Data Protection and the Right to Privacy: Tajikistan's Legislation from the Perspective of the ECHR and EU Law

by Shavkat Akhmedov

Dissertation submitted to the Kent Law School
in fulfillment of the requirements of the University of Kent
for the award of the degree of
Doctor of Philosophy in Law

28 March 2024

University of Kent
Brussels School of International Studies

1st Supervisor: Professor Yutaka Arai
2nd Supervisor: Professor Anneli Albi
Word count: 92,351

Abstract

Data Protection and the Right to Privacy: Tajikistan's Legislation from the Perspective of the ECHR and EU Law

The thesis explores the evolution of the concepts of privacy and data protection in the ECHR and EU law against the background of the development of advanced technologies, and aims to examine what lessons can be learnt from the relevant Tajik law perspective. The key objective is to provide critical evaluations of the pertinent laws in Tajikistan with a view to bringing them in alignment with European standards. The original contribution of this thesis can be highlighted by the fact that virtually no research has hitherto been carried out on this theme. As Tajikistan is neither a member of the Council of Europe nor a party to EU association agreements, the thesis additionally explores issues regarding the extraterritorial applicability of European norms, the 'Brussels effect', and legal transplants. Data protection and privacy are of increasingly acute importance because, in addition to the more long-standing concerns around state surveillance, people are challenged to rethink the boundaries of their privacy given the worldwide development of information technologies, along with the extensive data gathered by private corporations.

The main findings of the thesis are threefold. First, the thesis shows that Tajikistan's laws related to surveillance and data protection reflect post-Soviet – and especially Russian – legal thought on the right to private life, indicating differences in comparison with Western concepts of privacy. Secondly, through the in-depth analysis of the European Court of Human Rights (ECtHR) jurisprudence on the one hand, and EU rules – including the EU Charter and the General Data Protection Regulation (GDPR) – on the other hand, the thesis identifies a range of overlapping rules as well as some divergencies in the two European human rights systems. In particular, the thesis argues that the ECtHR case law is marked by a more nuanced approach when its notion of privacy seeks to accommodate economic, political, and other differences. By contrast, the EU data protection rules, mostly because of the EU's harmonization drive, and partly due to their more technical formulation, seem to be intended to provide a more universally applicable standard. Thirdly, in relation to the surveillance and data protection laws in Tajikistan, the thesis suggests that there is considerable scope to enhance fundamental rights protection in line with EU law as well as the standards set by the ECtHR.

A supplementary contribution of this thesis is to help initiate wide-ranging deliberations on how the concept of privacy could be reconceived in the Tajik legal discourse while, providing a critique of the current post-Soviet concept of privacy.

Acknowledgments

I am deeply grateful for the invaluable support and guidance I have received throughout my PhD journey, without which this thesis would not have been possible.

First and foremost, I extend my heartfelt appreciation to my supervisor, Professor Yutaka Arai, whose unwavering dedication and insightful guidance have been instrumental in shaping this research. Your encouragement, wisdom, and willingness to engage in countless discussions have significantly enriched my academic experience.

I am particularly indebted to my second supervisor, Professor Anneli Albi, whose exceptional support, insightful feedback, and dedication went above and beyond what is typically expected. Your guidance and pertinent suggestions have played a pivotal role in the development and refinement of this work. Your tireless commitment to my academic growth has been truly inspiring.

My sincere gratitude goes to all fellow PhD students and all members of the faculty at the Brussels School of International Studies, for their continuous support and encouragement. Special thanks are extended to Professor Harm Schepel, with whom I engaged in numerous discussions regarding my thesis. His invaluable insights, comments, and critiques greatly enriched my work, and I am truly grateful to him. I also extend my thanks to the dedicated administrative staff, for their assistance throughout my academic journey.

I am endlessly thankful for the tremendous support of my family. To my beloved wife Nodira, your patience and understanding have been my rock throughout this journey. Your belief in me has been a constant source of strength and motivation. I am especially grateful for the countless hours you spent listening to my ideas, offering invaluable feedback, and providing much-needed encouragement. Thank you for being by my side during this challenging, yet exciting academic journey.

I am also deeply grateful to my parents for their endless prayers, love, and encouragement. Your faith in my abilities has been a guiding light, and I am forever grateful for your unconditional support.

Lastly, I extend my appreciation to all my colleagues and friends who have supported me along the way. Your encouragement and shared passion for knowledge have made this journey memorable and enriching.

Table of Abbreviations

AFSJ	Area of Freedom, Security and Justice
BVerfG	German Federal Constitutional Court
CAT	Convention Against Torture and other Cruel Inhuman or Degrading Treatment or Punishment
CFSP	Common Foreign and Security Policy
CDI	Tajikistan Law on Crime Detection and Investigation
CEDAW	Convention on Elimination of all Forms of Discrimination Against Women
CERD	Convention on Elimination of all Forms of Racial Discrimination
CFREU	Charter of the Fundamental Rights of the European Union
CIS	Commonwealth of Independent States
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CPC	Criminal Procedure Code of the Republic of Tajikistan
CRC	Convention on the Rights of the Child
CCTV	Closed-Circuit Television
DPD	Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (1995) OJ L281/31
DRD	Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54
EDPS	European Data Protection Supervisor
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)
ECtHR	European Court of Human Rights
EU	European Union

HRC	Human Rights Council
GDPR	Regulation of EU 216/679 dated 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant of Economic Social and Cultural Rights
ICMW	International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families
LED	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 "On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA" (Law Enforcement Directive)
IMEI	International Mobile Equipment Identifier
MTDs	Mobile Communication Devices
RT	Republic of Tajikistan
TEU	Treaty of the European Union
TFEU	Treaty on the Functioning of the European Union
UCC	Unified Commutation Centre
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
US	United States
USA	United States of America
USSR	the Union of the Soviet Socialist Republics

Table of Laws and International Treaties:

Treaties

- Charter for Fundamental Rights of the European Union [2012] OJEU, C 326/391
- Convention for the Protection of Human Rights and Fundamental Freedoms adopted by the Council of Europe on 4 November 1950 and entered into force on 3 September 1953
- Treaty Establishing the European Coal and Steel Community (ECSC) on 18 April 1951
- (Treaty of Paris), Treaty Establishing European Economic Community (EEC) dated 25 March 1957 (Treaty of Rome),
- Treaty Establishing European Atomic Energy Community (Euratom) dated 25 March 1957 (Euratom Treaty)
- Merger Treaty 1965
- Treaty on European Union (TEU) signed 7 February 1992 Maastricht Treaty
- Treaty of Amsterdam amending the Treaty of the European Union, the Treaties Establishing the European Communities and certain related acts, signed 2 October 1997 and entered into force 1 May 1999
- Treaty of Nice amending the Treaty of the European Union and the Treaty of Rome signed 26 February 2001 and came into force 1 February 2003
- Treaty of Lisbon: Two main EU treaties were amended and restated: the Maastricht Treaty of 1992, called Treaty on European Union (TEU), and the Treaty of Rome (TEC), now called the Treaty on the Functioning of the European Union (TFEU)
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) dated 28 January 1981, amended later with Additional Protocol of 2001 (ETS 181), and, recently, modernized through Amending Protocol (CETS 221). Now, it is the Modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the CoE Committee of Ministers on 18 May 2018, CM/Inf(2018)15-final
- International Covenant on Civil and Political Rights, adopted by the UN GA on 16 December 1966 and entered into force on 23 March 1976.
- The American Convention on Human Rights, adopted on 22 November 1969 and entered into force on 18 July 1978.
- Universal Declaration of Human Rights, G.A. RES. 217A, U.N. GAOR, 3d Sess., 1st. plen mtg., U.N. Doc A/810 (Dec. 12, 1948)

Secondary EU Law:

- Council Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54
- Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (1995) OJ L281/31
- Directive 89/552/EEC of the European Parliament and the Council of 3 October 1989 on the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the provision of audiovisual media services [1989] OJ L 298/23
- Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) [2010] OJ L 95/1
- Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspect of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1 ('E-commerce Directive')
- EDPS Opinion 8/2016 'On Coherent Enforcement of Fundamental Rights in the Age of Big Data' dated 23 September 2016
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 'On the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data', (21.11.2018) OJEU, L 295/39
- Regulation (EU) 216/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), (2016) OJ L119/1
- Decision 2000/520 of the European Commission, OJ L 215, 25.8.2000
- Directive 2002/58/EC (E-Privacy Directive) dated 12 July 2002
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 "On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA" (Law Enforcement Directive)

- Directive 95/46/EC of the European Parliament and of the Council EU Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), Official Journal L 215 , 25/08/2000 P. 0007 – 0047
- EU Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), OJ L 207, 1.8.2016

Tajikistan Laws:

- Bulletin of Majlisi Oli of the RT
- The Constitution (Basic Law) of Tajik Autonomous Soviet Socialist Republic, adopted by the Resolution of the 2nd Congress of the Soviets of the Tajik ASSR on 28 April 1929
- The Constitution (Basic Law) of Tajik Soviet Socialist Republic, adopted by the Resolution of the 4th All-Tajik Congress of the Soviets of the Tajik SSR on 25 February 1931
- Constitutional Law of the RT "On Prosecution Bodies of the Republic of Tajikistan" No 102 dated 15 July 2005
- The Constitution of the Tajik SSR dated 1 March 1937 and the Constitution of the Tajik SSR of (April 1978)
- The Constitution of the USSR, adopted by the 8th All-Union Extraordinary Congress of the Soviets on 5 December 1936, and the Constitution of the USSR, adopted the Supreme Soviet of the USSR on 7 October 1977
- Constitution of the Republic of Tajikistan, dated 6 November 1994
- The Criminal Procedure Cade of the Tajik SSR (1961) contained a separate chapter called 'Judicial Investigation'. See Chapter 24 of the Criminal Procedure Cade of the Tajik SSR dated 17 August 1961
- The Constitutional Law of the RT 'On the Constitutional Court of the RT', No 672 dated 17 July 2014

- The Law of the RT "On Streamlining Traditions, Celebrations and Rituals in the Republic of Tajikistan", No 584, dated 30 May 2007
- The Law of the RT "On Responsibility of Parents on Education and Upbringing of Children", No 210, dated 21 July 2011
- The Law of the RT "On civic registration", No 188, dated 29 April 2006
- The Law of the RT 'On Public-Private Partnership', No 439 dated 13 December 2012
- The Law of the RT 'On Pledge of Movable Property', No 1576 dated 2 January 2019
- Law of the Republic of Tajikistan (RT) "On Crime Detection and Investigation", No 352 dated 2 March 2011
- The Law of the RT "On Combating Terrorism", No 1808, dated 23 December 2021
- The Law of the RT "On Personal Data Protection", No 1537, dated 3 August 2018
- The Civil Code of the RT (Part I)
- The Law of the RT "On Militia" of 1992
- The Law of the RT "On Militia", No 544 dated 3 May 2004
- The Law of the RT "On the Informatization" No 40 dated 6 August 2001
- The Law of the RT "Information", No 55 dated 10 May 2022
- The Law of the RT "On the Protection of Information" No 631 dated 15 May 2002
- The Law "On the Right of Access to Information" No 411 dated 18 June 2008
- The Law of the RT 'On the Protection of Personal Data', No 1537 dated 3 August 2018
- The Labour Code of the RT of 2016
- Regulation (EU) 216/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), (2016) OJ L119/1)
- The Law of the RT "On the Access to the Information on Activities of the Court", No 1783 dated 25 June 2021
- The Criminal Code of the RT of 1998
- Law of the Republic of Tajikistan (RT) "On Crime Detection and Investigation" No 352 dated 2 March 2011
- Criminal Procedure Code of the RT dated 3 December 2009, No 12
- Law of the RT 'On National Security Bodies' dated 6 March 2008, No 443
- Law of the Republic of Tajikistan 'On Electric Communication' dated 10 May 2002 No 56
- Law of the RT 'On Legal Normative Acts', No 1414 dated 30 May 2017

- The Law of the Republic of Tajikistan "On Personal Data Protection", No 1537, dated 3 August 2018
- The Government of Tajikistan passed Resolution No 208 dated 31 March 2020 'On the Procedure of Registration of Mobile Communication Devices and Defining Functions of the State System of Identification of Mobile Communication Devices'
- The Resolution of the Government of the Republic of Tajikistan 'On the Unified Commutation Centre of Electric Communications' dated 30 December 2015, No 765
- Presidential Decree 'On Establishment of the Council of Justice of the Republic of Tajikistan' dated 14 December 1999, No 48
- Presidential Decree 'On Liquidation of the Council of Justice of the Republic of Tajikistan' dated 9 June 2016, No 698
- Law on "State Registration of Legal Entities and Individual Entrepreneurs" dated 19 May 2009, No 508
- Law on "Pledge of Movable Property" dated 1 March 2005, No 93; the Law "Mortgage" dated 20 March 2008, No 364
- Resolution of the Government of Tajikistan 'On the Issues of Maintaining the Unified System of State Registration of Immovable Property and Immovable Property Rights' dated 2 July 2015, No 432
- Law of the Republic of Tajikistan 'On State Registration of Immovable Property and the Rights to Immovable Property' dated 16 January 2008, No 833

Other Legal Instruments:

- Article 29 Working Party, Opinion 4/2007 'On the Concept of Personal Data' adopted on 20 June 2007, 01248/07/EN WP 136
- Basic Law of the German Federal Republic of 23 May 1949
- CCPR General Comment No.16: Article 17 (Right to Privacy) dated 8 April 1988
- Communication from the Commission to the European Parliament and the Council 'Exchanging and Protecting Personal Data in a Globalised World' COM (2017) 7 final
- Commission on Human Rights, Report on its 9th Session, 6 June 1953, E/CN.4/689 ('Commission Report 2447')
- Council Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54

- Council of Europe's European Commission for Democracy through Law 'Report on the Democratic Oversight of Signals Intelligence Agencies', CDL-AD(2015)011
- EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1 dated 12 November 2019
- EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1 dated 12 November 2019
- European Commission's Amended Proposal on the draft DPD, see COM (92) 422 Final – SYN 287, 15 October 1992
- Explanations Relating to the Charter of Fundamental Rights, OJEU, 2007/C 303/02, 14 December 2007
- Guide on Article 10 of the European Convention on Human Rights, published by European Court of Human Rights, last updated on 31 August 2022
- Guide on Article 8 of the European Convention on Human Rights, published by European Court of Human Rights, last updated on 31 August 2022
- UN Human Rights Council 'Report of the Working Group on the Universal Periodic Review. Tajikistan', A/HRC/49/12 dated 6 January 2022
- The Constitutional Charter' for the Electorate of Hesse of 1831 and the Belgium Constitution of 1831.

Table of Cases

ECtHR:

Ismayilova v Azerbaijan, Judgment of 10 April 2019

Johnston and Others v Ireland (1986) Series A no 112

Kennedy v UK, Judgment of 18 August 2010

Klass and Others v Germany (1978) Series A no 28

Kroon and Others v The Netherlands (1994) Series A-297-C

Kudrevicius v Lithuania, Judgment of 15 October 2015

Laske and Others v UK, Judgment of 19 February 1997

Leander v Sweden (1987) Series A no 16

Leyla Sahin v Turkey, Judgment of 10 November 2005

Lopez Ribalda and Others v Spain, Judgment of 17 October 2019

Lozovyye v Russia, Judgment of 24 July 2018

Malone v UK (1984) Series A no 82

Marckx v Belgium (1979) Series A no 31

Mikulic v Croatia, Judgment of 4 September 2002

M.K. v France, Judgment of 18 July 2013

M.L. v Germany, Judgment of 28 September 2018

M.N. and Others v San Marino, Judgment of 7 October 2010

Mosley v. the United Kingdom, Judgment of 15 September 2011

Murray v UK (1994) Series A no 300-A

N.C. v Italy, Judgment of 18 December 2002

Niemietz v Germany (1992) Series A no 251-B

Odievre v France, Judgment of 13 February 2003

Paradiso and Campanelli v Italy, Judgment of 24 January 2017

Peck v UK, Judgment of 28 April 2003

Peruzzo and Martens v Germany, Decision of 4 June 2013

P.G and J.H v UK, Judgment of 25 December 2001

P.N. v Germany, Judgment of 16 November 2020

Prado Bugallo v Spain, Judgment of 18 February 2003

Prokopovich v Russia, Judgment of 18 February 2005

P.T. v Moldova, Judgment of 26 August 2020

Rees v. the United Kingdom (1986) Series A no. 106

Rotaru v Romania, Judgment of 4 May 2000

S and Marper vs UK, Judgment of 4 December 2008

S.A.S. v France, Judgment of 1 July 2014

Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland, Judgment of 27 June 2017

Segerstedt-Wiberg and Other v Sweden, Judgment of 6 September 2006

Silver and Others v UK (1983) Series A no.61

Szabo and Vissy v Hungary, Judgment of 6 June 2016

Trajkovski v Macedonia, Judgment of 13 June 2020

Tysiąc v. Poland, Judgment of 24 September 2007

Uzun v Germany, Judgment of 2 December 2010

Valenzuela Contreras v Spain, Judgment of 30 July 1998

Von Hannover vs Germany (No 1) App No 59320/00 (ECtHR 24 June 2004)

Von Hannover v Germany (No.2) , Judgment of 7 February 2012

Vukota-Bojic v Switzerland, Judgment of 18 January 2017

Wagner and J.M.W.L v Luxembourg, Judgment of 28 June 2007

Weber and Saravia v Germany, Admissibility Decision of 29 June 2006

Wieser and Bicos Beteiligungen GmbH v Austria, Judgment of 16 January 2008

Z v Finland ECHR, Judgment of 25 February 1997

Zakharov v Russia, Judgment of 4 December 2015

CJEU

Case 4/73 Nold v Commission, Judgment of 14 May 1974

Case 6/64 Costa v ENEL [1964] ECR 585

Case 11/70 Internationale Handelsgeselschaft, Judgment of 17 December 1970

Case 12/86 Demirel v Stadt Schwaebisch Gmuend [1987] ECR 3719

Joined cases 21 to 24/72 International Fruit Company v Produktschap voor Groenten en Fruit [1972] ECR 1219

Case 22/70 Commission v Council [1971] ECR 263 (ERTA case)

Case 26/62 NV Algemene Transport en Expeditie Onderneming Van Gend en Loos v Nederlandse administratie der belastingen [1963] ECR 1

Case 29/69 Stauder v City of Ulm, Judgment of 12 November 1969

Case C-36/02 Omega Spielhallen und Automatenaufstellung v Oberburgermeisterin der Bundesstadt Bonn, CJEU Judgment of 14 October 2004

Case C-41/674 Yvonne van Duyn v Home Office [1975] 1. C.M.L.R. 1

Case 44/79 Hauer v Land Rheinland-Pfalz, Judgment of 13 December 1979

Joined Cases C-54/88, C- 91/88 and C-14/89 Nino and Others [1990] ECR I-3537

Case 64/16 Associcao Sindical dos Juizes Portugueses v Tribunal de Contas [2017] ECR

Case 81/87 Daily Mail and General Trust [1988] ECR 5483

Opinion 2/94 [1996] ECR-I-1759

Opinion of Advocate General Cruz Villalon in Weltimmo s.r.o. v Nemzeti Adatvedelmi es Informacioszabadsag Hatosag, (Case C-203/14), EU:C:2015:426;

Case C-92/09 and C-93/09 Volker und Markus Schecke and Hartmut Eifert [2010] ECR I-11063, Opinion of Advocate General Sharpston

Opinion of AG Trstenjak dated 22 September 2011 on Case C-411/10

Opinion of AG Sanches-Bordona on case C-128/18, ECLI:EU:C:2019:334, Paragraph 107

Opinion of Advocate General Cruz Villalon in Weltimmo s.r.o. v Nemzeti Adatvedelmi es Informacioszabadsag Hatosag, (Case C-203/14), EU:C:2015:426, para.23

Other Case Law:

Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion I.C.J. Reports 1949

BVerfG, 65, 1 of 15 December 1983

Wünsche Handelsgesellschaft (22 October 1986) BVerfGE 73, 339, 2 BvR 197/83 (Solange II)

Internationale Handelsgesellschaft (29 May 1974) BVerfGE 37, 2712, 2 BvL 52/71 (Solange I)

Chapter 1. Introduction

1.1. The Context and the Objective of the Research

There is no universally accepted notion of privacy among scholarship, because privacy, as BeVier has put it, "[…] is a chameleon-like word used denotatively to designate a range of wildly disparate interests – from confidentiality of personal information to reproductive autonomy."[1] This thesis focuses on the aspect of privacy related to the protection of personal information. The research conducted within this thesis endeavours to investigate the regulatory frameworks pertaining to privacy and data protection as delineated by the European Convention on Human Rights[2] (ECHR) and the legislation of the European Union (EU). Thereafter, it aims to assess avenues through which Tajikistan's legislation concerning privacy and data protection could be improved to align with the established standards within the aforementioned European legal regimes. Additionally, this study will delve into the foundational principles guiding privacy and data protection laws in Tajikistan, alongside an examination of the conceptual frameworks informing contemporary data protection legislation within the above-mentioned European legal systems.

One of the mainstream Western concepts of privacy, which explains the nexus between privacy and personal data protection, has been formulated by Westin in his book "Privacy and Freedom" in 1967.[3] Westin has outlined the contemporary concept of privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".[4] His account of privacy has emerged as a response to the development of advanced technologies, which have enabled public and private authorities to conduct surveillance over the individual.[5] In the 21st century, the digital age triggered fundamental changes in surveillance techniques, including processing large amounts of personal data, which became an integral part of State surveillance.[6] Westin's control-based account of privacy, when individuals allegedly claim that they ultimately make decisions over the fate of their personal information, has influenced the development of data protection laws not only in Europe but also in other parts

[1] Lillian R. BeVier 'Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection' (1995) 4 William & Mary Bill of Rights Journal, p. 455.
[2] Convention for the Protection of Human Rights and Fundamental Freedoms adopted by the Council of Europe on 4 November 1950 and entered into force on 3 September 1953.
[3] Westin A., *Privacy and Freedom* (New York: Atheneum, 1967).
[4] Westin A., *Ibid.*, p. 5.
[5] Westin A., n 3 above, p. 3.
[6] See Daragh Murray and Pete Fussey 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communication Data' (2019) 52(1) Israel Law Review, p.31.

of the world.[7] Large amounts of personal data are processed by private businesses in the pursuance of their economic activity. However, the danger of private surveillance should not be underestimated. As Richards puts it, "[p]ublic and private surveillance are simply related parts of the same problem, rather than wholly discrete".[8]

In the above-discussed framework, it is crucial to acknowledge the unique challenges faced by countries like Tajikistan. The central focus of this thesis revolves around Tajikistan, situated as a post-Soviet nation in the midst of transitioning to a market-based economy. Herein lies a notable absence of historical precedence in safeguarding individual privacy rights, coupled with a dearth of experience in formulating domestic data protection legislation. Notably, Tajikistan has embarked on the adoption of its Law on Personal Data Protection[9] (Law on DP) relatively recently, in 2018.

In contrast to the privacy concept delineated by Westin, which underpins contemporary data protection laws in Europe, Tajik post-Soviet legal scholarship shows a deficiency in thorough analysis within the realm of privacy and data protection. There is an insufficient amount of literature on the Tajik concept of privacy.[10] Tajik scholars are predominantly informed by Russian or other post-Soviet literature and make references to Russian scholars in their analysis of Tajik laws. This is explained by similarities in Tajik and Russian laws, and by the common post-Soviet legal heritage of Tajikistan and some other post-Soviet States.

In the Soviet times, collective values prevailed over personal ones, as will be outlined more fully in this thesis. The term 'private' had a negative connotation associated with a capitalist society, where through private property one class exploited another class, which was contrary to the socialist idea of living in a society. Civil and political rights were also not prioritized during Soviet times. Priority was given to the protection and development of

[7] See Lisa Austin 'Re-reading Westin' (2019) 20 Theoretical Inquiries in Law 53, at p.1; Adekemi Omutobora and Subhajit Basu 'Next Generation Privacy' (2020) Information and Communication Technology Law 151, at p.156.
[8] Neil Richards 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934, p.1935.
[9] The Law of the RT "On Personal Data Protection", No 1537, dated 3 August 2018.
[10] For the limited number of existing works see Sh. Tagainazarov and Babadzhanov I. 'K teorii lichnykh neimuschestvennykh prav' [On the Theory of Personal Non-proprietary Rights] (2018) 4 Hayoti Huquqi 4 [Legal Life 209]; Sh. Tagainazarov and K. Kurbanov 'Sovremennye podkhody k probleme instituta prava na chastnuyu zhizn v grazhdanskom prave' [Contemporary Approaches to the Problem of the Concept of the Right to Private Life in Civil Law] (2018) 4 Hayoti Huquqi [Legal Life 2014]; K. Kurbanov 'Stanovlenie teoriy prava na chastnuyu zhizn' [Formation of the Theory of the Right to Private Life] (2018) 4 Hayoti Huquqi [Legal Life] 220; K. Kurbanov 'Pravo na neprikosnovennost chastnoy zhizni kak lichnoe neimuschestvennoe pravo' [The Right to Inviolability of Private Life as a personal non-proprietary right] (2013) 4 Hayoti Huquqi [Legal Life] 58; and K. Kurbanov 'Ponyatiye Chastnoy Zhizni v Grazhdanskom Prave' [The Concept of Private Life in Civil Law] (2016) 16 Hayoti Huquqi [Legal Life] 132.

social rights, which 'were, indeed, delivered'.[11] Soviet legislation and Soviet legal science did not pay sufficient attention to the right to private life as an individual human right.

As a result of the influence the Soviet legacy has had on Tajik legal scholarship, the concept of privacy in Tajikistan is mainly formulated from the private or civil law point of view.[12] Tajik scholars do not discuss the right to private life in the context of State interference with privacy. Privacy is mainly subject to Tajik's legal analysis when it is breached by private parties. The State or its agents are not seen as perpetrators, but rather as protectors of the right to the private life of individuals. This vision of privacy is reflected in Tajikistan laws, as will be seen in the thesis.

In Europe, the year 2018 was a remarkable year for the development of data protection legislation: the General Data Protection Regulation (GDPR)[13] has become directly applicable within the European Union. It is argued that the GDPR has set high standards of data protection not only for the EU Member States but also for the wider world.[14] Its significance as a global standard-setting instrument has been highlighted by the current scholarship.[15] The GDPR reflects the idea that the right to the protection of personal data is a fundamental right, which is also enshrined in the Charter of the Fundamental Rights of the EU (CFREU).[16]

The right to personal data protection is also ensured, albeit implicitly, by another European human rights protection instrument – the European Convention on Human

[11] See Bill Bowring 'Russia and Human Rights: Incompatible Opposites?' (2009) 1 Goettingen Journal of International Law 257, at p.263.
[12] See, e.g., K. Kurbanov 'Ponyatiye Chastnoy Zhizni v Grazhdanskom Prave' [The Concept of Private Life in Civil Law] (2016) 16 Hayoti Huquqi [Legal Life] 132.
[13] Regulation (EU) 216/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), (2016) OJ L119/1, is applied since 24 May 2018.
[14] See Christopher Kuner 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2016) 18 German Law Journal 881, at 893; Anu Bradford 'The Brussels Effect' (2012) 107 Northwestern University School of Law 2, at 23; Jan Philipp Albrecht 'How the GDPR will Change the World' (2016) 2 European Data Protection Law Review 287, at 288; Edoardo Celeste and Federico Fabbrini 'EU Data Protection Law Between Extraterritoriality and Sovereignty' in Fabbrini F., Celeste E. and Quinn J (eds.) *Data Protection Beyond Borders: Transatlantic Perspective on Extraterritoriality and Sovereignty* (Hart, 2021) 3.
[15] See Michael Rustad and Thomas Koenig 'Towards a Global Data Privacy Standards' (2019) 71 Florida Law Review 365; Stefano Saluzzo 'The EU as a Global Standard-Setting Actor: The Case of Data Transfers to Third Countries' in E. Carpanelli and N. Lazzerini (eds.) *Use and Misuse of New Technologies* (Springer Nature Switzerland AG, 2019); Graham Greenleaf 'The Influence of the European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108' (2012) 2 International Data Privacy Law 68; Claes Granmar 'Global Applicability of the GDPR in Context' (2021) 3 International Data Privacy Law 225; Anu Bradford 'How the EU Became a Global Regulatory Power' in A. Bradford *The Brussels Effect* (OUP, 2020).
[16] The CFREU was adopted by the European Parliament, European Council and the Council on 7 December 2000 and entered into force together with the Treaty of Lisbon on 1 December 2009. Article 8 CFREU defines the right to personal data protection. The GDPR in Paragraph 1 of its Preamble refers to the right to data protection as a fundamental right.

Rights.[17] The European Court of Human Rights (ECtHR) in its case law has examined the issue of personal data protection as part of the protection of private life[18] and has recognized the right of an individual to informational self-determination.[19] The ECtHR has also developed a case law on surveillance issues, which sets a standard of human rights protection to be followed by law enforcement agencies in the course of conducting surveillance measures. It is important to mention that this thesis does not address EU Member States and comparative European law in the field of privacy and data protection, apart from occasional coverage of Germany and other constitutional provisions in a broader context.

