Global Campus Europe

UNIVERSITY OF GRAZ

European Master's Programme in Human Rights and Democratisation

A.Y. 2020/2021

FROM PASTORAL NOMADS TO GLOBAL CITIZENS

The Development of Privacy and Data Protection in Mongolia
Lessons from the European Acquis

Author: Oyundari Batmunkh

Supervisor: Gerd Oberleitner

Gregor Fischer

ABSTRACT

The right to privacy is a fundamental human right that is protected in a majority of constitutions worldwide as well as a number of international human rights instruments in addition to national legislations. The right per se demonstrates the premise of human freedom and dignity which is an integral value in democratic society. The violation of the said right might range from the state's intrusion upon private life, arbitrary or unlawful interference by private entities, to the disclosure of private information by an individual without the owner's consent and so forth. The violation of these rights leads to severe consequences. Furthermore, the emergence of the information and communication technology and the rapid evolution of the Internet has changed the traditional concept of privacy. Mass processing of personal data on the Internet poses a serious threat to the right to privacy. The correlation between the right to privacy and data protection has long been debated among scholars, however it is incomplete to explain the right to privacy without also touching upon the concept of data protection. This paper examines the privacy and data protection legislations in Mongolia, a young democratic country landlocked between two big powers, in accordance with historic and cultural aspects. On the same note, it researches the European legislation practice, which claimed to be the global standard setter in the field.

TABLE OF ABBREVIATIONS

BC	Before Christ
CCTV	Closed-Circuit Television
CITA	Communications and Information Technology Authority
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DMA	Digital Markets Act
DPA	Data Protection Authorities
DPB	Data Protection Board
DPD	Data Protection Directive
DSA	Digital Services Act
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EEA	European Economic Area States
EU	European Union
EUCFR	European Union Charter of Fundamental Rights
GDPR	General Data Protection Regulation
HIV	Human Immunodeficiency Viruses
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICT	Information and Communication Technology
ID	Identity Document

IP	Internet Protocol
IQ	Intelligence Quotient
NGO	Non-Governmental Organization
SA	Supervisory Authorities
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
USD	United States Dollar
VAT	Value Added Tax
WHO	World Health Organization
WWW	World Wide Web

TABLE OF CONTENTS

1.INTRODUCTION

1.1 Background

In the 13th century, the Great Mongolian empire under the rule of Genghis Khan conquered almost half of the world. The abrupt conquest that took place much of the world had a significant impact on that century's political, cultural, economic, mercantile, and spiritual environment as the forces of globalization are having on the world today.[1] Genghis Khan is claimed to be not only a conqueror but also a world unifier and the success of establishing the contagious precedent of amassing a land empire in world history is described from various perspectives. The Mongols were the last over many centuries of successive nomadic invaders of the sedentary world.[2] As such, still even today one third of Mongolia's population live in a traditional nomadic way of life as nomadic herders[3]. The flocks of animals are integral to nomads' lives and it has been presented to highly distinguished guests as a symbol of respect for centuries. Taking a recent example amid the global pandemic, the President of Mongolia donated 30,000 sheep as humanitarian assistance to China after the pandemic had started in Wuhan as a symbol of good neighbor policy.[4] Therefore, the livestock animals play a significant role not only to nomads but also to the state diplomacy even until today. Nomadic herders have lived in tribes across the wide steppe grazing their livestock in the lush grassland by moving their household from one place to another. The main dwelling is a round shaped, "the earth reminiscent" white tent called a "yurt" which stands as part of Mongolian identity. The portable yurt is easily assembled and considered to be resistant in harsh and unpredictable climates. Inside, all family members would fit and live in it collectively without any separation of rooms.

Accordingly, the word privacy per se didn't prevail and practice contextually until the democratic revolution in the 1990s, whereas the context had already been introduced and the

---

[1] George Lane, *Genghis Khan and Mongol Rule* (Greenwood Publishing Group 2004).

[2] Joseph Fletcher, 'The Mongols: Ecological and Social Perspectives' (1986) 46 Harvard Journal of Asiatic Studies 11 <https://www.jstor.org/stable/2719074?seq=1#metadata_info_tab_contents>.

[3] Sharon Hudgins, 'Tsatsal' (2014) 36 Mongolian Studies 41 <https://www.jstor.org/stable/26865343>.

[4] Jennifer Rigby Sarah Newey, 'Warrior Spirit and Sheep Diplomacy: How Mongolia Is Sprinting Ahead in Vaccine Race' (*The telegraph*) <https://www.telegraph.co.uk/global-health/science-and-disease/warrior-spirit-sheep-diplomacy-mongolia-sprinting-ahead-vaccine/> accessed 3 June 2021.

right was protected through legislation in the west long ago. Although due to democratization and globalization, three million Mongolians stepped into the world's trend quickly. Mongolians equally use newly released technological devices, access information and communicate with the world without major restrictions. On the same note, as the information and communication technologies (ICT) has evolved tremendously fast within the last two decades, keeping up the pace of responsible and legitimate application is a challenging task for such a recently transitioned country as Mongolia. According to statistics, two thirds of the population in Mongolia including children use the internet on a daily basis.[5]

The technological advancement and use of the internet are undeniably related with core fundamental rights inter alia the right to privacy and protection of personal data. Privacy is essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.[6] It protects an individual and a society against arbitrary and unjustified use of power by reducing what can be known and done to an individual and a society, while protecting from others who may wish to exert control. Moreover, privacy online is considered to be the power over the flow of data and in the context of the internet, it is understood as "the control we have over information about ourselves."[7] Personal data can be used as a powerful tool when in the wrong hands. Data protection rules that are closely related to the fundamental right of privacy overlap in a mode whereby data protection is both broader and narrower than privacy.[8]

That being said, these rights are violated in Mongolia severely due to lack of legislations and norms. As such, these infringements can vary from unlawful surveillance to privacy disclosure in all levels such as public, private and individual. Consequently, this study discusses and highlights the distinction between the right to privacy and data protection by explaining the current context of Mongolia. Moreover, these will be analyzed in relation to the European

---

[5] Simon Kemp, 'Digital 2020: Mongolia' (*Data reportal*) <https://datareportal.com/reports/digital-2020-mongolia> accessed 15 May 2021.

[6] Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philosophy & Technology 307 <https://doi.org/10.1007/s13347-016-0220-8>.

[7] Zuzanna Warso, 'There's More to It than Data Protection – Fundamental Rights, Privacy and the Personal/Household Exemption in the Digital Age' (2013) 29 Computer Law & Security Review 491 <https://www.sciencedirect.com/science/article/pii/S0267364913001295>.

[8] Raphaël Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 Computer Law & Security Review 522 <https://www.sciencedirect.com/science/article/pii/S0267364913001325>.

legislations such as in the context of the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (EUCFR).

1.2 Research problem

Supposing that the conception of privacy did not exist in human life, so that people would eavesdrop and leak personal information to public knowledge, or an employer could reveal a sensitive data about an employee, or doctors could disclose medical records without a patient's consent, or states could arbitrarily investigate and collect data of individuals and misuse it, and so forth. The consequences are unquestionably harmful without an adequate protection of privacy. The notion of privacy was derived many centuries ago and has been enhanced throughout history, whereas data protection emerged in international fora and secondary legislations quite recently and has only recently acquired fundamental rights status in the European Union (EU).[9] The interaction of these rights is critical and oftentimes overlaps. However, they are not interchangeable and there are certain distinctions that the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) interpret in addition to primary and secondary laws. The legal framework and regulations of such rights in the European countries are accurate and well enforced. Whereas, for developing countries like Mongolia, it is questionable if these rights are exercised adequately in practice. As a result of inadequate legal frameworks, there is a high risk of human rights violations in regards to the right to privacy and data protection in Mongolia. However, the use of new technologies by both private and public entities has been increasing dramatically fast. Therefore, this study assesses the overall development of the right to privacy and data protection in Mongolia in comparison to the European legislation.

[9] Sonia Morano-Foadi and Stelios Andreadakis, 'Reflections on the Architecture of the EU after the Treaty of Lisbon: The European Judicial Approach to Fundamental Rights' (2011) 17 European Law Journal 595 <https://doi.org/10.1111/j.1468-0386.2011.00568.x>.

1.3 Research questions

The main research questions for this study focus on the right to privacy by researching Mongolia's relevant legal frameworks along with its historic, socioeconomic context. Moreover, this study will examine the European regulations in accordance with the ECHR and the EUCFR since the region has a prominent role in shaping the global norms and standards on privacy and data protection. The questions are as follows:

- What is the right to privacy? Why is it worth protecting and how valuable is this right?
- What is the distinction between the right to privacy and data protection?
- What is the legal framework for regulating the right to privacy in Mongolia?
- Is the right to privacy protected and secured in Mongolia? What are the challenges?
- How are the ECtHR and the EUCFR interpret the right to privacy and data protection through their respective case laws?
- What are the differences between two systems and which principles should be enhanced?

1.4 Methodology

This study employs a desk research methodology. Primary sources relied on are human rights and the privacy protection instruments, treaties, case laws, court decisions, while secondary sources include books, online journals, articles, government reports, and statistics. Also, this overviews Mongolia's socioeconomic and legal context, particularly examining the current legislations in the right to privacy and data protection. Some court decisions will be considered in accordance with the legislation to better illustrate the country context. Moreover, the legal comparison will be conducted in regards to the ECHR and EUCFR case laws in addition to studying the overall European context in relation to the advanced regulations on privacy and data protection. Additionally, the study analyses the notion of privacy in general by explaining from the historic perspectives and touching upon data protection regulations, which is closely linked with the right to privacy.

1.5 Objectives and scope of the study

This study focuses on the in-depth concept of the right to privacy and data protection discussing in the context of Mongolia in comparison to the Europe's two highest courts jurisprudence. Particularly, the ECtHR interprets privacy extensively through case laws, while the EUCJ ensures such right is applied in all EU countries in accordance with the EUCFR. In addition, the EU is claimed to be the standard setter especially in terms of data protection regulations. Another ground for studying the topic in comparison to the European legal frameworks is based on the democracy value of an individual self-determination. The value of individualism is of great significance to the right to privacy, where in European culture this perception was prevailed long ago. Contrastingly, Eastern culture prioritizes collectivism more yet nomadic culture that has lived in tribes collectively is still in a long process of acknowledging the importance of one's privacy until present day. The privacy concept had only started prevailing late in the 19th century in Mongolia due to traditional and cultural implications. Consequently, the legal frameworks are explained in addition to historic and socioeconomic perspectives. Current legislations on privacy are considered to be vague and according to local scholars, the relevant laws need to be updated immediately. Furthermore, the EU plays a prominent role not only in the region but also in the global context in shaping the global norms and standards, thus the EU legal frameworks will be studied and compared with the respective regulations in Mongolia. This thesis specifically focuses on the right to privacy, data protection and its distinction. For the sake of conciseness, this thesis does not touch upon freedom of speech, freedom of assembly, cybercrime, Big data, internet governance and the use of the Internet for terrorist purposes.

2. THE PRIVACY CONCEPT EXPLAINED

"Secrets are lies, sharing is caring, privacy is theft"

by Dave Eggers

2.1 Introduction

The previous introductory part gives an overall background of the study by highlighting the importance of the right to privacy. According to widely accepted dictionaries, the term privacy is defined as "the state or condition of being alone, undisturbed, or free from public attention."[10] Then how this interpretation has evolved throughout the history? This chapter explains the concept of privacy over time particularly from the historic perspective, the importance of protecting it and distinction between the right to privacy in addition to its values and drawbacks.

2.2 The right to privacy: conceptual explanation

2.2.1 The privacy in antiquity: the distinction between private and public spheres

Since antiquity, the privacy issue was brought up from gossip to eavesdropping and then it proliferated into protecting one's body, home and one's information.[11] Digging deep into ancient history, Aristotle (384-322 BC) defined "polis*"* as the public sphere of politics, while "oikos*"* was interpreted as the private or domestic sphere of the family.[12] Accordingly this was the most classical distinction made between the private and public sphere. In particular, human beings dwell in constant communication and in social needs which reflect the outer sphere.

---

[10] 'Oxford English Dictionary' <https://www.oed.com/view/Entry/151596?redirectedFrom=privacy#eid> accessed 17 May 2021.

[11] Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087. P.1096

[12] Sjoerd Keulen and Ronald Kroeze, '1. Privacy from a Historical Perspective' in Bart van der Sloot and Aviva de Groot (eds), *The Handbook of Privacy Studies* (Amsterdam University Press 2018) <https://doi.org/10.1515/9789048540136-002>. P.24

Whereas, one's private and family life takes place at home, where one can enjoy his/her personal freedom without any social pressure. Furthermore, a relevant concept is found in many ancient, prominent philosophers' works such as the liberal theorist John Locke (1632-1704). He asserts on "Two Treaties of Government" that "cooperation in and stability of a political society is the result of the legitimate aim of rational individuals to protect their private life, liberty, and property."[13] By stressing so, he draws an importance of maintaining a clear distinction between the private familial sphere and public political spheres in order to pursuit an individual liberty and freedom.[14] Most importantly, he underlines the concept of individualism, personal autonomy which relates with the concept of personal right.

2.2.2 Privacy in the 19th century: the right to be let alone

Later after the 1800s, democratic revolutions shaped the notion of privacy into different directions. In particular, a French historian addressed in his work that "the nineteenth century was the golden age of private life, a time when the vocabulary and reality of private life took shape."[15] Particularly a number of movements and revolutions during that time had led to the foundation of democracy and freedom. This included The French Revolution that lays as a foundation of the Declaration of the Rights of Man and of the Citizen in 1789.[16] Moreover, in the first half of the 19th century the written correspondence, the urbanization process in the west impacted on privacy significantly. Specifically, British population doubled during that time, so the city had to put rules in place for individuals including keeping physical distance in crowded places such as train cabins and so forth.[17] In regards to written correspondence, a postal system started to emerge and became more accessible to people. Journalism had flourished so that journalists working for mass media newspapers were focusing on gossip, scandal, celebrity

---

[13] Bart van der Sloot and Aviva de Groot (eds), *The Handbook of Privacy Studies* (Amsterdam University Press 2018) <http://www.jstor.org/stable/j.ctvcmxpmp>. p.26

[14] Roisin A Costello, "'Warren and Brandeis and The Right to Privacy's Hollow Core" Article Róisín A Costello' 361 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059762&download=yes>.

[15] Paul Veyne Ares Philippe Georges Duby, *A History of Private Life* (4th edn, Harvard University Press 1987).

[16] Keulen and Kroeze (n 12).

[17] David Vincent, *Privacy: A Short History* (John Wiley & Sons 2016).

life.[18] Journalists at that time captured the lives of upper-class elites by publishing pictures in magazines. The depicted persons, however, mostly members of wealthy families, were not fond of this development. Curiosity over others' business became, and has remained, a prime example of the invasion of one's privacy. Besides, another aspect of privacy transformation was related with the way how states governed. Governments' duty to protect however infringed human rights through various ways at that time. For instance, sensitive data such as marriage and childbirth records were collected through social welfare system in England[19] as early as the late 19th century. Consequently, misuse of collected data had derived from this time on in accordance with change of social transformation.

Furthermore, it is crucial to point out another important notion of privacy which was introduced by American lawyers Samuel D. Warren and Louis Brandeis in 1891. The lawyers presented the concept on Harvard Law Review article "The Right to Privacy" and defined privacy as "the right to be let alone" or being free from intrusion, which played an important role in shaping the views on privacy today.[20] Specifically, the authors claim that under a government of law, one's life should be free from intrusion or invasion except when they can be justified. This depicts that states are responsible for protecting the people and if necessary they have the right to interfere in private life as the form of legal protection of the public interest under a local laws and regulations. Also, they characterized privacy in connection to solitude or "retreat from the world", which lays as a foundation to the later theory of seclusion. Additionally, they described privacy as a mental pain rather than a physical injury considering one's thoughts, sentiments and emotions in communication with others. This notion is interpreted as an intangible concept since privacy infringements are related to defamation, freedom of thoughts and conscience, freedom of speech and so forth. The law of defamation protects from injuries to reputation, while privacy involved "injury to the feelings," a psychological form of pain that was difficult to translate into the law, which focused more on tangible injuries.[21] The latter concept of distinguishing the right to privacy from physical

---

[18] Huub Wijfjes, 'Digital Humanities and Media History: A Challenge for Historical Newspaper Research 1' (2017) 20 TMG Journal for Media History.

[19] Daniel Solove, 'A Brief History of Information Privacy Law' [2006] GWU Law School Public Law Research Paper 1.

