900-0999/0934/Sections/0934.50.html [accessed 5 Nov 2020]

https://law.justia.com/codes/arkansas/2015/title-5/subtitle-6/chapter-60/subchapter-1/section-5-60-103/[accessed 5 Nov 2020]

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1708.8.&lawCode=CIV[accessed 5 Nov 2020]

https://www.leg.state.nv.us/NRS/NRS-193.html#NRS193Sec130[accessed 5 Nov 2020]

https://www.flsenate.gov/Laws/Statutes/2013/934.50[accessed 5 Nov 2020]

https://casetext.com/statute/florida-statutes/title-xlvii-criminal-procedure-and-corrections/chapter-934-security-of-communications-surveillance/section-93450-searches-and-seizure-using-a-drone/analysis?PHONE_NUMBER_GROUP=C&citingPage=1&sort=relevance[accessed 5 Nov 2020]

https://law.justia.com/codes/mississippi/2013/title-97/chapter-29/in-general/section-97-29-61/[accessed 5 Nov 2020]

https://law.lis.virginia.gov/vacode/title19.2/chapter5/section19.2-60.1/[accessed 5 Nov 2020]

http://europa.eu/rapid/press-release_IP-14-384_en.htm [accessed 23 Jan 2019] and

http://europa.eu/rapid/press-release_STATEMENT-14-110_en.htm [accessed 25 Jan 2019]

https://www.easa.europa.eu/easa-and-you/civil-drones-rpas [accessed 25 Mar 2019]

http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/519221/IPOL_IDA(2015)519221_EN.pdf [accessed 25 Mar 2019]

http://europa.eu/rapid/press-release_IP-14-384_en.htm

http://europa.eu/rapid/press-release_STATEMENT-14-110_en.htm [accessed 19 Apr 2019]

http://europa.eu/rapid/press-release_IP-14-384_en.htm

http://europa.eu/rapid/press release_STATEMENT-14-110_en.htm [accessed 19 Apr 2019]

http://europa.eu/rapid/press-release_IP-14-384_en.htm

http://europa.eu/rapid/press release_STATEMENT-14-110_en.htm [accessed 19 Apr 2019]

http://europa.eu/rapid/press-release_IP-14-384_en.htm&http://europa.eu/rapid/press release_STATEMENT-14-110_en.htm [accessed 19 Apr 2019]

Civil Aviation Authority (CAA) Flying Drones - Guidance on the safety rules https://register-drones.caa.co.uk/drone-code/flying-safely-and-responsibly

[accessed 22 Feb 2018]

Statewatch, *Back from the Battlefield – Domestic Drones in the UK*, May 2014 https://www.caa.co.uk/Consumers/Unmanned-aircraft-and-drones/ [accessed 22 Feb 2018]

CAA, Approved SUA operators, as at 17 February 2017 https://uavcoach.com/drone-laws-in-italy/ [accessed 31 Oct 2018]

https://www.uavsystemsinternational.com/drone-laws-by-country/italy-drone-laws/ [accessed 31 Oct 2018]

https://www.uavsystemsinternational.com/drone-laws-by-country/italy-drone-laws/ [accessed 31 Oct 2018]

https://www.uavsystemsinternational.com/drone-laws-by-country/hungary-drone-laws/ [accessed 1 Nov 2018]

http://www.cms-lawnow.com/ealerts/2017/02/hungary-new-drone-regulations[accessed 1 Nov 2018]

https://www.uavsystemsinternational.com/drone-laws-by-country/hungary-drone-laws/ [accessed 1 Nov 2018]

https://www.uavsystemsinternational.com/drone-laws-by-country/hungary-drone-laws/[accessed 1 Nov 2018]

https://dronerules.eu/en/professional/eu_regulations_updates [Accessed 24 Jun 2020]

https://eur-lex.europa.eu/legal

content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN [accessed 9 Jan 2019].

https://lawshelf.com/shortvideoscontentview/the-torts-of-invasion-of-privacy/ or https://www.stimmel-law.com/en/articles/legal-right-privacy [accessed 5 Jan 2021]

https://criminal.findlaw.com/criminal-rights/is-there-a-difference-between-confidentiality-and-privacy.htmland https://injury.findlaw.com/torts-and-personal-injuries/invasion-of-privacy.html[accessed 6 Jan 2021]

California's "Peeping Tom" Laws. https://www.shouselaw.com/ca/defense/laws/peeping-tom-laws/

https://www.law.cornell.edu/constitution/fourth_amendment[accessed 6 Jan 2021]

https://www.oyez.org/cases/1967/35[accessed 6 Jan 2021]

https://www.law.cornell.edu/wex/first_amendment [accessed 6 Jan 2021]

https://criminal.findlaw.com/criminal-rights/is-there-a-difference-between-confidentiality-and-privacy.html and https://injury.findlaw.com/torts-and-personal-injuries/invasion-of-privacy.html [accessed 6 Jan 2021]