Against the above background, the broader aim of the research is to explore what lessons Tajikistan could learn from the privacy and data protection standards established by the ECHR and EU law. In the light of this broader research aim, the thesis is centered around the following three main and one supplementary research objectives and corresponding research questions.

The first main research objective is to find out about the conceptual understanding of privacy and data protection in the theoretical literature and the relevant national and international legal instruments. This is centered around three key research questions. The first is how the protection of privacy has historically emerged and developed in national constitutions, and international treaties, as well as in the literature in the field, and what are the differences in the conceptualizations. It will be seen in the thesis that the European approach to privacy has been a result of the development of legal thought on the right to privacy since the 19th century when some elements of the right to privacy, such as the right to privacy of correspondence, were stipulated in some European States' constitutions.[20] Further, the right to private life has become part of the international human rights law after World War II – it is enshrined in the 1948 Universal Declaration of Human Rights (UDHR)[21] and the ECHR. Further development of surveillance techniques has sparked the emergence of the first data protection laws in Europe in the 1970s.[22] The thesis shows that a key role in the protection of privacy has been played by the German Federal Constitutional Court, which

[17] The ECHR, see n 2 above.
[18] See *Leander v Sweden* (1987) Series A no.116, Paragraph 48; *P.G and J.H v UK* Judgment of 25 December 2001, Paragraph 59; *Peck vs UK,* Judgment of 28 April 2003, Paragraphs 60-63; *Uzun v Germany,* Judgment of 2 December 2010, Paragraph 52; *Aycaguer v France,* Judgment of 22 September 2017, Paragraph 38.
[19] *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland,* Judgment of 27 June 2017, Paragraph 137.
[20] The Constitutional Charter for the electorate of Hessen of 1831 and the Constitution of Belgium of 1831 are referred to by current scholarship as the first constitutions in Europe to have stipulated the elements of the right to privacy. See Thomas Snyder 'Developing Privacy Rights in Nineteenth-Century Germany: A Choice Between Dignity and Liberty?' (2018) 58 American Journal of Legal History p.188-2007.
[21] Universal Declaration of Human Rights, G.A. RES. 217A, U.N. GAOR, 3d Sess., 1st. plen mtg., U.N. Doc A/810 (Dec. 12, 1948).
[22] Germany adopted its first Data Protection Law in 1977 and France in 1978.

in 1983 proclaimed the right of an individual to informational self-determination as the ability of such an individual to make decisions freely based on the knowledge of what personal data is known to and could be disclosed by others.[23] The second key research question is what the nexus between the development of data protection laws in Europe and the evolution of the concept of privacy is, including the historical development of the right to informational self-determination of individuals. The third key research question is how Tajik legal scholarship on privacy and data protection is influenced by the Soviet academic legacy in the post-Soviet period.

The second main research objective is to assess the prevailing standard of privacy protection within the framework of the European Convention on Human Rights. In pursuit of this objective, a central inquiry will delve into the manner in which the European Court of Human Rights has interpreted the right to privacy enshrined in the ECHR within its jurisprudence, and how this protection has undergone evolution over time. Moreover, this thesis seeks to find out whether the ECtHR jurisprudence on surveillance cases could be regarded as the standards-setting instrument for improving Tajikistan's laws on surveillance, crime detection, and investigation. Other related instruments will also be explored; in particular, within the framework of the Council of Europe, there is a special legal instrument related to data protection issues – Convention 108,[24] to which the ECtHR makes references in its case law on privacy and data protection.[25] Convention 108 is open to accession by non-member States.[26] The research undertaken in the thesis is of central importance in order to enhance the standard of data protection in the legislation of Tajikistan, laying the groundwork for potential accession to Convention 108.

The third main research objective is to explore the right to privacy in EU law, where, notably, enhanced protection has been granted to personal data by virtue of the General Data Protection Regulation in 2018.[27] To this end, the thesis seeks to outline the main rules in this

[23] See BVerfG, 65, 1 of 15 December 1983.
[24] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) dated 28 January 1981, amended later with Additional Protocol of 2001 (ETS 181), and, recently, modernized through Amending Protocol (CETS 221). Now, it is the Modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the CoE Committee of Ministers on 18 May 2018, CM/Inf(2018)15-final.
[25] See *Amann v Switzerland,* Judgment of 16 February 2000, Paragraph 65; *Barbulescu v Romania,* Judgment of 5 September 2017, Paragraph 42; *Big Brother Watch and Others v* UK, Judgment of 4 February 2019, Paragraphs 205-207; *Bernh Larsen Holding AS and Others v Norway,* Judgment of 8 July 2013, Paragraphs 76-79; *Benedik v Slovenia,* Judgment of 24 July 2018, Paragraph 46.
[26] Article 23 of Convention 108. Currently, 9 non-member States acceded to Convention 108: Argentina, Burkina Faso, Mauritius, Mexico, Morocco, Russia, Senegal, Tunisia, and Uruguay. See https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108, last time accessed on 15 February 2024.
[27] The GDPR, n 13 above.

and other relevant EU instruments, including the Charter of Fundamental Rights of the European Union. An analysis of the case law of the Court of Justice of the European Union will be undertaken to explore the judicial protection of the respective rights. The thesis thus seeks to analyse what standards of data protection established by the GDPR and other EU laws on data protection could be accepted by Tajikistan in order to improve the laws related to data protection, especially the Law on DP.

In the light of the above two human rights regimes in Europe, one important question that arises for a country potentially seeking to apply European rules is what are the similarities and differences in the protection of the right to privacy. To this end, throughout the examination and analysis, the thesis will seek to articulate where the ECHR and EU rules are convergent, where there are divergencies in the respective rules, and, in particular, where the EU rules provide more enhanced protection during personal data processing. It will also be essential to outline the broader differences between the ECHR and EU legal regimes, as these have shaped and influenced the approach to fundamental rights protection. Indeed, in the light of the initial literature review, the thesis will put forward, and explore, the hypothesis that these two systems have different approaches to privacy and data protection. The European Union has elevated the right to the protection of personal data to a rank of the fundamental right separating it from the right to private life, while the European Court of Human Rights in its jurisprudence has recognized the right to personal data protection as part of the right to private life.

In particular, on the basis of the initial literature review, one key research question that emerged and will be explored is whether the right to personal data protection has come to be distinguished from the right to private life in the Court of Justice of the European Union (CJEU) jurisprudence and European legal scholarship.[28] By way of example, Kokott and Sobbota, as well as Linskey, have examined the CJEU's jurisprudence, pointing out that the scope of the right to data protection is broader than the right to private life.[29] For them, the right to data protection provides individuals with more rights over more types of data than the right to privacy does.[30] This thesis seeks to engage in the emerging legal discourse among

[28] See Juliane Kokott and Christoph Sobotta 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 4 International Data Privacy Law 222; Orla Lynskey 'Deconstructing Data Protection: the "Added Value" of the Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569; Van Der Sloot 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in Ronald Leenes, Rosamunde van Brakel Serge Guthwirth, Paul De Hert (eds) *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer International Publishing AG, 2017).
[29] Juliane Kokott and Christoph Sobotta, n 28 above; Orla Lynskey, n 28 above, p.573.
[30] Kokott and Sobotta, and Lynskey, *Ibid*.

European scholars on how the right to data protection could be conceptualized separately from the right to private life taking into account the different approaches to this problem taken by the ECHR and EU Law. The present writer offers his assessment of the right to data protection as a separate fundamental right, distinct from the right to private life, thus making a contribution to the current European legal discourse on what the right to data protection represents.

In the examination of the two aforementioned European legal frameworks, another question arises: whether the EU's foundation in a market-oriented organisation influences the system for safeguarding fundamental rights. The literature and case law analysis of the Court of Justice of the EU examines an extensive critical discourse on EU protection of fundamental rights.[31] It is pointed out that in actual adjudication, the CJEU often prioritizes market freedoms and economic values over fundamental rights. The Data Retention Directive (DRD)[32] exemplifies such legislation, establishing a comprehensive framework for surveillance used by security forces and police in counterterrorism efforts. Under the DRD, law enforcement agencies were granted access to all necessary communications data – specifically retained by private companies for surveillance purposes.

The supplementary research objective, stemming from the fact that neither of the above European legal regimes is binding for Tajikistan and the country is not a member of the Council of Europe, is to briefly explore questions around the legal nature and grounds for the application of the ECHR and EU law in Tajikistan. Through the extraterritorial application of the GDPR, data protection rules are accepted beyond the territory of the EU, and such countries as Tajikistan tend to adopt necessary legislation, which would be in compliance with the highest standards set by the GDPR on data protection. This thesis thus examines the possibility of accepting standards of data protection established by the GDPR and other EU laws on data protection by Tajikistan through the avenues proposed by the GDPR's rules ensuring extraterritorial application of GDPR standards abroad.

This thesis will discuss the application of GDPR rules through a so-called 'Brussels Effect', whereby the standards set by GDPR are adopted by third countries to enable their businesses to access the EU market for goods, services, and capital. This thesis also engages

[31] See Anneli Albi 'Erosion of Constitutional Rights in EU Law: A Call for Substantive Cooperative Constitutionalism' Part 1 [2015] 9/2 Vienna Journal of International Constitutional Law (ICL Journal) 151; Stijn Smismans 'The European Union's Fundamental Rights Myth' [2010] 1 JCMS 45; Aidan O'Neill and Jason Coppel *The European Court of Justice Taking Rights Seriously?* (EUI, 1992).

[32] Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54 (DRD).

in the discussion about legal transplants, their advantages and disadvantages. It is submitted that after the collapse of the Socialist system, the newly emerged States in Central and Eastern Europe became recipients of 'imported' laws from the West.[33] For a developing country with limited resources and a lack of know-how in law-making, such as Tajikistan, it could be advantageous to adopt a law in a particular area, which is designed and successfully implemented in the developed country. At the same time, such a law ought to fit into the local context, political, economic, or cultural. It is argued that more technical and less political laws, such as contract law, company law, etc., could be transplanted quite easily.[34] This thesis discusses whether the GDPR could be seen as a technical piece of legislation rather than political, which could help Tajikistan to adopt its standards in its local legislation on data protection.

Although Tajikistan is not a party to the ECHR, the choice of the ECHR is substantiated by several factors. The ECHR was drafted after the Universal Declaration of adopted, and its drafting history may better explain the emergence of the right to privacy as an umbrella term for a wide range of interests, which include respect for dignity, identity, autonomy, freedom from home search and interference with correspondence.[35] Moreover, the ECtHR has developed an extensive case law on the right to private life and data protection, especially in surveillance cases. The standards established by the ECtHR on surveillance cases represent the standards from the human rights law perspective. Those standards influence the domestic public law of the ECHR Member States.

1.2. The Structure of the Thesis. An Outline of the Chapters and the Main Argument

The overarching argument of this thesis is that Tajik laws on privacy and data protection could provide better safeguards to individuals if privacy and data protection concepts are revised and reformulated by Tajik scholarship in the light of modern concepts of privacy, which inform the contemporary data protection legal framework in Europe. By way of a brief outline of the chapters, which is explained more fully below, Chapter 2

[33] On 'Importation of law' see Dupre C. *Importing the Law in Post-Communist Transitions: The Hungarian Constitutional Court and the Right to Human Dignity* (Hart Publishing, 2003) 192.
[34] See Thomas Waelde and James Gunderson 'Legislative Reform in Transition Economies: Western Transplants – A Short-Cut to Social Market Economy Status?' (1994) 43 International and Comparative Law Quarterly 347, at pp. 368-369.
[35] On the history of drafting ECHR see Schabas W. *The European Convention on Human Rights Commentary* (OSAIL 2015); Oliver Diggelmann and Maria Nicole Cleis 'How the Right to Privacy Became a Human Right' (2014) 14 Human Rights Law Review 441.

provides a background to the historical development of the concept of privacy and the data protection laws in Tajikistan. It explains that the Tajik concept of privacy has been formulated under the influence of Soviet legal thought. Thereafter, Chapter 3 as a theoretical chapter discusses how privacy is conceptualized in the West and explores the contemporary concept of privacy which informs modern development of data protection laws in Europe. Chapter 4 outlines the right to data protection as part of the right to private life under the ECHR and explores standards of privacy and data protection established by the ECtHR case law on surveillance matters. Subsequently, Chapter 5 discusses how EU law establishes standards for ensuring the right to privacy and data protection within the EU Member States and beyond the EU. Finally, Chapter 6 juxtaposes the privacy and data protection laws of Tajikistan with the standards established by the ECHR and EU law, and discusses what lessons Tajikistan could learn from the ECHR and EU law in order to further develop its domestic legislation on data protection. The contents of all chapters of this thesis are next outlined in greater detail below.

Chapter 2 begins with the introduction of Tajikistan's Soviet legal background, which is important for understanding the current legal system and the development of legal scholarship in Tajikistan. It emphasizes that Tajik legal scholars are informed by Soviet and post-Soviet legal literature. The Chapter explores that as a socialist Constitution, Tajik Soviet Constitutions were anti-liberal, did not provide for separation of powers, did not respect individuals, and, generally, did not provide fundamental rights of individuals. It explains why the current Tajik concept of privacy is informed by an outdated Soviet idea of personal life. As a result of the influence of the Soviet legacy on Tajik legal scholarship, the concept of privacy in Tajikistan is mainly formulated from the private or civil law perspective.[36] These shortcomings of the Tajik concept of privacy, the Chapter argues, result in the current Tajik laws[37] not fully providing necessary privacy and data protection safeguards to individuals, because the State or its agents are not seen as perpetrators, but rather as protectors of the right to the private life of individuals. The final parts of Chapter 2 discuss in detail the main laws of Tajikistan, which regulate the issues of public and private surveillance: the Law on Data Protection and the Law on Crime Detection and Investigation, and explore the problems and gaps within those laws. Chapter 2 contends that the primary obstacle hindering the implementation of the Law on DP in Tajikistan is the absence of a

[36] See, e.g., K. Kurbanov, n 12 above.
[37] The Law of the RT "On Personal Data Protection", No 1537, dated 3 August 2018; and the Law of the Republic of Tajikistan (RT) "On Crime Detection and Investigation", No 352 dated 2 March 2011.

comprehensive conceptualization of privacy within Tajik legal scholarship, which should deviate from the Soviet interpretation of privacy.

Chapter 3 as a central conceptual chapter of this thesis seeks to identify from the myriad of concepts of privacy within Western legal scholarship the concept of privacy, which reflects a contemporary understanding of privacy in the context of personal data protection. The Chapter argues that Westin's account of privacy is an accurate and suitable concept of privacy which explains the modern development of data protection laws in Europe. Subsequently, the Chapter draws up distinctions in the understanding of privacy within Western countries. Through reading Whitman,[38] this thesis discusses different perceptions of privacy in Europe and the United States of America, based on the underlying value that privacy aims to protect.

The Chapter thereafter provides an overview of how the concept of privacy has been developed in Europe both in national constitutions and later as a human right enshrined in the ECHR. It is argued that in Europe the concept of privacy stems from the broader theme of the right to dignity and the right to personal development.[39] For the completeness of the account, this thesis explicates a critique of the mainstream Western concepts of privacy provided by modern legal and sociolegal scholarship, according to which privacy should be considered as a common value as opposed to individualistic approaches of the mainstream concepts.[40] Privacy, it is argued, must be explained within the context of society.[41] The final part of Chapter 3 turns to the issue of protecting privacy in the context of large private companies processing extensive amounts of personal data, where greater threats to privacy could emerge from government agencies using private databases of personal data. Since the mainstream concept of privacy informs contemporary standards of human rights protection and modern data protection laws in Europe, further two chapters – Chapter 4 and Chapter 5

[38] James Q. Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty", in "The Yale Law Journal", 2004, vol 113, p. 1151 - 1221.
[39] See Julie Cohen 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1; Stig Strömholm *Right of Privacy and Rights of the Personality: A Comparative Survey* (Nordic Conference on Privacy organized by the International Commission of Jurists, Stockholm, 1967); Edward Eberle 'Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview' (2012) 33 Liverpool Law Review 201; Lynskey, n 28 above.
[40] See Spiros Simitis 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania Law Review; Daniel Solove 'The Meaning and Value of Privacy' in Beate Roessler and Dorota Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP, 2015) 71; Lisa Austin, n 7 above; Priscilla Regan 'Privacy and Common Good: Revisited' in Beate Roessler and Dorota Mokrosinska (eds.) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP 2015) 50.
[41] See Helen Nissenbaum 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119; Helen Nissenbaum 'Privacy and Common Good: Revisited' in Beate Roessler and Dorota Mokrosinska (eds.) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP 2015) 278.

– are devoted to the identification and examination of those standards for the protection of the right to personal data secured by the ECHR and EU law.

Chapter 4 examines the ECHR as a standard-setting instrument, against which Tajikistan laws are evaluated later in Chapter 6. It is divided into two main sections. The first section provides a general overview of Article 8 of the ECHR – the right to private life. The scope of Article 8 is explained as protecting a wide range of private interests, including personal data. The Chapter further shows that the right to private life is not an absolute right. The ECtHR examines whether interference with private life by the public authorities could be justified by certain public aims and social needs, such as national security. The first section of Chapter 4 finds that the ECtHR engages in a balancing exercise while determining whether the interference was lawful and necessary in a democratic society. The ECtHR examines the proportionality of measures taken to protect legitimate aims in the event of interference with privacy by government authorities. The ECtHR could widely employ the doctrine of margin of appreciation when there is no unified practice among Member States.[42]

The second section of Chapter 4 engages in examining the ECtHR case law on surveillance issues. It points out that State surveillance could take the form of interception of communications and the use of retained personal data. Through examination of the case law, this thesis elucidates what standards of protection the ECHR has been establishing with respect to the right to private life in surveillance cases. This section of Chapter 4 synthesises the emerging case law on the protection of private life in bulk surveillance cases. Bulk surveillance is usually conducted with respect to communications data, which is different from the content data. Communications data provides information about the communications, i.e., time, frequency, addresses, place, and other characteristics of the sent communication. The Chapter argues that the ECtHR in new realities changes its approach to the processing of communications data as an equally intrusive form of surveillance as the processing of content data.[43] The main finding of this section is that it provides a list of requirements for the domestic law of the Member States of the Council of Europe to protect private life from new types of intrusion that emerge in connection with bulk surveillance.

[42] On 'margin of appreciation' see Yutaka Arai 'Margin of Appreciation Doctrine in the Jurisprudence of Article 8 of the European Convention on Human Rights' (1998) 1 Netherlands Quarterly of Human Rights 16, p.41; Steven Greer 'The Interpretation of the European Convention of Human Rights: Universal Principle or Margin of Appreciation' (2010) 3 UCL Human Rights Review 1; Koen Lemmens 'The Margin of Appreciation in the ECtHR's Case-Law' (2018) 20 European Journal of Law Reform 2-3, p.78; Eva Brems 'Positive Subsidiarity and its Implications for the Margin of Appreciation Doctrine' (2019) 3 Netherlands Quarterly of Human Rights 37, p.210.

[43] *Big Brother Watch*, n 25 above, Paragraph 356.

They are called 'Weber requirements',[44] and the ECtHR has been governed by them while considering recent cases including *Zakharov v Russia*.[45] The Chapter concludes that some crucial provisions of the Russian law on crime detection and investigations have been found by the ECtHR to be incompatible with the Weber requirements.

Subsequently, Chapter 5 represents another core part of this thesis, which engages in discussing the standards of privacy and data protection established within EU law. It also consists of two main sections. The first main section discusses the right to privacy and data protection as a fundamental right enshrined in the Charter of the Fundamental Rights of the EU.

The second main section of Chapter 5 examines secondary legislation of the EU in the field of data protection, with the aim of explaining standards of data protection, which may be of interest to Tajikistan in terms of improving its data protection law standards. It starts with the Data Protection Directive (DPD),[46] which was in force in 1995 – 2018. It is argued that the main purpose of enacting the DPD was the intention of the drafters to harmonize the data protection laws of the EU Member States by introducing a conflict of laws mechanism. That mechanism was designed to identify the law of which State within the EU would apply to a cross-border transfer of personal data.[47]

It shows the evolution of the protection of fundamental rights within the EU bearing in mind that the EU legal order initially was based only on market integration and did not contain a fundamental rights dimension. Chapter 5 thus engages in the discussion of whether market freedoms, such as freedom of movement of goods, services, and capital proclaimed at the time of the creation of the EU – at the time, the European Community (EC) – prevail over fundamental rights of individuals in the jurisprudence of the CJEU.[48] The Chapter elucidates the critical discussion in the example of the DRD, which, it is argued, became regarded as an instrument for Orwellian surveillance by government authorities over

[44] The ECtHR initially identified six main requirements to safeguard the right to private life in surveillance cases in *Weber and Saravia v Germany* in 2006. Then, in 2021 the Court revisited that list of criteria in the case of bulk surveillance *Big Brother Watch v UK*. Now, 'Weber requirements' consist of 6 criteria. See *Weber and Saravia v Germany*, Admissibility Decision of 29 June 2006, Paragraph 95; and *Big Brother Watch and Others v* UK, Judgment of 25 May 2021, Paragraph 361.
[45] *Zakharov v Russia,* Judgment of 4 December 2015.
[46] Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (1995) OJ L281/31(Data Protection Directive, DPD).
[47] Article 4 DPD is called 'National Law Applicable'.
[48] See Anneli Albi, n 31 above; Stijn Smismans, n 31 above; and Aidan O'Neill and Jason Coppel *The European Court of Justice Taking Rights Seriously?* (EUI, 1992), at p.31.

people.[49] The purpose of the DRD has been the harmonization of data retention laws among EU Member States with the main focus on market freedoms rather than fundamental rights.[50] The validity of the DRD was challenged before the CJEU two times. The first time, in 2006[51] it failed as the CJEU focused on the protection of the single market rather than the protection of fundamental rights of individuals.[52] Only in 2014, did the CJEU invalidate the DRD as the latter failed to provide sufficient safeguards for the protection of the right to privacy.[53] By examining similarities and differences between the CFREU and the ECHR, Chapter 5 points out that the aim of the ECHR is to provide basic protection for the right to private life in cases where such protection has failed at the national level. By contrast, EU law is meant to establish a uniform standard of protection for all EU Member States.

The first section of Chapter 5 concludes by drawing out the differences in approaches to privacy and data protection taken by EU law and by the ECHR. There, this thesis is engaged in the discussion among European legal scholars on why and how the right to data protection is separated from the right to private life under the EU law, and what is the substantial difference between these two fundamental rights. Chapter 5 shows that the CJEU conflates these two fundamental rights in its case law. This thesis proposes its assessment of the right to data protection and interprets it as a procedural or technical right.

The analysis of the GDPR and the DPD has shown that all references from the DPD to the right to private life were substituted with references to the fundamental right to data protection in the GDPR. The GDPR has become an instrument for the protection of personal data when large amounts of data are transferred beyond the territory of the EU. Chapter 5 concludes that the extraterritorial application of the GDPR takes different forms: through the application of GDPR to the foreign controllers and processors that process the personal data of EU residents, and through the adequacy decisions taken by the European Commission with respect to the data protection regime in a particular third country.

The sixth Chapter revisits the examination of the privacy and data protection laws of Tajikistan which began in Chapter 2, and connects two previous chapters of this thesis with an argument that there is much scope for improvement of Tajik laws in the light of the

[49] Anneli Albi "The EU Data Retention Directive in Twenty-Eight Member States: An emblematic case study of blind spots, lost higher national standards and systemic flaws in autonomous EU human rights law and discourse" p.19. Unpublished paper, cited with the permission of the author.
[50] For the critique of the CJEU's approach to promote market freedoms and economic values over fundamental rights, see Anneli Albi, n 31 above, p.159; and Stijn Smismans, n 31 above.
[51] Case C-301/06 *Ireland v Parliament and Council,* Judgment of 10 February 2009.
[52] Albi, *ibid.*, p.33.
[53] See Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others,* Judgement of the Grand Chamber dated 8 April 2014.

standards set by the ECHR and EU law on privacy and data protection. This Chapter recalls the shared historical legacy between Tajikistan and Russia under the Soviet regime and points out that the ECtHR case law could be relevant to Tajikistan as a standard-setting instrument. It posits that the ECtHR's findings in *Zakharov v Russia*[54] could offer valuable insights into the Law of the Republic of Tajikistan on Crime Detection and Investigation that requires enhancement to safeguard the privacy of individuals in surveillance cases. Consequently, this thesis undertakes an examination of the CDI through the lens of the 'Weber requirements' delineated in the ECtHR jurisprudence, particularly as exemplified in the *Zakharov v Russia* case.

The sixth Chapter subsequently turns to the question of bulk surveillance in Tajik laws. It explains that the laws in Tajikistan do not expressly and in detail regulate this area of surveillance. It is argued that some governmental legal normative acts, which are below the laws in the hierarchy of legal sources, provide for the possibility of conducting bulk surveillance by law enforcement bodies contrary to the standards of privacy and data protection established by the ECHR. It is submitted that in some instances law enforcement bodies in Tajikistan could establish a direct connection with the private entities' databases containing large amounts of their customers' personal data.[55]

The sixth Chapter thereafter explains that the Tajikistan Law on Data Protection does not provide sufficient safeguards in respect of data processing as established by the GDPR. It is designed not to protect individuals from the State data controllers. On the contrary, the law gives the State organs almost unlimited powers to collect and use the personal data of individuals without their consent, and for almost any purpose. In line with the findings of the second Chapter of this thesis, this Chapter shows that the laws in Tajikistan reflect the Tajik legal thought on the right to private life and data protection: State organs could not be seen as perpetrators, as they are called to protect individuals from other individuals, whose actions may interfere with their private lives. The government uses a human rights protection narrative to process personal data without any constraint. Private data processors and controllers are put in an unequal situation compared to the State controllers because the only lawful ground for them to collect and process personal data is receiving the consent of the data subject. For instance, the law does not foresee other lawful possibilities for private controllers and processors in Tajikistan to process the personal data of their customers on the

[54] *Zakharov v Russia,* see n 45 above.
[55] Resolution of the the Government of Tajikistan No 208 dated 31 March 2020 'On the Procedure of Registration of Mobile Communication Devices and Defining Functions of the State System of Identification of Mobile Communication Devices', Paragraph 56.

basis of performing contracts between them and their customers or in other cases, which are allowed by EU law.[56]

Finally, Chapter 6 is engaged in the discussion on whether Tajikistan needs to adopt similar standards of data protection, which are established and used in the EU. The Chapter discusses the 'Brussels effect', which means that the standards established by EU law, specifically data protection law, could be adopted by third countries in order for the businesses of such third countries to have access to the EU market of goods, services, and capital. This thesis thereafter engages in the discussion about legal transplants,[57] their advantages and disadvantages. It is explored that Tajikistan as one of the post-Soviet States has been a recipient of many laws, both in the public and private sphere, from the European States. The thesis points out that not all 'imported'[58] laws to Tajikistan are implemented to the fullest extent, and that a transplanted law ought to take into consideration Tajikistan's economic, cultural, and political context.

In the concluding Chapter, this thesis calls for the need for debate among legal scholars in Tajikistan to challenge the understanding of the right to privacy that has been established since Soviet times. The result of such a discussion may lead to a reconfiguration in the Tajik point of view on the relationship between the State and the individual in matters related to protecting privacy. This thesis submits that the individual must have a sufficient set of guarantees for the protection of his private life from encroachments by the State itself, and not just from the interference of third parties.

1.3. Methodology

The present author addresses all the research questions mentioned in Section 1.1 above by employing a legal positivist method of research. It is the research process used to identify, analyse, and synthesize the content of the law.[59] Its principal goal is to describe what the law is and how it applies. The doctrinal research also provides an analysis of the

[56] See the Law on DP, Articles 8 and 11.
[57] On the theoretical discussion about legal transplants see Otto Kahn-Freund 'On Uses and Misuses of Comparative Law', (1974) 37 Modern Law Review 1; Watson A. *Legal Transplants: An Approach to Comparative Law* (Scottish Academic Press, 1974; American ed. University Press of Virginia, 1974); Andrew Harding 'The Legal Transplants Debate: Getting Beyond the Impasse?' in Breda V. (ed.) *Legal Transplants in East Asia and Oceania* (CUP, 2019) p.13; Pierre Legrand 'The Impossibility of Legal Transplants' (1997) 4 Maastricht Journal of European and Comparative Law 111; Glanert S., Mercescu A., and Samuel G. *Rethinking Comparative Law* (2021, Edward Elgar Publishing Limited); and Jennifer Corrin 'Transplant Shock: The Hazard of Introducing Statutes of General Application' in Breda V. (ed.) *Legal Transplants in East Asia and Oceania* (CUP, 2019) p.34.
[58] See Dupre, n 33 above, who introduced the term 'importation of law' to a wider discourse.
[59] See Hutchinson T. 'Doctrinal Research' in Watkins D. (ed.) *Research Methods in Law* (2nd ed., Routledge, 2017), p.13.

law development through judicial reasoning and legislative enactment.[60] The thesis will also engage with the discourse and methodology regarding legal transplants, outlined more fully above.

The focus of this thesis is threefold: 1) Tajikistan laws on privacy and data protection; 2) the ECHR and ECtHR jurisprudence on privacy and data protection; and 3) EU law on privacy and data protection. For each of these three legal systems, the present author has identified, examined, interpreted, and analysed different sets of sources.