[20] Roisin A Costello (n 14).

[21] Ibid. at 197

damage still has a profound impact on current law and devoted to many scholars' works have been devoted to furthering the concept of privacy.

2.2.3 Privacy in the 20th century: seclusion

In the early twentieth century, states started to take measures in order to foster privacy in various ways. Among other initiatives, unlike in nomadic tribal culture, western countries acknowledged the importance of being alone quite early due to individualistic way of life. In particular, Great Britain and the Netherlands in 1918 and 1919 respectively established new town planning acts by setting basic standards for housing. It prescribed new acts stating that new houses, especially in the social housing sector, should have a separate kitchen, an indoor toilet, and preferably three bedrooms so that all family members sleep in their own room and have their privacy.[22] In accordance with the concept of being alone, in the late twentieth century, a legal scholar Ruth Gavison presented the idea of seclusion by explaining that "a person enjoys perfect privacy when in completely inaccessibility to others."[23] On the same note, Alan Westin explained it as the "voluntary and temporary withdrawal of a person from the general society through physical means in a state of solitude."[24] It somehow connects with the idea of enjoyment of privacy at home. Additionally, he states that privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them should be known to others.[25] In his publication of 1968 he highlighted a few aspects of privacy such as one's autonomy and personal development, and one's emotional state that also links with issue of privacy.

In regards to historic events that happened in previous century, a major change occurred not only in the context of privacy but also in other rights due to mass violations of human rights during the two world wars. Legal scholars emphasize that initiatives to strengthen the formal

---

[22]Vincent (n 17).

[23] Herman T Tavani, 'Philosophical Theories of Privacy: Implications for an Adequate Onilne Privacy Policy' (2007) 38 Metaphilosophy 1 <http://www.jstor.org/stable/24439672>.

[24] ibid.

[25] Alan F Westin, 'Social and Political Dimensions of Privacy' (2003) 59 Journal of social issues 431.

legal protection of individual rights at the international level were widely supported.[26] Consequently, the United Nations (UN) were founded in 1945 and article 12 of the Universal Declaration of Human Rights (UDHR) of 1948 stressed that "no one shall be subjected to arbitrary interference with his privacy."[27] The 1950 ECHR issued that "Everyone has the right to respect for his private and family life, his home and his correspondence."[28] In order not to repeat the past atrocity, nations collectively started to raise the human rights concerns and made steps to protect them. However, as the right to social security and right to free movement was put in place through human rights instruments, state surveillance on collected personal data became an emerging issue.[29] In order to receive social welfare, people had to trade their personal data as it still happens today.

Lastly, the concept of individuality was again presented by Edward Bloustein, who described self-determination and human dignity as a core value of privacy.[30] Subsequently, the notion of privacy is closely connected to individualism, which emphasizes the moral worth of one's state of autonomy and independence from in-groups or community. Privacy of an individual is valued more and introduced earlier than people living in communal or collective way of culture. Therefore, reassuring one's dignity and individualism after the several wars in world history was a crucial step in promoting human rights.

2.2.4 From 1970 onwards: new technologies and the Internet

Scholars describe this period as "the digitalization of privacy"[31] or the digital age. The whole spectrum of privacy was impacted with the emergence of computers, the Internet, and

---

[26] Keulen and Kroeze (n 12). P.32

[27] The General Assembly, 'Universal Declaration of Human Rights (Chuukese)' (2007) 8 Asia-Pacific Journal on Human Rights and the Law 101.

[28] CA Hopkins, 'European Convention on Human Rights' (1966) 24 The Cambridge Law Journal 4.

[29] CA Bayly, 'The Birth of the Modern World, 1780-1914 Global Connections and Comparisons' [2004] Malden, MA: Oxford: Blackwell.

[30] Edward J Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser'' (1964) 39 New York University Law Review 971 <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/nylr39&id=997&men_tab=srchresults>.

[31] Keulen and Kroeze (n 12).

the World Wide Web in 1960, 1983, 1993 respectively.[32] An extensive use of computers, the Internet, and digital technologies lead to mass collection and processing of personal information of countless numbers of users. Jerry Rosenberg argued already in 1969, that "computers were in use with complete access to personal data" in his work "The Death of Privacy."[33] Therefore, he mentions the rise of "privacy-destroying technologies" that threaten privacy such as routine collection of transactional data, growing automated surveillance in public places, development of facial recognition, biometrics, cell-phone tracking, vehicle tracking, satellite monitoring, workplace surveillance and so forth.[34] These technologies have developed at an extensively rapid pace, so states have access to mass data and misuse it under the duty to protect principles. Rosenberg rightly stresses that if data is collected on everyone's activity, it should be possible to achieve perfect law enforcement.[35] However, unlawful surveillance as well as misuse of data is still a heated debate around the world. Especially after the 9/11 terrorist attack, states surveillance conducts increased significantly[36] in order to maintain public security.

Moreover, mass use of the Internet and social media is integral to digitalization of privacy. Some argue that nowadays privacy does not exist anymore since one's personal data can easily be traced and found or misused. Indeed, it is true that we live in a world where based on given data on the Internet such as date of birth, password, and so on, business companies misuse, analyze, track, and predict behavior. We can name several examples such as a business company that traced behavior of the buyer so that she was recommended pregnancy products before her father found out she was pregnant.[37] Similarly, the Cambridge Analytica scandal on misuse of 87 million users' data on Facebook[38] without a proper consent. These examples illustrate how the modern use of technology can potential cause a serious harm to one's privacy.

---

[32] ibid

[33] A Michael Froomkin, 'The Death of Privacy?' (2000) 52 Stanford Law Review 1461 <http://www.jstor.org/stable/1229519>.

[34] ibid.

[35] ibid.

[36] Keulen and Kroeze (n 12).

[37] Kashmir Hill, 'How Target Figured out a Teen Girl Was Pregnant before Her Father Did' (2012) 16 Forbes, February 2.

[38] J Isaak and MJ Hanna, 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection' (2018) 51 Computer 56.

The UN especially paid attention to the growing use of the Internet and potential threat to human rights. In July 2012, the UN Human Rights Council adopted a key resolution on the promotion, protection and enjoyment of human rights on the Internet. The Resolution affirms that the "same rights that people have offline must also be protected online."[39] However, the notion of applying the same rights both offline and online has been a heated debate among scholars. Professor Matthias argues that laws that apply offline must be narrowly tailored, specific and meet the traditional three-part-test and take into account the existing rights rather than inventing new rights online.[40] Therefore, there is no need to develop new laws especially in regards to regulating communications online rather to elaborate what exists now and move forward. In addition to the United Nations Resolution on the right to privacy in the digital age, the High Commissioner report characterizes privacy as "the presumption that individuals should have an area of autonomous development, interaction and liberty, a private sphere with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."[41] This definition of privacy is well integrated and expressed in accordance with all above stated historic findings by scholars.

In general, privacy has a long-dated history and the importance of highlighting it varies on timely events and people's lifestyle. The more a person has access to information and ownership of it, the more power that person has. Information per se is comparable with power and money. Once the information is disclosed it's no longer considered to be a secret and cannot be eradicated from the minds. Solove once stated that privacy is "the right most valued by civilized men."[42] Indeed, privacy is a fundamental right, the beginning of all freedoms in democratic society. However, time after time philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy.[43] One's privacy seems to be too broad that has a broader understanding of freedom of acquiring information in

---

[39] United Nations General Assembly, 'UN Resolution on the Promotion, Protection and Enjoyment Ofhuman Rights on the Internet'.

[40] Matthias C Kettemann, 'UN Human Rigts Council Confirms That Human Rights Apply to the Internet' (*Blog of the European Journal of International Law*) <https://www.ejiltalk.org/un-human-rights-council-confirms-that-human-rights-apply-to-the-internet/> accessed 21 April 2021.

[41] UNGA, 'The Right to Privacy in the Digital Age' <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement>.

[42] Daniel J Solove, 'Understanding Privacy' 1.

[43] Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 The Yale Law Journal 421 <http://www.jstor.org/stable/795891>.

democratic society, somehow, it's narrow at the same time that individuals are restricted to disclose it arbitrary.

2.3 Data protection: distinguishing from the right to privacy

2.3.1 Data protection explained

Some might think that the right to privacy and data protection are two sides of the same coin. However, a number of researches and studies shows that there is a key difference between these two concepts, despite their being intertwined with each other. Unlike the right to privacy, data protection has not been protected as a fundamental right and entrenched in treaties and conventions, as it is quite a modern concept. Particularly in the European context, France and Germany implemented its first data protection regulation in the 1970s among other European countries. Hijmans explains that "as two rights would be part of the same system: privacy as a substantive right (the game) and data protection as a procedural right (its rules), protecting the same array of rights and freedoms."[44] They are interlinked with each other and it's impossible to discuss privacy without touching upon data protection.

Due to some scholars in the field, the concept of Data protection has three historic pillars: [45]

The first pillar lies in the growth of the government record system in general, including the intensive use of the postal system, the telegraph, and the telephone between 1950 and 1970. Consequently, the connotation of "computers and privacy" was determined.[46]

---

[44] HIelke HIjmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (1st ed. 20, Cham : Springer International Publishing : Imprint Springer, 2016) <https://limo.libis.be/primo-explore/fulldisplay?docid=32LIBIS_ALMA_DS71188876170001471&context=L&vid=KULeuven&lang=en_US&search_scope=ALL_CONTENT&adaptor=Local Search Engine&isFrbr=true&tab=all_content_tab&query=any,contains,The European Union as Guardian>.

[45] Anuj C Desai, 'Wiretapping before the Wires: The Post Office and the Birth of Communications Privacy' (2007) 60 Stanford Law Review 553 <http://www.jstor.org/stable/40040416>.

[46] *ibid*

The second regulatory pillar belongs to the early 1980s when computers were introduced at homes for individual use and national legislation focused on the individual, echoing the idea of data privacy as freedom.[47] This idea was not brought into consideration of states and governments until it was brought up to the German Constitutional Court in 1983 that a "novel right to informational self-determination was considered any processing of personal data is seen as an interference with the right, unless the data subject exercises her self-determination by consenting to it."[48]

While in the 1990s, the use of computers was widely spread and the emergence of the Internet and the World Wide Web (www) had greatly impacted data protection as was discussed in the previous sub chapter. Access to information and technology was getting widely available and the notion of protecting users' personal data was in a heating debate.

2.3.2 The emergence of data protection regulations

As a consequence of an emerging issue of protecting personal data, the proposal for a directive on the protection of individuals in relation to the processing of personal data was introduced by the European Commission in 1990. This was the fundamental component of the Data Protection Directive (DPD),[49] a cornerstone of the EU data protection law. The directive highlighted the importance of both free flow of information and the protection of privacy as fundamental rights. Moreover, the EU made a major step by enshrining the protection of personal data as a fundamental right in Article 8 of the EUCFR of 2012. The Article 8 states as follows: 1. "Everyone has the right to the protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access data which has been collected concerning him or her, and the right to have it rectified."[50]

---

[47] Serge Gutwirth, *Privacy and the Information Age* (Rowman & Littlefield 2002).

[48] Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 Computer Law & Security Review 84 <https://www.sciencedirect.com/science/article/pii/S0267364908001660>.

[49] Directive 95/46/EC 24 October 1995.

[50] The Charter of Fundamental Rights of the European Union 2012 51.

The Charter drew a clear line of distinction from the right to privacy, which was preserved in Article 7. Additionally, protecting the free flow of personal data between people is critical, therefore the Council of Europe enacted the first binding instrument for data protection: "Convention 108" for the Protection of individuals with regard to automatic processing of personal data. The Convention is more about the data protection of individuals and privacy in the field, by contrasting the distinction between the ECHR Article 8, where these two connotations had been used to interpret at the same time under this article. In line with enhancing data protection regulations, the new legislative instrument was adopted in 2016-the General Data Protection (GDPR) and the Law Enforcement Directive. This law plays a prominent role not only for the EU but for the world.[51] According to the literature, the world follows the EU in this area[52] and adoption of data protection law increases constantly nowadays that more than 128 out of 194 countries have put the legislation in place.[53] Moreover, in regards to data protection legislations, it is crucial to highlight the Digital Services Act (DSA) package initiated by the European Commission. The sole aim of these laws is "to protect the fundamental rights online, to maintain fair and open online platform."[54] These acts consist of DSA that protects consumer's rights and transparency, the Digital Markets Act (DMA), which allows business owners in online platforms to have less and fair competition.

2.3.3 The distinction between the two rights

While the right to privacy and the right to data protection have started to be considered as two distinctive concepts, the interrelation is still close. Specifically, there is a tendency that the data protection is evolving away from privacy into something entirely distinct, albeit still connected to it.[55] Before the Charter, data protection was framed as an individual's self-

---

[51] Ram Aliya Gordon Sarah, 'Information Wars: How Europe Became the World's Data Police' FInancial Times <www.ft.com/content/1aa9b0fa-5786-11e8-bdb7-f6677d2e1ce8>.

[52] ibid

[53] 'Data Protection and Privacy Legislation Worldwide' (*UNCTAD*) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

[54] 'The Digital Services Act Package' (*European Commission*).

[55] Dara Hallinan and others, *Data Protection and Privacy: Data Protection and Democracy* (Bloomsbury Publishing 2020).

determination and dignity and "has historically been tied to privacy."[56] Compared to the right to privacy, data protection is a modern phenomenon that derived with the advancement of modern technology. According to Lynsey, it is necessary to consider the overlap between Article 8 of the ECHR and Article 7 of the EUCFR.[57] Article 8 of the Convention and Article 7 of the Charter do not specifically have a direct effect on data protection. While Article 8 of the Charter does have a direct effect. That being said, the right to privacy focuses on certain dimensions of individual rights that draws a line within the personal and private life. Whereas the right to data protection according to the Charter is considered to have a broader perspective. Regarding the jurisdictions, the ECtHR recognizes all kinds of personal data can potentially interfere with the scope of Article 8 ECHR[58] and this is explained in the fourth chapter.

Another notion of distinction between the right to privacy and data protection is made by the scholars De Hart and Gutwirth. But before making a comparison, it is necessary to define privacy according to the scholars. They describe privacy as a "tool of opacity", which protects individuals against interference by the state and by private actors by requiring abstention from undesired intervention.[59] They claim that privacy curtails power by setting normative limits to it, while data protection is mainly a tool of transparency, regulating and channeling the exercise of power rather than stopping it.[60] In particular, the ground for defining privacy as a "tool of opacity" is related to the early concept of separation between the public and private spheres. A person finds freedom at their homes without any interference by the state or politics. This is so-called "shield" of opacity from the intrusion of external interference and that leads to a sphere of individual autonomy and self-determination.[61] However, the opacity can be derogated in times of a search warrant due to a criminal suspect by the government "in accordance with the law."[62] Regarding the "tool of transparency", the authors depicted the tool as the democratic

---

[56] Maria Tzanou, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 International Data Privacy Law 88 <https://doi.org/10.1093/idpl/ipt004>.

[57] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).

[58] Lorenzo Dalla Corte, 'A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection' [2020] Data protection and privacy 27.0

[59] Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' [2006] Privacy and the criminal law 61.

[60] Ibid

[61] The Charter of Fundamental Rights of the European Union (n 50).

[62] ibid.

system of checks and balances.[63] With an accountable and responsible form of governance by the state and private sectors, people will enjoy the benefits of secured information. The system of checks and balances, for example, installs the mutual transparency of state powers, while the controllability and accountability of government by the citizens implies free and easy access to readily available government information, the enactment of swift control and participation procedures.[64] The creation of specialized and independent bodies to control and check the doings of government.[65] Consequently, according to this explanation one can understand that measuring privacy dimensions is quite vague, whereas data protection has a clear-cut perception.

2.4 The value of privacy

2.4.1 Confidentiality

Human dignity, freedom of self-determination, and autonomy to engage in relationships as regards-for example-their "sexuality, health, personality building, social appearance, and behavior"[66] are each an important value of privacy. Privacy protects us from many unwanted situations such as bad reputation, shame, wrongdoings of others, and "having bad actions discovered."[67] These descriptions are correlated with human dignity, which translates as "the ability to transcend one's animal nature, to be civilized, to feel worthy of respect."[68] When social practices relating to dignity are disrupted, the result can be severe and sometimes a debilitating humiliation and loss of self-esteem.[69] One of the prominent scholars in privacy research, Gavison proves this argument by stating that privacy is essential for autonomy and freedom. Especially, the word autonomy is integral to the topic. The word per se is derived

---

[63] ibid.

[64] ibid.

[65] De Hert and Gutwirth (n 59).

[66] ibid.

[67] Cressida Gaukroger, 'Privacy and the Importance of "Getting Away With It"' (2020) 17 Journal of Moral Philosophy 416 <https://brill.com/view/journals/jmp/17/4/article-p416_416.xml>.

[68] Aurel Kolnai, 'Dignity' (1976) 51 Philosophy 251 <http://www.jstor.org/stable/3749604>.

[69] Miller William Ian, 'The Anatomy of Disgust' [1997] Cambridge MA Harvard UP.

from the ancient Greek words "autos" (self) and "nomos" (law)[70] meaning an individual takes a decision and holds an account of his own actions. A scholar in the field Becker argues that privacy is a "way of controlling one's own personal environment." Yet invasion of privacy disturbs access to one's personal sphere, which is associated with secrecy or confidentiality.[71] In particular, he explains that a person deliberately gaining access to information that another person wants to keep secret is violating the other person's autonomy through information control.[72] In other words, an individual has a choice whether to protect his or her own privacy from the public sphere. Some claim that "innocent people have nothing to hide."[73] However, I argue that control over our own information is critical in the modern world, where sophisticated technologies collect mass data, and people are under mass surveillance that can cause an unprecedented harm. Moreover, as explained in the previous chapter, private entities mine big data and use them to meet their interest, which is as a result of tracking one's behavior and action. Additionally, in the literature it stresses that confidentiality focuses on relationships, which "involves trusting others to refrain from revealing personal information to unauthorized individuals."[74] Thus, privacy can be an invasion into one's body, space and liberty; while confidentiality is breached when control or access to one's information; this correlation shows how closely these issues are intertwined with each other.

2.4.2 Moral implications

As stated in the previous chapter, privacy is an opacity tool, but it is one which does not have a concrete definition. Judith, a philosopher, claims that privacy is derivative and that there is no need to define the boundaries.[75] Some scholars argue that this concept is "one's own ability

---

[70] Marcel Becker, 'Privacy in the Digital Age: Comparing and Contrasting Individual versus Social Approaches towards Privacy' (2019) 21 Ethics and Information Technology 307 <https://doi.org/10.1007/s10676-019-09508-z>.

[71] ibid.

[72] ibid.

[73] ibid.

[74] Neil M Richards and Daniel J Solove, 'Privacy's Other Path: Recovering the Law of Confidentiality ' 96 Georgetown Law Journal 123 <https://heinonline.org/HOL/P?h=hein.journals/glj96&i=126>.

[75] J Angelo Corlett, 'The Nature and Value of the Moral Right to Privacy' (2002) 16 Public Affairs Quarterly 329 <http://www.jstor.org/stable/40441333>.

to delimit what others know about oneself."[76] This notion of privacy is explained among many schools of thought and is related to the moral value of privacy. Specifically, from an individual level to state entity, breaching one's confidentiality is often discussed in relation to one's moral behavior. Confidentiality is focused on relationships, especially the notion of trust within individuals. Therefore, the breach of it can lead to a number of serious harms. For instance, publication of the HIV positive status of a pregnant woman in some areas of sub-Saharan Africa reportedly may lead to beating or death.[77] Or disclosing one's sensitive data can lead to many social problems such as family divorce, domestic violence, loss of job, even a suicide.

People do such things at their home which is morally unacceptable in public. However, this umbrella of discretion does not extend to illicit activities such as domestic violence or so on. Arendt rightly proclaimed, "to live an entirely private life means above all to be deprived of things essential to a truly human life. Even the most intensely private actions cannot be fully understood until they are made public to others."[78] Consequently, privacy is deemed to find the shield between the inner and outer sphere and have the tight moral and legitimate standards that people in society have to follow.

2.4.3 Lessons learned from the history

Privacy should be used as a means of protecting and promoting human rights, but not as a tool of oppression. Looking back at history, humankind suffered from many heartbreaking experiences in the past. In particular, we witnessed that data misuse lead to the Holocaust genocide during the World War II by obtaining data using a "punch card" system which was part of German Social Security program.[79] As a consequence, millions of Jews were killed and still until today we learn and do our best not to repeat the same daunting mistakes again. For instance, in 1983, German Federal Constitution Court had declared that people have a

---

[76] ibid.

[77] Leslie Pickering Francis, 'Privacy and Confidentiality: The Importance of Context' (2008) 91 The Monist 52 <http://www.jstor.org/stable/27904065>.

[78] Margaret Canovan and Hannah Arendt, *The Human Condition* (University of Chicago Press 1998).

[79] Waxman Olivia, 'The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History' (*Time*) <https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/> accessed 22 April 2021.

fundamental right of self-determination over personal data to remedy the wrongs of the past and ensure that something like holocaust never happened again.[80] The same happened to Rwanda in 1994 when Hutu extremists took over the monarchy and started the ethnic cleansing by slaughtering the Tutsi minority. They identified Tutsis by the ID cards that had people's ethnic group in it and as a result approximately 800,000 Tutsis were slaughtered brutally within 100 days.[81] There are many devastating examples to raise in regards to violation of privacy but these two cases depict the clear example of how harmful an invasion of privacy can become.

2.5 Privacy drawback

Most people are concerned about their privacy, but they don't necessarily know what it means, due to uncertainty, and ambiguity of the concept that the scholars explain from different angles. On the same note, the landscape of privacy is constantly changing, for it is shaped by the rapid pace of technological invention. Generally, the state governments adopt laws that maintain great flexibility in conceptualizing privacy problems. However, not all privacy problems are the same, and different conceptions of privacy work best in different contexts. Literatures claim that the pace of technology has changed since the 9/11 terrorist attack and that states use technology for privacy and protection and for democracy. Consequently, people nowadays are under the constant surveillance and face the unwanted threat of unfettered access to their personal data. Undoubtedly the use of ICTs brings a substantial contribution to the society that people benefit from in their daily lives. However, these sophisticated technologies such as video surveillance systems- Closed-Circuit Television (CCTV) on the streets have become an inspection tool for government or other entities that possess a threat to personal data. In particular, modern instruments such as psychological testing and lie detectors that collect one's personality, Intelligence Quotient (IQ), fingerprints, and emotions are being used for data collection.[82] And the reason for using these data is criticized among the scholars. Identity theft has become a common fraud that the incidence has increased within the last few years.

---

[80] Sanjay (Financial executive) Sharma and Pranav Menon, *Data Privacy and GDPR Handbook*.

[81] Matthew J Newcomb, 'Feeling the Vulgarity of Numbers: The Rwandan Genocide and the Classroom as a Site of Response to Suffering' (2010) 30 JAC 175 <http://www.jstor.org/stable/20866942>.

[82] Jan Henrik Ziegeldorf, Oscar Garcia Morchon and Klaus Wehrle, 'Privacy in the Internet of Things: Threats and Challenges' (2014) 7 Security and Communication Networks 2728.

Especially during the pandemic times when people had to follow stay at home rules or during the strict lockdowns, the use of online purchases, and transactions has increased dramatically. As a consequence, identity thieves steal personal information such as names, bank account information and impersonate them by committing identity fraud. Data warehousing and data mining is used mostly for business purposes that collects the consumers' data and uses to track behavior pattern. Specifically, big data are collected in data warehouse and used mostly by business purposes in order to track the consumers purchasing behavior pattern. All in all, privacy shortcomings are mostly related to modern technologies in regards to data protection nowadays. As much as people benefit from technological advancement, tradeoff with personal information causes a threat to society.

2.6 Interim conclusion

All in all, the notion of privacy has evolved throughout human history in accordance with patterns of people's living in societies. Ranging from the ancient concepts of the right to be left in seclusion to autonomy of an individual until the modern technological advancement: all these changes have impacted matters of privacy significantly. The right for a person to choose who they want to be with, without any external interferences is one of those valuable freedoms. Privacy is protected especially in most democratic constitutions as a fundamental right and expressed through a variety of legislative instruments. As stated above, privacy of an individual has evolved remarkably over time, therefore novel discussions such as data protection has emerged into a debate over the time. Consequently, distinguishing the line between the interconnected concepts such as privacy and data protection is integral to the topic. Particularly according to findings from the research, privacy is defined in broad and ambiguous way, while data protection has a clear definition which will be explained in the European legislations on the next chapter. Moreover, the massive use of the Internet has brought a significant benefits and opportunities, while at the same time it has brought a threat risk as a tradeoff. Accordingly, the importance of protecting privacy is central to individual self-determination, human dignity, autonomy, and being free from public scrutiny.

3. MONGOLIA'S LEGAL FRAMEWORK FOR THE RIGHT TO PRIVACY

"For the Great Khan their king is, I tell you, the wisest and most accomplished man, the greatest Captain, and best to govern men and rule an Empire, as well as the most valiant, that ever existed among the Tribes of Mongols"

-Marco Polo, Venetian traveler, special envoy for Kublai Khan court in Mongolia during the 13th century

3.1 Privacy from the 13th century to the current democratic society: overview of the Mongolian socioeconomic context and legal system

Mongolia, with a land area of 1.5 million square kilometers and population of only 3.3 million,[83] landlocked between two great nations of the Russian Federation and People's Republic of China. Population density is 2 persons per square kilometer of surface area which makes it the most sparsely populated country in the world. Currently, half of the population live in the capital city, while a significant number of people still live a traditional nomadic life practicing animal husbandry in the outset. Nomadic herders have lived collectively in tribes for centuries and the notion of privacy has not prevailed in their mindset accordingly.

3.1.1 Historic overview

Travelling back to the 13th century, the Great Mongol Empire founded by great Genghis khan, conquered most of the modern European territory that at its height spanned from Korea to Hungary covering around 23 million square km[84] of territory, making it the largest and

[83] 'Mongolia Population 2021' (*World Population Review*) <https://worldpopulationreview.com/countries/mongolia-population> accessed 26 April 2021.

[84] 'Mongolian History Encyclopedia' <https://mongoltoli.mn/history/h/504> accessed 2 May 2021.

contiguous empire in world history. The backbone of success consisted of a number of factors such as the khan's administration under the "Yasa law," domesticated horses that are strong and tireless and most importantly the convertible and practical way of living-the yurt.[85]

Firstly, according to the historic overview of Mongolian legal system, the roots of were formed during the Mongol Empire when Genghis khan promulgated "Ikh Zasag" law or "Yasa law", the first legal document that codifies the general principles of tribes under his command throughout the conquered territories. In many historic sources it depicts the spirit of the "Yasa law" on the importance of maintaining peace and order. For instance, "as soon as the Mongol tribes submitted themselves to Genghis Khan he was displeased by certain habits of theirs such as theft and adultery and resolved to abrogate them in order to adorn them with so much safety and ease that they would be able to carry gold on their heads all over his dominions without any danger of being robbed in the same way as people were accustomed to carry plain vases."[86] Historians claim that this was the safest and most peaceful period which resonates as "Pax-Mongolica" or Mongol Peace. In general, "Yasa law" regulated criminal conducts, hunting, military order, other customary law, inter alia, and a postal system.[87] According to the historic literatures, the first communication network is somehow related with this period of time with the advent of horse based postal relay, which then became a foundation of information delivery across the world for many centuries. Specifically, postal stations situated about 40 km apart from one another and each station provided shelter, food and spare horses where a messenger would rest and shift continued delivery into another messenger. The speed of delivery was amazingly fast. As a result, the khan's order spread only within three days in the massive and vastly occupied empire. This horseback postal system paved the route for multicultural cross path for traders, diplomats as well and made a great impact on the global postal system advancement.

Needless to say, that without strong and tireless horses it was impossible to conquer and achieve such success. Mongolians are nomads that practice pastoral nomadism by herding and

---

[85] The Scope, 'Harvard-Yenching Institute' (2015) 3 337.

[86] ibid.

[87] ibid.

domesticating livestock that graze from one place to another. The livestock is their wealth and used for living until today.

3.1.2 The traditional dwelling "yurt"

The crucial part of nomadic culture is a main dwelling that is adaptable to migrating. In particular, during the winters, nomads would settle down next to the vast mountains in order to have protection from any harsh climate, while in the summer they would change location to an vast open area where the livestock would gaze with lush grass. The "yurt," a white round tent that is easily assembled, made of twigs and slender sticks and covered with felt/wool layers that keeps out the heat in summer and maintains warmth in winter. Plano Carpini, a Catholic spy and ambassador to the Mongol Empire in the 13th century, made a detailed observation about the Empire and illustrated as wherever they go, be it to war or anywhere else, they always take their dwellings with them. While the Venetian traveler Marco Polo wrote about the "yurt" as "they have their small houses like tents of rods of wood and cover them with felt; and they are round; and they always carry them with them on four-wheeled waggons wherever they go. For they have the wooden rods tied so well and orderly that they can fit them together like a pack and spread them, take them up, put them down, and carry them very easily where they please. And every time that they stretch and set up their house they set it so that the door is always looking towards midday. They have beside this very beautiful carts with only two wheels covered with black felt which is so good and so well prepared that if it rained all day on the cart water would soak nothing that was in the cart under that cover of felt. And they have them brought and drawn by horses and by oxen and sometimes by good camels. And on these carts their wives and their children and all the things and food which they need."[88] Indeed an easily assembled yurt has been the main dwelling of Mongolians for centuries. Inside the yurt, there is no solid room or walls that separate family members so that everything is shared with each other. Even in Mongolian nomadic culture, there is no culture of knocking doors of yurts. The doors are always open for visitors, which greatly shows the hospitality of the people. In relation to this, the context of privacy did not play a substantial role in daily lives of nomads up until

[88] Polo Marco, *The Description of the World* (Kinoshita Sharon ed, Hackett Publishing 2016).

the democratic transition, whereas the concept was brought up in the 17th century in the Western countries.

3.1.3 Socioeconomic context

Mongolia peacefully transitioned into a democratic regime in 1990 by adopting the democratic constitution after seven years of Communist rule after the collapse of the Soviet Union in the late 1980s. The economy had been greatly dependent on Soviet aid such as energy, food, and infrastructure, while the country made a brave step in transitioning from a centrally planned, communist economy to an independent, market economy. Consequently, state owned enterprises, banks, and public services were privatized in the country. According to Dwight H. Perkins, a leading authority on transition economies, "the move from a centrally planned economy to a market economy is more complex than often assumed. A wide variety of institutions must be created—often from scratch—when a country transitions from a command system to a market system. The managers of these new institutions must also learn to operate in a very different way than in the old system, and that can take time."[89] Indeed, Mongolia still faces the hardship of transition until today due to a lack of experience at economic management by the government.[90] According to the World Bank classification as of 2021, Mongolia is listed as a "lower-middle-income country"[91] and the main economic sources rely on agriculture and mining sectors. Mongolia's economy flourished in the 2000's with a booming mining sector that holds abundant mineral reserves such as copper, gold, coal, uranium, molybdenum, and silver deposits. According to BTI report, the combined value of resources estimates more than 1.2 trillion USD.[92] As reported by the World Bank data, the formal mining industry sector

---

[89] Dwight H Perkins, 'Has China's Economic Reform Already Peaked?' (*East Asia Forum*) <https://www.eastasiaforum.org/2018/08/31/has-chinas-economic-reform-already-peaked/> accessed 2 June 2021.

[90] 'Mongolia: Shift from Relief to Resilience Crucial to Economic Recovery' (*The World Bank*) <https://www.worldbank.org/en/news/press-release/2021/02/05/mongolia-shift-from-relief-to-resilience-crucial-to-economic-recovery> accessed 27 April 2021.

[91] 'World Bank Country and Lending Groups' (*The World Bank*) <https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups> accessed 26 April 2021.