With respect to Tajik primary sources for this thesis, Tajikistan laws are reviewed and analysed. The Constitution of the Republic of Tajikistan stands on top of the hierarchy of domestic laws and provides a bill of rights, which includes the right to privacy and data protection.[61] The focus of this thesis will be on the laws regulating surveillance issues. Surveillance in the 21st century could be conducted by both public and private entities because the main sources of collecting and using personal data for the purposes of surveillance are private businesses – controllers and processors, which hold databases.[62] Thus, two different sets of laws, which regulate the use of personal data by public authorities on the one hand, and by private entities, on the other hand, will be examined and analysed:

1) laws regulating surveillance directly by public authorities – law enforcement bodies in Tajikistan – mainly, the Law of the Republic of Tajikistan "On Crime Detection and Investigation" (CDI), but also additionally the Law "On the Organs of National Security of the Republic of Tajikistan", Criminal Procedure Code of the Republic of Tajikistan and others;
2) laws regulating data protection issues, which enable public authorities to conduct surveillance by accessing large amounts of personal data collected and processed by private entities, mainly, the Law of the Republic of Tajikistan "On Personal Data Protection", and also the Law of the Republic of Tajikistan "On Information" and others.

Other legal acts, which are subordinate to the laws and the Constitution of Tajikistan, will also be subject to analysis in this thesis: the "Procedure of Registration of Mobile Communication Devices and Defining Functions of the State System of Identification of Mobile Communication Devices", approved by the Government of Tajikistan; the

[60] Dobinson I. and Jones F. 'Legal Research as Qualitative Research' in McConville M. and Chui H.W. (eds.) *Research Methods for Law* (Edinburgh University Press, 2017), p.21.
[61] Article 23 of the Constitution of the Republic of Tajikistan of 4 November 1994 implies the protection of the right to private life and the right to personal data protection.
[62] For more on public and private surveillance see Neil Richards, n 8 above.

Resolution of the Government of Tajikistan "On the Unified Commutation Centre of Electric Communications", and other legal acts. These acts provide possibility for the government agents to conduct surveillance by using privately held databases. This author accesses a privately held database of laws and other legal normative acts of the Republic of Tajikistan in two languages – Tajik and Russian.

Judicial decisions in Tajikistan are not considered precedents, as Tajikistan's judiciary system belongs to a system in the civil law tradition. There are no accessible online or other databases of Tajik court judgments, and it is not usually within the Tajik legal scholarship tradition to refer to the case law of the Tajik courts in academic research papers. The possibilities for the present author to access data from the Tajik court jurisprudence have been limited.

A key source of law for this thesis is international human rights treaties, as privacy and data protection are considered to be part of human rights law. In terms of treaties to which Tajikistan is a party, these include:

- the International Covenant on Civil and Political Rights (ICCPR)[63] and its optional protocol allowing the UN Human Rights Committee (HRC) to receive individual communications from Tajik nationals, whose rights and freedoms are allegedly violated by the State;[64]
- the Commonwealth of Independent States Convention on Human Rights and Fundamental Freedoms dated 26 May 1995. This Convention has been in force since 1998 but has not been implemented and has played only a political window-dressing role. Its main body – the Commission has not been formed until November 2023.

The choice of examining the ECHR approach and the ECtHR's jurisprudence on privacy and data protection is explained in Section 1.1 above. The European Court of Human Rights has developed an extensive case law on the right to private life and data protection. This thesis reorganizes the case law into coherent categories.[65] Almost 80 different

[63] International Covenant on Civil and Political Rights (ICCPR), adopted by the UN GA on 16 December 1966 and entered into force on 23 March 1976.
[64] Tajikistan is a party to the ICCPR since 4 January 1999. There were no communications against Tajikistan on the alleged violation of the right to privacy related to personal data protection.
[65] According to Martha Minow, legal research involving case law should include: a) organization and reorganization of case law into coherent elements, categories, and concepts; b) acknowledgment of distinction between settled and emerging law; and c) identification of the difference between majority and 'preferred' or 'better' practice. See Martha Minow 'Archetypal Legal Scholarship – A Field Guide' (2013) 63(1) Journal of Legal Education 65, at pp.65-66.

judgments of the ECtHR on privacy and data protection are examined, which allows this thesis to analyse the evolution of the concept of the right to private life through the development of personal data protection rights. This thesis explains the settled and emerging law in surveillance cases. Up to 25 judgments of the ECtHR on State surveillance issues are part of this thesis; almost half of them concern bulk surveillance, which involves interception and processing of communications data. 'Bulk surveillance' is understood as a method of indiscriminate and large-scale processing of communications data by intelligence and law enforcement agencies for the detection and prevention of crimes. This thesis explains the 'Weber requirements' as an emerging and changing law.[66] These requirements serve as standards of privacy and data protection during State surveillance established by the ECtHR. Especially, examining the case of *Zakharov v Russia*[67] will be pertinent to the aims of the present thesis. The ECtHR in that case has scrutinized the Russian law on crime detection and investigation, which is almost identical to its Tajikistan counterpart.

The choice of examining EU data protection laws[68] lies on the premise that the EU primary law has separated the right to data protection from the right to private life, giving the former the significance of a fundamental right.[69] The EU law approach is thus different from the ECHR approach – the latter implies that the right to data protection is an integral part of the right to privacy. The difference between the two fundamental rights under the EU data protection legal framework is examined to better understand current developments in the concept of privacy.

In order to examine the EU approach to the right to data protection and conceptualise this right as a separate fundamental right, a set of primary and secondary literature on EU law on data protection is examined and analysed. The primary literature on EU law consists of the main treaties of the EU: the Treaty of the European Union and the Treaty on Functioning of the European Union,[70] as well as the CFREU as part of the primary EU law.

[66] On 'Weber requirements' see n 44 above.
[67] *Zakharov v Russia,* see n 45 above.
[68] The GDPR, n 13 above; the DPD, n 46 above; and the DRD, n 32 above.
[69] See Article 16 of the Treaty on Functioning of the European Union and Article 8 of the EU Charter of Fundamental Rights (CFREU). In 2007 two main EU treaties were amended and restated: the Maastricht Treaty of 1992, now called the Treaty on European Union (TEU), and the Treaty of Rome (TEC), now called the Treaty on the Functioning of the European Union (TFEU). The CFREU was adopted by the European Parliament, European Council and the Council on 7 December 2000 and entered into force together with the Treaty of Lisbon on 1 December 2009.
[70] In 2009 TEU and TFEU entered into legal force. Article 16(1) of the TFEU establishes that everyone has the right to the protection of personal data concerning them.

The following EU legislative acts, current and old, are examined: the General Data Protection Regulation,[71] the Data Protection Directive,[72] and the Data Retention Directive.[73]

This thesis engages in critical discussions on conceptualisation of the fundamental right to data protection and the CJEU's stance in cases where the protection of fundamental rights has been at stake. The CJEU plays a key role in the interpretation and application of EU law on data protection.[74] In general, 30 different judgments of the CJEU are used in this thesis. Its emerging case law on privacy and data protection, such as *Schrems*,[75] *Digital Rights Ireland*,[76] and *Googe Spain*,[77] is analysed with a view to explaining the CJEU stance on the right to data protection as a fundamental right and the application of EU law beyond the territory of the EU.

Opinions of the Advocates General of the CJEU are used in this thesis along with the scholarly articles and books, which will help to engage in the discussions on the right to data protection under EU law. The ECtHR and the CJEU case law are worked through, respectively, the Eur-Lex and Hudoc online free databases, and all necessary general legal and thematic periodicals, as well as some books are used in the University of Kent's electronic library accessible online.

After examining privacy and data protection laws in three legal systems: Tajikistan, ECHR, and EU, the thesis turns to analyse Tajik legislation in the light of international human rights and data protection standards set by the ECHR and EU. Such analysis helps to determine possible shortcomings in the Tajik legislation and suggests areas of improvement in order for it to be compatible with the highest standards of privacy and data protection.

This thesis additionally engages in the discussion of the 'Brussels effect'[78] in relation to data protection issues. It seeks to identify what particular laws and what particular provisions of laws in Tajikistan could be improved or changed in order to provide adequate

[71] See the GDPR, n 13 above.
[72] The DPD, n 46 above. The DPD was in force until 2018 when the GDPR came into legal force.
[73] See DRD, n 32 above.
[74] See Christopher Docksey and Hielke Hijmans 'The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law' (2019) 5 European Data Protection Law Review 300.
[75] There are two cases: *Schrems v Data Protection Commissioner,* Judgment of the GC dated 6 October 2015; and Case C-311/18 *Data Protection Commissioner v Facebook and Maximillian Schrems,* Judgment of the GC dated 16 July 2020.
[76] See Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others,* Judgement of the Grand Chamber dated 8 April 2014.
[77] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez,* Judgment of the GC dated 13 May 2014.
[78] The term 'Brussels effect' is coined by Anu Bradford and borrowed from the term 'California effect', which has been in use since the 1990s. See Anu Bradford, n 14 above.

protection to individuals as understood by the GDPR. Thus, the extraterritorial application of GDPR is discussed. A scholarly debate on the possibility of legal transplants and their adaptability in the political, economic, and cultural context of a receiving State, such as Tajikistan will be examined. Additionally, the laws of Tajikistan will be examined not only from the perspective of what the law is but also from the point of view of what the law ought to be.[79] In this regard, possible changes in the laws of Tajikistan will be discussed from the perspective of contextual adaptability of rules and principles of data protection transplanted from one jurisdiction to another.

[79] According to Bhat both the 'is' and 'ought' aspects of law are addressed by doctrinal legal research. See P. Bhat 'Doctrinal Legal Research as a Means of Synthesising Facts, Thoughts and Legal Principles' in P. Bhat *Idea and Methods of Legal Research* (OUP, 2019) 627, at p.148.

Chapter 2. Tajikistan Laws Related to Privacy and Data Protection Issues

2.1. Introduction

This Chapter provides an overview of the laws of the Republic of Tajikistan related to privacy and data protection issues. It is divided into five parts: (i) a general introduction to the Tajikistan legal system; (ii) the Tajik law approach to the concept of privacy; (iii) legal background for privacy and data protection in Tajikistan; (iv) laws regulating activities of the law enforcement bodies in combatting serious crimes; and (v) laws regulating personal data processing by businesses in the context of their economic activity. This Chapter will help the reader to understand the historical and legal context of Tajikistan's approach to privacy and data protection.

A division of Tajikistan laws into two sets of laws is explained by different rights and values, which the laws are designed to protect. Laws regulating activities of the law enforcement organs will be examined from the perspective of the protection of privacy interests from the interference of State agencies with correspondence and privacy of individuals. Laws on data protection will be examined in the context of private parties: corporations and companies interfering with the privacy of individuals. The Tajik constitutional provision on the right to privacy creates the ground for such division.

A general introduction to the Tajik legal system is necessary for a fuller understanding of the nature of the emergence and development of Tajik legal thought regarding the protection of privacy and personal data. A short digression into the Soviet legacy of Tajikistan will help in understanding why the Tajik legal scholarship, relying mainly on Russian authors, discusses the concept of private life from the point of view of civil law, and why it practically does not pay attention to this problem from the public law point of view.

This Chapter will explain the main problem of defining the concept of private life by the Tajik academy. In its understanding, the private life of an individual must be protected from encroachment by other individuals. Everyone recognizes that the right to privacy is a constitutional human right; however, in the works of Tajik authors, there is no significant discussion regarding the violation of this human right by State bodies, in particular, those that conduct crime detection and investigation activities. This approach to understanding the

right to privacy leads to some inconsistencies in the legislation of the Republic of Tajikistan on the protection of personal data.

In preparing this Chapter, the present writer encountered some challenges that deserve special mention. Firstly, the Tajik legal literature is as yet in the early stages and not extensively developed regarding the study of the right to privacy and personal data. Secondly, Tajik authors mainly refer to their Russian or other post-Soviet colleagues, whose works are not always possible to access due to recent events,[1] when it is almost impossible to purchase a book from Russia or register in Russian paid academic resources to gain access to the literature. Thirdly, some Tajik authors are not always careful when referring to Russian or other sources. Sometimes the present writer could not find the necessary thought in the text of the sources, to which Tajik authors referred, and sometimes the present author found the thoughts of Russian authors in the works of Tajik scientists but did not find pertinent references to Russian authors there.

Despite these problems, this thesis managed to show in this Chapter the Tajik approach to the issue of privacy and how the emergence of legislation on personal data can change the perception of privacy. The challenges to Tajikistan's legislation explicated in this Chapter are more fully addressed if this thesis refers to the approach to privacy and personal data protection adopted under the European Convention on Human Rights, as well as European Union (EU) data protection legislation, which set a high standard of such protection. Chapter 4 will elaborate on the jurisprudence of the European Court of Human Rights in relation to the right to privacy and discuss the standards for the protection of this human right established by this Court in surveillance cases.

2.2. A General Introduction to the Tajik Legal System and Its Historical Background

2.2.1. The Soviet Period (1924-1991)

The development of the Tajik legal system during the Soviet period was an important underpinning for the modern legal system in Tajikistan. In order to grasp the full legal nature of Tajik data protection and privacy law, it is important to evaluate that period in the light of the distinct legal background against which the Tajik law has evolved.

[1] After the Russian invasion of Ukraine in February 2022, Western countries subjected Russia to new economic sanctions, making it almost impossible to buy books or articles online from Russia.

In the period from 1924 to 1991, Tajikistan was a part of the Union of the Soviet Socialist Republics (the USSR), initially as an autonomous republic within the Uzbek Soviet Socialist Republic, and then, since 1929, as a separate union republic.[2] The first two Tajik Constitutions of 1929[3] and 1931[4] thus reflected the political and organizational structure of the transitional[5] state: the 1929 Constitution was the constitution of the Tajik autonomous division within the Uzbek Republic, and the 1931 Constitution defined Tajik statehood as a separate polity within the USSR. According to Tajik archives, those two constitutions were only available in the Russian language and were not yet translated into Tajik.[6]

The next two Tajik Soviet Constitutions (1937 and 1978)[7] were adopted in accordance with the USSR Constitutions of 1936 and 1977.[8] They were reflecting 'the victory of socialism' and 'a developed socialism' in the country, respectively.[9]

The Tajik State power system during the Soviet time was identical to the system at the Union level in the USSR: there was no separation of powers, known in the liberal democratic States. The Soviet concept of State power was based on the Marxist ideas of 'an operating corporation, which legislates and executes the laws at the same time.'[10] Grimm explains that socialist constitutions 'break with liberalism'.[11] Speaking about the Chinese Constitution as an example of a socialist constitution, Grimm further elucidates that the 'anti-liberal' nature of socialist constitutions rejects the liberal idea of the separation of power and the rule of law.[12]

---

[2] From 1924 to 1929 its official name was Tajik Autonomous Soviet Socialist Republic, and from 1929 to 1991 – Tajik Soviet Socialist Republic.
[3] The Constitution (Basic Law) of Tajik Autonomous Soviet Socialist Republic, adopted by the Resolution of the 2nd Congress of the Soviets of the Tajik ASSR on 28 April 1929.
[4] The Constitution (Basic Law) of Tajik Soviet Socialist Republic, adopted by the Resolution of the 4th All-Tajik Congress of the Soviets of the Tajik SSR on 25 February 1931.
[5] Transitional to socialism State. See Shamolov A.A. (ed.) *Majmuai Konstitutsiyahoi Tojikiston* [*The Compilation of the Constitutions of Tajikistan*] (Instituti Falsafa, Siyosatshinosi va Hukuki Akademiyai Ilmhoi Jemherii Tojikiston [The Institute of Philosophy, Political Science and Law of the Tajik Academy of Sciences], 2015) 633, at 22 (in Tajik and Russian).
[6] *Ibid.* at 5
[7] The Constitution of the Tajik SSR dated 1 March 1937 and the Constitution of the Tajik SSR of (April 1978).
[8] The Constitution of the USSR, adopted by the 8th All-Union Extraordinary Congress of the Soviets on 5 December 1936, and the Constitution of the USSR, adopted the Supreme Soviet of the USSR on 7 October 1977.
[9] See Shamolov, n 5 above, at 22.
[10] Karl Marx in 'The Civil War in France' wrote about the Paris Commune, which must be 'a working, not a parliamentary body, executive and legislative at the same time.' See Karl Marx and Friedrich Engels *The Civil War in France* (English edition of 1871. Marc Harris, 2010).
[11] See Dieter Grimm 'Types of Constitutions' in Rosenfeld M. and Sajo A. (eds) *Comparative Constitutional Law* (OUP, 2012), p.98-132, at p.128.
[12] Grimm, n 11 above.

Soviet Tajikistan, as part of the USSR, was a totalitarian State. Müllerson points out that it was almost impossible to speak about human rights in the totalitarian USSR.[13] He explains that 'human rights, which are often rights of the individual versus the state, presuppose the existence of […] an autonomy of the individual *vis-à-vis* the state. This was not a case in the Soviet Union.'[14]

The legislative power belonged to the Soviets, which were represented by the people's deputies elected on a non-alternative basis.[15] The Soviets were considered the supreme organs of power. People's deputies mainly represented their voting circuit due to their responsibility to take into account the demands of people from their voting circuit, and responsibility to implement the electoral mandate.[16] Organs of executive power at the central level were subordinated to the Soviets. At the local level they were even an integral part of the Soviets, and were formed from among the people's deputies.[17] They were called 'executive committees of the Soviets'.

The Tajik Constitutions of 1937 and 1978 partially contained a bill of rights, which included a provision on the right to privacy.[18] Economic, social and cultural rights were given priority over civil and political rights in those Constitutions.[19] According to Bowring, it should not be surprising. Speaking about the USSR Constitution of 1977, he explains that social and economic rights were, indeed, delivered:[20]

> [i]t is generally recognised that the USSR provided first rate free education and health care; and every Soviet town had its art gallery, theater and concert hall. The constitutional guarantee and genuine implementation of [social, economic and cultural] rights was perhaps the main source of legitimacy of the Soviet state, and the reason it was not overthrown[…].

---

[13] See Müllerson R. *International Law, Rights and Politics (Developments in Eastern Europe and the CIS)*, (Routledge, 1994) at p.160.
[14] Müllerson R., see n 13 above.
[15] The Soviet Constitutions did not contain any provisions prescribing non-alternative or prohibiting alternative elections. However, the special role of the single political party in the USSR – the Communist party – made it in fact impossible for alternative candidates to be elected to the Soviets.
[16] Articles 93-94 of the Tajik Constitution of 1978.
[17] Articles 119 and 134 of the Tajik Constitution of 1978.
[18] According to the Constitution of 1937, Article 115 'inviolability of home and correspondence secrecy was secured.' Article 54 of the Constitution of 1978 read: 'Personal life of citizens, secret of correspondence, telephone calls and telegraph communications are protected by law', so the term 'personal life' was used instead of 'private life'.
[19] For instance, social and cultural rights are stipulated in articles 37-45, and civil and political rights – in articles 46-54 of the Constitution of 1978. For the discussion of the official Soviet concept of human rights see Lauri Mälksoo 'The Controversy Over Human Rights, UN Covenants, and the Dissolution of the Soviet Union' (2018) 61 Japanese Yearbook of International Law 260.
[20] See Bill Bowring 'Russia and Human Rights: Incompatible Opposites?' (2009) 1 Goettingen Journal of International Law 257, at p.263.

Mälksoo, referring to Müllerson, points out that the problem with civil and political rights in the Soviet Union are explained in the foundation of the State and society.[21] The USSR always placed collectivist and government interests over the interests of the individual. He thus suggests that those flaws with civil and political rights stem from the philosophical foundations of the USSR, and 'its problems probably could not be fixed within the confines of the Soviet system'.[22]

At the same time, the Constitution of 1978 contained a provision on the leading role of the Communist Party, which in fact exercised the State power.[23] In the late 1980s, there were attempts to describe the power system in the USSR featuring a separation of powers into two: the State power belonging to the Soviets, and the political party power belonging to the Communist Party.[24] The Tajik Constitution of 1978, has been subjected to numerous amendments before and after the dissolution of the USSR in 1991[25] in order to reflect large changes in the political, economic, and social life of Tajik people.[26]

Tajik laws in the period of 1924-1991 were almost identical to the USSR laws, with minor differences, which reflected Tajik peculiarities. The court system comprised the Supreme Court, regional courts, and district courts, which were all the courts of general jurisdiction – they had competence over criminal and civil cases. State arbitration courts had jurisdiction over economic disputes between legal entities.[27] The judicial system belonged to the Roman-German legal family, where judgments of the courts were not considered precedents, and the judges were not guided by them in examining subsequent cases. The courts were partly involved in the investigation of cases, and this was a feature of the inquisitorial legal system.[28]

Prosecutors played a decisive role in the criminal proceedings. They had a dual role: on the one hand, they represented an accusing party to the proceedings, which brought charges in the court, and, on the other hand, they supervised the implementation of law during the court proceedings by all parties, including by judges. That effectively meant that

[21] See Lauri Mälksoo, n 19 above, p.278-279.
[22] See Lauri Mälksoo, n 19 above, p.279.
[23] Article 6 of the Constitution of 1978.
[24] See Byalt V.S., Demidov A.V. 'Razdeleniye vlastey v istorii polotiko-pravovoy mysli Rossii' [Separation of Powers in the Historical and Legal Thought of Russia] (2017) 1 (47) Leningradskiy Yuridicheskiy Zhurnal [Leningrad Legal Journal] 35.
[25] The main amendment was an introduction of a new state organ – the President, who became the head of the state and the government in 1991 (Article 117 – 125 of the Constitution of 1978 with amendments).
[26] For a detailed historical account of those amendments see S. Shokulova 'Tadjikistan v Svete Konstitutsii 1994 goda' [Tajikistan in the Light of the Constitution of 1994] (2014) 2 Hayoti Huquqi [Legal Life] 20.
[27] Articles 152 and 164 of the Constitution of 1978.
[28] The Criminal Procedure Cade of the Tajik SSR (1961) contained a separate chapter called 'Judicial Investigation'. See Chapter 24 of the Criminal Procedure Cade of the Tajik SSR dated 17 August 1961.

the prosecutors had power over judges even during the court hearings. Prosecutors had the powers to sanction an arrest of a suspect. No *habeas corpus* was known to Tajik Soviet legal system. If the prosecutors failed to present to the court sufficient evidence of the guilt of the accused, the court would give the prosecutor more time (up to two months) to conduct an additional investigation in order to collect more or better evidence. This was contrary to the adversarial principle of court proceedings, and it was a violation of the presumption of innocence.

Data protection or data privacy was not regulated by any laws as the Soviet system was more focused on ensuring social and economic rights rather than civil and political rights. Social rights were foregrounded in the two latest Soviet constitutions, while some civil and political rights were mentioned in the context of the interests of the working class and strengthening the socialist system. Some Tajik authors are of the opinion that the reason for not regulating data privacy issues in Soviet Tajikistan was the fact that the computing system had not been developed in the USSR, and there was no threat to personal data processed by automatic means, as there were no automatic means at the first place.[29]

2.2.2. Tajik Legal System After Gaining Independence (1991-2024)

Tajikistan gained its independence on 9 September 1991, and after the dissolution of the USSR started building its new statehood. The Tajik civil war (1992-1997) influenced political and economic life in Tajikistan in different ways. This thesis, however, does not focus on its impact on the legal system in Tajikistan for the purposes of this Chapter of the thesis. The current Constitution of Tajikistan (1994) reflects new Tajik statehood and declares Tajikistan as a secular, democratic, and rule-of-law-based State.[30] According to it, 'the Republic of Tajikistan' and 'Tajikistan' are equal terms. The Constitution of 1994 was adopted through a referendum in 1994, and it was amended three times via different referenda in 1999, 2003 and 2016. It was drafted after Tajikistan gained its independence and reflects a principle of separation of powers to legislative, executive, and judicial branches of power.[31]

[29] See A. A. Faizulloev 'Ta'rikhi tashakkul va rushdi zuhuroty 'malumoti shakhsi' dar qonunguzorii Jumhurii Tojikiston va digar davlatho: tahlili qonunguzori va nazariyavi' [History of formation and development of 'personal data' in the legislation of the Republic of Tajikistan and other states: legislative and theoretical analysis] (2022) 5 Vestnik TNU [Bulletin of TNU] 231.
[30] See Article 1 of the Constitution of the Republic of Tajikistan, dated 6 November 1994.
[31] Article 9 of the Constitution.

The Constitution is a supreme legal act, and laws and other normative legal acts must conform to the constitutional norms and provisions. International legal acts recognized by Tajikistan are an integral part of the legal system, and in case of discrepancy between Tajik domestic laws and international legal acts, the latter are given priority.[32] There is a debate on whether or not international legal acts recognized by Tajikistan must conform to the Tajik Constitution.[33]

The Tajik Constitution contains an extensive bill of rights, which reflects international human rights norms and standards, as well as new trends in constitutional law science in the post-Soviet countries.[34] Tajikistan is a party to the main UN human rights instruments. It acceded to the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic Social and Cultural Rights (ICESCR) in 1999, to the Convention Against Torture and other Cruel Inhuman or Degrading Treatment or Punishment (CAT) in 1995, the Convention on Elimination of all Forms of Discrimination Against Women (CEDAW) in 1993, the Convention on Elimination of all Forms of Racial Discrimination (CERD) in 1995, the Convention on the Rights of the Child (CRC) in 1993 and the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICMW) in 2002.

The judicial system in Tajikistan has inherited its Soviet structure with some deviations. There are courts of general jurisdiction, which have the competence to examine criminal and civil cases, on the one hand, and economic courts, which consider economic or commercial disputes between legal entities and/or individual entrepreneurs, on the other hand.[35] The Supreme Court, regional courts, and district/town courts have general jurisdiction, which includes competence over administrative, labour, tax, family, inheritance, and other cases. The High Economic Court of Tajikistan and the regional economic courts have competence to resolve not only economic disputes, but also supervise insolvency cases, or resolve administrative disputes when legal entities and individual entrepreneurs are involved. Further, the Constitution establishes the Constitutional Court of Tajikistan, which

[32] Article 10 of the Constitution.
[33] See Sh. Kamolov 'Mutobiqati sanadhoi baynalmillali ba Konstitutsiyai Jumhurii Tojikiston' [Conformity of international acts to the Constitution of the Republic of Tajikistan] (2013) 3 Hayoti Huquqi [Legal Life] 52.
[34] See A. Dinorshoev 'Sravnitelno-pravovoy analiz zakrepleniya prav I svobod cheloveka I grazhdanina v Konstitutsiyakh Rossiyskoy Federatsii i Respubliki Tadjikistan' [Legal comparative analysis of rights and freedoms of an individual and a citizen in the Constitutions of the Russian Federation and the Republic of Tajikistan] (2014) 2 Hayoti Huquqi [Legal Life 47].
[35] Article 84 of the Tajik Constitution of 1994.

has the competence to examine the conformity of laws and other legal normative acts to the Tajik Constitution.[36]

Tajikistan, as a party to the Commonwealth of Independent States (CIS), puts in place domestic legislation, which is mostly in line with the CIS model laws. The CIS – the Commonwealth of Independent States – was established on 8 December 1991 by a majority of the former Soviet States, including Tajikistan. There are eight States currently within the CIS: Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan.

At the same time, Tajikistan has sought to develop some laws which take into account particularities of Tajik culture and traditions, religious and national specificities, and such laws predominantly relate to the private lives of individuals. For instance, there is a law which regulates traditions, celebrations, and rituals in Tajikistan.[37] That law is designed to alleviate poverty and prevent excessive financial expenditure by individuals for organizing their celebrations or commemorations. Another law prescribes that parents must educate their children about the predominance of national interests over personal ones.[38] Ethnic Tajik parents must give their newborn children names in accordance with Tajik national values.[39]

Tajikistan is open to adopting laws which originate from other than CIS countries. Being a recipient of international and foreign technical assistance, Tajikistan has enacted several laws as legal transplants from different jurisdictions. For instance, the law on public-private partnership and the pledge law were drafted by external and internal experts with the assistance of the International Finance Corporation, which is a member of the World Bank Group.[40] Even those laws, which have been elaborated in accordance with the laws of some CIS countries, have been originating from the legal thoughts of some Western countries. As one of the Tajik authors puts it, the roots of the Tajik Civil Code go to the Soviet civil legislation; before that – the Russian Empire civil legislation; before that – the Code

[36] Article 89 of the Constitution of 1994. See further Article 34 of the Constitutional Law of the Republic of Tajikistan 'On the Constitutional Court of the RT', No 672 dated 17 July 2014.
[37] The Law of the Republic of Tajikistan 'On Streamlining Traditions, Celebrations and Rituals in the Republic of Tajikistan', No 584, dated 30 May 2007.
[38] The Law of the Republic of Tajikistan 'On Responsibility of Parents on Education and Upbringing of Children', No 210, dated 21 July 2011.
[39] *Ibid.,* Article 8. Tajik parents must choose a name for their child from the Register of names proposed by the Government according to the Law of the Republic of Tajikistan 'On Civic Registration', No 188, dated 29 April 2006. People of non-Tajik ethnic origin are not obliged to use the names from the Register.
[40] The Law of the Republic of Tajikistan 'On Public-Private Partnership', No 439 dated 13 December 2012; The Law of the Republic of Tajikistan 'On Pledge of Movable Property', No 1576 dated 2 January 2019.