[92] 'Mongolia Country Report 2020' (*Transformation index*) <https://www.bti-project.org/en/reports/country-report-MNG-2020.html> accessed 4 May 2021.

employs over 12,000 people and the informal "artisanal" mining sector may involve more than twice this number.[93] In regards to the Mongolian National Statistics database research conducted in 2019, 81.6% of population was of working age between 25-54, while the elderly group comprised of 10,6%, and 7.8% were children under the age of 14.[94] According gender assessment data in Mongolia, men work in higher paid sectors such as mining, energy, construction and transport, whereas the majority of female workforce are in tourism (hotel, restaurant), health and education sectors where the salary rate is lower.[95] Moreover, women tend to do unpaid household work and focus on children's upbringing. The child mortality rate is high in comparison with the developed world and one of the driving factors is the air pollution that derives from yurt areas that surround the capital city. Over the last ten years there has been strong urbanization and around 2.1 million people live in the capital city Ulaanbaatar, which was initially built for about 300,000 inhabitants. As a consequence of the big scale of migration towards the city, people residing on the outskirts of yurt district have increased significantly. Therefore, the use of coal for heating and cooking in yurts plays a driving factor of severe air pollution. According to the National statistics, Mongolia's total life expectancy is 69.8 years: from which 65.7 for males and 74.2 for females,[96] which is lower than the average indicator as it relates to the quality of basic social services such as housing, health, education, and food safety. Regarding the education system, a recent study shows that the primary net enrollment rate was 97.9% in 2017, which is 9% points higher than the world average[97]. However, the quality of education is low and uneven. Specifically, out of 798 schools in Mongolia, 146 are private with annual tuition fees ranging from USD 1500 to USD 15000[98], whereas public schools are mostly crowded and operate in two or three shifts with shortage of well-qualified teachers and learning resources. As mentioned earlier, due to resource mismanagement and

---

[93] 'Mongolia Mining Sector: Managing the Future' <https://documents1.worldbank.org/curated/en/867261468323101510/pdf/332480ENGLISH01ng1sector1report1ENG.pdf>.

[94] 'Mongolia's Workforce Research' (*National Statistics data base*) <https://www.1212.mn/BookLibraryDownload.ashx?url=LFS_2019_q4.pdf&ln=Mn> accessed 2 May 2021.

[95] 'Mongolia: Country Gender Assessment' (2005) <https://www.adb.org/sites/default/files/institutional-document/32236/cga-mongolia.pdf>.

[96] ibid

[97] Matthias Helble, Hal Hill and Declan Magee, 'Mongolia's Economic Prospects: Resource-Rich and Landlocked between Two Giants' (2020) <https://www.adb.org/sites/default/files/publication/611416/mongolia-economic-prospects.pdf>.

[98] 'Mongolia Country Report 2020' (n 92).

unequal distribution, international debt increased significantly and the populist leaders' practice "shock therapy" by taking short term stop-gap measures.[99]

Since democratization, Mongolia holds multiparty elections and rights and freedom of civil societies and media is protected in the democratic constitution. The constitution guarantees freedom of association and assembly, and the coexistence of religion and the state. Political parties are claimed to be very corrupt so the public trust in politics has been decreasing. All in all, an unequal and disproportionate allocation of resources has led to a widening gap between rich and poor in the past years. Therefore, the social and political exclusion for those who are underprivileged has become a major issue and it therefore affect the equal opportunity of enjoying their fundamental rights and freedom.

3.1.4 Legal and political system

The Mongolian legal system is based on the civil law of Roman-German tradition. The democratic Constitution was adopted in 1992, which protects fundamental rights such as human rights and freedom. The "State Great Khural" or the Parliament of Mongolia is the highest organ of state power that has 76 seats in its chamber and has supreme legislative power. The majority of seats is held by the Mongolian People's Party and the Democratic Party, which are the two leading political forces in the country. Throughout its establishment in 1992, the Parliament has enacted 782 laws in total which are in force now.[100] The judicial system consists of the Constitutional Court, Supreme court, provincial and city courts and district courts. Courts are specialized as criminal, civil and administrative courts. Due to a Constitutional amendment passed in 2019, the President has the power to appoint the justices of the Supreme Court, which is the highest court in the judicial system of Mongolia. In respect to the executive branch, the Prime Minister heads the government by appointing the 14 ministers, the selection of which is then subject to the Parliament's approval. The Prime Minister and the Deputy Minister are

[99] Matthias Helble, Hal Hill and Declan Magee, *Mongolia's Economic Prospects: Resource-Rich and Landlocked between Two Giants* (2020) <https://www.adb.org/sites/default/files/publication/611416/mongolia-economic-prospects.pdf>.

[100] 'The Laws in Mongolia' (*State legal database*) <https://www.legalinfo.mn> accessed 10 May 2021.

nominated by the ruling party (currently the Mongolian People's Party) and confirmed by the President.

The democratic constitution, which was drafted in line with international norms and standards, declares that "ratified international treaties and conventions shall be valid as domestic laws". According to Memorandum of the Understanding on human rights between the Government of Mongolia and the UN country team, Mongolia is a party to 29 human rights international treaties in total.[101] Most notably, the International Covenant on Economic, Social and Cultural Rights (ICESCR), The International Covenant on Civil and Political Rights (ICCPR), The Convention on the Elimination of All Forms of Racial Discrimination, The Convention on the Elimination of All Forms of Discrimination Against Women, and The Convention on the Rights of the Child have been ratified.[102] Moreover, the Mongolian Parliament recently adopted the Law on the Legal Status of Human Rights Defenders, making it the first country in Asia to provide a framework of protection for people who bring up human rights violations in the country.

3.2 Current legislations on the Right to Privacy in Mongolia

3.2.1 The right to privacy

Article 1 of the Constitution of Mongolia guarantees human rights by declaring to "respect and uphold the human rights and freedom and develop a humane, civic and democratic society."[103] Human rights are universal and protected by national laws that are drafted in line with international instruments. Accordingly, the Constitution assured the core rights, inter alia, the right to privacy by Article 16.13 stating that personal, family, and correspondence privacy

[101] Cassandra Mudgway, 'Memorandum of Understanding' [2018] Sexual Exploitation and Abuse by UN Peacekeepers 28 <http://forum.mn/res_mat/Memorandum of Understanding on Human Rights.pdf>.

[102] ibid.

[103] The Constitution of Mongolia 1992 Art 1.

of a citizen must be protected by law and Article 16.17 provides that the safety of an entity, and individual's secret must be protected by adopting laws.[104]

In regards to binding laws in the field, the sole law that regulates an individual's right to privacy is the law of Mongolia on Personal Privacy.[105] Besides, there are other applicable laws with privacy provisions such as the Law on Privacy of organizations,[106] the Law of Mongolia on State and Official Secrets,[107] the Criminal Code "The same crime committed by a medical expert, an educator, lawyer, law enforcement officer, notary, social worker, public servant, psychologist, mediator, bank officer or auditor who has learnt such personal, business or commercial secrets by virtue of his/her job or position shall be punishable by a fine equal to from five thousand four hundred to twenty seven thousand units of amount, or a penalty of limitation of free travel right for a term from one to five years, or imprisonment for a term from one to five years,"[108] the Civil Code "A legal person who caused damage to others' rights, life, health, dignity, business reputation or property deliberately or due to negligent action (inaction) shall compensate for that damage; Article 511 "If the party responsible to distributing information damaging honor, dignity and business reputation of others fails to prove that it is true, it shall be liable to compensate the non-material damage in monetary or other form separately from the material damage,"[109] the Minor Offences law "Taking photographs, audio, video, audio-visual recordings without permission A person shall be fined in the amount of two hundred units togrogs (local currency) and a legal person shall be fined in the amount of two thousand units togrogs for taking photographs, sound, video and audio-visual recordings of the indoor or outdoor environment without the permission of the resident,"[110] and the Law on Information Transparency and Right to Information.[111] In practice, the laws on Privacy of

[104] ibid. Art 16

[105] The Law of Mongolia on Personal Privacy. Available only in Mongolian

[106] The Law of Mongolia on Privacy of organizations.

[107] The Law of Mongolia on State and Official Secrets.

[108] Criminal Code Art 13.11.2.

[109] Civil Code Art 497.

[110] The Law of Mongolia on Minor offences Art 6.22.

[111] The Law of Mongolia on the Information Transparency and Right to Information.

organizations and State and official secrets are implemented accordingly compared to the law on Personal privacy.

3.2.2 The law on personal privacy

This law was adopted in 1995 and consists of only three chapters and nine articles, which was broadly drafted right after the transition to the market economy. The law on Personal Privacy classifies the types of privacy as follows:

- communications and correspondence;
- health;
- assets and property;
- family;
- other matters that may be personal secrets as prescribed by law.

It is claimed that the law has a narrow scope of regulations to meet the needs of fast evolving technological life. The law defines personal privacy as the sphere of "information, documents, or tangible items, the confidentiality of which are protected in accordance with laws and regulations of Mongolia, and which if disclosed, would cause harm to the lawful interests, rights, reputation, and good standing of an individual."[112] This provision is vaguely defined and does not explicitly explain or provide judicial precedent nor interpretation on what information is deemed to be confidential and protected by law. In particular, it is unclear to which extent the context of "causing harm" would apply within the framework in this modern, fast-developing world. Moreover, the law states that maintaining and determining confidentiality of personal secrets is the responsibility of an individual, health and other personal secrets of an individual may be disclosed for the purposes of national defense and security or health and lawful interests of the public based upon a decision of the relevant state authority. Unfortunately, in practice, the law is not implemented as envisaged. Intrusion to private emails, disclosure of either health and bank information, and so forth is very common practice in Mongolia mostly due to lack of public knowledge on this issue and legal regulations. For instance, according to Mongolia's National Commission for Human Rights report, the cases of

[112] The Law of Mongolia on Personal Privacy. Art 2.2

intrusion to privacy has increased in recent years such as disclosing health information by either health professionals and individuals that cause harm to one's dignity and reputation.

The law on Personal Privacy was amended only once due to the Constitutional Court judgement within the past 25 years since its adoption and it clearly depicts the lack of regulations in the field. Specifically, the Article 4.4 of the law on Personal Privacy stated that "medical records except for the specific illness including infectious diseases that are not curable shall be protected by law."[113] Accordingly, HIV was considered under this provision, thus an HIV positive person's medical record had not been protected by this law. The Court considered in 2014 that the Article 4.4 violated human rights and dignity in addition to violation of right to reputation. Therefore, the Court decided to remove HIV from this provision by making the amendment to the law.

As a result of inadequate legal protection and regulations in the country, most cases brought to courts are barely discussed in regards to the right to privacy. As the precedent is not considered to be a source of law in the country, court decisions do not create a precedent. State organizations, business companies, and banks have separate regulations within their scope of operations, which again shows the absence of common binding rules. According to a study conducted by the Human rights NGO forum of Mongolia, business companies do not have a normative set of guidance and regulations on protecting, using and processing a client's information. Consequently, it derives an adverse impact among the society due to uncertainty and unclarity in every level. Accordingly, the need for more robust legislation in the field is required hence the European legal practice, which is deemed to be a standard setter, will be discussed in its fourth chapter.

3.2.3 Criminal Code of Mongolia

In regards to the Criminal Code of Mongolia, the law protects intrusion to privacy by the Article 13.11 stating "Interference to Privacy and Disclosure of personal information."[114] However, to the author's knowledge, cases discussed in local courts are quite sparse. Only a

---

[113] *The law of Mongolia on Personal Privacy Article 44 Dispute resolution* (2014) 5.

[114] Criminal Code.

few cases in regards to breach of health privacy are discussed. In particular, the Criminal Court of First Instance ruled the case in violation of the Article 13.11-Disclosure of personal information of the Criminal Code and the Article 4.2-Intrusion to health secrecy of the Law on Personal Privacy in 25 March 2021.[115] The applicant complained about unlawful disclosure of his health data record by the Social Welfare office to the state-owned company where he worked. The applicant requested to receive the act of the medical verification on his disability record to be able to benefit from Social insurance and Personal Income Tax discount that these laws allow. Specifically, the applicant's loss of ability to work was equivalent to 75% due to insulin dependent diabetes. However, the Social Welfare office disclosed the applicant's medical record to the company he worked for by providing inquiries with health secrecy. Consequently, the company used the record against the applicant and fired them from the job. Article 16.13 of the Mongolian Constitution protects the right to personal liberty and safety, inter alia, privacy of citizens, their families, correspondence, and homes are protected by law. The law on Personal Privacy defines health privacy as "health record information of diseases except for a classification of outbreak cases that are contagious and threatening to the health of the public." However, there is no exhaustive list of aforementioned diseases approved by the Ministry of Health, however to follow the WHO guidance. In this case, insulin dependent diabetes does not refer to this list, therefore, the case is subject to violation of right to privacy. Unlawful disclosure of the applicant's health record information causes a direct harm by dismissing the applicant from work. Therefore, the Court ruled that there had been a violation of the law on Personal Privacy, more specifically a breach of the Article 13.11[116] (Disclosure of personal information, provision 2) under the Criminal Code of Mongolia. The sanction foreseen by the provision of imprisonment for a term from one to five years[117] is considerably harsh when the law per se is vaguely drafted, yet there lacks a specific law on protection, use, storage of one's data.

3.2.4 Related legislations on the right to privacy

---

[115] *The first instance criminal court prosecutor's decision* (2020) 2021/ШЦТ/0.

[116] Criminal Code.Art 13.11.2.

[117] ibid

There are a number of legal gaps to fill in order to advance the law. To name a few, the Law on Privacy of organizations[118] demonstrates that "organizations shall protect privacy of individuals, to which they had access in the course of their activities, in the same way as their own privacy". It is questionable whether private and business companies adhere to this general regulation by setting rules and norms internally. In other words, the moral and legal approaches as enshrined in the Constitution and the mentioned laws, are in contradiction with practice.

In general, the respective laws do not have precise regulations in respect of privacy and how these need to be handled. The lack of clear definition and broad legal concept of personal privacy harms one's right to privacy, therefore the social knowledge on protection of one's own privacy is insufficient. According to the "broadly drafted law", any information of relating to an individual could potentially be regarded as personal privacy. As a matter of fact, guaranteeing privacy is a demanding task to practice in Mongolia both morally and legally, especially for the people who traditionally and culturally had nomadic lifestyles. Therefore, on the one hand educating and enlightening the society is crucial, while the law needs to be amended immediately in order to avoid severe violations of human rights.

3.3 Data Protection in Mongolia

3.3.1 Relevant legislations on data protection

Technological advancement and mass use of the Internet has impacted the need to further enhance legislations on data protection around the world. According to UNCTAD, 128 out of 194 countries in the world had put in place legislation to secure data protection.[119] Mongolia is one of the countries that has not (yet) adopted the law regulating data protection per se. However, it is encouraging that the Government of Mongolia has recently started to take actions in regard to data protection and linked it to the enjoyment of individual right to privacy. In practice, there are a number of human rights violations which occur due to breaches of data

[118] The Law of Mongolia on Privacy of organizations.

[119] 'Data Protection and Privacy Legislation Worldwide' (*UNCTAD*) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 6 May 2021.

protection such as unlawful surveillance, face recognition systems that violate the Constitutional provision on the right to privacy. Thus, there are only a handful of existing national laws exist that regulate data protection for specific purposes.

First of all, a legislation that has provision on data protection is the law of Mongolia on Automated System of Elections which was adopted in November 2011. This law regulates the privacy of voters by defining "the data allowing to establish the personality of the citizen contained in the ID as prescribed by the law, a photo, and unique physical data (fingerprints).[120] Nonetheless, this provision applies only during the elections, not throughout the term. Secondly, the General Law on State Registration of Mongolia that regulates a personal information of citizens by the following provision: "citizen identity card's memory" refers to digital memory, which incorporates personal information of citizen in accordance with law and which enables the information to be written, read and changed."[121] This regulation is applicable for specific purposes of registration, rather than in general purposes, for state and private entities particularly.

Moreover, a few national legislations have provision on data protection within the law, such as the State Registration office, Police office, National Statistics Commission, National Archives of Mongolia, State Bank. In accordance with the Government order No.146, these state entities have responsibility to disseminate data to the National database system. However, it is unclear on how data is used and protected by the state, therefore the cases of unlawful surveillance by state officials have increased in the past few years.

3.3.2 National survey on needs assessment of data protection law

The Communications and Information Technology Authority (CITA) of the Government of Mongolia has conducted a surveillance survey on the needs and assessment of data protection law in 2016. Accordingly, 97% of the total 120 participants use the internet in order to access social media, do bank transactions and communications both at home and work. However, the study shows that 60% of them did not have full control on their privacy online

[120] The Law of Mongolia on the Automated System of Elections. Art 4.1.2 1

[121] The General Law of Mongolia on State Registration. Art 3.1.6.,

and in case of violation, most of the participants responded that they don't know how the compliant mechanism worked. Correspondingly, raising awareness and enlightening the internet and technology users is very important due to the increasing trend. In regards to the Communications Regulatory Commission of Mongolia, the number of Internet users and smartphone users reached to 2,3 million and 2 million respectively since 2016.[122] This is a huge number compared to the whole population, and whether the legislation in this field has put in place accordingly is a daunting issue.