Napoleon, and before that – the Roman civil law.[41] Tajik Tax Code is a Roman type of law by its shape, but it is an Anglo-Saxon type of law by its substance.[42] A new Tajik Civil Code, which includes even more Common Law concepts, was introduced in 2023.

2.3. Tajik Law Approach to the Concept of Privacy

Tajik legal scholarship is not particularly extensive in relation to the right to privacy and data protection problems. There are some academic articles written by a few scholars, which are mainly published in three Tajik periodicals since 2012.[43] Many Tajik authors, having Soviet and post-Soviet education, hold views similar to Russian or other post-Soviet authors. It is thus not surprising that Tajik authors mainly rely on the knowledge of their peers from other post-Soviet countries, and in their own works they make references mostly to Russian legal thought. The right to privacy was not widely considered in Soviet times as one of the constitutional human rights, and Soviet science studied personal non-proprietary rights to a greater extent as an institution of law within the framework of civil or private law. Human rights law was not considered fully part of constitutional law until the adoption of the current Constitution of the Republic of Tajikistan in 1994, although certain rights and freedoms of individuals were enshrined in the latest Soviet Constitution.[44]

According to a Russian author, there were two main reasons why the right to private life was not subject to research in the Soviet time: 1) the right to privacy as a legal category emerged in the Western countries relatively recently: in the late XIX – early XX century, and became part of the constitutions of different countries only in the second half of XX century, and 2) there was an uncertainty in understanding the subjective right to protection of personal life, introduced into the Soviet Constitutions.[45]

---

[41] See A. Kholiqzoda 'Nazare ba tabiati huquqii 'qonuni milli' va vizhagihoi on' [The view on the nature of the 'national law' and its peculiarities] (2018) 2 Davlatshinosi va Huquqi Inson [State Science and Human Rights] 5.

[42] *Ibid.,* at p.10.

[43] 'Bulletin of the Tajik National University', established in 2012, may be accessed at: http://g.vestnik-tnu.com/index.php/ru/, 'Hayyoti Huquqi (Legal Life)', a journal established and managed by a local law school – the Law Faculty of the Tajik National University since 2013, may be accessed at: https://law.tnu.tj/index.php/ru/izdaniya/pravovaya-zhizn, and 'Davlatshinosi va Huquqi Inson (State Science and Human Rights)', another journal by the Law Faculty of the Tajik National University, which is published since 2016, may be accessed at: https://law.tnu.tj/index.php/ru/izdaniya/gosudarstvovedenie-i-prava-cheloveka.

[44] See n 18 above.

[45] See Romanovskiy G.B. *Pravo na neprikosnovennost chastnoy zhizni* [*The Right to Inviolability of Private Life*] (MZ-Press, 2001) at 5.

According to Albi, a pervasive State surveillance during Soviet times was a factor for disregarding the right to privacy discourse in the Soviet Union.[46] An author from Belarus explained that in the Soviet time the concept of 'private life' was associated with the Anglo-Saxon system of law and, as a result, that concept within the Soviet legal thought was gradually excluded from usage, as it had bourgeois connotations, not characteristic of the Soviet people and the socialist way of life.[47]

Thus, Soviet civil law regulated the personal life of a person. Legal science studied this area of human life mostly from the point of view of horizontal relations, i.e., relations between individuals. On the other hand, the vertical relationship between the State and individuals in matters of protecting personal or private life remained outside the attention of Soviet legal science. Individuals did not have a private life – they enjoyed a personal life that did not fall under the concept of human rights. Human rights were not part of the Soviet Constitution for a long time, and when they were eventually included in the Constitution, the right to private life was not properly reflected there.

As a result, Tajik legal scholarship treats the right to private life mainly from the civil law point of view.[48] This leads to confusion about statutory regulation of the right to private life. Some authors contend that it is part of civil law, and at the same time, they argue about the necessity of intrusion of State agencies into the private lives of individuals.[49] They indicate that the right to private life is stipulated in the current Civil Code, while the history of many States confirms that the totalitarian States proclaim human rights and freedoms in their domestic law in order to create an ideological curtain that allows them to hide their failure.[50] Other scholars make references to international human rights instruments, such as the UN Charter, Universal Declaration of Human Rights (UDHR), ICCPR, and ICESCR in

[46] See Anneli Albi 'The EU Data Retention Directive in Twenty-Eight Member States: An emblematic case study of blind spots, lost higher national standards and systemic flaws in autonomous EU human rights law and discourse'. Unpublished paper, cited with the permission of the author.
[47] See Anastasiya Kunets 'Nauchnye podkhody k ponimaniyu konstitutsionnogo prava na lichnuyu zhizn' [Scientific Approaches to Understanding Constitutional Right to Personal Life] (2018) 60 Trud, Profsoyuzy, Obschestvo [Labour, Trade Unions, Society] 20.
[48] See, e.g., K. Kurbanov 'Ponyatiye Chastnoy Zhizni v Grazhdanskom Prave' [The Concept of Private Life in Civil Law] (2016) 16 Hayoti Huquqi [Legal Life] 132. There are however a few articles by Tajik authors on the right to private life from the human rights law perspective too.
[49] See K. Kurbanov 'Pravo na neprikosnovennost chastnoy zhizni kak lichnoe neimuschestvennoe pravo' [The Right to Inviolability of Private Life as a personal non-proprietary right] (2013) 4 Hayoti Huquqi [Legal Life] 58.
[50] K. Kurbanov 'Stanovlenie teoriy prava na chastnuyu zhizn' [Formation of the Theory of the Right to Private Life] (2018) 4 Hayoti Huquqi [Legal Life] 2020). K. Kurbanov makes reference to the Russian author – Romanovskiy G.B. *Pravo na Neprikosnovennost' Chastnoy Zhizni* [*The Right to Inviolability of Private Life*] (M. M-3 Press, 2001) at p.184.

the context of personal non-proprietary rights under civil law.[51] In the works of such scholars as Kurbanov, there tends to be acceptance that the concept of the right to privacy cannot be shaped exclusively from the civil law perspective.[52]

Most Tajik scholars agree that there is no universally accepted concept of private life.[53] In order to provide their own definition of private life they refer to both Anglo-American and Russian legal scholarship on the concept of privacy, indicating two main approaches employed by the above-mentioned scholarship: 1) by way of listing different elements of the right to privacy, and 2) by way of rejecting any definition on the premise that the individuals themselves define the substance of the concept of privacy.[54] They propose a definition of private life according to which an individual lives their personal, family, and household life based on the principles of an independent determination of the natural course of private life and the ability to maintain its confidential nature.[55] The main purpose of this right is the protection of human dignity, independence, and freedom.[56]

The confusion of the right to private life as a part of human rights law, i.e., public law, which considers the interaction between individuals and State agencies, with civil law, which is private law, has led to an inability to give a meaningful account of the right to private life in Tajik legal scholarship. The attempts to define 'private life' purely from the civil law perspective may limit the understanding of this right as freedom from government encroachments. Tajik scholars criticized the lack of civil-law liability for the breaches of privacy in Tajik law,[57] which in their view leads to the misuse of the right to private life and mistakes by law enforcement bodies.[58]

This portrays the approach of Tajik legal scholars in defining the right to private life, as something which must not be misused by individuals and must not give them too much discretion in defining what they can do in order to fully realize their right to private life.

[51] See Sh. Tagainazarov and Babadzhanov I. 'K teorii lichnykh neimuschestvennykh prav' [On the Theory of Personal Non-proprietary Rights] (2018) 4 Hayoti Huquqi [Legal Life] 209.
[52] K. Kurbanov concedes that some elements, which comprise the concept of private life, such as bodily integrity, are not covered by the civil law regulation. See K. Kurbanov 'Problemy sovershenstvovaniya grazhdansko-pravovogo regulirovaniya osuschestvleniya i zaschity prava na chastnuyu zhizn' [Problems of Improvement of Civil Legal Regulation of Implementation and Protection of the Right to Private Life] (2020) 1 Davlatshinosi va Huquqi Inson [State Science and Human Rights] 45.
[53] Sh. Tagainazarov and K. Kurbanov 'Sovremennye podkhody k probleme instituta prava na chastnuyu zhizn v grazhdanskom prave' [Contemporary Approaches to the Problem of the Concept of the Right to Private Life in Civil Law] (2018) 4 Hayoti Huquqi [Legal Life] 2014.
[54] *Ibid.,* at p.216.
[55] *Ibid.,* at p.216.
[56] See K. Kurbonov, n 52 above, at p.50.
[57] *Ibid.,* at 48.
[58] *Ibid.,* at 51.

Government agencies are not seen as potential perpetrators, as main violators of the right to private life, but rather they are considered as a punishing authority, which could be prone to mistakes, but not to misuse of power. In the example of China, Grimm explicates a socialist approach to constitutional rights as not opening spheres of self-determination of the individual:

> [i]n the socialist system the interests of society and the interest of the individual are objectively in harmony […]. […] the subjective view of the individual deserves no legal protection. It can be disregarded and even suppressed. The distinction between state and society, public and private is obsolete. The legal system is based on duties, instead of rights. Fundamental rights no longer guarantee a private sphere free of state intervention[…][59]

It is common among Tajik legal scholars to put an emphasis on the need to ensure the rights and freedom of other individuals as the lawful limitations to the enjoyment of the right to private life. Human rights in general and the right to private life in particular are seen as an interaction between individuals, where every individual has the freedom to act only to the extent, limited by the rights and freedoms of others.[60] Those who discuss surveillance and other methods of detecting and combatting crime do not offer any insight into the right to privacy of individuals.[61]

2.4. Legal Background of Tajikistan Data Protection Laws

The current Constitution of the Republic of Tajikistan, in its Article 23, provides for the right to private life and data protection[62] as follows:

> The secrecy of correspondence, telephone calls, telegraph and other personal communications shall be guaranteed, except as otherwise provided by the law.
>
> Collection, storage, use and dissemination of information about the personal life of an individual without their consent is prohibited.

The cited provision of the Constitution has no references to the 'privacy' or 'private life'. It rather uses the term 'personal life' borrowed from the wording of the Tajik Soviet

[59] See Dieter Grimm, n 11 above, p.129.
[60] See K. Kurbonov, n 52 above, at p.50.
[61] See e.g., A. Nazarov and K. Davlatzoda 'Istifodai tekhnologiyai raqami dar fa'oliyati operative-justujui' [Use of Digital Technology in the Crime-Detection Operations] (2022) 4 Payomi Donishgohi Millii Tojikiston [Bulletin of the Tajik National University] 207.
[62] There is no evidence that at the time of the adoption of the Constitution (1994) the drafters wanted to include data protection rights, however, the wording of the second sentence in Article 23 can imply data protection rights of individuals.

Constitution of 1978.[63] Some post-Soviet scholars do not see a distinction between 'personal' and 'private' in this context.[64] Other scholars discuss the differences between these two terms. They argue that 'privacy' or 'private' is a wider concept than 'personal'. For them, 'personal life' covers the intimate part of human relationships, while 'private life' apart from intimacy, also relates to the choice of friends, personal preferences, and planning their path of life'.[65]

At the time of drafting the new Constitution (1992-1994), the term 'private' or 'privacy' was not much in use, except in the context of the introduction of private property in post-Soviet Tajikistan. People in Soviet Tajikistan had no private property and were allowed to have only personal property, which could not be utilized for the purposes of exploiting other people. Thus, the word 'personal' was in use in relation to property rights and non-proprietary rights, such as life, health, honour, dignity, etc. The lack of use of the term 'private' in Tajik legal science, thus, has led the drafters of the Tajik Constitution of 1994 to use the word 'personal' in relation to non-proprietary rights.

Effectively, the words 'personal life' in the cited constitutional provision means 'private life'. The right to private life as a human right was a new concept in Tajik legal science. Like Soviet legal science, it considered this sphere of an individual's life through the prism of civil law thought, where the terms 'personal non-proprietary rights' and 'personal non-proprietary benefits' were used.[66]

The Constitution of 1994 has a separate provision on lawful limitations to the enjoyment of rights and freedoms, and such limitations apply in relation to the right to private life. Article 14 provides that the limitations of rights and freedoms of citizens could be permitted only with the aim of ensuring the rights and freedoms of other citizens, public

[63] A. Dinorshoev has mentioned such word borrowing in the current Tajik Constitution, while the Russian Constitution uses the term 'private live'. See A. Dinorshoev, n 34 above, at p.49.
[64] See A. Dinorshoev, n 34 above.
[65] See K. Kurbonov 'Pravo na chastnuyu zhizn v sisteme lichnykh neimuschestvennykh prav' [The right to private life in the system of non-proprietary rights] (2019) 3 Hayoti Huquqi [Legal Life] 128. Kurbanov makes reference to the Russian author – S. Chernichenko and his article 'Perspektivy razvitiya mezhdunarodnykh standartov v oblasti obespecheniya prava na neprikosnovennost chastnoy zhizni' [The perspectives of development of international standards in the field of securing the right to inviolability of private life in *Pravo Grazhdan na informatsiyu i zaschita neprikosnovennosti chastnoy zhizni (Sbornik nauchnykh trudov)* [*Rights of Citizens to Information and Protection of the Inviolability of Private Life (Compilation of scientific works)*] (Part I, Novgorod, 1999); A. Faizulloev 'Ba'ze munosibathoi jam'iyatie, ki vobasta ba giriftan va korkardi ma'lumoti shkhsi paido meshavand: Tahlili tabiati huquqi [Some social relations, which appears in connection with collection of and processing personal data: analysis of legal nature] (2022) 6 Vestnik TNU [Bulletin of TNU] 233. Faizulloev further made references to different Russian authors.
[66] See Section 2.3. 'Tajik Law Approach to the Concept of Privacy' above.

order, protection of constitutional order, security of the State, defense of the country, public morale, health of the population and territorial integrity of the State.[67]

Tajik law does not attribute data protection issues to one area of law. Data protection could relate to Tajik public law, which covers criminal and criminal procedure law, as well as administrative and constitutional law on the one hand, and could be covered by private law, which includes civil law, and all the laws associated with the economic activities of entities, particularly, data protection interests, on the other hand. This thesis focuses on the current data privacy legislation of Tajikistan in the following fields: (i) laws related to the protection of privacy when law enforcement organs conduct operations to combat crimes,[68] and (ii) laws related to data protection in the context of economic activities of businesses.[69]

Tajik law defines the exhaustive list of law enforcement bodies, which may use technical means for conducting surveillance:[70] organs of national security, internal affairs, drug control and anticorruption. Special laws regulate the activities of each of the mentioned law enforcement bodies. Those laws set the principles and norms, according to which law enforcement agencies conduct their operations. In the 1990s those laws contained no reference to the protection of data privacy, and only after the adoption of the Tajik Civil Code (Part I) in 1999,[71] some provisions related to the protection of privacy of individuals and protection of personal data were introduced in those laws. For instance, the old Law on militia, which was enacted in 1992, had a reference to the inviolability of home, secrecy of correspondence, telephone, telegraph, and other communications through technical channels.[72] The new Law on militia (2004) has a more express reference to the private life of individuals. It establishes that the militia has no right to collect, retain, use, and disseminate information about the private life of an individual without their consent, except as otherwise prescribed by the law.[73]

The Law of the Republic of Tajikistan 'On Crime Detection and Investigation' (CDI) mentions both 'personal life' and 'private life' in its text. First, it prescribes law enforcement

[67] Constitution of the Republic of Tajikistan of 1994. See n 30 above.
[68] For instance, the Law of the Republic of Tajikistan (RT) 'On Crime Detection and Investigation', No 352 dated 2 March 2011 (CDI), and the Law of the Republic of Tajikistan 'On Combating Terrorism', No 1808, dated 23 December 2021.
[69] The Law of the Republic of Tajikistan 'On Personal Data Protection', No 1537, dated 3 August 2018.
[70] The Law of the Republic of Tajikistan 'On Crime Detection and Investigation', No 687 dated 25 March 2011 (CDI), Article 6, Paragraph 6.
[71] The Civil Code of the Republic of Tajikistan (Part I) was the first Tajik law apart from the Constitution of 1994, which contained provisions on the inviolability of private life (Articles 140 and 170).
[72] The Law of the Republic of Tajikistan 'On Militia' of 1992 with subsequent amendments. That law was substituted with the new law in 2004. 'Militia' in Tajikistan carries out police functions. The name is inherited from the Soviet militia.
[73] The Law of the Republic of Tajikistan 'On Militia', No 544 dated 3 May 2004, Article 5.

bodies to secure the right of individuals to inviolability of personal life, personal and family secrecy, inviolability of home, secrecy of correspondence, telephone, telegraph and other personal communications.[74] Then, it prohibits law enforcement bodies and their officers to disclose data, which could influence the inviolability of the private life of citizens, their personal and family secrets, honour, and other values, if such data is obtained in the course of taking crime detection and investigation measures without the consent of citizens unless otherwise provided by law.[75]

The information laws in Tajikistan were adopted from 2001 to 2008, with some subsequent amendments thereto.[76] They defined the term 'personal data'[77] as information on facts, events, and circumstances of the life of a citizen, which allows identification of their personality.[78] Information is recognized as a commodity, but its owner must treat personal data as confidential.[79] At the same time, the law differentiates personal data from information on the private life of citizens. The owner of any information, including personal information, must not use or disseminate the information on the private life of citizens without their consent.[80] Some Tajik scholars argue that the information as such cannot be regarded as an object of ownership because the information has a non-proprietary value.[81] They suggest that the term 'holder' of information or database is more accurate, which is currently used in the new Law on the Protection of Personal Data of 2018.[82]

Individuals have the right to know who and for what purposes has used or is using information about them if such information is contained in databanks. The owners of databanks must provide personal information on demand, except in cases when such

[74] See Law on Crime Detection and Investigation, n 70 above, Article 5(1).
[75] *Ibid.*, Article 5(7)(3).
[76] The Law of the Republic of Tajikistan 'On the Informatization' No 40 dated 6 August 2001; The Law of the Republic of Tajikistan 'On Information', No 55 dated 10 May 2022; the Law of the Republic of Tajikistan 'On the Protection of Information' No 631 dated 15 May 2002; The Law 'On the Right of Access to Information' No 411 dated 18 June 2008.
[77] The Law on Information used three terms in respect of personal data: 'information on personality', 'information on citizens' and 'personal data'.
[78] The Law on Information, n 76 above, Article 1.
[79] *Ibid.,* Articles 20 and 35.
[80] *Ibid.,* Article 38.
[81] Sh. Gayurov *Lichnoe informatsionnoe pravo grazhdan : problemy grazhdansko-pravovogo regulirovaniya v Respublike Tadzhikistan* [*Personal Information Right of Citizens: Problems of civil law regulation in the Republic of Tajikistan*] (Moskva [Moscow], 2010) 371; A. Faizulloev 'Ba'ze munosibathoi jam'iyatie, ki vobasta ba giriftan va korkardi ma'lumoti shkhsi paido meshavand: Tahlili tabiati huquqi [Some social relations, which appears in connection with collection of and processing personal data: analysis of legal nature] (2022) 6 Vestnik TNU [Bulletin of TNU] 233.
[82] The Law of the Republic of Tajikistan 'On the Protection of Personal Data', No 1537 dated 3 August 2018, Article 1.

information is of limited access.[83] Individuals, however, are entitled to seek judicial redress if their rights and interests are violated by the owner or the user of the information.[84] The law prescribes that the State agencies, which collect and/or retain personal information, must not give anyone access to the information about the private life of another individual without the consent of such an individual.[85]

In 2016, Tajikistan enacted the new Labour Code, which contains a separate chapter on data protection.[86] Data processing by the employer takes place on the basis of the prior consent obtained from the employee. The employee is entitled to have access to all their personal data and to demand making changes and amendments to their personal data, as well as blocking or deleting their personal data, which was collected or processed unlawfully.[87] The employer may not request sensitive personal information from the employee, such as their political or religious beliefs, their membership in public associations and trade unions, as well as their private life.[88]

In August 2018, Tajikistan adopted the new Law on Personal Data Protection (Law on DP),[89] which has yet to be tested by the legal practice. That Law contains provisions similar to the main principles and rules stipulated in the EU General Data Protection Regulation (GDPR)[90] albeit with certain deviations and differences. Its definition of personal data, however, is almost identical to the one used in the Law on Information of 2001:[91] 'information about facts, events, and circumstances of the life of the subject of personal data, which allows identification of their personality.'[92]

The latest law containing data protection rules in Tajikistan is the Law on access to the information about activities of the courts.[93] That law prescribes that when the judgments and the court rulings are made public, all references to personal data must be substituted with initials, pseudonyms, and other signs or symbols, which would not allow participants

[83] The Law on Informatization n 76 above, Article 21(2). Information of a limited access is a documented information, which is attributed to State secret or confidential information (Article 3).
[84] *Ibid.,* Article 21(3).
[85] The Law on Access to Information, see n 76 above, Article 14(1)(b).
[86] Chapter 4 of the Labour Code of the Republic of Tajikistan of 2016 is called 'Collection, processing, and protection of personal data of employees.
[87] Articles 57-58 of the Labour Code.
[88] *Ibid.,* Article 58(2).
[89] The Law on DP, n 69 above.
[90] Regulation (EU) 216/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), (2016) OJ L119/1).
[91] See The Law on Information n 76 above.
[92] The Law on DP, n 69 above. See further n 78 above.
[93] The Law of the Republic of Tajikistan "On the Access to the Information on Activities of the Court", No 1783 dated 25 June 2021.

of the court proceedings to be identified.[94] The following are personal data in relation to the judgments and the court rulings according to that law:

- name of the participants of court proceedings, their date and place of birth, place of residence, telephone numbers, passport or other ID details, tax-payer individual number;
- information about the location of the land parcel, building, premises, residence house, vehicle, other property, bank accounts, if this information is related to the substance of the court case.[95]

Sensitive personal data, such as information on minors, family matters, information on sex crimes, placing a person to the psychiatric clinic and civic registration changes, contained in the judgments and rulings of the court must not be publicly accessible. The law further prohibits publishing information, which affects national security in court judgments and rulings.[96]

The next two sections of this Chapter will examine Tajik laws related to the following: (i) data privacy issues in the context of the activities of law enforcement bodies; and (ii) data protection issues related to economic activities.

2.5. Protection of Privacy in the Context of Surveillance in Tajikistan

The main law regulating surveillance by the State agencies in Tajikistan is the Law on Crime Detection and Investigation of 2011 with subsequent amendments in 2014 and 2017 (CDI).[97] The CDI is very similar to the Russian law of 1995. Law enforcement bodies[98] are given certain powers to conduct surveillance in order to detect, prevent and suppress crimes, as well as to detect and identify individuals, who have conducted or have been conducting crimes. Further, surveillance is conducted with the purpose of obtaining information about events or actions, which create threats to human rights and freedoms, as well as to public, military, economic, information, or ecological security of Tajikistan.[99]

The CDI establishes an exhaustive list of crime detection and investigation measures, among which the following surveillance measures could be explored:

[94] *Ibid.,* Article 15(3).
[95] *Ibid.,* Article 15(4).
[96] *Ibid.,* Article 15(5).
[97] See the CDI, n 70 above.
[98] Organs of national security, internal affairs, drug control, and anti-corruption. See the CDI, n 70 above.
[99] See the CDI, n 70 above, Article 3.

- operational surveillance;
- operational control over postal correspondence, telegraph and other communications;
- tapping and recording telephone conversations;
- taking information from the technical channels of communication; and
- obtaining computing information.[100]

Law enforcement bodies must have legal grounds for taking surveillance measures, and such grounds must be stipulated in the law. The existence of a criminal case is a valid ground for conducting investigation and taking all necessary surveillance measures. If the criminal case is not initiated for any reason, the law enforcement bodies may nevertheless conduct surveillance if they have information about:

- signs of a criminal act in the stage of its preparation, during performing the act or after the criminal act has been committed, as well as individuals, who prepare and commit criminal acts;
- events and acts, which create threat to public, military, economic, information or ecological security of Tajikistan;
- individuals, who hide from prosecution and justice.

Formal request from other law enforcement bodies, prosecution office, the court and foreign State competent agencies can serve as a ground for conducting surveillance measures.[101]

Some Tajik authors propose new grounds for crime detection measures to be in place in Tajik law in order to give law enforcement bodies possibilities of preventing crimes and detecting 'latent' crimes.[102] For them, prevention of crime can take place in the form of the identification of persons, who are willing to commit crimes. Special attention must be given to a) previously convicted persons; b) persons, who live antisocial life; c) alcohol or drug addicts; and d) persons, who disrespect the community, laws, and law enforcement bodies.[103] They acknowledge that the right to the private life of individuals will be limited as a result

[100] See the CDI, n 70 above, Article 6(1).
[101] See the CDI, n 70 above, Article 7.
[102] D. Qodirzoda, B. Shodiev 'Asosho va sharthoi guzaronidani chorabinii operativii gush kardani suhbathoi telefoni' [Grounds and conditions of conducting surveillance measures of tapping telephone conversations] (2020) 6 Vestnik TNU [Bulletin of TNU] 256. They made reference to the Russian author – A. Shumilov, who made those proposals to the Russian Law on Crime Detection and Investigation in 2004. See A. Shumilov *Novaya redaktsiya operativno-rozasknogo zakona Rossii: otkrytyi proyekt* [*New Redaction of the Crime Detection and Investigation Law of Russia: Open Draft*] (Moskva [Moscow], 2004) 33.
[103] *Ibid.,* p. 258.

of covert surveillance, which they think is the only effective measure of preventing crimes, but insist that according to Article 14 of the Constitution of 1994, the right to private life may be limited if certain public goals are achieved, such as securing other individuals' rights and freedoms, public order, national security, country defense, morals of the society and the health of the population.[104]

Surveillance measures, which limit the constitutional right to secrecy of correspondence, telephone, telegraph, and other communications that are transmitted via electric network, may be carried out in accordance with a reasoned resolution of the law enforcement body, which conducts those measures, upon the request of an authorized prosecutor and with the sanction of the authorized judge.[105] Such a three-step procedure is meant to serve as a safeguard for the protection of human rights. Moreover, such surveillance measures may be taken only in case of the existence of certain information about crimes and persons preparing or committing crimes, when such crimes are subject to a mandatory preliminary investigation.[106] Tajik Criminal Code foresees four categories of crimes depending on their gravity,[107] and the preliminary investigation by the law enforcement bodies is mandatory in respect of all, but the pettiest categories of crimes.

The law allows law enforcement bodies to take surveillance measures even without prior approvals of the prosecutor and the judge, who nevertheless must be notified within 24 hours of the commencement of surveillance. This must happen in very urgent cases when there is a threat of committing grave crimes (punishable by more than five years of imprisonment), or in case of an event or act, which threatens public, military, economic, information, or ecological security. The head of the law enforcement body passes a resolution to take such surveillance measures, and within 48 hours from its commencement, they must receive judicial permission or terminate the surveillance activity.[108]

Tapping of telephone or other conversations could be allowed only in respect of individuals, who are suspected or accused of committing grave or especially grave crimes

[104] *Ibid.,* p. 257.
[105] See the CDI, n 70 above, Article 8.
[106] Law enforcement bodies must possess information about the signs of a criminal act, as well as individuals, who prepare and commit criminal acts, and the events and acts, which create a threat to the public, military, economic, information, or ecological security of Tajikistan.
[107] The Criminal Code of the Republic of Tajikistan of 1998 with subsequent amendments. Article 18 lists four categories of crimes depending on their gravity. 1) up to 2 year of imprisonment (up to 5 years in case of careless crime); 2) 2-5 years imprisonment; 3) 5-12 years of imprisonment, and 4) more than 12 years of imprisonment.
[108] See the CDI, n 70 above, Article 8(2)(3).

punishable by at least five years of imprisonment, or in respect of persons, who may have information about such crimes.[109]

The judge usually grants permission to conduct surveillance on the ground that both the head of the respective law enforcement body and the prosecutor have taken their respective actions or decisions to validate such measures. In some cases, the judge may request some other documents and information related to the grounds for conducting surveillance measures, which would not expose the undercover agents though.[110] The permission granted by the judge cannot be valid for more than six months unless otherwise provided in the resolution of the judge. This means that the judge may in fact grant permission for conducting surveillance for a period higher than foreseen by the law, and there is no limit set by the law for the judge to establish lengthy permission. Moreover, the judge may issue a second permission based on the new documents presented to them by the law enforcement body in charge of the operation.[111]

The CDI contains provisions on personal data retention. All personal data collected in respect of an individual, whose guilt eventually was not proved, are retained for six months after the criminal case is closed. After that, the retained data must be destroyed or further retained if the interests of the service or justice require so.[112] Again, this is a legal possibility for law enforcement bodies to retain personal data for an indefinite period of time.

2.6. Personal Data Protection Law in Tajikistan

The Law of the Republic of Tajikistan on 'Personal Data Protection'[113] was adopted after the EU General Data Protection Regulation (GDPR)[114] has entered into force in 2018 and the modernized Council of Europe Convention 108 was adopted the same year.[115] One could assume that this is not a coincidence, and Tajik lawmakers, keeping up with the times, decided to pass a law that would reflect the latest development of the concept of personal data in the light of the protection of the right to privacy in the context of the rapid

[109] *Ibid.,* Article 8(2)(4).
[110] *Ibid.,* Article 9(3).
[111] *Ibid.,* Article 9(5).
[112] *Ibid.,* Article 5(6).
[113] See the Law on DP, n 69 above.
[114] Regulation of EU 216/679 dated 27 April 2016 'On the protection of natural persons with regards to the processing of personal data and on the free movement of such data' OJ EU 119/1 (GDPR).
[115] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) dated 28 January 1981, amended later with Additional Protocol of 2001 (ETS 181), and, recently, modernized through Amending Protocol (CETS 221). Currently, it is the Modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the CoE Committee of Ministers on 18 May 2018, CM/Inf(2018)15-final.

development of modern technologies. However, the approach to personal data in this law is reminiscent of the approach to the legislation on information that existed in Tajikistan even earlier.

The approach to the right to privacy not as a separate human right, but as a civil law phenomenon in Soviet and post-Soviet literature, to some extent, reflected the approach of Tajik legislators to the definition of personal data and the legal regime for their protection. As mentioned in Section 2.4 above,[116] the Law on DP defines 'personal data' as information about facts, events and circumstances of the life of data subjects, which lead to the identification of their personality.[117] This definition is borrowed from the old Tajik Law on Information,[118] which has been in force since 2002. It does not reflect a modern understanding of personal data as any information related to an identified and identifiable physical person, and it does not clarify what facts, events, or circumstances of the life of a person could qualify as personal data.

The Law on DP defines biometric data as personal data, which indicates the physiological and biological characteristics of the data subject. It is again a generic definition, which gives little guidance to what it is. It does not speak about the behavioral characteristics of a natural person, which eventually can confirm the unique identification of such a natural person. No examples of biometric data, such as photographs or dactyloscopy are given in that law, although biometric data is given special attention under that law[119]. There is no indication as to why biometric data was singled out in a separate article in the Law on DP. There is no division of personal data into ordinary and sensitive ones, where the latter could be regarded as requiring special treatment.

The Law on DP differentiates personal data into (i) publicly available and (ii) of restricted use.[120] Any personal data, the use of which was consented to by the data subject, or the data, which is not subject to secrecy under the law, may be considered publicly available personal data. Examples of such publicly available personal data are biographical directories, telephone or address books, publicly available databases, and mass media.[121] The law emphasizes that access to such personal data is ensured for the purpose of providing information to the population.

---

[116] See n 92 above.
[117] The Law on DP defines them as 'personal data subjects', but the present writer will use a shortened version – 'data subjects' as GDPR or Convention 108 do.
[118] See the Law on Information, n 76 above.
[119] The Law on DP devotes a separate article (Article 17) to biometric data.
[120] Article 9 of the Law on DP. See n 69 above.
[121] *Ibid.*

The Law on DP does not clarify what kind of consent of the data subject is sufficient for qualifying their personal data as publicly available. A controller (data holder), a processor, or a third party[122] can use personal data in accordance with the terms and conditions of the consent provided by the data subject.[123] But this must not apply to the publicly available data.[124] This means that the consent given by the data subject for the use of personal data as publicly available data is a *carte blanche* consent, given to everyone and to all for any and all purposes because the population is entitled to know this information. The data subject cannot withdraw their consent in respect of the publicly available personal data.[125]

The Law on DP does not clearly explain what type of personal data has to be under the restricted regime of access.[126] Another law – the Law on Access to information, which is relatively old (2008), provides the definition of restricted access to information: information, access to which is restricted in the interests of ensuring national security in accordance with the legislation on state secrets and other regulatory legal acts regulating relations in the field of protecting state secrets.[127]

One can recognize that the drafters of the Law on DP have mixed the concepts of 'personal data protection' with 'access to personal data'. Those are intertwined and interrelated notions, but they can serve different purposes and can relate to different human rights. On the one hand, every individual has the right to know if their personal information is in use by third parties, including government agencies, and if so, demand erasure or rectification, or discontinuation of the misuse of their personal data. In this sense, the right to access the personal data of an individual is a part of their right to private life.[128] The Law on DP has regulated this further in its text.[129]

On the other hand, individuals have the right to seek information as part of their freedom of expression.[130] The Law on DP while classifying personal data into publicly

[122] The Law on DP has defined the data holders and processors as a state organ, legal or physical person, who has the right to hold, use and dispose of personal data (data holders) and who carries out processing and protection of personal data (processors). See Article 1 of the Law on DP. See n 69 above.
[123] Article 10 of the Law on DP. See n 69 above.
[124] *Ibid.*
[125] Article 11 of the Law on DP. See n 69 above.
[126] The Law on DP makes a blanket reference to the Law of the Republic of Tajikistan "On the Right of Access to Information" dated 5 June 2008, No 507 (Law on Access to Information), which provides a definition of restricted information.
[127] *Ibid.,* the Law on Access to Information Article 2.
[128] The European Court of Human Rights (ECtHR) has qualified personal data protection rights as part of the right to the private life of individuals in its jurisprudence. See more in detail in Chapter 3 of the thesis.
[129] Article 22 of the Law on DP. Article 11 of the Law on DP. See the Law on DP, n 69 above.
[130] See Article 19 of the International Covenant on Civil and Political Rights, which reads: 'Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers[…]' (Emphasis added). UN General

available data and data with a restricted use, has borrowed the approach employed by the Law on access to information,[131] which was enacted in 2008. That law was about individuals' access to information, and such a law's intention was to define what type of information may not be made available and accessible to individuals: state secrets and personal data of other individuals. The Law on access to information was not designed to protect the personal data of individuals from misuse by government agencies, it was partly designed to protect the personal data of individuals from the access of other individuals.

The Law on DP, ideally, had to protect the personal data of individuals not from access by other individuals but primarily by the government agencies and large businesses – holders of such personal data. It was the lack of understanding of the purposes of the Law on DP, and the lack of conceptual underpinning in respect of the right to private life and data protection, which led the drafters of that law to mix two different albeit similar and intertwined rights of the individual: the right to private life and the right to seek information. As a result, the Law on DP apart from regulating the data protection rights of an individual has also included the classification of personal data from the Law on Access to Information, which in some parts negated the idea of personal data protection.

This is in line with the Tajik approach to the concept of private life, where the main perpetrators are other individuals, not the government. It is other individuals, who must not collect, retain and use the personal data of an individual without the latter's consent. Even one of the main principles of data processing included in the Law on DP – ensuring the security of the State – supports this idea.[132]

This erroneous approach to the classification of personal data not only did not improve the rights of the data subject to the protection of their personal data but aggravated some of the rights that they previously enjoyed under other laws. Thus, under the Law on Access to Information (of 2008), third parties or government agencies, as holders of personal information, must not provide access to information about the private life of individuals without their consent to other individuals.[133] The Law on DP (of 2018), on the other hand, provides that once an individual consents to the use of their personal data by publicly available databanks, they may not withdraw their consent in the future. If some personal

Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, 171.

[131] The Law "On the Right of Access to Information", see n 76 above.

[132] Principles of data processing are listed in Article 4 of the Law on DP: observance of rights and freedoms of individual, lawfulness, fairness, transparency, confidentiality of personal data of a restricted use, equality of data subjects, holders and processors, and ensuring security of personality, society and state. The Law "On the Right of Access to Information", see n 76 above.

[133] Article 14 of the Law on access to information, see n 76 above.

information becomes public, it will be public forever, irrespective of the will of the data subject.[134]

The right to access personal information as part of the data protection right concerns the right of access to person's own personal data, not the personal data of other persons. This right empowers individuals to know the purposes of the use of their information by third parties and to demand the erasure of their personal information. The Law on DP foresees that the data subject is entitled to access their personal data, which is held by the data holder, processor, or third party. For these purposes, the data subject may request clarification of which particular personal data is processed by those entities. They may request blocking or erasing their personal data from the database, if their personal data is incomplete, outdated, inaccurate, illegally obtained, or not necessary for the stated purpose of processing, as well as take necessary lawful measures to protect their rights.[135] At the same time, the data subject is unable to enjoy these rights if their personal information is considered publicly available.[136]

The Law on DP establishes a consent-based data processing regime. Almost in all cases, it is required to receive the consent of the data subject.[137] There are only two exceptions to this rule when personal data may be processed without such a consent of the individual: (i) when State organs carry out functions foreseen by the law, and (ii) when the rights and freedoms of other individuals need to be protected.[138]

Thus, when non-state data holders (controllers) or processors carry out their functions, such as providing certain services to the population, they will not be exempted from taking the data subject's consent for processing their personal data. The consent-based Law on DP does not foresee other legal bases for a private controller or processor to collect and use personal data. There is no mention of the following widely recognized[139] legal bases for data processing, when:

- processing is necessary for the performance of a contract, where the data subject is a party;
- processing is necessary for compliance with a legal obligation to which the controller is a party;

[134] See Law on DP, n 69 above.
[135] See Article 22 of the Law on DP, n 69 above.
[136] *Ibid.*
[137] Article 8 of the Law on DP.
[138] Article 12 of the Law on DP.
[139] The GDPR has established certain data protection standards within the EU, but at the same time those standards are accepted by other jurisdictions. This will be discussed in more detail in Chapter 5 'EU Law Rules Regarding Data Protection and Privacy Rights'.

- processing is necessary in order to protect the vital interest of the data subject or another natural person (although, Tajik law foresees protection of human rights as a legal basis of data processing);
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Only State organs are privileged to avoid receiving consent from data subjects. The rights and freedoms of other individuals need to be secured effectively by government agencies, and the Law on DP allows them not to seek the data subject's consent for data processing.

The collection and processing of personal data must be limited to the achievement of specific, predetermined, and legitimate purposes. It is not allowed to process personal data that is incompatible with the purposes of its collection. The content and scope of the collected and processed personal data must comply with the stated purposes of collection and processing. The data subject must be informed about the data collected about him, he is provided with access to the data concerning him, and he has the right to demand the correction of inaccurate or misleading data. The period of storage of personal data is determined by the date of achievement of the purposes of their processing.

The data subject can claim rectification of their personal data, which ought to be carried out by the controller, processor, or third party. Transfer of personal data is possible if the previous consent of the data subject to data processing has covered possible transfers to third parties. Apart from this, data transfer ought to be possible only if it does not affect the lawful interests of [other] legal or natural persons. The law does not specify exactly what lawful interests could prevent data transfer.

Transborder flow of personal data is allowed only to those third countries which have adequate data protection regimes in place. There is no definition of what 'adequate' means in the law. As the law is still dormant (there is no case law or any legal normative acts or instructive guidance of the data protection authorities), there is no clear idea how Tajik data protection authorities can prohibit such a transborder flow of personal data.

Cross-border transfer of personal data to the territory of foreign States that do not ensure the protection of personal data may however be carried out in the following cases:

- the consent of the subject or his legal representative to the cross-border transfer of their personal data;

- provided for by international treaties recognized by Tajikistan;
- provided for by the legislation of the Republic of Tajikistan, if necessary, in order to protect the constitutional order, protect public order, the rights and freedoms of man and citizen, the health and morals of the population, ensure the defense of the country and the security of the State;
- protection of the constitutional rights and freedoms of a person and a citizen, if obtaining the consent of the subject or his legal representative is impossible.

The law does not foresee any other mechanisms or tools for the lawful transborder transfer of personal data such as binding corporate rules or standard data protection clauses in the contracts.[140]

Personal data ought to be deleted after the contract between the data subject and the controller was terminated or the period for retaining personal data has expired.

The controller, operator and third party are obliged to take the necessary measures to protect personal data, ensuring that the following tasks are fulfilled:

- prevention of unauthorized access to personal data;
- timely detection of facts of unauthorized access to personal data;
- minimizing the adverse effects of unauthorized access to personal data.

The Law on DP indicates the difference between data processing regimes for governmental controllers and private controllers or processors. The government controllers are in a more privileged position in comparison to their private counterparts.

This Chapter makes a general introduction to the Tajik legal system as a post-Soviet legal system and discusses the Tajik legal thought on the right to private life as conceptualized under the influence of post-Soviet legal scholarship. As a result, it is indicated that Tajik legal scholarship fails to give a meaningful account of the right to private life as a human right. A Tajik concept of privacy thus is enshrined in the Tajik surveillance and data protection laws.

The next step for this thesis is to discuss the concept of privacy as understood in Western legal scholarship in the next Chapter. After that, this Chapter explores how the right to privacy and data protection are protected by two European legal systems: the European Convention on Human Rights, and European Union Law in Chapters 4 and 5 of the thesis. In the end, in Chapter 6, the thesis turns to possible lessons that Tajikistan can learn from the

[140] Bunding corporate rules and standard contractual data protection clauses are in wide use in the world as foreseen by the GDPR and similar data protection instruments in other countries.

standards of privacy and data protection established by the above-mentioned European legal systems.

Chapter 3. The Concept of Privacy

3.1. Introduction

International human rights law stems from the idea that on the one hand, an individual enjoys rights and freedoms, and on the other hand, the public authorities are obliged to secure those rights and freedoms and limit the exercise of public power. Except for a few rights, such as the right of peoples to self-determination,[1] all rights and freedoms are individual. A Western idea of 'individualism' is opposed to the 'collectivism' of the East,[2] where the context around individuals plays a primordial role. The right to privacy, therefore, has emerged and developed as a Western concept based on the autonomy of the individual.[3]

In Chapter 2 this thesis has explained the Tajik concept of privacy, which is influenced by the Soviet and post-Soviet legal thought, while in this Chapter the thesis seeks to explore the Western concept of privacy, which underpins the contemporary approach to the right to privacy and data protection taken by European Convention on Human Rights (ECHR) and by European Union (EU) law. This Chapter will provide a basis for the examination of the European Court of Human Rights (ECtHR) jurisprudence in Chapter 4 followed by an exploration of EU law in Chapter 5 of the thesis. It will further help to instigate discussions about the necessity of improving Tajik data protection and surveillance laws in the light of the standards established by the ECHR and the EU General Data Protection Regulation (GDPR) in Chapter 6 of the thesis.

The right to privacy is perceived as an individual value that is opposed to the public interests, and in case of a conflict between the right to privacy and the legitimate public interest, a balancing exercise is usually carried out to find out what must prevail – an individual right (to privacy) or a public interest in each particular case. Sometimes, a public interest represents other rights and freedoms of individuals, such as freedom of expression. So, theoretically, the protection of separate rights and freedoms can be considered a legitimate public interest.

The European Court of Human Rights has constantly portrayed the freedom of expression as a public good: it has stated that under the freedom of expression, the press has the task of imparting information and ideas on all matters of public interest, and the public

[1] Article 1 of the International Covenant on Civil and Political Rights (ICCPR) foresees a collective right of peoples to self-determination. This collective right is enshrined in the UN Charter (Article 1) as well.
[2] Here it mainly means Far East (Japan, China, Korea etc). See, e.g., Yuanye Ma 'Relational Privacy: Where the East and West Could Meet' (2019) 56 ASIS&T 196.
[3] See generally Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

has the right to receive them.[4] On the other hand, the right to privacy, as opposed to the freedom of expression, is different in that it is in most cases perceived as an individual value,[5] although some scholars argue that the right to privacy may be seen as a public good.[6] The ECtHR has indicated that the protection of the reputation of others is a value to be protected by the ECHR.[7]

This Chapter discusses the European roots of the right to privacy as a right to personal development and informational self-determination. The Chapter uses the German Federal Constitutional Court's jurisprudence to demonstrate the development of the right to privacy and data protection and its influence to the case law of the ECtHR on the right to private life.

A critique of the liberal theory of privacy is focused on denying privacy as a mere individual value stemming from the idea of individual self-determination. It is argued that privacy is more than ever evident to be a common or public good with the development of high technologies and inevitable and almost entire shift of our life activities, and, consequently, our privacy concerns, personal, or business, into cyberspace or virtual reality.

3.2. A Brief History of the Evolution of the Notion of 'Privacy'

Most of the authors notice the absence of a clear and exhaustive definition of privacy, which would guide national or supranational judicial or semi-judicial bodies while deciding cases that involve privacy protection issues. Judith Jarvis Thomson presumes that 'the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is.'[8] BeVier indicates that the '[p]rivacy is a chameleon-like word used denotatively to designate a range of wildly disparate interests – from confidentiality of personal information to reproductive autonomy.'[9] Solove proposes to structure the concept of privacy calling it a taxonomy of privacy,[10] which, in his view, focuses 'more specifically on the different kinds

[4] See e.g., the case of *Von Hannover v Germany (No.2)* (2012) ECLI:CE:ECHR:2012, Paragraph 118.
[5] See Kirsty Hughes 'A Behavioural Understanding of Privacy and its Implications for Privacy Law' (2012) 75 MLR 806;
[6] See Priscilla Regan 'Privacy and Common Good: Revisited' in Beate Roessler and Dorota Mokrosinska (eds.) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP 2015) 50. According to Regan, privacy is a common value for three reasons: 1) all individuals enjoy privacy and have shared vision of what privacy is, 2) privacy has worth to all aspects of democratic political process, and 3) technology and market forces make it hard to an individual to have privacy without all persons having a similar minimum level of privacy.
[7] See *Axel Springer AG v Germany* (2012) ECLI:CE:ECHR:2012, Paragraph 84.
[8] Judith Jarvis Thompson 'Right to Privacy' (1975) 4 Philosophy and Public Affairs 295.
[9] Lillian R. BeVier 'Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection' (1995) 4 William & Mary Bill of Rights Journal 455.
[10] Daniel Solove 'Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477.

of activities that impinge upon privacy.'[11] However, it is accepted that a generally recognized definition of privacy does not exist.[12]

According to Whitman,[13] there are different perceptions of privacy in the Old and New World (Europe vs USA). The European concept of the right to privacy is based on the premise that a right to privacy (or private life) is a fundamental human right enshrined in Article 8 of the ECHR and Article 7 of the Charter of Fundamental Rights of the EU (CFREU), and it ought to be protected by the State not only in cases of State interference or intrusion into individual's private life, as American concept suggests, but also when third parties interfere with individual's privacy.[14] Whitman explains such differences in the legal culture and mentality of Europeans and Americans, where the former consider dignity to be a cornerstone of their being, and the latter emphasises their liberty as a core value of the society.[15] Whitman however does acknowledge that such differences are not of an absolute character but are rather of a relative nature.[16]

Whitman brings in an example of differences in understanding of privacy in data protection laws, especially the laws protecting consumer rights in the USA and the EU. The Europeans, according to him, do not understand why businesses can be given access to the entire credit history of consumers without interfering with any privacy rights. He claims that the difference in perception of privacy results in a costly transatlantic legal battle resolved by a 2000 Safe Harbour agreement.[17]

Further, Whitman has a different explanation than the Europeans of the origins of the recognition of human dignity as the highest value in Europe. In his opinion, the main argument of the Europeans was that after the horrors of Nazism in World War II, dignity has become the defining value of rights and freedoms in Europe, particularly in Germany. He suggests that 'Europeans […] give a dramatic explanation for why dignity figures so prominently in their law […]'.[18] He concedes further that '[…] indeed, it is hard to resist a story with so much drama [...] but the real story is different'.[19] In his opinion, the history of continental law in relation to dignity dates back long before World War II. According to him, since 17th or 18th century, continental law has included respect for dignity, initially, for

[11] Solove, *Ibid*.
[12] See Oliver Diggelmann and Maria Nicole Clais 'How the Right to Privacy Became a Human Right' (2014) 14 Human Rights Law Review 441.
[13] James Q. Whitman 'The Two Western Cultures of Privacy: Dignity versus Liberty', in 'The Yale Law Journal', 2004, vol 113, p. 1151 - 1221.
[14] *Ibid.*, p.1161.
[15] *Ibid.*
[16] *Ibid.,* p. 1164.
[17] *Ibid.*, p.1157.
[18] *Ibid.,* p. 1165.
[19] *Ibid.*

persons of high social status. The courts in Germany and France protected dignity of high-status persons.[20]

Modern continental society is a product of the struggle against the hierarchical society that existed two and a half centuries ago. Germany and France, in his opinion, have been the center of leveling up the rights of different classes, in which '[e]verybody is now supposed to be treated in ways that only highly placed and wealthy people were treated a couple of centuries ago.'[21]

Snyder contests that the German perception of privacy is not purely explained by the adherence to the value of dignity, i.e., privacy in Germany is understood not only as the right to be protected by the State from the interference of third parties.[22] In Snyder's opinion, early laws containing the right to privacy in the home and the correspondence in German-speaking Europe in the 1830s reflected the importance of individual freedom against the State.[23]

Speaking about the history of the right to privacy, Snyder mentioned that the German notions of privacy in the home and correspondence are not directly related to the American or French constitutional traditions.[24] He argues that the first mention of the right to privacy of correspondence was made in the 'Constitutional Charter' for the electorate of Hessen in January 1831.[25] A month later, in February 1831, the Constitution of Belgium was adopted containing provisions on the inviolability of the home and privacy of correspondence. The inviolability of home and the respect of the secrecy of correspondence, has 'deep roots' in the continental constitutional tradition,[26] for instance, the French Constitution of 1848 contained provisions on the inviolability of the home.[27] Separately, the Frankfurt Constitution of 1849 contained provisions on the inviolability of dwelling and privacy of correspondence.[28]

In the United States, the first definition of the right to privacy appeared in the late XIX century as 'the right to be let alone', formulated by Thomas Cooley.[29] This has been

[20] *Ibid.*
[21] *Ibid.*, p.1165 – 1166.
[22] Thomas Snyder 'Developing Privacy Rights in Nineteenth-Century Germany: A Choice Between Dignity and Liberty?' (2018) 58 American Journal of Legal History p.188-2007.
[23] *Ibid.,* p.191.
[24] *Ibid.,* p.192.
[25] *Ibid.,* p.193.
[26] Gerard Hogan, as cited in Anneli Albi 'The EU Data Retention Directive in Twenty-Eight Member States: An emblematic case study of blind spots, lost higher national standards and systemic flaws in autonomous EU human rights law and discourse', p.25. Unpublished paper, cited with the permission of the author.
[27] Article 3 of the French Constitution of 1848 read: 'The dwelling of every person inhabiting the French territory is inviolable, and cannot be entered except according to the forms and in the cases provided against by law'.
[28] Paragraph 140 of the Frankfurt Constitution of 1849 read 'The dwelling is inviolable […]' and Paragraph 142: 'The secrecy of communications is guaranteed […]'
[29] Referred to by Samuel Warren and Louis Brandeis in 'The Right to Privacy' (1890) Harvard Law Review 4.

developed by others, including Warren and Brandeis, who in their famous article 'The Right to Privacy' have indicated that the harm to privacy involves more incorporeal rather than bodily injury. They contend that privacy entails 'injury to the feelings'[30]. Since the right to privacy was not and is not indicated in the US Constitution, American scholars, such as Prosser[31] in 1960, attempted to explicate the meaning of 'privacy' through an American tort law by identifying four types of actions, harmful to the privacy of an individual: 1) intrusion into private affairs of a person; 2) public disclosure of uncomfortable information on the private life of an individual; 3) publicity, which gives the erroneous impression to public about the life of a person; and 4) appropriation of the name of another person for gaining the advantage. But Daniel Solove points out that the right to privacy is more than only a tort law. In his opinion, the right to privacy extends far beyond torts and covers the constitutional right to privacy, the Fourth Amendment law, evidentiary privileges, and federal and state privacy statutes[32].

Solove argues that 'privacy', as an umbrella term, refers to a wide group of related things, and his taxonomy demonstrates certain connections between different kinds of privacy. He employs the family resemblance concept of Wittgenstein to indicate that different aspects of privacy might not share one common characteristic, but they are nevertheless 'related' to one another in many ways. Under his taxonomy, he highlights four groups of harmful activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion.[33] Solove concedes that the first three groups of activities involve necessarily personal information, while the fourth group includes invasive acts that interfere with the solitude of an individual. It is submitted that those four groups suggested by Solove may be effectively classified as two groups: 1) related to the use of personal information, and 2) related to the invasion.

Further, Westin interprets privacy as the right of an individual to define the extent and circumstances of the use of their personal information communicated to others[34]. Westin claims that privacy is 'the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behaviors to others'[35]. He explains different states, in which privacy could emerge: solitude, intimacy, anonymity, and reserve.[36] Solitude and intimacy entail freedom from being observed by third parties, with

[30] *Ibid,* 196-197.
[31] William L. Prosser 'Privacy' (1960) 48 California Law Review 383.
[32] Solove n 10 above.
[33] Solove n 10 above.
[34] Westin, n 3 above, p.5.
[35] Westin, *ibid*.
[36] Westin, *ibid*.

the difference that solitude involves an individual alone, while intimacy infers a small group of individuals. Anonymity is a state of privacy, which enables individuals to conceal their identities from others. Reserve means the right of an individual to refrain from disclosing their personal information. An individual may immerse in one of those states of privacy when they do not want to share information about themself. For Westin, these are all examples of social withdrawal as opposed to social disclosure. Individuals may withdraw to a state of privacy when they avoid being identified, or limit disclosure of their personal information. The point is not how much information a person receives or gives up, but rather who must have access to such information, and the nature of their relationship with us.

Altman offers a conceptualization of privacy as the selective control of access to the self, involving dialectic, optimization, and multimodal processes.[37] He suggests that privacy is more than just an attempt for individuals to avoid interaction with others. In different situations, places, or times people make themselves open to others, and in other situations and contexts, they close themselves off from others.[38] Privacy presupposes a close to 'optimal' situation when an individual finds themself in a state that keeps them away from crowds on the one hand, and from being totally isolated, on the other hand. A person may use different mixes of behaviour to achieve a desired level of privacy, depending upon circumstances.[39] Altman's perception of privacy echoes Westin's account of control-based privacy: 'If I can control what is me and what is not me, if I can define what is me and not me, and if I can observe the limits and scope of my control, then I have taken major steps toward understanding and defining what I am. Thus, privacy mechanisms serve to help me define me.'[40]

Privacy as a claim of individual control suggests that individuals are exercising their right to privacy when they choose to share information with another: so long as they determine for themselves what to communicate, how, and to whom, then there is no violation of privacy. A violation of privacy is a violation of our claim to control information about ourselves.[41] Yet this seems wrong to many critics, who argue that in disclosing information individuals are choosing, but they are choosing to give up privacy. According to Solove, privacy presupposes more than just keeping secrets – it is about how individuals regulate the transfer of data, how we ensure that third parties use our information responsibly, how we

[37] Irwin Altman *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Brooks/Cole Publishing, 1975).
[38] *Ibid.*
[39] *Ibid.*
[40] *Ibid.*, p.50.
[41] See Lisa Austin 'Re-reading Westin' (2019) 20 Theoretical Inquiries in Law 53.

exercise control over our information, and how we may limit the way others can use our data.[42]

With the development of high technologies, which make it much easier to collect, process, and transfer personal information in large amounts, some authors call on revising the idea of privacy as an individual's control over personal data. Inspired by Westin's control-based account of privacy, some of them contend that the definition of privacy must be more focused on making meaningful choices rather than on individual control.[43] The law is interpreted as whether the actions of others violate individual control over personal data, while data privacy must be more focused on whether the context, or environment maintains choices that develop our autonomy.[44] The individual's ability to choose a state of privacy is shaped by society's political and legal system.[45] Rössler gives an example of a person who falls into a crevice and thus becomes alone and inaccessible. According to her, such a person would not enjoy privacy.[46] Austin, on the other hand, uses that example and elaborates that such a person in fact experiences privacy but has not chosen it and, in those circumstances, has not valued it.[47]

3.3. Protection of Privacy Under International Human Rights Instruments

The right to privacy has become an international human right since WWII according to some authors, mainly, due to a coincidence.[48] While usually international human rights law stems from the national constitutional legal order, the right to privacy as an international human right appears to grant a substantially more extensive guarantee than national legal orders would provide. Something, which is far beyond the mere respect for home, correspondence, and reputation, is enshrined in the Universal Declaration of Human Rights (UDHR), the ECHR, and later in other international human rights instruments. In the drafting history of the International Bill of Rights the United Nations ECOSOC's drafting Committee of the Commission of Human Rights (dated 1947), the wording of Member States' constitutions was provided. The right to privacy, or the right to private life as an umbrella

[42] Daniel Solove 'The Meaning and Value of Privacy' in Beate Roessler and Dorota Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP, 2015) 71
[43] See Austin, n 41 above.
[44] Austin, *ibid.* at 56.
[45] *Ibid.*
[46] Beate Rössler, *The Value of Privacy* (Polity Press, 2005).
[47] See Lisa Austin n 41 above, at 58.
[48] See Oliver Diggelmann and Maria Nicole Clais, n 12 above. They argue that the drafters of the ECHR 'decided to include an umbrella term in the provisions of privacy, but […] made this step without being aware of the potential implications of such a guarantee.'

term was not known by any of the constitutions. They all referred to inviolability of home and correspondence, or privacy of home and correspondence or freedom from intrusion or searches at home, etc.[49] The ECtHR's jurisprudence, as will be explored in Chapter 4, widened the realm of privacy rights even further.