3.3.3 State surveillance

In 2020, the Parliament passed a resolution on approval of the government action plan for 2020-2024 and as part of the plan it states its goal to introduce an integrated camera system, implement a set of measures to prevent, reduce and detect crime, and ensure public security. Accordingly, in line with "Safe city of Ulaanbaatar" initiation, a total of 2000 surveillance cameras were installed around the city in order to prevent and combat criminal conduct. The city's mayor plans to introduce a smart system to recognize faces, and in case of not recognizing, then to find them by their movements, actions and characteristics.[123] While the technology shall be implemented rapidly, there is no general data protection law in place specifically on how collected data is used, processed, protected and which organization is responsible for the operation of the system. In particular, the number of criminal cases of misuse of surveillance camera has increased by state, private entities and individuals. The Law on Crime Prevention states in its Article 30.1.5 that "in accordance with crime prevention and safety around a property, surveillance video access should be merged into the state police office database."[124] Accordingly, the government urges business and private companies as well as state organizations to have surveillance cameras in- and outside of a property. However, all this data being collected by the state is vaguely regulated, especially with regards to further use,

---

[122] 'Main Parameters of the Communications Sector of Mongolia in 2016' (*Communications Regulatory Commission of Mongolia*) <https://crc.gov.mn/en/k/2n9/1H> accessed 2 May 2021.

[123] L.Misheel, 'Public Face Recognition Cameras Violate the Cnstitution' *The UB Post* (Ulaanbaatar, 14 October 2020) <https://www.pressreader.com/mongolia/the-ub-post/20201014/281801401434768>. accessed 29 May 2021

[124] The Law of Mongolia on Crime Prevention.

storage and protection of data. In relation to this, there is a provision under the Criminal Code of Mongolia stating that illegal persecution of others by an officer not authorized to undertake a criminal investigation.[125]

Unfortunately, cases in practice of arbitrary persecution by state and private entities go beyond the boundaries due to the same reason. As a human rights activist and member of Human Rights Commission in Mongolia stressed, the right to personal liberty and safety is protected by the Constitution and in case of intrusion to privacy, there has to be a legal ground. Introducing facial recognition violates the Constitution provision. In this particular case where the city installs surveillance cameras with face detectors, then it has to comply with specific norms and rules. Also, the scope of use as well as protection of data should be clearly regulated.[126] The truth is, such, data is very prone to any invasion or use in unlawful persecution and bullying by anyone who has data. In relation to cyber-attack, Mongolia barely allocated any state budget to fight against cyber-attack likely. And to make matters worse, all these surveillance cameras are purchased from neighboring China, which means a willful tradeoff of big data to another country. According to a legal journal article, in 2019 a total of 31,524 criminal cases were registered and of those 20,261 were conducted in the capital city, where the half of Mongolia's population of 1.5 million resides.[127] Assuming that in order to investigate more than 20 thousand criminals, the whole citizens are unlawfully surveilled and persecuted without their own consent. Introducing and using new technologies for various good reasons is encouraging, however, the state should carefully consider the consequences or harm that potentially might bring to the national security and individuals as well. The need for a balance between security and privacy is utterly important.

Besides this, not only is surveillance camera data not protected in Mongolia, but also individuals use video devices in order to collect personal information unlawfully and misuse it for the purpose of defamation and bullying. Unlawfully acquiring and disclosing personal secrets without consent is subject to criminal sanction under the Criminal Code of Mongolia. According to the law on Personal Privacy, it implies that when personal information is lawfully

---

[125] Criminal Code. Art 13.12

[126] '2000 Face Detector Cameras and Its Side Notes' *I see* (Ulaanbaatar, 20 June 2020) <http://isee.mn/n/10805>. accessed 3 June 2021

[127] S.Uyanga, 'Face Detector System and Human Rights, Personal Privacy' *Zuunii medee* (Ulaanbaatar, 15 September 2020) <http://www.zms.mn/a/80711>. accessed on 3 June 2021

transferred to another party, such a receiving party is prohibited from transferring the information to third parties.[128] Therefore, it is still unclear whether such prohibition applies even after such information is disclosed.

3.3.4 Use of the Internet and digital technology

As mentioned in the previous chapter, the more people access the Internet and use digital devices, the more privacy legislation should further be elaborated. Specifically, during the world pandemic, almost every aspect of our lives has digitized, and the use of the internet and digital devices has increased dramatically fast not only in Mongolia but in the whole world. As a consequence of abrupt digital transformation, the number of cyber-crimes has increased exponentially. For instance, according to the Mongolian Police Agency, 57 cases of cyber-crime were registered in 2019, while by September of 2020 the number had reached to 114.[129] The Government of Mongolia bans and filters sexually explicit contents on social media, however, except for this regulation people enjoy the rights to access information and free speech. Looking at the most recent survey conducted by the CITA, separate entity than the Communications Regulatory Commission of Mongolia, which was discussed earlier, in 2019, the number of the Internet users reached to 2,910,000 and interestingly, Mongolia has 2.2 million Facebook users and 2.1 million of them are connected to Facebook through mobile phone.[130] Therefore, social media platforms play a pivotal role in economic, political and social activities. In particular, 25% of people use e-commerce and the majority of transactions are made through the social media.[131] Moreover, the UNICTAD has recommended setting personal data protection regulations.[132] Additionally, there is no state regulation to restrict the Internet users in Mongolia to access any domestic and foreign websites and to join social media. The

---

[128] The Law of Mongolia on Personal Privacy.

[129] 'Department of Cyber-Crime Prevention' (*National Police Agency of Mongolia*) <https://police.gov.mn/a/3833> accessed 23 May 2021.

[130] 'Main Parameters of the Communications Sector of Mongolia in 2016' (n 122).

[131] ibid.

[132] UNCTAD, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' [2016] United Nations Conference on Trade and Development 154 <https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf%0Ahttp://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf>. accessed 21 May 2021

Mongolian Government adopted resolution No1 on "Unified System of Comments in Websites" in 2013. As per this resolution, the CRC was assigned to develop a regulatory procedure on requirements for news websites and issuing domain names. The National Data Center will ensure the technical reliability of this Unified System of Comments and the General Authority for State Registration will register the information of users who post comments on websites based on their civil data and the database of mobile phone users. The resolution on restricting the right to online anonymity is still in effect.

3.3.5 Introduction of the E-Mongolia project

Mongolia's long-term development policy "Vision-2050" and the Government's Action Program for 2020-2024 outlined works to digitize government services step by step. The "Vision 2050" policy has the goal of setting plans for the three decades 2021-2030, 2031-2040 and 2041-2050 goals consecutively. On the first chapter it proposes to "establish smart and sustainable governance that ensures the development of Mongolian people, mature civil service with well-organized administrative structure, shift to citizen-centered public services based on electronic technology, expand public-private civil society cooperation in all fields, fully respect human rights and strengthen a system of justice that is mature and free of corruption" under the fifth goal of Good governance.[133] Under this policy initiation, the Communications and Information Technology Authority launched "E-Mongolia" unified digital service system on 1 October, 2020. The system offers 181 services of 23 government organizations. According to the CITA survey conducted in 2019, with the advent of "E-Barimt", the unified Value Added Tax (VAT) promotion system that was introduced in 2016, there is a total of 1,7 million people who use the system.[134] The Government claims that the digital transformation through the E-Mongolia initiative has great impact for the sparsely populated Mongolians both economically and time efficiently. The head of CITA highlights that one citizen receives six types of services in a year, meaning that they spend at least 2 hours on average to obtain government services in a traditional form, taking into account the time to be spent on traffic congestion and service

[133] 'Mongolia Today' [2015] Mongolia in the Twentieth Century: Landlocked Cosmopolitan 16 <https://cabinet.gov.mn/wp-content/uploads/MT2020-5-last-compressed.pdf>. accessed 4 May 2021

[134] ibid.

queues and bureaucracies.[135] Moreover, besides the increasing number of state services, the plan is to have public services find citizens using the advances in artificial intelligence rather than having the citizens seek them. However, this mass data collection and processing regulations still need to be adopted by the government. Without a doubt that every new initiative that benefits the majority has a great impact. However, without proper and adequate governance and regulations, the consequences are more harmful.

3.3.6 Draft law on Data Protection

Action Plan of the Government of Mongolia for 2020-2024, under the provision of "E-Mongolia" Responsive Public Service, Article 4.1.2 states to create a legal environment that respects human rights, promotes e-governance, and regulates technological safety, and take public-private partnership into a new level of development, and Article 4.1.6 states to strengthen the information safety and security system that ensures the protection of national interests, and completeness, confidentiality and accessibility of public, individual and private sector information and increase its capacity,[136] which demonstrates the urge of Government's action on the importance of protecting and further embellishing the personal data protection. Within this framework, the draft law on Data protection is in the waitlist for discussion and underway to be approved by the Parliament of Mongolia. The draft law has 8 chapters and 29 articles that have specific regulations in regards to collection, process and use of personal data and ensure its security. [137] Moreover, the law is drafted based on needs assessment and the UPR recommendation of 2020 to the Government of Mongolia, which will enable legal frameworks in line with international norms and standards. It is also noted that Mongolia has become a party to thirty-six conventions[138] and drafting the novel law in line with international instruments will be an important step for Mongolia to undertake its obligation under these conventions.

---

[135] ibid.

[136] Approval of the Action Plan of the Government of Mongolia for 2020-2024 2020. accessed on 23 May 2021

[137] ibid.

[138] 'Mongolia - Data Protection Overview' (*One Trust Data Guidance*) <https://www.dataguidance.com/notes/mongolia-data-protection-overview> accessed 18 May 2021.

Moreover, the Government of Mongolia established the Standing Committee on Innovation and Digital Policy in charge of accelerating ICT development and an improvement of legislations. Accordingly, as data duplication in private sectors and state entities is an emerging issue in the field, the government plans to integrate the partnership through robust regulations. The integration will be exercised by advancing legal frameworks on personal information privacy and e-governance among all stakeholders including the state, business and citizens. In particular, members of the Parliament and head of the Standing Committee plays a leading role in promoting and accelerating the initiative by urging the government to adopt necessary law and regulations, particularly, the package laws reflecting new regulations on information security, privacy, protection, data maintenance and e-communications among public organizations, private entities and citizens.

3.4 Interim conclusion

From the Silk road to horse rail postal system, the Great Mongolian empire marked a significant footprint in modern civilization of the world. Mongolia has an abundant culture, and especially the way of dwelling as pastoral nomads in the "yurt" has impacted people's mindset significantly. For a young democratic country like Mongolia, it is remarkable that the speed of civilization has taken place quite fast so that the people nowadays enjoy core rights in accordance with the democratic constitution. Despite the country's location between the two great powers and with only a population of 3 million, the use of the Internet and digital devices are quite remarkable. However, the enjoyment and protection of these rights should go hand in hand. In Mongolia's context, vague and broadly drafted law on the Personal Privacy is not enough to handle the modern relation. Moreover, with the emergence and the use of ICTs, one's privacy is violated frequently without the owner's knowledge. To make matters worse, it is daunting to observe that the country itself trades the state privacy by purchasing and using the neighboring countries' devices, whereas developed countries spend many resources in order to protect the privacy. Privacy is about the individual rights and national security which is central to preserving and maintaining democracy. All in all, the rise of the government's attention to data protection is a significant step to further protect the core values of democracy.

4. THE RIGHT TO PRIVACY AND DATA PROTECTION IN THE EUROPE

4.1 Introduction

Privacy is a fundamental right that is enshrined in core international instruments including the ICCPR.[139] The Covenant has been ratified by 165 States[140] including all the EU and Council of Europe (CoE) Member States. Explicitly, the right to privacy is attained the constitutional right across the EU and means of sustainable democracy. Scholars in the field claim that there is no democracy without privacy and it is prerequisite to a non-totalitarian state.[141] Rossler stresses in his work that it is difficult to imagine being able to enjoy the freedom of expression, freedom of association or freedom of religion without some accompanying right to privacy.[142] Indeed, these statements clearly demonstrate that core rights of democracy are intertwined with privacy. In the EU, human dignity is recognized as an absolute fundamental right and respect of fundamental rights is part of the constitutional principles of the EU.[143] In this notion, privacy is closely connected to human dignity and it is equally protected as a fundamental right. Regarding the human rights legislations, the right to privacy is safeguarded through both the EU and CoE instruments. Specifically, the EUCFR guarantees the fundamental rights enjoyed by people within the territory of the 27 Member States. The Charter applies "only when they are implementing the Union law"[144] and the CJEU in Luxemburg examines the legality of the EU measures and ensures the application of EU law.[145] Moreover, the ECHR is an important

---

[139] International Covenant on Civil and Political Rights 1966. Art 17, Right to Privacy, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation"

[140] Martin Scheinin, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism' (2009).

[141] Beate Roessler and Dorota Mokrosinska, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015).

[142] ibid.*236*

[143] *Joined Cases C-402/05 P and C-415/05 P Kadi and Al Barakaat International Foundation v Council and Commission* (2008) ECR I-6351 para 285.

[144] Charter of Fundamental Rights of the European Union 2012 para 51(1).

[145] 'The Court of Justice in the Legal Order of the European Union' (*Court of Justice of the European Union*) <https://curia.europa.eu/jcms/jcms/Jo2_7024/en/> accessed 13 June 2021.

international treaty that protects and promotes human rights within all 47 State Parties of the CoE including non-EU states such as Switzerland, Russia and Turkey. The final arbiter of the Convention is the ECtHR in Strasbourg. Both the ECHR and the EUCFR have provisions on privacy in Article 8 and Article 7 respectively and both systems play a complimentary role and are closely linked to each other. However, the Court interprets Article 8 of the ECHR in a manner that includes a right to data protection and data protection jurisdictions interpreted in accordance with this Article.[146] Interestingly, the Data Protection Convention or Convention 108 for data protection regulation does not fall under the jurisdiction of the Strasbourg Court. Additionally, the EU made a significant impact on separating data protection from privacy. Specifically, Article 8 of the EUCFR guarantees the right to data protection as a fundamental right, which makes a clear distinction with the right to privacy. The CJEU reasoned that compared to the right to privacy as enshrined in the ECHR, the EU rules on data protection create a specific and reinforced system of protection.[147] Indeed, the EU adopted a strong regulating instrument on data protection that is acknowledged not only in the region but also in other countries.

4.2 Right to Privacy in Europe – The Right to Privacy in the ECHR and ECtHR case law

As mentioned above in this study, interpretation and application of the ECHR and EUCFR is brought to ECtHR and CJEU respectively. However, due to the fact that CJEU interprets not only the Charter but EU law[148] in general and also Charter correspond to rights guaranteed by the ECHR,[149] meaning the Charter subsequently follows the ECHR practice. Therefore, the author will examine the topic mostly in relation to the ECtHR jurisdictions and some important principles of Article 8(1) and 8(2) of ECHR.

---

[146] *Amann v Switzerland* (2000) 27798/95 para 65.

[147] *European Commission v The Bavarian Lager* (2010) C-28/08 P para 60.

[148] 'Overview of Court of Justice of the European Union' (*European Union*) <https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en> accessed 15 June 2021.

[149] 'Article 52 - Scope and Interpretation of EU Charter of Fundamental Rights' (*EU Agency for Fundamental Rights*) para 3 <https://fra.europa.eu/en/eu-charter/article/52-scope-and-interpretation-rights-and-principles> accessed 15 June 2021.

4.2.1 Article 8 (1): Private life, family life, home, and correspondence

ECtHR and CJEU both interpret "private life" not to be restrictive. The Luxembourg Court interprets the jurisprudence from Strasbourg as meaning that "private life" includes the protection of personal data, being defined as any information relating to an identified or identifiable individual.[150] The fundamental right to protection of personal data is not an absolute right and may be limited, however the right has a very broad interpretation within the relevant EU law, the GDPR. The ECtHR established the case law relating to the "private life" of an individual within the Article 8(1) pointing out the respect for private life comprises the right to establish and develop relationships with other human beings; furthermore there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life."[151] The collection, storage, or disclosure of information relating to private life interferes with the right to privacy.[152] Interference requires justification; that is, under Article 8 of the ECHR it must be in accordance with the law, it must pursue one or more legitimate aims and, in addition, it must be 'necessary in a democratic society' to achieve those aims.[153]

The Court interprets "family life" as an autonomous right linking to the right to live together so that family members enjoy each other's company.[154] In this regard, each family members right is considered under this provision, such as marriage, parenthood and the child's rights. In particular, the child's legal status, adoption, relationship with biological parents, and so forth are connected to the right to privacy. Accordingly, this notion expands into a wide range of complex family relation.