The underlying principles for the right to privacy under the ECHR have been substantially influenced by the European countries' constitutional and legal order and thought. The European (mainly French and German) approach to privacy focuses on the protection of dignity.[50] German Constitution, for instance, starts with the statement of the inviolability of human dignity, and it further provides for the right to personal development.[51]

3.4. Dignity As One of the Main Values Determining 'Privacy'

The idea of human dignity stems from natural law, and it is incorporated in the UDHR in 1948 from Western philosophical and political conceptions.[52] Although the ECHR contains no express notion of human dignity, it is implied that human dignity is in the gist of certain rights and freedoms, covered by the ECHR.[53] The ECtHR has mentioned 'human dignity' while examining the individual's right to private life under Article 8 ECHR.[54] It has held that the very essence of the ECHR is the respect for human dignity and human freedom and that personal autonomy was an important principle underlying the interpretation of guarantees of protection under Article 8 including the right to establish an identity as individual human beings.[55] It is perceived as a conceptual instrument, which lies at the basis of all fundamental rights.[56]

---

[49] See Drafting Committee on an International Bill of Human Rights, Documented Outline, 11 June 1947, E/CN.4/AC.1/3/Add.1 ('Drafting Commission Documented Outline') pages 78-94.
[50] James Q. Whitman, n 13 above.
[51] Articles 1 and 2 of the Basic Law of the German Federal Republic of 23 May 1949.
[52] On the history of the concept of human dignity see Christopher McCrudden, 'Human Dignity and Judicial Interpretation of Human Rights' (2008) 19 EJIL 655. See also Giovanni Bognetti 'The Concept of Human Dignity in European and US Constitutionalism' in Georg Nolte (ed) *European and US Constitutionalism* (CUP 2005).
[53] As Nolte explains it, the ECtHR while interpreting and/or applying the ECHR, can mention human dignity in connection with its efforts to define what degrading treatment under Article 3 is. See Georg Nolte, 'Introduction – European and US Constitutionalism: Comparing Essential Elements' in Georg Nolte (ed) *European and US Constitutionalism* (CUP 2005).
[54] *Goodwin v UK,* Judgment of 12 July 2002, Paragraph 90; *Pretty v UK,* Judgment of 29 July 2002, Paragraph 65; *Söderman v Sweden* Judgment of 12 November 2013, Paragraph 81.
[55] See *Goodwin v UK,* Judgment of 12 July 2002, Paragraph 90.
[56] Bognetti makes reference to Duerig saying that 'human dignity determines and influences the purport, extension and limit of all other rights'. See Giovanni Bognetti 'The Concept of Human Dignity in European and US Constitutionalism' in Georg Nolte (ed) *European and US Constitutionalism* (CUP 2005) at p.90.

Bluestein, in 1964, although being an American scholar, in his response to Prosser's understanding of privacy as four distinct torts,[57] interpreted Warren and Brandeis' concept of privacy as based on the principle of human dignity.[58] He contended that privacy intrusions do not intentionally inflict mental distress, but rather represent a blow to human dignity.[59]

The promotion of human dignity in the UDHR has found its way into the constitutions of some European states, such as Germany.[60] Under the German Basic Law, it represents the main value: Article 1 stipulates that dignity shall be inviolable. It further indicates the centrality of human rights to the concept of dignity. The German Federal Constitutional Court (BVerfG) in 1977 in its *Life Imprisonment* case indicated that the intrinsic dignity of the person consists of acknowledging him as an independent personality. It further held that the free human person and their dignity were the highest values of the German constitutional order. The State is obliged to respect and protect it, because a human is a spiritual-moral being that has the potential to determine and develop themself in freedom.[61]

Thereafter, the BVerfG in 1983 echoed Westin's interpretation of privacy premised on the idea of having an individual decide on the fate of their personal information: how, for what purposes, and by whom it can be used.[62] This right of informational self-determination is based on the right to dignity and personality, which later was proclaimed by the ECtHR.[63]

Some authors indicate that the difficulty in conceptualizing privacy lies with the two competing core ideas: privacy as freedom from society and privacy as dignity.[64] They contend that the drafting history of the right to privacy as an international human right does not allow for the conclusion that one of the two competing ideas can claim the status of the primary idea, and support the view that the very concept of privacy is inextricably linked to more than one idea.

Some critics of liberal privacy theories claim that conceptions of dignity are themselves culturally constructed.[65] According to Cohen '[E]ven if one posits a decontextualized, universal starting point, such as the Kantian categorical imperative, matters rapidly become more complex. Different societies articulate and perform

[57] See Prosser, n 31 above.
[58] Edward J. Bluestein 'Privacy as an Aspect of Human Dignity' (1964) 39 NYULR 962.
[59] *Ibid.* at p.974.
[60] See Neomi Rao 'On the Use and Abuse of Dignity in Constitutional Law' (2007) 14 Columbia Journal of European Law 201.
[61] See BVerfGE 45, 187 of 21 June 1977.
[62] See BVerfG, 65, 1 of 15 December 1983.
[63] *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland,* Judgment of 27 June 2017, Paragraph 137.
[64] See Oliver Diggelmann and Maria Nicole Clais, n 12 above.
[65] See Julie Cohen 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1.

commitments to dignity differently — for example, by adopting different norms about the extent to which various activities and functions may be discussed or observed'.[66]

3.5. The Right to Personal Development

Strömholm indicates that the term 'privacy' as understood in Anglo-American legal scholarship, has been defined as 'the right to personality' in continental Europe, primarily in Germany.[67] German scholarship, starting approximately from the time when Warren and Brandeis wrote 'The Right to Privacy' in the USA, and until the adoption of the German Basic Law in 1949, has identified the right of personality as a right for an individual to organize their life as they like, a right to a person's name and their honour, a catalog of other rights, such as to a person's body and life, liberty, social position, free activity, name, and mark.[68] A general right to personality examined by German scholars entitled every individual to claim recognition as such, and such a general right to personality included many limited rights, such as the right to a sphere of intimacy and the likeness of a person.[69] Such a right to personality is understood as a wider concept than a negative right 'to be let alone'.

The German Basic Law in article 2(1) proclaims that a person shall enjoy the right to free development of their personality if they do not violate the rights of others or offend against the constitutional order or the moral law.[70] According to Eberle the notion of the free development of personality is fundamentally a Kantian one and stems from the dignitarian jurisprudence as a more concrete freedom in respect of a general right to human dignity.[71]

The BVerfG thus made it clear that the human person as an autonomous being must be able to develop freely within the social community.[72] Strömholm concedes that, on the one hand, the right to personality is different from the right to privacy as understood in the US in that the former is a wider concept than just a right to be let alone. But, on the other hand, the actual conflicts covered by both terms coincide largely.[73] As will be observed later in Chapter 4, it is argued that the ECHR's right to private life has been developed by the

---

[66] *Ibid.,* p.4.
[67] See Stig Strömholm *Right of Privacy and Rights of the Personality: A Comparative Survey* (Nordic Conference on Privacy organized by the International Commission of Jurists, Stockholm, 1967).
[68] See Strömholm, n 67 above, where he makes reference to Gareis 'Das juristische Wesen der Autorrechte, sowie des Firmen- und Markenschutzes', *Busch's Archiv* (new series), vol.XXXV, 1877; Gierke, *Deutsches Privatrecht*, vol.1 1895 (Systematisches Handbuch der Deutschen Rechtswissenschaft, ed. by Binding, part II.3.I); Kohler, 'Das Autorrecht' in *Iherings Jahrbücher*, XVIII, new series VI.
[69] See Strömholm n 67 above, p.30.
[70] Basic Law of the Federal Republic of Germany, adopted on 23 May 1949.
[71] See Edward Eberle 'Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview' (2012) 33 Liverpool Law Review 201.
[72] BVerfGE 30, 173 of 24 February 1971.
[73] See Strömholm n 67 above, p.43.

jurisprudence of the ECtHR from a negative right to be let alone into a wider concept, which includes the right to develop a personality.[74]

3.6. Right to Informational Self-Determination

Further evolution of the right to personal development is reflected in the BVerfG jurisprudence. The *Population Census* judgment[75] redefined the conditions of access to personal data. The Federal Census Act of 1983 contained numerous questions covering *inter alia* housing records and workplace census through the intended systematic use of computerized processing aimed at unlimited surveillance of citizens. The Act required citizens to reveal details of their sources of income, educational background, transportation, and way of commuting to and from work. The BVerfG stated that the duty to protect the individual's dignity and their freedom to develop their personality through technologies enabling the processing of large amounts of personal data ought to be complemented by the right to informational self-determination.[76] Individuals may freely form, express, and defend their opinions only if they can determine who can use their data, for what purpose, under what conditions, and for how long.[77] The BVerfG sees the right to informational self-determination as a necessary precondition of a democratic society, where an individual is capable of acting autonomously and participating in the life of society due to the knowledge and control, that such an individual enjoys over their data.[78]

The BVerfG further reasoned that an individual's right to plan and make decisions freely could be drastically diminished, if they could not foresee what personal data was known to and could be disclosed by others.[79] It is destructive for the community if citizens are unaware of who possesses their personal data and for what purposes. This may lead citizens to cut their activities and abstain from enjoying their rights, such as the right to association, freedom of expression, and religious or occupational freedoms.[80] This could harm an individual's personal development, which could be seen as damage to the common good.[81] Thus, in essence, informational self-determination stems from human autonomy. It is about

[74] See Bart Van der Sloot 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interest Might Prove Indispensible in the Age of 'Big Data' (2015) 31 Utrecht Journal of International and European Law 25.
[75] BVerfG, 65,1 of 15 December 1983. See n 62 above.
[76] *Ibid.* at 43.
[77] See Spiros Simitis 'Privacy – An Endless Debate' (2010) 98 California Law Review 1989.
[78] Simitis *ibid.*
[79] BVerfG, 65, 42, see n 62 above.
[80] *Ibid.*
[81] *Ibid.* See also Eberle at 225, see n 71 above.

control over personal information, which means power over an individual's fate. The right to informational self-determination is essential to the free development of personality.[82]

The ECtHR has adopted the German approach in its judgment of *Satakunnan*,[83] recognising the right to informational self-determination as a right to the protection of personal information, which forms part of the right to private life under Article 8 ECHR. This case and the right to informational self-determination will be examined in Subsection 4.1.4.4 of Chapter 4 of this thesis.

3.7. Privacy – a Common Good?

Westin's interpretation of 'privacy' as a control over personal information has deeply influenced the development of data protection law. With the current digital revolution, which creates an overwhelming infrastructure for surveillance, it is next argued that the focus ought to be on the meaningful choice that an individual has to make.[84] Such choices may be available within the social context, where an individual's need for the protection of their personal data emerges. It is not always up to individuals to control information about them. It is up to the context, which sustains choices that promote an individual's autonomy and well-being.[85] It is argued that in the digital age, all individuals appreciate some degree of privacy and share some common perceptions of privacy, so it becomes a collective value.[86]

It has been mentioned in Chapter 2 of the thesis that Soviet Tajikistan was part of the totalitarian USSR, and its socialist Constitutions reflected the priority of collectivist over individualistic values. Austin claims that Westin's account of control-based privacy is much wider than traditionally thought or interpreted and criticized by other scholars. According to her, Westin speaks about the 'social balance' between privacy and surveillance.[87] Social balance is fundamentally shaped by the political system of a society. Austin further argues that

> '[t]otalitarian systems display a different balance than liberal democracies, and even within the category of liberal democracies there are multiple variations. This social balance involves social norms, but they are different from the interpersonal norms that Westin often discusses when he discusses how curiosity or limited disclosure

[82] Eberle, *ibid.*
[83] See *Satakunnan,* see n 63 above.
[84] See Lisa Austin, n 43 above.
[85] *Ibid.* at 56.
[86] See Priscilla Regan, n 6 above.
[87] See Lisa Austin, n 41 above, at 65.

between individuals operates. These are norms that underpin our political and legal institutions and structure the relationship between individual and State.'[88]

When an individual balances his interest in privacy with the government's interest in conducting surveillance, then their ability to entertain such a balancing exercise is affected by a political and legal system in the society, and the extent to which privacy is protected in relation to other values.[89]

Other authors go further to criticize Westin's control-based account of privacy, as well as other conceptualizations of privacy based on a liberal political theory.[90] For them, the problem of theorizing privacy as an individual value lies in unsuccessful attempts to link privacy to one of the overarching principles, such as liberty or control. Thus, for instance, when privacy is seen as a commodity to be traded against other goods, such as security, one fails to consider the collective and social nature of privacy benefits.[91] Simitis argues that 'privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone.'[92] In this vein, privacy must not be seen as a demonstration of the individual against society's norms and values, but as the protection of the individual according to society's norms and interests.[93]

Some authors propose a concept of privacy based on the integrity of the different contexts creating grounds for the use of personal data by third parties.[94] Different privacy expectations are influenced by the context of a promise, relationship, conversation, or event. Context, they claim, as a place (home, office, park, café, supermarket), plays a crucial role in defining privacy.[95] They argue that different social contexts are governed by different social norms that govern the flow of information within and outside of that context.[96] Protecting privacy entails ensuring appropriate flows of information between and among contexts. Privacy is a social norm, which defines what information is suitable to disclose and how that information ought to be transferred in different social contexts.[97] Other authors

[88] *Ibid.*
[89] *Ibid.*
[90] See Priscilla Regan, n 6 above; Julie Cohen, n 65 above, Helen Nissenbaum 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119.
[91] See Priscilla Regan, n 6 above.
[92] Spiros Simitis 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania Law Review, p.709.
[93] See Daniel Solove 'The Meaning and Value of Privacy' in Beate Roessler and Dorota Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP, 2015) 71.
[94] See Helen Nissenbaum, n 90 above.
[95] See Helen Nissenbaum 'Privacy and Common Good: Revisited' in Beate Roessler and Dorota Mokrosinska (eds.) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP 2015) 278.
[96] See Helen Nissenbaum *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford University Press, 2010).
[97] *Ibid.*

explain that individuals are born and remain situated within social and cultural contexts, and their relationship to such social and cultural contexts is dynamic.[98] Privacy incursions harm individuals, but not only individuals. Privacy invasions for the sake of progress, innovation, and ordered liberty endanger the continuing vitality of the political and intellectual culture.[99]

Detailed regulation of data protection by national and supranational laws provides a similar minimum standard of privacy for everyone.[100] Some authors argue that the value of privacy ought to be assessed based on its contributions to society, and its benefits, which it confers to society by remedying certain harms to individuals.[101] Protection of privacy is the protection of the individual based on society's norms and practices.[102] Privacy may be seen as a common good: it prevents going into a totalitarian regime, promotes intellectual development by providing the necessary context for freely forming, developing, and expressing ideas, and encourages individuals to form different kinds of social relationships.[103]

At the same time, the ECtHR's jurisprudence covering the issues of privacy and surveillance has been criticized for its incoherence in addressing the social value of privacy.[104] Hughes examines the ECtHR's case law involving not only the right to privacy, but similarly protecting a catalog of non-absolute rights: freedom of thought and religion, freedom of expression, and freedom of association (Articles 9-11 ECHR).[105] She compares the reasoning in the ECtHR's judgments in cases involving the protection of those rights and freedoms, and concludes that the ECtHR sees the right to private life more as an individual value as opposed to other rights, which are of utmost importance to society.[106]

Hughes refers to a few examples of relevant case law. In *Eweida v UK,* the ECtHR held that the freedom of religion was one of the foundations of a democratic society, and that 'the pluralism indissociable from a democratic society, which ha[d] been dearly won over the centuries depends on it'.[107] Freedom of expression was called by the ECtHR one of the essential foundations for a democratic society, and one of the basic conditions for its

[98] See Julie Cohen 'What Privacy is For' (2013) 126 Harvard Law Review 1904.
[99] *Ibid.*
[100] *Ibid.*
[101] See Daniel Solove 'The Meaning and Value of Privacy' in Beate Roessler and Dorota Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP, 2015) 71.
[102] *Ibid.,* p.78.
[103] See Kirsty Hughes 'The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse' in Beate Roessler and Dorota Mokrosinska (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives* (CUP, 2015) 225.
[104] *Ibid.,* p. 234-236.
[105] *Ibid.*
[106] *Ibid.,* p.232
[107] *Eweida v UK,* Judgment of 27 May 2013, Paragraph 79.

progress.[108] In *Kudrevicius v Lithuania* the ECtHR explained 'that the right to freedom of assembly is a fundamental right in a democratic society and like the right to freedom of expression is one of the foundations of such a society'.[109]

Cohen criticizes liberal privacy theory based on the premise of individual autonomy. For her, an individual has no autonomous role because people are born and act within social and cultural contexts. She claims that 'privacy is not a fixed condition, nor could it be, because the individual's relationship to social and cultural contexts is dynamic. These realities do not weaken the privacy case; they strengthen it. But the nature and importance of privacy may be understood only about a very different vision of the self and the self-society connection'.[110] Individuals do have identities and find themselves making choices. But such experience and therefore their eventual identification is socially built in many crucial respects.[111]

Regan in her book *Legislating Privacy* observes privacy as three different values: as a social value, which is a common value (shared by individuals), as a public value (of value to the democratic political system), and as a collective value (technology and market forces make it increasingly difficult for any one person to have privacy unless everyone has a minimum level of privacy).[112] Essentially this means that privacy is something we all value, it is important for the democratic political system and we cannot have it unless we work together. A definition of privacy as the right of the individual to control access to himself or herself, in effect, rests upon an 'exaltation of the powers of the individual'. Regan explains that the interests of the organizations collecting and using personal information must be taken into account, where the individual is given the means to mediate their relationship with such organizations. By placing the burden on the individual, there is less need to evaluate whether organizational interests are indeed social interests or whether individual privacy interests could be conceived as social interests.[113]

Privacy as a common value according to Regan means that all individuals have an interest in privacy. Those individuals or groups of individuals may have different perceptions of what the right to privacy is, but they all have a common interest in the right to privacy.

[108] *Handyside v UK* (1974) A24, Paragraph 49.
[109] *Kudrevicius v Lithuania,* Judgment of 15 October 2015, Paragraph 91.
[110] Julie Cohen, see n 98 above, p.1908.
[111] Julie Cohen, see n 65 above.
[112] Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995) p.212.
[113] *Ibid,* p.219.

Individuals recognize the importance or need to develop privacy boundaries, and this establishes grounds for individual choice as to what must remain private.[114]

The public value of privacy is expressed in its importance not just to individuals, but to the 'democratic political system'. The right to privacy is important to the exercise of other rights, which are essential to democracy, e.g., freedom of expression.[115]

The concept of collective value used by Regan derives from the economists' concept of collective good, where 'no one member of society can enjoy the benefit of collective good without others also benefiting'.[116] Private companies nowadays hold a massive amount of personal data. These institutional-individual relationships are not just necessary for the individual to function in modern life but are also necessary for the functioning of a modern economy and society. Payment of taxes, social security matters, engaging in social media, political life, buying goods and services, and many other aspects of life require interaction between individuals and private companies or organizations, and if a large number of people opt out of these systems, the consumer economy will be less efficient.[117]

3.8. Privacy in the Context of Large-Scale Personal Data Collected by Corporations

Regan explains that for the last couple of decades, dramatic changes in our personal, business, community, political, and professional lives have occurred, which affects our ability to protect our private life and changes our perception of the value of privacy.[118] Almost everything in our life is mediated or facilitated in any way or another by systems put in place by large private companies. Some of them have several billions of users, who participate in a daily life of the platforms managed by such private companies.[119] Newspapers, universities, energy companies, healthcare providers, banks, and retail stores have all opened their operations online. Almost every 'bricks and mortar' company has its online platform for operating business as well. Moreover, pure online services and stores emerged, and operate successfully in the market. Regan views these systems as not simply

[114] *Ibid,* p.221-222.
[115] *Ibid,* p.225.
[116] *Ibid,* p.227.
[117] *Ibid,* p.228.
[118] Priscilla Regan, see n 6 above.
[119] E.g., there were 3,065 billion active users of Facebook during each month of the last quarter of 2023. https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/#:~:text=How%20many%20users%20does%20Facebook,used%20online%20social%20network%20worldwide. The link has been last time accessed on 12 March 2024.

technological information systems, but as complex interdependent systems of technical artifacts, cultural practices, social actors, and situated meanings.[120]

The behavioral activity of individuals concerning privacy in two aspects of our contemporary life – social networking platforms and national security surveillance systems – provides an argument that privacy is viewed in common terms and as similarly important for different groups of people.[121] A 'networked public'[122] makes it much more difficult for any individual to set their own privacy standards and keep track of the flow of information about them. In a networked public, it is difficult for any individual to enjoy privacy without all other persons in that network enjoying a similar level of privacy. Instead, privacy is established as part of the network and the various databases and interconnections that compose the network and are shared collectively by those in the network.[123]

Thus, the concept of privacy has been developed for a couple of centuries as a freedom of individuals from State interference, as well as recently from interference of third parties. There were many attempts to define privacy by legal scholars, and in the age of advanced technologies, data protection laws are inspired by the concept of control of personal data, formulated by Westin, where an individual must decide the fate of their personal information: to whom, how, for how long and for which purposes their personal information may be made accessible. The right to personality determines the comprehensive personal development of an individual, including their informational self-determination.

Cohen points out that surveillance as a mode of social control, succeeds especially well within economically developed societies' 'ongoing shift from industrialism to informationalism'.[124] She further explains that 'surveillance has emerged as a distinct modality of profit generation'.[125] Zuboff called it 'surveillance capitalism'.[126]

The foregoing examinations show that the mainstream Western concept of privacy is different from the Tajik concept of privacy explored in Chapter 2 of the thesis. Although large private companies appear as the main processors of personal data, governmental agencies may have access to personal data gathered and processed by private entities to

[120] Priscilla Regan, see n 6 above, p.51.
[121] *Ibid.,* p.58.
[122] Marwick and Boyd explain the term 'networked public' as a space 'constructed through networked technologies and imagined communities that emerge as a result of the intersection of people, technology and practice'. This virtually means 'social media'. See Alice Marwick and Danah Boyd 'Networked Privacy: How teenagers negotiate context in social media' (2014) 16/7 New Media & Society 1051.
[123] Priscilla Regan, see n 6 above, p.65.
[124] Julie Cohen 'Surveillance vs Privacy: Effects and Implications' in Grey D. and Henderson S (eds) *Cambridge Handbook of Surveillance Law* (CUP, 2017) p.455-469, at p.457.
[125] Cohen, see n 124 above.
[126] See Shoshana Zuboff 'Big Other: Surveillance Capitalism and the Prospect of the Information Civilization' (2015) 30 Journal of Information Technology 75.

conduct surveillance measures. Next, Chapter 4 of the thesis analyses the ECtHR case law on surveillance issues with a view to exploring standards for protecting private life under the ECHR. This eventually brings about a discussion on lessons, which Tajikistan can learn from the ECtHR jurisprudence.

Chapter 4. The ECHR: General Principles Relating to Surveillance, Data Protection and Privacy Rights

4.1. Overview of Article 8 ECHR in View of Protecting Personal Data: Meaning and Interpretation

Before providing an analysis of the ECtHR case law on surveillance cases, this Chapter of the thesis will discuss the scope of Article 8 of the ECHR in general, and the scope of the right to data protection as an element of the right to private life protected by Article 8.

4.1.1. The Scope of Article 8 ECHR: General Overview

> Article 8 of the ECHR consists of two paragraphs, which provide as follows:
> 1) Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of rights and freedoms of others.

As is evident from the above text of Article 8, its Paragraph 1 stipulates the rights as those which individuals enjoy under the ECHR, and Paragraph 2 enshrines certain restrictions to the enjoyment of those rights. Four rights or freedoms, which are reflected in Paragraph 1, are intertwined with the idea of prohibiting the government to interfere with the privacy of individuals, i.e., something which is not a matter for publicity, but rather something private, intimate, or personal. It bears making preliminary examinations of four generic categories of legal interests protected by Article 8 before turning to specific issues of surveillance.

4.1.1.1. Private Life

The ECtHR as early as in 1992 has given up the idea of providing any exhaustive definition of 'private life', as the 'private life' is not limited to an 'inner circle', but must include the right to establish and develop relationships with other individuals.[1] A collection

[1] *Niemietz v Germany* (1992) Series A no 251-B, Paragraph 29.

of personal information by State officials without the consent of an individual has been always concerned with the private life of the individual, e.g., recording of fingerprints and photography by the police,[2] or in cases when the police register was not a public one,[3] recording and keeping fingerprints, DNA profiles and cellular samples[4]. In *Peck vs United Kingdom,*[5] the ECtHR holds that the identifiable picture of an individual on the street taken by the CCTV, constitutes personal data, and is therefore afforded protection under Article 8 of the ECHR and that the protection of personal data is of fundamental importance to the enjoyment by a person of the right to respect of their private life[6].

4.1.1.2. Family life

While it is generally understood that issues of data protection and surveillance are more squarely addressed by the concept of privacy, the three other concepts (or 'legal interests') under Article 8 (family life, correspondence, and home) entail bearing on those issues. Here, inquiries will be made into how an interpretation employed by the ECtHR in respect of those concepts in specific cases can shed light on its distinct approach and rationales. The notion of 'family life' differs from 'private life' in that it requires a stricter interpretation for the obvious reasons that the circle of persons concerned is limited to sometimes immediate members of a family, such as parents and children (natural or adopted) or husband and wife, and sometimes to other members of family depending on the context and types of cases.[7] The definition of 'family life' is an autonomous concept,[8] i.e., it must be interpreted independently from how it is reflected in domestic laws or construed by domestic courts. Who is included in a family may always vary depending on the existence of close personal ties.[9] De facto family ties may be regarded as a 'family life' in certain cases.[10] In other cases, it is the length of relationships that matters.[11]

[2] *Murray v UK* (1994) Series A no 300-A.
[3] *Leander v Sweden* (1987) Series A no 16, Paragraph 48.
[4] *S and Marper vs UK*, Judgment of 4 December 2008, Paragraphs 77 and 86.
[5] *Peck v UK,* Judgment of 28 April 2003.
[6] See also *Z v Finland,* ECHR, Judgment of 25 February 1997, Paragraph 95.
[7] See Alan Desmond 'The Private Life of Family Matters: Curtailing Human Rights Protection for Migrants under Article 8 of the ECHR?' (2018) 1 European Journal of International Law 29, where he describes that in cases of expulsion of migrants the right to respect 'family life' should be interpreted in a more restrictive way, which makes it different from the right to private life.
[8] See *Marckx v Belgium* (1979) Series A no 31, Paragraph 31.
[9] See *Paradiso and Campanelli v Italy*, Judgment of 24 January 2017, Paragraph 140.
[10] *Johnston and Others v Ireland* (1986) Series A no 112, Paragraph 56.
[11] *Wagner and J.M.W.L v Luxembourg*, Judgment of 28 June 2007, Paragraph 117.

In cases involving personal data protection, 'family life' is not invoked as a category, which is allegedly in breach. It is rather a right to 'private life', which is invoked, when personal data is processed, and an individual seeks protection under Article 8 of the ECHR.[12]

4.1.1.3. Home

The ECtHR in its jurisprudence has contended that 'home', as 'private life' or 'family life', depends on factual circumstances, such as, for instance, the existence of sufficient and continuous links with a specific place.[13] The notion of 'home' can equally apply to business premises[14] or even caravans.[15]

Personal data protection cases involving intrusion into the home of an individual have been resolved by the ECtHR under the concept of 'private life' because even if an unlawful collection of personal data or unlawful surveillance has taken place through violation of the right to respect for home, personal data represents the 'private life', which ought to be respected or protected by the government.[16] Thus, in *Alkaya v Turkey*, a home address was found to have constituted personal information that was a matter of private life, not of 'home'.[17]

4.1.1.4. Correspondence

The right to respect for the correspondence includes protection of both private and professional correspondence.[18] Telephone conversations with persons, who are not members of the family, can be regarded as 'correspondence', although 'telephone conversations' are not expressly mentioned in the Article 8(1) provision.[19] The ECtHR has stated that the metering, i.e., information on the telephone numbers used by an individual and the timing of the calls as well as their duration may be part of the concept of 'correspondence' even though metering is not related to the content of the phone calls.[20] Thus, interception of such metering information could amount to a breach of the right to respect for correspondence.[21] Similarly,

---

[12] See *Mikulic v Croatia,* Judgment of 4 September 2002.
[13] *Prokopovich v Russia*, Judgment of 18 February 2005, Paragraph 36.
[14] *Niemietz v Germany,* see n 1 above, Paragraphs 29-31.
[15] *Chapman v UK,* Judgment of 18 January 2001, Paragraphs 71-74.
[16] *Ismayilova v Azerbaijan,* Judgment of 10 April 2019, Paragraphs 106-107.
[17] *Alkaya v Turkey*, Judgment of 9 January 2013, Paragraph 30; *Ismayilova v Azerbaijan,* n 16 above, Paragraphs 140 and 142.
[18] *Niemietz v Germany,* see n 1 above, Paragraph 32.
[19] *Klass and Others v Germany* (1978) Series A no 28, Paragraph 41.
[20] *Malone v UK* (1984) Series A no 82, Paragraphs 82-84.
[21] *P.G and J.H v UK,* Judgment of 25 December 2001, Paragraph 42.

electronic mail and Internet usage at the workplace ought to be covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8(1) of the ECHR.[22] Electronic data stored on computer systems has been examined under the concept of 'correspondence'.[23] Not only interception or collection of metering data, but equally storage of such personal information about phone, e-mail, and Internet usage by an individual, can amount to a breach of the right to respect for correspondence.[24] There is good reason to suggest that the ECtHR in its jurisprudence has examined personal data protection under the right of an individual to respect for 'private life' and 'correspondence', but not necessarily for 'family life' or 'home'.