Furthermore, "home" is not limited to traditional residences, as such the Court defined home with much broader conception. Particularly, home is not limited to property of which the applicant is the owner or tenant, while it extends into long-term occupancy such as on an annual

---

[150] *Joined cases C-92/09 and C-93/09* (2010) ECR I-1106 para 52.

[151] *Niemietz v Germany* (1992) 72/1991/32 pp. 33.

[152] *Amann v Switzerland* (2000). 27798/95 para 69

[153] ibid.

[154] *Olsson v Sweden* (1988) 10465/83 para 59

basis, for long periods, of a house belonging to a relative.[155] Accordingly, the interference and invasion to home without an adequate legal ground violates this Article.

Lastly, "correspondence" is regarded as communication tools that the confidentiality is meant to be protected. These can be telephone conversions, written correspondence, electronic messages, emails, and private radio broadcasting, not including broadcasts on a public wavelength that are accessible to others.[156] Moreover, all communications in addition to sensitive correspondence such as between prisoners, doctors, lawyers, are considered under this provision.

4.2.2 Article 8 (2): In accordance with law

It is necessary to highlight the importance of Article 8(2) of the ECHR principles under the framework. According to *Benedik v. Slovenia* case law, it reinforces the importance of a legal basis in the case that "interference is foreseeable."[157] In other words, in order to meet the "in accordance with law" principle, interference should be foreseeable. In particular, the Court is of the view that the law on which the contested measure, that is the obtaining by the police of subscriber information associated with the dynamic IP address in question was located and the way it was applied by the domestic courts lacked clarity and did not offer sufficient safeguards against arbitrary interference with Article 8 rights.[158] In these circumstances, the Court finds that the interference with the applicant's right to respect for his private life was not "in accordance with the law" as required by Article 8(2) of the Convention.

In another case law, the ECtHR interpreted "in accordance with law" as "the phrase relates to the quality of the law, requiring it to be compatible with the rule of law and this follows from the object and purpose of Article 8 that there must be a measure of legal protection in domestic law against arbitrary interference by public authorities with the rights safeguarded by

---

[155] *Mentes and others v Turkey* (1997) 23186/94 para73

[156] *B.C. v Switzerland* (1995) 21353/93

[157] *Benedik v Slovenia* (2014) 62357/14.

[158] ibid.

paragraph."[159] Therefore, the domestic law has to indicate the scope and conditions of exercise of the authorities' discretionary power in the area under consideration.[160] The Court need not examine whether the measure had a legitimate aim and was proportionate as these indicators serve as pivotal principles of rule of law.

Moreover, in regards to the *Zakharov v. Russia* case, "foreseeable" is interpreted as meaning that any surveillance or investigation by the state of an individual has to be conducted lawfully and must meet quality requirements such as accessibility to the person concerned, who must be able to foresee its consequences and compatible with the rule of law.[161] Especially "where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident and it is therefore essential to have clear, detailed rules on interception."[162] In this sense, it is evident that the more the government action is implemented transparently, the better democracy is exercised. Therefore, the domestic law must be "sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures."[163]

4.2.3 Article 8(2): Necessary in a democratic society

One of the core elements of democratic society is the state's duty to protect. Maintaining national security is central to this element, however, states invade privacy under this duty by unlawful surveillance and interference. For the European context, the ECtHR noted that fostering democracy could both support and oppose the use of secret surveillance. In *Klass v. Germany* case, the Court states that "democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order to effectively to counter such threats, to undertake the secret surveillance of

[159] *Amann v Switzerland* (n 146). Para 56

[160] ibid. para. 62

[161] *Roman Zakharov v Russia* (2015) 47143/06 para 228.

[162] ibid.

[163] ibid.

subversive elements operating within its jurisdiction."[164] In general, the Court acknowledges the importance of use of technologies in order to prevent crime in the interest of national security. According to the literature, this reason for interference must be in accordance with the nature of legitimate aim.[165] In regards to assessing whether an interference in Article 8(2) rights is "necessary in a democratic society," the Court considers whether the measures were proportionate to the legitimate aims.[166] When determining whether an interference was "necessary", the Court will consider the margin of appreciation left to the State authorities. It is a duty of the respondent State to demonstrate the existence of a pressing social need behind the interference.[167] The Strasbourg Court maintains that "any interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued."[168] In this connection, it considers that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of interference involved.[169]

4.2.4 Article 8(2): Legitimate aim

The case law of the Court indicates that there is a basic understanding that democracy diminishes when privacy is neglected. Hughes accurately states that a healthy democratic state will enable its citizens to live independent and informed lives.[170] The ECHR provides a legitimate aim of interferences by providing a list of grounds, namely "the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms

---

[164] *Klass and others v Germany* (1978) 5029/71.

[165] Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222 <https://doi.org/10.1093/idpl/ipt017>.

[166] *Z v Finland* (1997) 9/1996/627 para 94.

[167] *Piechowicz v Poland* (1998) 38857/97 para 212.

[168] Kokott and Sobotta (n 162).

[169] *Segerstedt-Wiberg and Others v Sweden* (2005) 62332/00 para 88.

[170] Kirsty Hughes, 'The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse' (2015) 225 Social Dimensions of Privacy: Interdisciplinary Perspectives 228.

of others."[171] Any interference by the state authority has to have a legitimate ground in respect to legislation. Solove argues that "preventing disproportionate and unlawful intrusion into privacy serves as a shield to totalitarian states."[172] Otherwise, in case domestic law does not explicitly indicate the legal grounds of state interference, then Article 8 should be discussed in accordance with proportionality and necessity.

4.3 Data Protection – Autonomous Right

4.3.1 Data protection concept

In connection to data protection legislations in European countries' framework, scholars divide the concept into three generations. Firstly, data privacy related concerns spread in the European countries in 1970 due to the large scale of data processing with "computers and privacy issues."[173] Consequently, the CoE's Committee of Ministers adopted non-binding resolutions on the protection of privacy of individuals, especially in electronic data banks with the emergence of computers. The idea behind was that when personal data was to be collected through electronic data banks, the principle had to be fairly obtained, accurate, up-to-date, appropriate, relevant, time-limited, and kept secure. As a result, European countries started to adopt data protection laws prior to the end of 1990. In this development, the Nordic countries were particularly early adopters including Denmark and Norway in 1978 aside from Finland, which only enacted a law in 1981.[174] According to the literature, states adopting data protection

[171] Kokott and Sobotta (n 162).

[172] Daniel J Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2000) 53 Stan. L. Rev. 1393.

[173]Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer Science & Business 2014).

[174] Paddy Leerssen, 'European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?' 38.

prior to the 1980s tended to have become aware of human rights concerns deriving from data processing.[175]

Secondly, from 1990 to 2010, the notion of processing personal data was introduced. Particularly, the EU considered that ensuring free flow of personal data between Member States should not be restricted, thus DPD was adopted in 1995 with EU Member States and later in 1999 with the non-EU European Economic Area States (EEA) of Iceland, Norway and Liechtenstein.[176] In addition to the DPD requirement of transparency to notify data subjects about processing when personal data was obtained, the controller is also obligated to justify the processing of any personal data under one or more of a closed list of legal bases.[177] These provisions indicate the importance of discipline in personal data processing. According to Newman, he stresses the importance of this initiative by highlighting that all EEA States enacted data protection laws in addition to ensuring similar provisions concerning the collection, processing, and transfer of personal information in all sectors with proper enforcing mechanism.[178] Indeed, the DPD paved the way not only in Europe but also outside the region. In this regard, a scholar in the field Bygrave proves by his statement that DPD has continued the most important point of departure for national data privacy initiatives within and, to a large extend outside the EU,[179] which leads the EU to the global standard setter status.

Lastly, from 2010 onwards a major step was taken by the European Commission on proposing a set of measures on data protection by replacing the DPD with the General Data Protection Regulation (GDPR). Scholars claim that the emergence of GDPR was a timely effort in times of rapid advancement of ICTs within the last few decades. The text was adopted in 2016 and law became applicable across the EU on 25 May 2018 and with the wider EEA on 20 July 2018. [180] In addition to the previously established DPD regulations, GDPR reflected both

---

[175] Frits W Hondius, 'Data Law in Europe' (1980) 16 Stan. J. Int'l L. 88.

[176] Leerssen (n 171). p 40

[177] The protection of individuals with regard to the processing of personal data and on the free movement of such data 1995 Art 7.

[178] Abraham L Newman, 'Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive' (2008) 62 International Organization 103 <http://www.jstor.org/stable/40071876>.

[179] Hielke Hijmans, 'Lee A. Bygrave, Data Privacy Law, an International Perspective' (2015) 5 International Data Privacy Law 88 <https://doi.org/10.1093/idpl/ipu031>.

[180] General Data Protection Regulation 2016 Art 99(2).

data protection's new status as a fundamental right in the EU. Most importantly the threats posed by rapid technical developments and globalization, the reform also seeks to ensure a strong and more coherent data protection framework backed up by strong enforcement.[181] The GDPR is a robust instrument mainly because of its enforcement mechanism and high penalty, which will be elaborated more on the next sub chapter.

Data protection regulations have developed fast since 1970 during an uneasy time of major technological and social change. Privacy invasive technologies shift beyond the traditional concept of privacy. Therefore, the EU Member States that share common goals and interests, ultimately moved one step ahead in data protection regulations.

4.3.2 As an autonomous right

As stated above, both the ECHR and the EUCFR have provision of the right to privacy, and the EUCFR specifically guarantees 'the right to the protection of personal data' which confers rights of processing personal data. Data protection is not a later 'spin off' of privacy, but clarifies the conditions through which 'processing of information' concerning the individual becomes legitimate. Some scholars in the field claim that privacy is a substantive right and data protection is procedural.[182] Furthermore the notion of distinguishing between substantive and informational privacy is integral to data protection. Substantive protection allows the individual to engage in daily affairs free from the threat of state coercion or harm, while privacy creates the environment through which informational autonomy can be exercised.[183] The right to the protection of personal data is not an absolute right and therefore, it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. To the author's knowledge, an absolute right cannot be limited or lawfully interfered with, while in contrast it is subject to a balance with other rights or interests. According to the EUCFR, everyone has the right to the protection of

[181] GDPR Recitals 7.

[182] Norberto Nuno Gomes de Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights', *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (Springer 2010).

[183] Helen Fenwick, Kevin Kerrigan and Richard Glancey, *Q&A Civil Liberties and Human Rights 2007-2008* (Routledge 2009).

personal data concerning him or her and such data must be processed fairly for specified purposes.[184] This has the meaning that every individual is entitled to have their personal data protected. Also, there may be security concerns associated with certain instances of data processing. For example, in case of investigation or espionage cases the necessary access by independent authorities poses the risk that confidential data may be disclosed. However, even in such cases it should be possible to identify persons who can be entrusted with the independent control of data protection and the maintenance of confidentiality at the same time.

According to the survey conducted in 2017 on data protection legislation and policies across the EU, the citizens' weekly use of social media networks, instant messaging and chat websites, online banking, online shopping constituted 57%, 53%, 43%, 17% respectively.[185] Overall trend shows the frequent use of the Internet by EU citizens. Regarding the control over personal information, 15% of the citizens were feeling completely in control, while the trend of accepting the processing of personal data constituted 71%, however, only 6% feel comfortable with companies using personal data to tailor advertisements and content.[186] This figure shows that the awareness of data processing among the citizens is quite high, however, trust in business companies on processing personal data is rather low.

Data protection laws have evolved consistently with technological developments and effective data protection regulations empower people with control over personal information. Some scholars argue that data protection is a distinct right and necessary to ensure its continued expansion as "hard law" at EU constitutional level.[187] Especially European countries where the value of democracy is fundamental, protecting individual's private sphere is not an option but rather an important task to maintain. It is central to the protection of human dignity and forms the basis of any democratic society.[188]

---

[184] The Charter of Fundamental Rights of the European Union (n 50). Art 8

[185] Bart Custers and others, 'A Comparison of Data Protection Legislation and Policies across the EU' (2018) 34 Computer Law & Security Review 234 <https://www.sciencedirect.com/science/article/pii/S0267364917302856>.

[186] ibid.

[187] Kokott and Sobotta (n 162).

[188] Warso (n 7).

4.3.3 Data Protection Directive (DPD)

In regards to European citizens' initiative, a ban on biometric mass surveillance practices are highly debated. According to a survey by the Fundamental Rights Agency, 83% of Europeans are against sharing their face data with authorities and 94% are against sharing it with private entities.[189] Therefore, it is claimed that such unlawful mass surveillance violates fundamental rights. The European Parliament and the Council approved the Data Protection Directive within legal frameworks in privacy and data protection in respect to state authorities, particularly police and criminal justice sector. This legal instrument ensures that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action.[190] It protects everyone regardless of whether they are a victim, criminal or witness and must comply with the principles of necessity, proportionality and legality with appropriate safeguards for the individuals.[191] In respect to use of biometric data through CCTV in order to identify an individual, certain minimum levels of quality are required in order to prevent mistakes such as the wrong person being identified or person unable to be identified due to low quality. Therefore, according to the directive, a human intervention and decision is compulsory in order to make impactful decisions based on recognition of a face. State and private entities gather large scales of personal data through various instruments including the CCTV. However, with strict regulations that are in place such as DPD for state entities and GDPR for private entities, people have a better chance to enjoy the rights and freedom in Europe.

4.4. Scope of regulations under the GDPR

The GDPR is the toughest privacy and security law in the world.[192] A number of scholars in the field argue that the GDPR is the standard setter not only in the European context, but also

---

[189] 'Civil Society Initiative for a Ban on Biometric Mass Surveillance Practices' (*European Citizens' Initiative*) <https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en> accessed 14 June 2021.

[190] Max Snijder, 'Biometrics, Surveillance and Privacy' <https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC104392_biometrics_surveillance_and_privacy_final.pdf>.

[191] European Commission, 'Data Protection Revision- Proposal for a Directive' (2012) 0010 COM (2012) 10 final <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN>.

[192] 'What Is GDPR, the EU's New Data Protection Law?' (*GDPR EU*).

for non-EU countries that shape local law in accordance with it. Many of these laws are strongly influenced by the EU rules, which have long been considered the gold standard in data protection law. GDPR applies to all "processing of personal data" regarding the EU and its citizens[193] or is often referred to as personally identifiable information (PII), belonging to any living citizen of, or any living individual, no matter the nationality, residing in the EU who must comply with the Regulation.[194] The GDPR consists of 11 chapters, 99 articles and 173 recitals, that builds upon many longstanding concepts in European data protection law, which provides comprehensive and exhaustive regulations.

4.4.1 Principles

The main principles of data processing are addressed on the GDPR Article 5 and in case of failing to follow these principles could result in a maximum fine of 20 million euros, which is forty times higher than the DPD. The principle of personal data shall be lawful, fair, transparent[195] processing of data. Specifically, 'lawful' means processing operations must be in full compliance with the regulation; 'fair' data collection must be minimized and limited to its state purpose and 'transparent' means all aspects of processing and data collection must be initiated to the data subject and relevant authorities.[196] All collected data should be used to fulfill a necessary purpose. In order to ensure that personal data is not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review and personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of personal data and equipment used for the processing.[197]

---

[193] General Data Protection Regulation (n 177). Art 2

[194] Mark Foulsham, Brian Hitchen and Andrew Denley, *GDPR: How To Achieve and Maintain Compliance* (Routledge 2019).

[195] General Data Protection Regulation (n 177). Art 5.1 (a)

[196] Sanjay Sharma, *Data Privacy and GDPR Handbook* (John Wiley & Sons 2019).

[197] GDPR Recitals (n 178). 39

4.4.2 Scope of regulations

In order to determine the scope of regulations under the GDPR, it is essential to define the key stakeholders such as controller and processor of personal data, which are subject to Article 4.7 and 4.8 of the Regulation respectively. The Controller can be a natural person, legal entity, public authority, public agency, or other body that shoulders the most responsibility under GDPR and determines the purposes and means of the processing of personal data.[198] While the processor is an entity that processes personal data on behalf of the controller.[199] The processor has a more limited compliance than the controller and is able to make daily operational decisions in line with a controller's instruction. It is the controller that makes decisions about processing activities and exercises overall control of personal data being processed and are ultimately in charge of and responsible for the processing.[200] Under the GDPR, processing comprises any set of operations or treatments performed on personal data, regardless of whether it is carried out manually or with the help of automated mechanisms.[201]

In respect to definition of personal data, article 4 (1) of the GDPR defines it as 'any information' relating to an identified or identifiable natural person and a list of identifying information such as a name, an identification number, location data. Under this provision, personal data has quite a broad concept and due to the research conducted in measuring the concept, it implies "where there is a reasonable risk of identification, data ought to be treated as personal data, whereas risk is merely negligent, data can be treated as non-personal data".[202] 'Any information' includes "objective" information, such as an individual's height, and "subjective" information, like employment evaluations and also not limited to any particular format. For example, a child's drawing of their family that is done as part of a psychiatric evaluation to determine how they feel about different members of their family could be considered personal data, insofar as this picture reveals information relating to the child (their

---

[198] General Data Protection Regulation (n 177). Art 4 (7)

[199] ibid. Art 4 (8)

[200] 'What Are "Controllers" and "Processors"?' (*Information Commissioner's Office*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/> accessed 12 June 2021.

[201] General Data Protection Regulation (n 177). Art 4.2

[202] GDPR Recitals (n 178). 26

mental health as evaluated by a psychiatrist) and their parents' behavior.[203] The definition of personal data is not restricted to data of an identified person but also an identifiable person because of the relative ease of linking personal information to identify a person using technology.[204] Accordingly, the term is quite broad that indeed can relate to an individual based on reasonable risk of identification.

Moreover, the regulation only affords protection to the personal data of natural persons, which implies that legal persons such as companies are not provided protection. The EUCJ has excluded legal persons from data protection, though they can rely on the right to privacy.[205] Similarly the binding French version of the Convention uses the clearer term 'personne physique' that also excludes legal persons.[206]

4.4.3 Lawful processing

An entity that processes personal data, has to have justifications in accordance with the Regulation. Article 6 of the Regulation states lawfulness of processing personal data in several instances. These include consent by the data subject; performance of a contract; compliance with a legal obligation and so forth where each interpretation can be found from the recitals. If these requirements are not met then data is not to be processed under the GDPR. Moreover, Member States have a right to introduce more specific provisions to adapt the application of the Regulation.[207]

4.4.4 Territorial scope

---

[203] 'What Is Considered Personal Data under the EU GDPR?' (*GDPR EU*) <https://gdpr.eu/eu-gdpr-personal-data/> accessed 21 June 2021.

[204] GDPR Recitals (n 178). 26

[205] *Joined Cases C–92/09 and C–93/09 Volker und Markus Schecke and Eifert* (2011) OJ C 13, 1 para 52.

[206] Kokott and Sobotta (n 162). P 225

[207] General Data Protection Regulation (n 177). Art 6

Use of the internet and processing of data has no territorial dimensions or anyone who is on one side of the world can make a purchase from the other side of the world. Data protection laws are national but in the online environment, data does not respect borders. Under the GDPR regulations, Article 3 indicates the territorial scope which no matter if the processing takes place in or is not established in the Union, the Regulation is subject to the offering of goods or services in the Union or the monitoring of their behavior as far as their behavior takes place in the Union.[208] Furthermore, the processing of personal data which is in the Union, where the controller or a processor is not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services in one or more Member States of the Union as well as the use of language or a currency generally used in one or more Member States of the Union.[209] In other words a company based in a third country that provides service to the European countries where the website language and currency is in service providing countries' context then this company is subject to the GDPR. Moreover, when data-collection activities based outside the EU, it is mandatory for the Controller to designate a representative[210] and shall be based in the EU in one of the Member States where the subject matter of processing takes place.[211]

4.4.5 Derogation

Certain categories of personal data processing are exempted from regulation such as activities that fall outside of EU law; processing by competent authorities for crime including prevention, detection, investigation, prosecution, penalty execution, safeguarding and prevention of threats to public security.[212] Particularly, GDPR permits the processing of personal data for a purpose other than that for which it has been collected which is not based

[208] ibid. Art 3 (1-2)

[209] GDPR Recitals (n 178). 23

[210] General Data Protection Regulation (n 177). Art 27

[211] ibid.

[212] ibid. Art 2(2)

on the user's consent or on the law.[213] This leeway is granted if such processing is a necessary measure in a "democratic society" to safeguard the objectives of the restrictions placed on processing under Article 23 of the Regulation.[214] In connection to this, processing for purposes which is neither based on Consent nor based on EU or Member Law is allowed if such action is necessary, proportionate and a measure in a "democratic society" to safeguard the objectives of the restrictions.[215] As mentioned earlier in order to maintain the balance between other rights, the compatibility test is exercised in these particular circumstances. If the above mentioned requirements are fulfilled, processing for undisclosed purposes is permitted by the Controller. However, when making that judgement as to further processing, the Controller must ascertain whether the new purpose of processing is compatible with the purpose for which it was collected. This is done by considering the link between the purpose of collection and further processing; the context of collection, specifically the relationship between the Controller and the user; the nature of personal data collected, specifically special categories of data or criminal conviction data; and the possible consequences of further processing and the existence of security in the processing such as pseudonymization or encryption.[216] The balancing should be done in a way that protects the fundamental rights and interests of others.

4.4.6 Sensitive data

Article 9 of the Regulation prohibits processing of personal data that refers to special categories. These include racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and genetic data, and biometric data concerning a person's sex life or sexual orientation.[217] Personal data which is by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their

---

[213] Paul Voigt and Axel Von dem Bussche, 'The Eu General Data Protection Regulation (Gdpr)' (2017) 10 A Practical Guide, 1st Ed., Cham: Springer International Publishing 12.

[214] Sharma and Menon (n 80). P 145

[215] *ibid* p.144

[216] *Ibid* p.145

[217] General Data Protection Regulation (n 177). Art 9(1)

processing could create significant risks to the fundamental rights and freedom.[218] The GDPR has more tighter controls by including genetic and biometric data to the regulation compared to the DPD. Article 9 states the cases subject to lawful processing of sensitive data in certain circumstances. With the control of official authority and authorized by the Union Member State, processing of personal data relating to criminal convictions and offences can be carried out in respect to the Article 10 of the Regulation.

4.4.7 Enforcement

With the single set of rules that is applicable in all European Member States on processing data among citizens, businesses, public administration and other organization, Data Protection Authorities (DPA) or the Supervisory Authorities (SA) are given the power to investigate, detect and punish violations as well as the responsibility to raise awareness of data protection rights and obligations of the data protection law. The SA is an independent public authority that has public authorities in each EU Member State and whose main responsibility is to monitor the application of GDPR, protect the fundamental rights in relation to processing, facilitate the free flow of information throughout the EU, contribute to the consistent application of GDPR throughout the EU by cooperating with other SAs and the Commission.[219] Articles from 51 to 59 and Recitals 117 to 123 of the GDPR contains regulations in respect to supervisory including conditions for the members, rules in the establishment, competence, tasks and so forth. One of the important tasks of the SA is advisory duties such as promoting knowledge and compliance. Any rule without a proper follow-up and awareness raising mechanism among the population has a short life, while the SA's tasks make the GDPR consistent and robust for the long run. SAs are independent from any political, government, or other influence. In the EU the requirement for SAs to be independent is laid down in law: Article 16(2) of the Treaty on the Functioning of the EU (TFEU) and Article 8(3) of the EUCFR. The CJEU, has consistently emphasized that control by an independent authority is an essential component of the right to data protection and has laid down the criteria for such independence.

---

[218] GDPR Recitals (n 178). 51

[219] General Data Protection Regulation (n 177). Art 51(1)

The EU Data Protection Board (DPB) is formerly known as the Working Party that played the oversight function. The DPB consists of the head of one SA of each EU Member State[220] and is an independent monitoring body tasked with issuing guidelines, recommendations, and best practices on data protection; making final decisions on conflicts in the cooperation and consistency mechanism.[221] Specifically, when the cooperation mechanism fails, the DPB takes part in reaching a consensus among SAs and considers the matter and issues binding decisions to resolve the disagreement.[222]

With the abovementioned properly functional overseeing, law enforcing mechanisms, the GDPR enforcement in the EEA countries is extensively strict. In addition to this, Article 83 of the Regulation states general conditions for imposing administrative fines. Article 83 (4) and (5) specifically indicate that the infringement of the provisions under the articles shall be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year[223] or 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[224] This amount of high penalty would make business enterprises bankrupt or heavily impact. Therefore, no entity would risk violating the Regulation but would instead attempt to follow accordingly.

4.5 Interim conclusion

This chapter discussed the right to privacy and data protection in the European context. Particularly, the right to privacy was explained through the ECtHR case law in accordance with core elements of Article 8 of the ECHR. Meanwhile the EU data protection instruments that scholars claimed to be the global standard setter were studied in accordance with DPD and GDPR. Accordingly, not only are data protection legislations advanced in Europe, but a

[220] ibid., Art 68(3)

[221] ibid., Art 68–76

[222] ibid., Art 64 and 65

[223] ibid., Art 83(4)

[224] ibid., Art 83(5)

fundamental right to privacy is protected through both ECHR and EUCFR. Most importantly, every concept within Article 8 of the ECHR is interpreted by the Court case law, which significantly removes the ambiguity and uncertainty of the law. In regards to data protection regulations, having two separate legislations such as one regulating state investigation and the other for personal data control, make a compelling contribution in data regulating legislations. Moreover, law enforcing mechanisms play a crucial role in making the laws more robust and sustainable. All in all, the processing of personal data is designed to serve mankind and indeed in Europe, the legislations are in place followed accordingly.

5. CONCLUSION

This study conducted in-depth research into the right to privacy and data protection in the context of the recently democratized country of Mongolia in comparison to the European legal frameworks. Due to the democratization after the collapse of Soviet Union and rapid pace of globalization, the transition shift has impacted the nomadic people's mindset significantly. Particularly, for the people that have lived in tribal communities in a yurt for centuries, the notion of privacy is not so prevalent considering the collectivist culture. Whereas, in European countries where the culture is primarily focused on individualism, privacy and respect of an individual's personal sphere has been a settled discussion since long ago. Even the home development, and the standard of housing regulation to have separate rooms for each family members was introduced centuries ago in the Europe. The main concept of privacy was derived from ancient times, where the distinction of public and private sphere was introduced by Aristotle, and nowadays these theories have blossomed in accordance with the human rights core principles inter alia one's autonomy and self-determination. The right to privacy is "recognized by a majority of constitutions worldwide"[225] and it is a fundamental right that is guaranteed in the ECHR in 1950. The ECtHR interpretation of law is very extensive so the gap or ambiguity is rarely known.

The proliferation of both ICTs and the Internet has changed the nature of traditional concepts of privacy. According to this research's findings, data protection has been tied into privacy and oftentimes they overlap. However, it is crucial to emphasize that the adoption of the EUCFR made a clear line of privacy and data protection by the Articles 7 and 8 respectively. Due to extensive interpretation of case law, the ambiguity among the society is quite less. Legislative measures taken by the EU and CoE make a remarkable impact on privacy and data protection. Particularly, recognizing data protection as a fundamental right through the EUCFR has been an important step to further develop legislations on data protection and processing. Moreover, in accordance with personal data and data processing legislations, DPD of 1995 was replaced by the more comprehensive and tougher law of the GDPR. The EU has extensive legislations on data protection and strong law enforcement mechanism, which is integral to sustainable and robust law implementation. For instance, the violation of the GDPR has the

[225] Simon Davies David Banisar, 'Privacy and Human Rights: An International Survey of Privacy Laws and Practice' <http://www.gilc.org/privacy/survey/ intro.html.> accessed 11 April 2021.

highest penalty up to the firm's worldwide annual revenue, which can cause a business entity to be in an unstable condition. Overall, most prominent scholars claim that these regulations have a global impact that set standards in non-European countries in the field.

Whereas in Mongolia, legal frameworks in respect to the right to privacy and data protection is very weak. Accordingly, several actions need to be taken in order to protect the right to privacy and data protection in Mongolia.

Firstly, the sole law on Personal privacy of 1995 was generally drafted that does not explicitly protect the right in accordance with rapid evolution of modern society. In practice, the narrow definition of personal privacy does not adequately protect an individual fundamental right to privacy. Mongolia's legal system is based on civil law, therefore there is no practice of case law interpretation. Consequently, the number of cases brought up to court is very limited. Only a few cases on the right to privacy are ruled by court, and sanctions were prescribed in accordance with the Criminal Code, which is deemed to be harsh and severe. There are relatively different practices in the private sector due to the lack of regulations on processing personal data. The absence of a holistic set of norms and regulations exacerbates the vulnerable socioeconomic context, therefore it leads to a number of human rights violations. Therefore, the law on privacy needs to be updated immediately in line with international norms and standards.

Secondly, as discussed on the third chapter, due to the political instability and frequent turnover of the government, law implementation and enforcement in the country is very inconsistent. There is no separate body to monitor law implementations apart from the Ministry of Justice. The legacy of state policies and laws are critically unsettled. Accordingly, ambiguity or civil disobedience to law is quite common in Mongolia. Therefore, establishing an independent law enforcing mechanism similar to the EU law enforcing body is crucial in Mongolia. The missing gap to enhance the public awareness and diminish social vulnerabilities and inequalities due to violation of rights will be covered this way.

Thirdly, in respect to significant use of the Internet and social media by Mongolians, it is necessary to promptly adopt the draft law on data protection. Although, it is crucial to precisely define the privacy connotation on the law beforehand. This way the ambiguity of the law application will be interpreted accordingly and the challenges faced as a result of technological advancement will be addressed properly.

Lastly, not only the law regulating personal data for companies and individuals has not been put in place yet but also it lacks a law regulating state operations on surveillance. Especially, mass data collection as a result of state surveillance has increased significantly fast last few years and a lack of legal framework on this violates one's privacy severely in Mongolia. Therefore, it should be further elaborated in order to protect one's data and privacy from misuse and interference.

In general, introducing new laws in accordance with international treaty obligations is important, however, the regulations have to be carefully developed in accordance with human rights principles. Adoption of a new law on data protection and upgrading the current law on privacy is a pressing task to Mongolia. To the author's extent of research, there was limited research conducted by experts on the right to privacy and data protection in Mongolia. This showcases the inadequacy of legislation and implementation of it. This research findings demonstrate the extend where Mongolia needs to improve in terms of the right to privacy and data protection in comparison with the European legal frameworks.