4.1.2. Personal Data

Personal data as an object of the protection of human rights of individuals is not specifically mentioned in the text of the ECHR. However, with the development of advanced technologies, personal data privacy become the right of an individual, which is protected by Article 8 ECHR through wide interpretation of that provisions by the European Court of Human Rights.[25]

In *Aycaguer v France*, the ECtHR held that personal data protection played a primordial role in the exercise of the right of individuals to respect their private life as enshrined in Article 8.[26] In that case, the ECtHR considered it an alleged violation of private life without mentioning any other categories of rights listed in Article 8, such as, e.g., 'family life'. In this respect, this thesis examines whether the other three categories of rights under Article 8 have been invoked without mention of any alleged breach of 'private life'. Telephone conversations are covered by both notions of 'correspondence' and 'private life' in *Zakharov v Russia,*[27] and internet communications – by the same two terms in another case.[28] However, in *Wieser and Bicos Beteiligungen v Austria*, the ECtHR found it necessary to examine the alleged breach of the right to respect for 'correspondence', but not for the 'private life'.[29] In *Bykov v Russia* an applicant claimed that his right to private life and home

[22] *Copland v UK,* Judgment of 3 July 2007, Paragraphs 41-42.
[23] *Wieser and Bicos Beteiligungen GmbH v Austria,* Judgment of 16 January 2008, Paragraph 45.
[24] *Copland v UK*, see n 22 above, Paragraph 44.
[25] See *Leander v Sweden*, see n 3 above, Paragraph 48; *P.G and J.H v UK*, see n 21 above, Paragraph 59; *Peck vs UK,* see n 5 above, Paragraphs 60-63; *Uzun v Germany,* Judgment of 2 December 2010, Paragraph 52.
[26] *Aycaguer v France,* Judgment of 22 September 2017, Paragraph 38.
[27] *Zakharov v Russia,* Judgment of 4 December 2015, Paragraph 173.
[28] *Barbulescu v Romania,* Judgment of 5 September 2017.
[29] *Wieser and Bicos Beteiligungen GmbH*, see n 23 above, Paragraph 45.

had been violated,[30] and the ECtHR in that case, while finding a violation of the right to private life, decided for this very reason not to proceed with looking at whether there had been a violation of the right to respect for his home.

Whenever the ECtHR refers to 'personal data' or considers cases involving personal data, which ought to be protected under the concept of the right to private life, the ECtHR examines only whether one or another type of personal data can be considered as personal data and/or whether it can be protected by the provision contained in Article 8 of the ECHR. For instance, in *S and Marper v UK* the ECtHR held that fingerprints, DNA profiles and cellular samples constitute personal data.[31] In *Amann v UK* the ECtHR found that creating and holding a card in a file containing personal data by the public authorities, ought to be protected by Article 8 of the ECHR.[32]

The ECtHR usually refers to the domestic law of the respondent State[33] and to the Council of Europe and EU legal instruments in its jurisprudence[34] for the purposes of using the term 'personal data' in its examination of the cases. In *Barbulescu v Romania*[35] the ECtHR made reference to the Council of Europe Convention 108 (Convention 108)[36] and to the EU Data Protection Directive (DPD),[37] which gave a definition of 'personal data'. The DPD is replaced by the European Union's General Data Protection Regulation (GDPR).[38] According to these EU legal instruments, 'personal data' means any information relating to an identified or identifiable natural person,[39] such as name, identification number, location data or any other physical, psychological, genetic, mental economic, cultural or social identity of an individual.[40]

---

[30] *Bykov v Russia,* Judgment of 10 March 2009.
[31] *S. and Marper v UK,* Judgment of 4 December 2008, Paragraph 68.
[32] *Amann v Switzerland,* Judgment of 16 February 2000, Paragraphs 77 and 80.
[33] *S. and Marper v UK,* n 4 above, Paragraphs 30-32; *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland,* Judgment of 27 June 2017, Paragraph 34; *Benedik v Slovenia,* Judgment of 24 July 2018, Paragraph 40.
[34] See *S. and Marper v UK,* n 4 above, Paragraph 50; *M.L. v Germany,* Judgment of 28 September 2018, paragraphs 52 and 57; *P.N. v Germany,* Judgment of 16 November 2020, Paragraphs 28-30.
[35] *Barbulescu v Romania*, see n 28 above, Paragraphs 42 and 45.
[36] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) dated 28 January 1981, amended later with Additional Protocol of 2001 (ETS 181), and, recently, modernized through Amending Protocol (CETS 221). Now, it is the Modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the CoE Committee of Ministers on 18 May 2018, CM/Inf(2018)15-final.
[37] Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (1995) OJ L281/31.
[38] Regulation of EU 216/679 dated 27 April 2016 'On the protection of natural persons with regards to the processing of personal data and on the free movement of such data' OJ EU 119/1 (GDPR).
[39] Article 4(1) GDPR. Article 2(a) of the Convention 108 provides the same definition of 'personal data'.
[40] Article 4(1) GDPR.

The ECtHR recognizes that some categories of data must be regarded as special or particularly sensitive, and therefore shall be afforded better protection by the domestic law of the States-parties to the ECHR, as the processing of such data may create significant risks to fundamental rights and freedoms. Personal data related to racial or ethnic origin,[41] political opinions,[42] religious or philosophical beliefs,[43] genetic data, biometric data, data concerning health[44] or sexual life or sexual orientation[45] of a person are included in such specially protected categories of personal data.[46]

Thus, the processing of personal data could serve as a necessary prerequisite to identifying individuals. The processing of personal data of an individual includes collection,[47] storage,[48] transfer, or other forms of use of data.[49]

As the ECtHR provides no definition of 'personal data', its jurisprudence relies on how the Convention 108,[50] DPD[51] or GDPR,[52] as a case may be, define it. This Chapter will include some examination of the EU law insofar as this is relevant for the specific purposes of understanding how 'personal data' have been interpreted within the framework of the DPD and understood under the GDPR.

4.1.3. Lawful restrictions or limitations

Article 8 Paragraph 2 of the ECHR foresees possibilities for public authorities to restrict the application of the rights enshrined in Paragraph 1 of that Article. Public authorities may in certain circumstances justify their interference with private and family

[41] *S. and Marper v UK,* n 4 above, Paragraph 66.
[42] *Catt v UK,* Judgment of 24 April 2019, Paragraph 112.
[43] *Folgerø v Norway,* Judgment of 29 June 2007, Paragraph 98.
[44] *Z v Finland,* see no 6 above, Paragraph 95.
[45] *B. v. France*, (1992) Series A no. 232-C, Paragraph 63; *Laske and Others v UK,* Judgment of 19 February 1997, Paragraph 36.
[46] See GDPR Article 9 and Convention 108 Article 6
[47] In *P.N. v Germany*, see n 34 above, the applicant claimed that their identification data had been unlawfully collected used, and retained.
[48] *Gaughran v UK,* Judgment of 13 June 2020, Paragraph 70; *Breyer v Germany,* Judgment of 7 September 2020, Paragraph 75.
[49] Convention 108 in its Article 2(b) defines 'data processing' as any operation or set of operations, such as the collection, storage, preservation alteration, retrieval, disclosure, making available, erasure or destruction of, or the carrying out of logical and/or arithmetical operations on such data.
[50] *Amann v Switzerland*, see n 32 above, Paragraph 65; *Barbulescu v Romania*, see n 28 above, Paragraph 42 ; *Big Brother Watch and Others v* UK, Judgment of 4 February 2019, Paragraphs 205-207; *Bernh Larsen Holding AS and Others v Norway,* Judgment of 8 July 2013, Paragraphs 76-79; *Benedik v Slovenia*, see n 33 above, Paragraph 46.
[51] *Barbulescu v Romania*, see n 28 above, Paragraph 45, *Big Brother Watch and Others v UK,* see n 50 above; *Lopez Ribalda and Others v Spain,* Judgment of 17 October 2019, Paragraph 63; *Centrum for Rattvisa v Sweden,* Judgment of 25 May 2021, Paragraphs 76-77.
[52] *Benedik v Slovenia*, see n 33 above, Paragraphs 53-55, *M.L. v Germany,* Judgment of 28 September 2018, paragraph 58; *Big Brother Watch and Others v UK,* see n 50 above, Paragraphs 219-220; *Lopez Ribalda and Others*, see n 51 above, Paragraph 63; *P.N. v Germany*, see n 34 above, Paragraph 30.

life in order to achieve certain public aims and social needs, such as national security, public safety, protection of health and morals and protection of the rights and freedoms of others. In this sense, i.e., in terms of stipulating limitations to the enjoyment of rights and freedoms, Article 8 is similar to Articles 9-11 (freedom of conscience, freedom of expression, and freedom of assembly) of the ECHR, which foresee protection against unlawful interference by the public authorities with those individual freedoms, and which have similar provisions establishing relevant restrictions or limitations.

Such interference ought to be strictly in accordance with the law and must be necessary in a democratic society. It is notable that a global human rights instrument, such as the International Covenant on Civil and Political Rights, has no reference to the social needs or public interests, which would justify an interference by the State in the right to private life. Article 17 mentions only that an interference must not be arbitrary or unlawful. As explained by Diggelmann and Cleis, the drafting history of the ICCPR suggests that the essence of Article 17 ICCPR is a reflection of the general rule contained in Article 12 UDHR with the only difference that the ICCPR provision protects from 'unlawful' interference with privacy.[53] Eventually, it was agreed to retain the general rule used in UDHR in Article 17 ICCPR, and give the States the discretion to decide individually on exceptions to the general rule and on methods of applications.[54]

Joseph suggests that since Article 17 provides for no specific ground of limitation of the right to privacy, the UN Human Rights Committee (HRC)[55] must conduct greater scrutiny of relevant laws to ensure that the States provide necessary safeguards against the arbitrariness of interferences with the privacy of individuals.[56] In its General Comment No 16, the HRC recommends the States to indicate in their reports the laws and regulations that govern authorized interference with private life.[57] Only a State authority competent and empowered by the law can take decision on using such authorized interference, and on a case-by-case basis.[58]

---

[53] Oliver Diggelmann and Maria Nicole Cleis 'How the Right to Privacy became a Human Right' (2014) 14 Human Rights Law Review 441 at 449.
[54] Diggelmann and Cleis, *ibid*., at 451. See also Commission on Human Rights, Report on its 9th Session, 6 June 1953, E/CN.4/689 ('Commission Report 2447'), Paragraph 67.
[55] The UN Human Rights Committee is a treaty body, established under the ICCPR, and its primary task is to monitor the compliance of the states-parties to ICCPR with their human rights obligations through receiving state reports and commenting on them, as well as though examining individual human rights complaints.
[56] Sarah Joseph and Melissa Castan *The International Covenant on Civil and Political Rights (Cases, Materials and Commentary)* (OSAIL 3rd ed. 2013) at 462.
[57] CCPR General Comment No.16: Article 17 (Right to Privacy) dated 8 April 1988, Paragraph 7.
[58] General Comment No.16, *Ibid*., Paragraph 8.

The ECtHR has developed a flexible formula for the interpretation and application of Article 8(2) of the ECHR, which would help in determining whether a particular interference with private life is in accordance with the law, pursues a legitimate aim, and is necessary in a democratic society. It is a step-by-step procedure, where the ECtHR first determines whether there is an interference with the private life. Only if this is answered in positive, the ECtHR goes on to examine whether the interference is in accordance with the law. The ECtHR may save its time if it finds that the impugned measures are not in accordance with the law. For instance, in *Vukota-Bojic v Switzerland*, the ECtHR found that the disputed measure was not taken 'in accordance with the law', and therefore it deemed unnecessary to go into making an analysis of whether the measure in question was 'necessary in a democratic society'.[59] In *Rotaru v Romania* it was decided that the holding and using of the personal data of an individual by the intelligence services was not in accordance with the law, constituting a violation of Article 8, and that prevented the ECtHR from reviewing the legitimacy of the aim and its necessity in a democratic society.[60]

Thereafter, the ECtHR, if the interference is found to be in accordance with the law, turns on the issue of whether the interference pursued a legitimate aim indicated in Article 8. Again, the ECtHR moves its focus further on whether the interference was necessary in a democratic society, only if it finds that the interference in fact pursues a legitimate aim or if parties, mainly the applicant, do not question or dispute the existence of a legitimate aim for the interference.

4.1.3.1. In accordance with the law

The ECtHR has held that the term 'in accordance with the law' ought to be interpreted in its 'substantive' sense, not its 'formal' one,[61] so it could include both 'written law' and 'unwritten law'.[62] In *Barthold v Germany,* although that case concerns Article 10 of the ECHR rights – freedom of expression, the ECtHR considered the act adopted by the independent professional body, but not the parliament, as the 'law' within the meaning of Article 10(2) provision.[63]

'In accordance with the law' means not merely a domestic law, but can also relate to the quality of the law, requiring it to be compatible with the rule of law concept. In other words,

[59] *Vukota-Bojic v Switzerland*, Judgment of 18 January 2017, Paragraph 78.
[60] *Rotaru v Romania*, Judgment of 4 May 2000, Paragaraph 62.
[61] *Leyla Sahin v Turkey*, Judgment of 10 November 2005, Paragraph 88;
[62] *Malone v UK*, see n 20 above, Paragraph 66.
[63] *Barthold v Germany* (1985) Series A no. 90, Paragraph 46.

it means that there ought to be a measure of legal protection in domestic law against arbitrary interference of public authorities with the rights protected by Article 8(1).[64]

Any interference with private and family life must have some basis in domestic law.[65] The law ought to be clear, foreseeable, and adequately accessible.[66] Domestic law cannot provide for every eventuality, but there ought to be a certain degree of clarity of legal provisions, which considerably depends on the content of the law, the area of its application, and the status of those to whom it is addressed.[67] In the context of covert measures of surveillance, the law must be sufficiently clear to give individuals an adequate indication, in what circumstances and under which conditions public authorities can be authorized to take such measures.[68] All circumstances of the case of surveillance must be assessed, e.g., nature, scope, and duration of measures, the ground required for ordering them, the authorities competent to permit, carry out and control them, and the type of redress provided by the domestic law.[69] Akin to the surveillance laws there ought to be clear legal norms on minimum standards of personal data retention by the authorities.[70]

4.1.3.2. Legitimate aim(s)

Legitimate aims or purposes, which may justify the interference of public authorities with private life are enumerated in Article 8(2) of the ECHR. These are: national security, public safety, economic well-being of the country, prevention of disorder or crime, protection of health or morals, and protection of the rights and freedoms of others. The ECtHR has conceded that in its jurisprudence it is a rare practice when the existence of legitimate aims has been extensively scrutinized.[71] For instance, in *Leyla Sahin v Turkey,* the ECtHR has accepted that protecting the rights and freedoms of others and protecting public order served as legitimate aims for public authorities' conduct, as there was no issue between parties in this regard.[72] The burden of proving the existence of a legitimate aim rests with the State authorities,[73] and in case it is not even mentioned by the responding government, the ECtHR

[64] *Malone v UK*, see n 20 above, Paragraph 67; See also *Halford v UK,* Judgment of 25 June 1997.
[65] *Silver and Others v UK* (1983) Series A no.61, Paragraph 86.
[66] *Ibid.*, *Silver and Others v UK*, Paragraphs 87-88.
[67] *S and Marper vs UK*, n 4 above, Paragraph 96; *M.K. v France,* Judgment of 18 July 2013, Paragraph 27.
[68] *Malone v UK*, see n 20 above, Paragraph 67; *Uzun v Germany*, see n 25 above, Paragraph 61;
[69] *Uzun v Germany*, see n 25 above, Paragraph 63;
[70] *S and Marper vs UK,* n 4 above, Paragraph 96; *Rotaru v Romania*, see n 60 above, Paragraphs 56-59; *P.N. v Germany*, see n 34 above, Paragraph 62.
[71] *S.A.S. v France,* Judgment of 1 July 2014, Paragraph 114.
[72] *Leyla Sahin v Turkey,* n 61 above, Paragraph 99.
[73] *P.T. v Moldova,* Judgment of 26 August 2020, Paragraph 29.

may come to a conclusion that there is no legitimate aim pursued by the actions of public authorities, which leads to the breach of Article 8 provisions.[74]

In cases involving personal data protection, the ECtHR held that 'prevention of crime' could be regarded as a legitimate aim for the government to retain DNA information,[75] 'safeguarding national security and/or prevention of crime or disorder' has served as legitimate aims in the case of secret surveillance conducted by public authorities.[76] In *M.N. and Others v San Marino,* the ECtHR indicated that the measures taken by public authorities pursued various legitimate aims, including the protection of the rights and freedoms of others and the economic well-being of the country.[77]

4.1.3.3. Necessary in a democratic society

The last component, which the ECtHR examines, if the previous two (law and legitimate aim) have been found to be complied with by the public authorities, is about striking a fair balance between competing public and private interests. As Schabas asserted, this is the most subjective part of the application of Paragraph 2, where the ECtHR ought to make subtle distinctions about the proportionality of measures taken by the States, which limit or restrict human rights.[78] The use of the word 'democratic' by the ECHR drafters was reasoned by the post-WWII desires to prevent the rebirth of totalitarianism and to ensure that the States – parties to the ECHR are democratic and remain democratic.[79]

In cases involving personal data the ECtHR held that because protection of personal data is of fundamental importance to the enjoyment of the right to respect for private life by an individual, the domestic law must afford guarantees to prevent any misuse of personal data.[80] The need for such guarantees increases if personal data is processed by automatic means.[81] In respect of data retention by public authorities, the ECtHR has made reference[82] to the Convention 108 safeguards, which establishes main principles of personal data processing. Retention of personal data ought to be used for certain purposes, and ought to be

[74] *Ibid*., *P.T. v Moldova,* Paragraph 30.
[75] *Trajkovski v Macedonia,* Judgment of 13 June 2020, Paragraph 49.
[76] *Szabo and Vissy v Hungary,* Judgment of 6 June 2016, Paragraph 55.
[77] *M.N. and Others v San Marino,* Judgment of 7 October 2010, Paragraph 75.
[78] See Schabas W. *The European Convention on Human Rights Commentary* (OUP, 2015) 369, p.406.
[79] Susan Marks, 'The European Convention on Human Rights and Its Democratic Society' (1995) 1 British Yearbook of International Law 66, p.210.
[80] *S. and Marper v UK,* n 4 above, Paragraph 103; *Gardel v France,* Judgment of 17 March 2010, Paragraph 62; *P.N. v Germany*, see n 34 above. Paragraph 70.
[81] *Gardel v France*, see n 80 above, Paragraph 62
[82] *S. and Marper v UK,* n 4 above, Paragraph 103; *M.K. v France*, see n 67 above, Paragraph 35; *P.N. v Germany*, see n 34 above. Paragraph 71.

stored for no longer than is required by those purposes, and the national law ought to prevent any abuse or misuse of personal data, especially, if it is a sensitive data.[83]

The jurisprudence of the ECtHR establishes that the test of necessity in a democratic society requires an examination of whether the impugned interference corresponds to a pressing social need, whether it is proportionate to the legitimate aim pursued, and whether justifications of public authorities are relevant and sufficient.[84] An initial assessment of these factors ought to be made by national authorities, while the final evaluation rests with the ECtHR.[85] The ECHR rights and freedoms are reflected in an abstract and 'universal' terms, which may lead to different interpretations, and such could be plausible or implausible, legitimate or illegitimate.[86]

4.1.3.4. 'Margin of appreciation and 'European consensus'

A certain margin of appreciation may apply in cases involving Article 8 rights.[87] 'Margin of appreciation' means a measure of discretion given to the States – parties to the ECHR for implementing the standards of that human rights instrument, taking into account their national particular interests.[88] The ECtHR, as explained by Greer, employs the doctrine of margin of appreciation as a room for manoeuvre the Court is prepared to accord national authorities in fulfilling their obligations under the ECHR.[89] McGoldrick points out that the

---

[83] Provisions of the Convention 108 referred to read as follows:
'Article 5 Legitimacy of data processing and quality of data [...]
4. Personal data undergoing processing shall be: […]
b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes […];
c. adequate, relevant and not excessive in relation to the purposes, for which they are processed; […]
e. preserved in a form, which permits identification of data subjects for no longer than necessary for the purposes for which those data are processed.
Article 6 Special categories of data
1. The processing of:
- genetic data;
- personal data related to offenses, criminal proceedings and convictions, and related to security measures;
- biometric data uniquely identifying a person;
- personal data […] relating to racial or ethnic origin, political opinions, trade-union membership, religious or other belief, health or sexual life,
shall only be allowed where appropriate safeguards are enshrined in law […]'

[84] *M.K. v France*, see n 67 above, Paragraph 33; *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland*, see n 33 above, Paragraph 164; and *P.N. v Germany*, see n 34 above, Paragraph 69.

[85] *S. and Marper v UK,* n 4 above, Paragraph 101.

[86] See Steven Greer 'The Interpretation of the European Convention of Human Rights: Universal Principle or Margin of Appreciation' (2010) 3 UCL Human Rights Review 1.

[87] On 'margin of appreciation' see Yutaka Arai 'Margin of Appreciation Doctrine in the Jurisprudence of Article 8 of the European Convention on Human Rights' (1998) 1 Netherlands Quarterly of Human Rights 16, p.41; Steven Greer, see n 86 above; Koen Lemmens 'The Margin of Appreciation in the ECtHR's Case-Law' (2018) 20 European Journal of Law Reform 2-3, p.78; Eva Brems 'Positive Subsidiarity and its Implications for the Margin of Appreciation Doctrine' (2019) 3 Netherlands Quarterly of Human Rights 37, p.210.

[88] See Yutaka Arai, n 87 above.

[89] Greer, see n 86 above, p.2.

margin of appreciation 'has become the central conceptual doctrine in the international and the jurisprudential architecture of the European Convention on Human Rights'.[90] The European human rights protection system operates on a division of responsibilities, where States primarily bear the responsibility, and the ECtHR intervenes through contentious proceedings only after domestic remedies have been fully utilized. The ECtHR recognizes States' prerogatives in sensitive domains like morality or religion, where consensus among European States is lacking, and domestic authorities are deemed better equipped to comprehend the societal context and manage the conflictive situations.[91]

Gerard points out that the margin of appreciation can be rationalized by the fact that national authorities, in principle, are better placed to evaluate whether restrictions or limitations are used in an appropriate way by the governments.[92] She further explains that the ECtHR 'is generally willing to leave a certain amount of discretion to the States in determining the reasonableness of interference with [the ECHR] rights'.[93]

The scope of the margin of appreciation can be different depending on certain particularities of the case, such as the nature of the right protected by the ECHR, its importance for the particular individual, the nature of the interference, and the object pursued by such interference.[94] The margin of appreciation may be narrow, if the right at issue is crucial to the effective enjoyment of intimate or key rights of individuals,[95] or it could be restricted if a particularly important facet of the existence or identity of an individual is at stake. However, if the ECtHR finds that there is no consensus among all States – parties to the ECHR on the relative importance of the interest at issue or on the best way to protect it, the margin of appreciation may be wider.[96] Thus, the ECtHR, in determining the margin of appreciation, may examine the issue of whether there is a consensus among States, parties to the ECHR. In situations where States lack consensus, either regarding the significance of the interest involved or the most effective methods of safeguarding it – especially when the case involves delicate social, moral, or ethical dilemmas – the margin of appreciation may

[90] Dominic McGoldrick 'A Defence of the Margin of Appreciation and an Argument for its Application by the Human Rights Committee' (2016) 65 International and Comparative Law Quarterly 21, at p.22.
[91] See Marisa Vila 'Subsidiarity, Margin of Appreciation and International Adjudication within a Cooperative Conception of Human Rights' (2017) 15(2) International Journal of Constitutional Law 393, at p.406.
[92] See Janneke Gerards, 'Margin of Appreciation and Incrementalism in the Case Law of the European Court of Human Rights' (2018) 18 Human Rights Law Review 495, at p. 498. This explanation is also given in the Copenhagen Declaration of 13 April 2018, Paragraph 28(b).
[93] Janneke Gerards, see n 92 above.
[94] *P.N. v Germany*, see n 34 above, Paragraph 75.
[95] *Peruzzo and Martens v Germany, Decision of 4 June 2013*, Paragraph 41.
[96] *S. and Marper v UK,* n 4 above, Paragraph 102.

be broader.[97] McGoldrick explains that usually, a strong consensus among States narrows the margin of appreciation and *vice versa*.[98]

Dzehtsiarou points out that the ECtHR uses different terminology for explaining the consensus among the State, such as 'European consensus', 'common European standard' and 'general trend'.[99] A 'European consensus' has been employed by the ECtHR to indicate a 'trend'.[100] While generally a 'European consensus' is widely used in the literature and by the ECtHR, Dzehtsiarou suggests that there is no need for the ECtHR to wait for the literal 'consensus among the Member States, which would mean that an issue is regulated by all States in an identical or a significantly similar way. According to him, 'European consensus' can be understood as a collectively accepted solution among Member States, which essentially gives the ECtHR authorization to impose this solution on States that may have diverging views, once a majority agreement is reached. However, if such consensus is lacking, the Court should refrain from imposing its own perspective on particular human rights issues.[101] In essence, Dzehtsiarou suggests that the ECHR operates as a subsidiary system, deferring to decisions made independently by the majority of the Member States. He examines 'European consensus' at two levels: at the level of rules and at the level of principles in the following way:

> [t]he level of consensus should predetermine the weight of the consensus in the [ECtHR's] reasoning, if there is a consensus at the level of rules, the respondent State should provide very convincing justification for diverging from the consensus. […] At the level of principles, [the ECtHR] uses 'consensus' […] to clarify the meaning of vague terms enshrined in the [ECHR].[102]

Protocol No. 15 amending the ECHR affirms the doctrine of margin of appreciation. The ECHR's Preamble was amended in 2013 to indicate that the Member States in accordance with principle of subsidiarity have the primary responsibility to ensure the protection of the rights and freedoms enshrined in the ECHR. The Member States enjoy margin of appreciation, which is however subject to supervision by the ECtHR.[103] Thereafter, the Copenhagen Declaration with respect to the ECHR, which was adopted by

[97] See McGoldrick, n 90 above, p.28-29.
[98] See McGoldrick, n 90 above, p.28.
[99] Dzehtsiarou K. *European Consensus and the Legitimacy of the European Court of Human Rights* (CUP, 2015), 229, at p.11.
[100] See Dzehtsiarou K, n 99 above, p 12.
[101] See Dzehtsiarou K, n 99 above, p 166.
[102] See Dzehtsiarou K, n 99 above, p.16.
[103] Protocol No 15 Amending the Convention on the Protection of Human Rights and Fundamental Freedoms European dated 24 June 2013. Council of Europe Treaty Series – No 213.

the Committee of Ministers of the Council of Europe in 2018, indicates the principle of subsidiarity in the following way:

> State Parties enjoy a margin of appreciation in how they apply and implement the Convention, depending on the circumstances of the case and the rights and freedoms engaged. This reflects the Convention system is subsidiary to the safeguarding of human rights at national level and that national authorities are in principle better placed than an international court to evaluate local needs and conditions. […]
>
> [In respect of Article 8,] [w]here a balancing exercise has been undertaken at the national level in conformity with the criteria laid down in the [ECtHR's] jurisprudence, the [ECtHR] has generally indicated that it will not substitute its own assessment for that of the domestic courts, unless there are strong reasons for doing so.[104]

Vila explores two main ways of interpreting the principle of subsidiarity as contemplated in Protocol No.15: statist view and cooperative approach.[105] It may be suggested that Protocol 15 emerged as a result of criticism at ECtHR's approach to margin of appreciation, focusing on its exercise of jurisdiction and perceived lack of self-restraint.[106] Some of the criticism came from the government of the United Kingdom.[107] These criticisms often stem from a statist normative understanding of subsidiarity, advocating for deference to national authorities. Vila further argues for a cooperative conception of subsidiarity that balances state autonomy with international supervision, distributing tasks in human rights protection while respecting pluralism and unity of purpose.[108] This cooperative subsidiarity standard entails both negative and positive dimensions: the former emphasizes non-interference in domestic matters of protection where appropriate, while the latter reinforces the Court's responsibility for effective protection of Convention rights, particularly when States prove incapable or lack impartiality.[109]

[104] Copenhagen Declaration of 13 April 2018, Paragraph 28(b)(c).
[105] See Marisa Vila, n 91 above, p.400-403.
[106] See Marisa Vila, n 91 above, p.401; McGoldrick, n 90 above, p.36.
[107] On Protocol No.15 and the UK Government criticism of the use of 'Margin of appreciation' by the ECtHR, see Ian Cram 'Protocol 15 and Articles 10 and 11 ECHR – the Partial Triumph of Political Incumbency Past Brighton?' (2018) 67 (3) International and Comparative Law Quarterly 477-503.
[108] See Marisa Vila, n 91 above, p.401.
[109] Marisa Vila, *ibid.*

4.1.4. Structure of the concept of 'Private Life' under Article 8 ECHR

In respect of Article 8 rights, of special relevance to discourses on the notion of privacy is the emphasis on the conceptual linkage between this notion and the overarching concept of human dignity. The ECtHR held that the following intrusion in the private life was affront to the human dignity:

> an intrusion into the applicant's home in the form of unauthorized entry into her flat and installation of wires and hidden video cameras inside the flat; a serious, flagrant and extraordinarily intense invasion of her private life in the form of unauthorized filming of the most intimate aspects of her private life, which had taken place in the sanctity of her home, and subsequent public dissemination of those video images; and receipt of a letter threatening her with public humiliation.[110]

According to some authors, the German approach to privacy as a positive right, which focuses on human dignity, is feasible in terms of protecting individual privacy in the 21st century. Development of new investigative technologies would not require new laws to be adopted or privacy standards to be changed, because eventually the issue would remain whether dignity of an individual was violated.[111]

The right to personal development is not about negative freedom, and in addition to privacy rights, personality rights contain an element of control over public image and over personal information of a person.[112] It is argued that Article 8 ECHR was originally adopted as a classic negative privacy right, but has gradually been interpreted by the ECtHR as a personality right.[113]

4.1.4.1. 'Privacy' v 'private life'

There seems to be no difference between 'privacy' and 'private life' as used in UDHR[114] and ECHR respectively. As Schabas notes, the use of the term 'private life' by the drafters of the ECHR might be related to the important role of the French language in the *travaux préparatoires* of the ECHR, where 'vie privée' was translated as 'private life'.[115]

---

[110] *Ismayilova v Azerbaijan,* see n 16 above, Paragraph 116.
[111] Nicole Jacoby 'Redefining the Right to be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States' (2007) 35 Georgia Journal of International and Comparative Law 433.
[112] Bart Van der Sloot 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interest Might Prove Indispensable in the Age of "Big Data"' (2015) 31 Utrecht Journal of International and European Law 25.
[113] Van der Sloot, see n 112 above, p.27.
[114] Article 12 UDHR reads as follows: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'
[115] Schabas W., see n 78 above.