BIBLIOGRAPHY

BOOKS AND ARTICLES

Bayly CA, 'The Birth of the Modern World, 1780-1914: Global Connections and Comparisons' [2004] Malden, MA: Oxford: Blackwell

Becker M, 'Privacy in the Digital Age: Comparing and Contrasting Individual versus Social Approaches towards Privacy' (2019) 21 Ethics and Information Technology 307 <https://doi.org/10.1007/s10676-019-09508-z>

Bloustein EJ, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser'' (1964) 39 New York University Law Review 971 <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/nylr39&id=997&men_tab=srchresults> accessed 2 May 2021

Canovan M and Arendt H, *The Human Condition* (University of Chicago Press 1998)

Corlett JA, 'The Nature and Value of the Moral Right to Privacy' (2002) 16 Public Affairs Quarterly 329 <http://www.jstor.org/stable/40441333> accessed 3 April 2021

Custers B and others, 'A Comparison of Data Protection Legislation and Policies across the EU' (2018) 34 Computer Law & Security Review 234 <https://www.sciencedirect.com/science/article/pii/S0267364917302856> accessed 20 May 2021

Dalla Corte L, 'A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection' [2020] Data protection and privacy 27

David Banisar SD, 'Privacy and Human Rights: An International Survey of Privacy Laws and Practice' <http://www.gilc.org/privacy/survey/ intro.html.> accessed 11 April 2021

De Andrade NNG, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights', *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (Springer 2010)

De Hert P and Gutwirth S, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' [2006] Privacy and the criminal law 61

Desai AC, 'Wiretapping before the Wires: The Post Office and the Birth of Communications Privacy' (2007) 60 Stanford Law Review 553 <http://www.jstor.org/stable/40040416> accessed 13 April 2021

Fenwick H, Kerrigan K and Glancey R, *Q&A Civil Liberties and Human Rights 2007-2008* (Routledge 2009)

Fletcher J, 'The Mongols: Ecological and Social Perspectives' (1986) 46 Harvard Journal of Asiatic Studies 11 <https://www.jstor.org/stable/2719074?seq=1#metadata_info_tab_contents> accessed 11 April 2021

Floridi L, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29 Philosophy & Technology 307 <https://doi.org/10.1007/s13347-016-0220-8> accessed 14 May 2021

Foulsham M, Hitchen B and Denley A, *GDPR: How To Achieve and Maintain Compliance* (Routledge 2019)

Francis LP, 'Privacy and Confidentiality: The Importance of Context' (2008) 91 The Monist 52 <http://www.jstor.org/stable/27904065> accessed 29 May 2021

Froomkin AM, 'The Death of Privacy?' (2000) 52 Stanford Law Review 1461 <http://www.jstor.org/stable/1229519> accessed 11 May 2021

Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer Science & Business 2014)

Gaukroger C, 'Privacy and the Importance of "Getting Away With It"' (2020) 17 Journal of Moral Philosophy 416 <https://brill.com/view/journals/jmp/17/4/article-p416_416.xml> accessed 13 May 2021

Gavison R, 'Privacy and the Limits of Law' (1980) 89 The Yale Law Journal 421 <http://www.jstor.org/stable/795891> accessed 15 May 2021

Gellert R and Gutwirth S, 'The Legal Construction of Privacy and Data Protection' (2013) 29

Computer Law & Security Review 522 <https://www.sciencedirect.com/science/article/pii/S0267364913001325> accessed 13 June 2021

Georges Duby PVAP, *A History of Private Life* (4th edn, Harvard University Press 1987)

Gordon Sarah RA, 'Information Wars: How Europe Became the World's Data Police' FInancial Times <www.ft.com/content/1aa9b0fa-5786-11e8-bdb7-f6677d2e1ce8> accessed 17 May 2021

Gutwirth S, *Privacy and the Information Age* (Rowman & Littlefield 2002)

Hallinan D and others (eds.), *Data Protection and Privacy: Data Protection and Democracy* (Bloomsbury Publishing 2020)

Helble M, Hill H and Magee D, 'Mongolia's Economic Prospects: Resource-Rich and Landlocked between Two Giants' (2020) <https://www.adb.org/sites/default/files/publication/611416/mongolia-economic-prospects.pdf> accessed 20 April 2021

——, *Mongolia's Economic Prospects: Resource-Rich and Landlocked between Two Giants* (2020) <https://www.adb.org/sites/default/files/publication/611416/mongolia-economic-prospects.pdf> accessed 7 April 2021

Hijmans H, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (1st ed. 20, Cham : Springer International Publishing : Imprint Springer, 2016)

Hijmans H, 'Lee A. Bygrave, Data Privacy Law, an International Perspective' (2015) 5 International Data Privacy Law 88 <https://doi.org/10.1093/idpl/ipu031>

Hondius FW, 'Data Law in Europe' (1980) 16 Stan. J. Int'l L. 88

Hopkins CA, 'European Convention on Human Rights' (1966) 24 The Cambridge Law Journal 4

Hornung G and Schnabel C, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 Computer Law & Security Review 84 <https://www.sciencedirect.com/science/article/pii/S0267364908001660> accessed 5

May 2021

Hudgins S, 'Tsatsal' (2014) 36 Mongolian Studies 41 <https://www.jstor.org/stable/26865343> accessed 11 April 2021

Hughes K, 'The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse' (2015) 225 Social Dimensions of Privacy: Interdisciplinary Perspectives 228

Kemp S, 'Digital 2020: Mongolia' (*Data reportal*) <https://datareportal.com/reports/digital-2020-mongolia> accessed 15 May 2021

Keulen S and Kroeze R, '1. Privacy from a Historical Perspective' in Bart van der Sloot and Aviva de Groot (eds), *The Handbook of Privacy Studies* (Amsterdam University Press 2018) <https://doi.org/10.1515/9789048540136-002>

Kokott J and Sobotta C, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222 <https://doi.org/10.1093/idpl/ipt017>

Kolnai A, 'Dignity' (1976) 51 Philosophy 251 <http://www.jstor.org/stable/3749604> accessed 10 April 2021

Lane G, *Genghis Khan and Mongol Rule* (Greenwood Publishing Group 2004)

Leerssen P, 'European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?' 38

Lynskey O, *The Foundations of EU Data Protection Law* (Oxford University Press 2015)

'Mongolia Today' [2015] Mongolia in the Twentieth Century: Landlocked Cosmopolitan 16 <https://cabinet.gov.mn/wp-content/uploads/MT2020-5-last-compressed.pdf> accessed 17 April 2021

'Mongolian History Encyclopedia' <https://mongoltoli.mn/history/h/504> accessed 2 May 2021

Morano-Foadi S and Andreadakis S, 'Reflections on the Architecture of the EU after the Treaty of Lisbon: The European Judicial Approach to Fundamental Rights' (2011) 17 European Law Journal 595 <https://doi.org/10.1111/j.1468-0386.2011.00568.x>

Mudgway C, ‘Memorandum of Understanding’ [2018] Sexual Exploitation and Abuse by UN Peacekeepers 28 <http://forum.mn/res_mat/Memorandum of Understanding on Human Rights.pdf> accessed 11 April 2021

Newcomb MJ, ‘Feeling the Vulgarity of Numbers: The Rwandan Genocide and the Classroom as a Site of Response to Suffering’ (2010) 30 JAC 175 <http://www.jstor.org/stable/20866942> accessed 19 April 2021

Newman AL, ‘Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive’ (2008) 62 International Organization 103 <http://www.jstor.org/stable/40071876> accessed 3 June 2021

Olivia W, ‘The GDPR Is Just the Latest Example of Europe’s Caution on Privacy Rights. That Outlook Has a Disturbing History’ (*Time*) <https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/> accessed 22 April 2021

Perkins DH, ‘Has China’s Economic Reform Already Peaked?’ (*East Asia Forum*) <https://www.eastasiaforum.org/2018/08/31/has-chinas-economic-reform-already-peaked/> accessed 2 June 2021

Polo Marco, *The Description of the World* (Kinoshita Sharon ed, Hackett Publishing 2016)

Richards NM and Solove DJ, ‘Privacy’s Other Path: Recovering the Law of Confidentiality ’ 96 Georgetown Law Journal 123 <https://heinonline.org/HOL/P?h=hein.journals/glj96&i=126> acessed 27 April 2021

Roessler B and Mokrosinska D, *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015)

Roisin A Costello, ‘“Warren and Brandeis and The Right to Privacy’s Hollow Core” Article Róisín A Costello’ 361 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059762&download=yes> accessed 17 May 2021

Sarah Newey JR, ‘Warrior Spirit and Sheep Diplomacy: How Mongolia Is Sprinting Ahead in Vaccine Race’ (*The telegraph*) <https://www.telegraph.co.uk/global-health/science-and-disease/warrior-spirit-sheep-diplomacy-mongolia-sprinting-ahead-vaccine/> accessed 3 June 2021

Scheinin M, ‘Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism’ (2009)

Scope T, ‘Harvard-Yenching Institute’ (2015) 3 337

‘Scope and Interpretation of EU Charter of Fundamental Rights’ Article 52 (*EU Agency for Fundamental Rights*) para 3 <https://fra.europa.eu/en/eu-charter/article/52-scope-and-interpretation-rights-and-principles> accessed 15 June 2021

Sharma S, *Data Privacy and GDPR Handbook* (John Wiley & Sons 2019)

Snijder M, ‘Biometrics, Surveillance and Privacy’ <https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC104392_biometrics_surveillance_and_privacy_final.pdf> accessed 3 June 2021

Solove D, ‘A Brief History of Information Privacy Law’ [2006] GWU Law School Public Law Research Paper 1

Solove DJ, ‘Privacy and Power: Computer Databases and Metaphors for Information Privacy’ (2000) 53 Stan. L. Rev. 1393

Solove DJ, ‘Conceptualizing Privacy’ (2002) 90 California Law Review 1087

Solove DJ, ‘Understanding Privacy’ (2008) Harvard University Press 1

Tavani HT, ‘Philosophical Theories of Privacy: Implications for an Adequate Onilne Privacy Policy’ (2007) 38 Metaphilosophy 1 <http://www.jstor.org/stable/24439672> accessed 13 April 2021

Tzanou M, ‘Data Protection as a Fundamental Right next to Privacy? “Reconstructing” a Not so New Right’ (2013) 3 International Data Privacy Law 88 <https://doi.org/10.1093/idpl/ipt004>

Van der Sloot B and de Groot A (eds), *The Handbook of Privacy Studies* (Amsterdam University Press 2018) <http://www.jstor.org/stable/j.ctvcmxpmp> accessed 18 May 2021

Vincent D, *Privacy: A Short History* (John Wiley & Sons 2016)

Voigt P and Von dem Bussche A, 'The Eu General Data Protection Regulation (Gdpr)' (2017) 10 A Practical Guide, 1st Ed., Cham: Springer International Publishing 12

Warso Z, 'There's More to It than Data Protection – Fundamental Rights, Privacy and the Personal/Household Exemption in the Digital Age' (2013) 29 Computer Law & Security Review 491 <https://www.sciencedirect.com/science/article/pii/S0267364913001295> accessed 19 April 2021

Westin AF, 'Social and Political Dimensions of Privacy' (2003) 59 Journal of social issues 431

Wijfjes H, 'Digital Humanities and Media History: A Challenge for Historical Newspaper Research 1' (2017) 20 TMG Journal for Media History

Ziegeldorf JH, Morchon OG and Wehrle K, 'Privacy in the Internet of Things: Threats and Challenges' (2014) 7 Security and Communication Networks 2728

OFFICIAL DOCUMENTS

INTERNATIONAL LAW

Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A (III)

International Covenant on Civil Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

'The Right to Privacy in the Digital Age' (3 August 2018) UNGA Res A/HRC/39/29

'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (27 June 2016) UNGA Res A/HRC/32/L.20

EU LAW

Charter of Fundamental Rights of the European Union (signed 12 December 2007, took effect 1 December 2009) 2012/C326/02

European Convention on Human Rights (signed 4 November 1950, took effect 3 September 1953) Ref. No.005

EU Directive 95/46/EC of 24 November 1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31

EU General Data Protection Regulation 216/679 of 27 April 2016 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1

General Data Protection Regulation Recitals

MONGOLIAN LAW

Civil Code of Mongolia (10 January 2002)

Criminal Code of Mongolia (3 December 2015)

The Constitution of Mongolia (13 January 1992)

The General Law of Mongolia on State Registration (21 June 2018)

The Law of Mongolia on Crime Prevention (6 June 2019)

The Law of Mongolia on Minor offences (11 May 2017)

The Law of Mongolia on Personal Privacy (21 April 1995)

The Law of Mongolia on Privacy of organizations (16 May 2019)

The Law of Mongolia on State and Official Secrets (1 December 2016)

The Law of Mongolia on the Automated System of Elections (10 November 2011)

The Law of Mongolia on the Information Transparency and Right to Information (16 June

2016)

CASE LAW

ECtHR CASE LAW

Amann v Switzerland (2000) 27798/95

B.C. v Switzerland (1995) 21353/93

Benedik v Slovenia (2014) 62357/14

Klass and others v Germany (1978) 5029/71

Mentes and others v Turkey (1997) 23186/94

Niemietz v Germany (1992) 72/1991/32

Olsson v Sweden (1988) 10465/83

Piechowicz v Poland (1998) 38857/97

Roman Zakharov v Russia (2015) 47143/06

Segerstedt-Wiberg and Others v Sweden (2005) 62332/00

Z v Finland (1997) 9/1996/627

CJEU CASE LAW

European Commission v The Bavarian Lager (2010) C-28/08 P

Joined Cases C-402/05 P and C-415/05 P Kadi and Al Barakaat International Foundation v Council and Commission (2008) ECR I-6351

Joined Cases C–92/09 and C–93/09 Volker und Markus Schecke and Eifert (2011) OJ C 13, 1

MONGOLIAN COURT DECISION

The Constitutional Court of Mongolia, The law of Mongolia on Personal Privacy Article 44

Dispute resolution (2014) 5

The first instance criminal court prosecutor's decision (2020) 2021/ШЦТ/0

OTHER SOURCES

European Citizens' Initiative *'Civil Society Initiative for a Ban on Biometric Mass Surveillance Practices*' <https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en> accessed 14 June 2021

European Commission, *'Data Protection Revision- Proposal for a Directive'* (2012) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=EN> accessed 16 May 2021

Department of Cyber-Crime Prevention '*National Police Agency of Mongolia*' <https://police.gov.mn/a/3833> accessed 23 May 2021

Hill K, '*How Target Figured out a Teen Girl Was Pregnant before Her Father Did'* (2012) 16 Forbes, <https://www.forbes.com/sites/kashmirhill/%202012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/> accessed 7 April 2021

I see *'2000 Face Detector Cameras and Its Side Notes'* (20 June 2020) <http://isee.mn/n/10805> accessed 11 June 2021

Isaak J and Hanna MJ, '*User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection'* (2018) < https://ieeexplore.ieee.org/document/8436400> accessed 8 April 2021

Kettemann MC, 'UN Human Rights Council Confirms That Human Rights Apply to the Internet' (*Blog of the European Journal of International Law 2012*) <https://www.ejiltalk.org/un-human-rights-council-confirms-that-human-rights-apply-to-the-internet/> accessed 21 April 2021

L.Misheel, 'Public Face Recognition Cameras Violate the Cnstitution' *The UB Post* (14 October 2020) <https://www.pressreader.com/mongolia/the-ub-

post/20201014/281801401434768> accessed 7 April 2021

'Main Parameters of the Communications Sector of Mongolia in 2016' (*Communications Regulatory Commission of Mongolia*) <https://crc.gov.mn/en/k/2n9/1H> accessed 2 May 2021

'Mongolia: Country Gender Assessment' (2005) <https://www.adb.org/sites/default/files/institutional-document/32236/cga-mongolia.pdf> accessed 19 April 2021

'Mongolia: Shift from Relief to Resilience Crucial to Economic Recovery' (*The World Bank*) <https://www.worldbank.org/en/news/press-release/2021/02/05/mongolia-shift-from-relief-to-resilience-crucial-to-economic-recovery> accessed 27 April 2021

'Mongolia's Workforce Research' (*National Statistics data base*) <https://www.1212.mn/BookLibraryDownload.ashx?url=LFS_2019_q4.pdf&ln=Mn> accessed 2 May 2021

'Mongolia - Data Protection Overview' (*One Trust Data Guidance*) <https://www.dataguidance.com/notes/mongolia-data-protection-overview> accessed 18 May 2021

'Mongolia Country Report 2020' (*Transformation index*) <https://www.bti-project.org/en/reports/country-report-MNG-2020.html> accessed 4 May 2021

'Mongolia Mining Sector: Managing the Future' <https://documents1.worldbank.org/curated/en/867261468323101510/pdf/332480ENGLISH01ng1sector1report1ENG.pdf> accessed 27 April 2021

'Mongolia Population 2021' (*World Population Review*) <https://worldpopulationreview.com/countries/mongolia-population> accessed 26 April 2021

'Overview of Court of Justice of the European Union' (*European Union*) <https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en> accessed 15 June 2021

'Oxford English Dictionary' <https://www.oed.com/view/Entry/151596?redirectedFrom=privacy#eid> accessed 17 May

2021

S.Uyanga, 'Face Detector System and Human Rights, Personal Privacy' *Zuunii medee* (5 September 2020) http://www.zms.mn/a/80711 accessed 9 April 2021

State Great Khural of Mongolia *'Approval of the Action Plan of the Government of Mongolia for 2020-2024'* (28 August 2020) <https://cabinet.gov.mn/wp-content/uploads/2020-2024_-ActionPlan_GOM_Eng_Edited_OE-2.pdf> accessed 16 April 2021

'The Court of Justice in the Legal Order of the European Union' (*Court of Justice of the European Union*) <https://curia.europa.eu/jcms/jcms/Jo2_7024/en/> accessed 13 June 2021

'The Digital Services Act Package' (*European Commission*) <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 23 June 2021

'The Laws in Mongolia' (*State legal database*) <https://www.legalinfo.mn> accessed 10 May 2021

UNCTAD, 'Data Protection and Privacy Legislation Worldwide' <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 30 May 2021

UNCTAD, Data Protection and Privacy Legislation Worldwide

<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 6 May 2021

UNCTAD, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' [2016] United Nations Conference on Trade and Development 154 <https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf%0Ahttp://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> accessed 3 May 2021

'What Is Considered Personal Data under the EU GDPR?' (*GDPR EU*) <https://gdpr.eu/eu-gdpr-personal-data/> accessed 21 June 2021

'What Is GDPR, the EU's New Data Protection Law?' (*GDPR EU*) <https://gdpr.eu/what-is-gdpr/> accessed 21 June 2021

'What Are "Controllers" and "Processors"?' (*Information Commissioner's Office*)

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/> accessed 12 June 2021

'World Bank Country and Lending Groups' (*The World Bank*) <https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups> accessed 26 April 2021