Some authors contend that those concepts represent an umbrella term for all rights and freedoms contained in Article 8 ECHR (or, respectively, Article 12 UDHR),[116] because those terms – 'privacy' in UDHR and 'private life' in ECHR, appear first in the list of rights protected by the respective article in those human rights instruments.[117] Such finding seems, however, unconvincing, as, e.g., the jurisprudence of the ECtHR indicates that each of the four categories enumerated in Article 8 of the ECHR may be invoked separately without necessarily invoking the term 'private life'.[118] The use of those words as umbrella terms in our view can only be meaningful for the purposes of informally referring to the rights and freedoms, which can be protected under Article 8 ECHR. The reason can be trivial: it is more practical to use a shortened version of long names and phrases in the texts of official legal instruments, judicial acts or academic writing. The title of Article 8, e.g., contains only two out of four categories of rights enshrined in Article 8 – 'private and family life'.

Sometimes 'privacy' is understood as a sub-section of the 'right to private life'.[119] The ECtHR in its Guide on Article 8[120] has classified the term 'private life' as covering three categories of rights:

1) physical, psychological, and moral integrity,
2) identity and autonomy, and
3) privacy.

The third category includes the right to an image or photographs of the person, protection of reputation, data protection, right to access to personal information, protection of information concerning health of the person, protection against filing or collection of data by public authorities, including police surveillance, and during custody. Some authors, following the ECtHR Guide's classification, concede that the right to private life in fact means the right to privacy, by using the latter term to indicate what Article 8 ECHR is essentially protecting.[121] The ECtHR may have for its own ease classified different aspects of the same rights or freedoms as separate categories or sub-sections of the term 'private life' in its Guide, and has named randomly one of such categories – 'privacy', but in doing so, the ECtHR makes no justice to our understanding of the term 'private life' as opposed to 'privacy' and vice versa.

---

[116] See Oliver Diggelmann and Maria Nicole Cleis, n 53 above.
[117] *Ibid*., at 447.
[118] *Wieser and Bicos Beteiligungen GmbH*, see n 23 above; *Zakharov v Russia*, see n 27 above; *Barbulescu v Romania*, see n 28 above;
[119] Guide on Article 8 of the European Convention on Human Rights, published by the European Court of Human Rights, last updated on 31 August 2020.
[120] Guide on Article 8 *Ibid*.
[121] See Özgür Heval Çınar 'The Current case-law of the European Court of Human Rights on privacy: challenges in the digital age' (2021) The International Journal of Human Rights 25:1, at 28.

4.1.4.2. Multifaceted 'private life'

It follows that the ECtHR has chosen not to give a specific definition to the term 'private life', but rather has opted for the inclusion of different aspects of life, different situations, statuses, origins, identities, desires, decision-making processes, and many others in the notion of 'private life'.

Such a wide range of rights covered by the term 'private life' precludes the ECtHR from providing a unified definition of this term. Within the contingent classification of three categories of the right to private life given by the ECtHR:[122] 'integrity', 'identity', and 'privacy', the data protection sub-section comprises a small part within the 'privacy' category. Taking into account the definition of 'personal data' used by the ECtHR in its jurisprudence, i.e., any information relating to identified or identifiable persons,[123] it will be unwise to limit data protection cases to a small sub-category of cases. For instance, in *Anchev v Bulgaria,* the applicant claimed that the publication by the public authorities of information about his alleged collaboration with the State security bodies in the past, had seriously affected his emotional and psychological integrity, reputation and ability to develop relations with others.[124] The ECtHR in that case, although making no clear references to any international legal instruments on data protection, has examined the case through the lens of data protection. It reiterated its previous case law,[125] maintaining that the release and publication of information systematically collected and stored by authorities, regardless of whether it concerned private or public activities of the individual, ought to constitute an interference with the right to private life.[126]

4.1.4.3. Data protection aspect within the right to 'private life'

The right to data protection relates to a far wider range of situations than a small sub-section within one of three main categories of rights covered by the term 'right to private life' as portrayed by the classification of the ECtHR. Within the 'privacy' framework suggested by the ECtHR,[127] it can be observed that data protection emerges in cases

[122] See Guide on Article 8, n 119 above.
[123] See e.g., *Amann v Switzerland*, see n 32 above, Paragraph 65.
[124] *Anchev v Bulgaria,* Decision of 5 December 2017, paragraph 87.
[125] Such as *Leander v Sweden,* n 3 above.
[126] *Anchev*, n 124 above*,* Paragraph 92.
[127] See Guide on Article 8, see n 119 above.

involving the right to image or photograph of the person,[128] the right to access personal information,[129] the information about the health of the person,[130] police surveillance,[131] and others. Moreover, references to the right to data protection can be found within the category of cases classified by the ECtHR as 'identity and autonomy' – for instance, the right to ethnic identity,[132] and as 'physical, psychological and moral integrity' – e.g., issues concerning burial and deceased people.[133]

Why is then the data protection aspect of the right to private life not considered by the ECtHR as covered by the 'identity' or 'integrity' categories? This Chapter will examine the logic behind the classification of the ECtHR in two case examples.

In the first case of *B v France*, the applicant, a female, who used to be a male, complained that the authorities refused to change some of her documents, which indicated her sex as a male and her previous, male, forename.[134] She thus complained that the respondent State forced her to disclose intimate personal information to third parties.[135] It is therefore the ECtHR that has included this case into the category of 'physical, psychological and moral integrity'. But, are there other facets of the right to private life in this case? Ms. B was forced to disclose her intimate personal information to third parties every time, such as banks accepting cheques with her name, or employers having her social number and the male name on the pay slips etc.[136]

This case was examined in 1992, so the ECtHR could theoretically refer only to the Convention 1981,[137] but not to DPD or GDPR, which were adopted in 1995 and 2016 respectively. The ECtHR however made no reference to domestic data protection laws or the Convention 108 in its examination of this case, but the data protection aspect was quite evident in that the State authorities failed to secure the laws, which would protect the applicant from unnecessary disclosure of her personal information to third parties. On the other hand, gender identity is classified by the ECtHR within the category of 'identity and autonomy'.[138] Ms B was concerned that she must be identified as a female in her identity documents, and she expressly claimed that the refusal to recognize her true sexual identity

[128] *López Ribalda and Others v. Spain,* Judgment of 17 October 2019.
[129] *Segerstedt-Wiberg and Other v Sweden,* Judgment of 6 September 2006.
[130] *Z v Finland*, see n 6 above.
[131] *Uzun v Germany*, see n 25 above.
[132] *S and Marper vs UK*, see n 4 above.
[133] *Lozovyye v Russia*, Judgment of 24 July 2018.
[134] *B v France* (1992) Series A no 232C, Paragraph 43.
[135] *Ibid.*
[136] *Ibid.,* Paragraphs 56-59.
[137] Council of Europe Convention 108, see n 36 above.
[138] See Guide on Article 8, n 119 above.

was a breach of Article 8.[139] This example of the case *B v France* suggests that all three categories of the rights under the term 'private life', which were classified by the ECtHR in its Guide, may cover one and the same case.

The second case of *S and Marper v UK*[140] was referred to by the ECtHR in its Guide in two different categories: 'privacy' – data protection, and 'identity and autonomy' – right to ethnic identity.[141] Two applicants claimed that their personal information, contained in their fingerprints, DNA profiles, and cellular samples, were unlawfully retained by public authorities after criminal proceedings against them had ended. Such personal information had to be considered sensitive information, as it concerned the ethnic identity of applicants.

This case is different from the first example – *B v France* in that the ECtHR classified it under two different categories, while there is only one category – 'privacy' (data protection), which is in fact at stake here. Applicants in *S and Marper* did not claim that their identity or autonomy ought to be respected. They claimed that the authorities ought not to retain sensitive information about applicants, which includes their identity information. The right to identity, as understood and classified by the ECtHR, is a positive right.[142] In *S and Marper* the ECtHR found that apart from such elements as gender identification, name and sexual orientation, or ethnic identity must be regarded as another such element, which falls within the personal sphere protected by Article 8.[143] The ECtHR has made relevant references to the previous case law,[144] and such case law has shown that Article 8 protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world.[145] In *S and Marper* however, the applicants were not seeking to establish or develop their relationship with a wider world by having their ethnic identity to be recognized by the authorities. On the contrary, the applicants wanted the authorities to erase their personal data from the public registers, as such personal data was not allegedly retained for valid and lawful reasons after the criminal proceedings against the applicants were discontinued.

From those two cases, it can be inferred that the right to private life under Article 8 ECHR may cover different or even the same situations from different angles, where the personal information of individuals is concerned. Personal information relating to the

[139] *B v France,* n 134 above. Paragraph 43.
[140] *S and Marper vs UK,* n 4 above.
[141] See Guide on Article 8, n 119 above, Paragraphs 175, 180, 185 and 264.
[142] There will be separate discussion on negative and positive rights and obligations in further sections.
[143] *S and Marper vs UK,* n 4 above, Paragraph 66.
[144] The ECtHR referred to *Peck vs UK,* see 5 above, Paragraph 57; *Burghartz v Switzerland* (1994) Series A no 280-B, Paragraph 24.
[145] *S and Marper vs UK,* n 4 above.

previous identity of an individual, if revealed to third parties, may inflict moral harm and thus affect the moral integrity of such an individual. At the same time, such individuals may claim recognition of their current identity in order to establish and develop their relationships with other people. However, individuals may claim that their personal data concerning their identity must not be in the possession of public authorities.

All three classified categories of the ECtHR may concern personal data issues, but only two of them: 'integrity' and 'privacy' have data protection elements in them. An 'identity' category as classified in the Guide and explained in its case law by the ECtHR, is about individuals enjoying their right to private life through demonstrating, revealing, declaring, or other ways of officiating their identities, be it gender identity, sexual orientation, ethnic identity or names. Data protection concerns, on the other hand, emerge when the consent of the individual to the use of their personal data is absent or not valid anymore. In cases where individuals expressly give their consent to the use of their personal data pertaining to their identity for the purposes of having their identity recognized by the public authorities, data protection concerns become redundant.

4.1.4.4. Informational self-determination

In *Satakunnan v Finland* the ECtHR held that Article 8 ECHR provides for the right to a form of informational self-determination:

> Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged.[146]

This author considers this as a reflection of the *Population Census* judgment of 1983 of the German Federal Constitutional Court (BVerfG), where it had proclaimed the right of an individual to informational self-determination.[147] The BVerfG held that the right to informational self-determination presupposes that the individual is given the freedom to decide about actions to be taken or not to take, and must be able to know who knows what, when and on what occasion about them.[148] Eberle cites the *Pupolation Census* judgment to explain the meaning of informational self-determination the ability of individuals to

[146] *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland*, see n 33 above, Paragraph 137.
[147] Cf. BVerfG, 65,1 of 15 December 1983.
[148] *Ibid.* BVerfG, 146.

determine primarily for themselves when and to what extent personal data can be disclosed.[149]

The BVerfG emphasised that due to the automatic means of processing personal data, the stored individual statements about personal situations can be pieced together with other data collections to create a complete personality profile, and in such a situation an individual will have no sufficient means of controlling such data processing.[150]

The ECtHR further in *Breyer v Germany* reiterated that Article 8 of the ECHR protects the individual's right to informational self-determination,[151] and throughout the judgment makes references to the BVerfG case law including the *Population Census* judgment.[152] According to some authors, the BVerfG acknowledged that privacy or data protection have 'intermediate' rather than 'final' value – they ought to be considered as tools for achieving more fundamental values: human dignity and the right to personality.[153] This also echoes Westin's understanding of the concept of privacy as the right of the individual to decide what information about themself ought to be communicated to others and under what circumstances.[154]

4.1.5. Negative and Positive Obligations with respect to Data Protection

The right of an individual to respect for private and family life presupposes the corresponding obligation of State authorities to respect that right of an individual. The ECtHR has explicitly mentioned that the essential object of Article 8 is to protect individuals against arbitrary actions of public authorities.[155] Article 1 ECHR contains a general provision establishing that all States, parties to the ECHR, have an obligation to respect all human rights enshrined in that human rights instrument. Among the whole set of human rights and freedoms contained in the ECHR, the right to private and family life is the only one, which is formulated using the term 'respect'. It was initially thought to be a so-called 'negative' obligation of the State, i.e., where the State ought to refrain from conducting actions, which

[149] See Edward Eberly 'Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview' (2012) 33Liverpool Law Review 201, at pp. 224-225.
[150] BVerfG, 145, see n 147 above.
[151] *Breyer v Germany,* see n 48 above, Paragraph 75.
[152] *Breyer v Germany,* see n 48 above, Paragraphs 12-16, 25 and 81.
[153] See Antoinette Rouvroy and Yves Poullet 'The Right to Informational Self-Determination and the Value of Self-Development. Reassessing the Importance of Privacy for Democracy' in *Reinventing Data Protection?* in Serge Gutwirth et al (eds.) (Springer Science + Business Media B.V., 2009) 45-75.
[154] Cf. Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967). More on this is provided in Chapter 3 'The Concept of Privacy'.
[155] *Kroon and Others v The Netherlands* (1994) Series A-297-C, Paragraph 31.

could result in violation of the right of an individual.[156] This was an embodiment of the 'right to be let alone' as suggested by Warren and Brandeis in the late 19th century.[157]

In relation to Article 8, however, the ECtHR has held that the notion of 'respect' is not clear-cut, especially where the positive obligations of the State implicit in this concept were concerned.[158] The ECtHR has interpreted the term 'respect' as not strictly meaning the obligations of States to abstain from interference with the private and family life of an individual, i.e., a negative obligation, but also as an obligation of the States to take necessary measures or steps to ensure the full enjoyment by individuals of their rights and freedoms when mainly third parties interfere with the private life of the individual.

As explained by Leloup, the ECtHR has played a major role in the evolution from negative to positive human rights by employing the principle of effective protection of rights by the ECtHR.[159] In *Marckx v Belgium* the ECtHR held that the Article 8(1) provision in addition to the negative undertaking of the State not to arbitrarily interfere with a 'family life', also could contain a positive obligation to ensure the right to family, inherent in the notion of 'respect' for family life.[160] Since then, the ECtHR has developed an extensive body of case law, where interference by private parties with the private or family life of individuals would trigger positive obligations of States to ensure the respect for private and family life, and failure to conduct certain positive actions by the State could amount to the breach of the Article 8(1) provisions.[161]

States or State agents are seen as ultimate duty-bearers, who violate human rights, and who therefore eventually must bear responsibility. States must ensure that the relations between private parties are regulated not only by private law instruments but also by public-law mechanisms. Such mechanisms include not only the laws providing for the due procedure and punishment for the wrongdoing but also the law-enforcement structures, including the judiciary, whereby individuals – victims of human rights violations can seek redress. Under international human rights law, thus, individuals can expect positive State

---

[156] See Schabas W., n 78 above.
[157] Samuel Warren and Louis Brandeis in "The Right to Privacy" in "Harvard Law Review", vol.4, 15 December 1890.
[158] See *Abdulaziz, Cabales, and Balkandali v. the United Kingdom*, (1985) Series A no. 94, Paragraph 67; *Rees v. the United Kingdom* (1986) Series A no. 106, Paragraph 37; *B. v. France*, see n 45 above, Paragraph 44; *Tysiąc v. Poland,* Judgment of 24 September 2007, Paragraph 112; *Mosley v. the United Kingdom,* Judgment of 15 September 2011, Paragraph 108.
[159] Matheu Leloup 'The Concept of Structural Human Rights in the European Convention on Human Rights' (2020) 20 Human Rights Law Review 480.
[160] *Marckx v Belgium,* n 8 above.
[161] *Barbulescu v Romania*, see n 28 above, Paragraph 111; *Craxy v Italy,* Judgment of 17 October 2003, Paragraphs 68-76; *Benediktsdottir v Iceland,* Decision on admissibility of 16 June 2009.

actions, which would ensure that their human rights are afforded meaningful protection even against the violations arising out of their relations with private parties.

Alexy, a German constitutional law theorist, in his strive to formulate the main distinctive feature of negative and positive obligations (for the purposes of revealing its importance in addressing proportionality principle) examines one of the elements of a positive action of the State: protective rights.[162] Protective rights are those which force the State to protect individuals from interferences by third parties. Protective rights thus correspond to the positive obligations of States to protect human rights. On the other hand, defensive rights correspond to the negative obligations of States to respect human rights. The main difference between protective and defensive rights, according to Alexy, is that protective rights have an alternative or disjunctive structure, while defensive rights have a conjunctive structure.[163] To illustrate an example of Alexy's vision of how negative and positive obligations may differ from each other, this thesis will examine the right to personal data protection and the positive obligations of the State under the right to private life as stipulated in Article 8 ECHR.

For complying with its negative obligation not to collect and store personal data, the State must only refrain from collecting and storing personal data. There are no other alternatives for the State behaviour to comply with its negative obligation. However, when it comes to positive obligations to protect the right to private life, the State has different alternative means to do so. If personal data is collected and stored by another individual or a company, e.g., internet services provider, the State is free to choose from different measures available at its disposal in order to prevent unlawful personal data processing, or to make such a private perpetrator responsible. The State can have in place internal laws prescribing any third party, which conducts processing of personal data, to introduce internal (corporate) policies and implement measures in accordance with the principles of data protection by design and by default.[164] Alternatively, the State can prescribe that internet services providers may lawfully collect and retain certain categories of personal information upon the consent of an individual for certain purposes and for certain periods of time. The State can foresee different types and degrees of punishments for breaching the data protection laws: it could be a monetary punishment in the form of a fine in a fixed amount or in a

[162] Robert Alexy 'On Constitutional Rights to Protection' (2009) 3 Legisprudence 1.
[163] Alexy, *Ibid*., at 5.
[164] Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the individuals to monitor the data processing, enabling the internet services providers to create and improve security features. See GDPR, n 38 above, Recital 78.

percentage to the annual turnover, or it could be a penalty prohibiting data processing for certain period of time. The State here is not prescribed to take all existing measures together, but it can choose and take only one of them. So, the State has a discretion in how to comply with its positive obligations to protect the right to privacy. According to Klatt, all important differences between negative and positive obligations follow from that fundamental difference.[165]

The content of positive obligations is usually understood to consist of substantive and procedural parts.[166] Substantive content implies putting in place legislation which would regulate the behaviour to the extent preventing it from conducting possible abuse or misuse. The procedural aspect presupposes the ability of redressing violations when prevention is not possible. The State ought to ensure that all means for redressing violations are at the disposal of the victim, and such means are real and effective. In *Ismayilova v Azerbaijan* the ECtHR held that positive obligations under Article 8 to safeguard physical and moral integrity of the individual could extend to the effectiveness of the criminal investigation, which give rise to procedural obligations.[167]

Even when private parties do not interfere with private life, positive obligations of the State may still emerge. In *Lozovyye v Russia,* State authorities failed to at least undertake reasonable steps to inform the parents of a deceased person about his death. He was a victim of a murder, and public authorities conducted investigation of the crime, but failed to identify any close relatives of the victim. This has been construed by the ECtHR as a failure by the State to comply with its positive obligations under Article 8 of the ECHR.[168]

The ECtHR held several times that the boundaries between negative and positive obligations are blurred, but the applicable principles are nonetheless similar. In both cases a fair balance ought to be struck between the competing interests of the individual and of the community as a whole, subject to margin of appreciation by the States.[169]

Van der Sloot argues that certain so-called 'personality rights', such as protection of reputation and honour, the right to data protection, and the right to intellectual property, often

---

[165] Matthias Klatt 'Positive Obligations under European Convention on Human Rights' (2011) 71 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV) 691, at p.695.
[166] See, e.g., Dimitris Xenos *The Positive Obligations of the State under the European Convention of Human Rights* (Oxon: Routledge 2012) 231, at 207.
[167] *Ismayilova v Azerbaijan,* see n 16 above, Paragraphs 115 and 119.
[168] *Lozovyye v Russia*, see n 133 above, Paragraphs 37-47.
[169] *Dickson v UK*, Judgment of 4 December 2007, Paragraph 70; *Odievre v France*, Judgment of 13 February 2003, Paragraph 40; *Barbulescu v Romania*, see n 28 above, Paragraph 112; *Ismayilova v Azerbaijan,* see n 16 above, Paragraph 112.

entail positive obligations from the part of the State.[170] In the *von Hannover v Germany II* case, the ECtHR held that an image of the person constituted one of the main features of their personality, revealing their unique characteristics, which distinguish them from their peers.[171] It further found that the right to the protection of an image, having been an essential element of personal development, entailed the right to control the use of that image by the individual.[172]

4.2. An Analysis of the Relevant Case law on Surveillance, Data Protection and Privacy Rights under Article 8 ECHR

The ECtHR has developed an extensive case law on surveillance and personal data protection. The main issues with personal data arise when such personal data are collected and stored for certain purposes by public authorities or upon their instructions by private parties. This Chapter divides the case law on secret surveillance into two main groups: 1) cases involving interception or collection of personal data, and 2) cases involving retention of personal data. Both 'interception' and 'retention' of personal data and either of these terms can be reflected by an umbrella term 'surveillance' of personal data elsewhere in the text of this Chapter, where the context allows the identification of the form of surveillance without directly referring to it.

4.2.1. Surveillance in the Form of Interception of Personal Data

At first sight, it may seem that personal data cannot become subject to surveillance. Public authorities conducting secret surveillance measures are not supposed to find out personal information about individuals, because they have already identified those individuals, whom they have subjected to surveillance measures. They are rather interested in the content of the correspondence of such individuals in order to have information about what those individuals are planning to commit. However, secret surveillance measures are taken by the public authorities in order to identify certain suspects, who have already committed or are planning to commit crimes.

The main difference between police and intelligence organs lies in their, goals and subsequently methods of operation. The police mainly interfere with the private life of the individual in order to investigate an already committed crime, while intelligence services conduct their operations mostly to prevent criminal or terrorist acts. Thus, intelligence

[170] Bart Van der Sloot see n 112 above, at p.26.
[171] *Von Hannover v Germany (No.2),* Judgment of 7 February 2012, Paragraph 96.
[172] *Von Hannover v Germany (No.2), ibid.*

services are expected to play more of a proactive role in identifying threats and persons representing such threats.

As long as 'personal data' means any information that is susceptible to identifying natural persons, public authorities through utilizing secret surveillance measures, may obtain information – so-called 'identifiers', which together with other data, assist in the identification of concrete individuals. Moreover, even the 'content' data may include personal data, such as the voice of an individual,[173] names of people, and other.

4.2.1.1. 'Victim of Secret Surveillance'

The ECtHR in cases involving surveillance conducted by public authorities, first of all, considers whether there was an 'interference' on the part of public authorities with the private life or correspondence of individuals under Article 8 of the ECHR.[174] Any individual, who claims to be a victim under the ECHR, must show that the actions of public authorities have been directed against them or have resulted in inflicting harm to them. As a general rule, an individual cannot claim to be a victim of a violation of their right *in abstracto*, i.e., by the mere fact of the existence of legislation or of certain measures pursued by public authorities simply because they feel it contravenes the ECHR. A person must prove that they were directly affected by the measure complained of.[175]

However, this criterion must not be applied in a rigid and mechanical way.[176] The ECtHR, in *Klass v Germany* in 1978, held that in cases involving secret surveillance measures, under certain conditions, an individual may claim to be the victim of violation caused by the mere existence of secret measures or legislation permitting secret measures without claiming that such measures had been directly applied to them.[177] The ECtHR explained that when public authorities conduct secret surveillance in respect of persons, who remain unaware of such secret measures, the effects of Article 8 could be reduced to a nullity. In such a situation, a person controlled may be treated in a manner contrary to Article 8 or even deprived of the rights and freedoms guaranteed by that article, without actually being able to contest such measures at the court and obtain meaningful remedy at the national level or before the ECtHR.[178]

---

[173] See *P.G. and J.H. v UK*, n 21 above.
[174] *Klass and Others v Germany,* n 19 above, Paragraph 41.
[175] *Klass and Others v Germany,* n 19 above, Paragraph 33; *N.C. v Italy,* Judgment of 18 December 2002, Paragraph 56.
[176] *Zakharov v Russia*, see n 27 above, Paragraph 164.
[177] *Klass and Others v Germany,* n 19 above, Paragraph 34.
[178] *Klass and Others v Germany,* n 19 above, Paragraph 36.

Since the *Klass v Germany* case, the ECtHR has developed different approaches to the victim status of applicants in surveillance cases. In one group of cases, the ECtHR has examined whether the existence of practices of secret surveillance measures could affect the applicants. In such cases, it was held to be sufficient to establish the existence of such practices and a reasonable likelihood that the security services had compiled and retained information concerning the private life of individuals.[179] In the other group of cases, the mere existence of domestic laws and practices, permitting and establishing a system for effecting secret surveillance, was alleged to have breached the Article 8 rights. Such a system posed a threat of secret surveillance for all those to whom the legislation might be applied. Such a threat in any way affects freedom of communication between individuals, and therefore it can be regarded as an interference with the rights protected by Article 8.[180]

In the relatively recent cases of *Kennedy v UK* and *Zakharov v Russia*, the ECtHR adhered to a third approach of defining whether interference was made in the secret surveillance cases. The main reason for departing from the general approach to deny individuals the right to challenge a law *in abstracto* was to ensure that the secrecy of measures did not result in deprivation of the possibility for individuals to effectively challenge the secret measures with the domestic judicial bodies and the ECtHR. It is always important in such cases involving secret surveillance to examine the availability of domestic remedies and the risk of secret surveillance measures being applied to an applicant.[181]

In *Zakharov v Russia,* the ECtHR made an attempt to harmonise all above-mentioned approaches in order to have a more uniform and foreseeable approach in its case law for determining whether an individual can claim to be a victim of interference by public authorities with his right to private life in the secret surveillance cases. The harmonized approach includes the following:

1) the scope of the legislation permitting secret surveillance ought to be analysed with a view to establishing whether the law targets the group of people, to which an applicant belongs, or whether the law directly affects all users of communication services, where such a system can intercept communications of any person; and

[179] *Halford v UK,* see n 64 above, Paragraph 47; *Iliya Stefanov v Bulgaria,* Judgment of 22 August 2008, Paragraph 49.
[180] *Malone v UK*, see n 20 above, Paragraph 64; *Weber and Saravia v Germany,* Decision on admissibility of 29 June 2006, Paragraph 78; *The Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria,* Judgment of 30 January 2008, Paragraphs 58-59.
[181] *Kennedy v UK,* Judgment of 18 August 2010, Paragraph 124; *Zakharov v Russia*, see n 27 above, Paragraph 169.

2) the availability of domestic remedies ought to be assessed, and, depending on effectiveness of such remedies, different degrees of scrutiny shall be applied by the ECtHR.

The second component of that harmonised approach mentioned above effectively means that if domestic legislation provides no meaningful remedies, there could be a wide suspicion and concern among the general public that the public authorities would be able to abuse their powers to conduct secret surveillance. In such a situation, a threat of surveillance can restrict free communication through the postal and telecommunication services and therefore constitute for all users, current and potential, a direct interference with their rights protected by Article 8.[182] Such a case therefore bears greater need for scrutiny by the ECtHR, and an individual is not required to demonstrate that there is a risk of the secret surveillance measures being applied to them. On the contrary, if national laws do provide for meaningful remedies, a widespread suspicion of abuse is difficult to sustain. In such cases, an individual will be required to demonstrate that due to their personal situation, they are at risk of being covered by secret measures.[183]

Thus, in *Szabo v Hungary*, the ECtHR employing the 'Zakharov test', has found that the domestic legislation directly affected all users of the communication system, and therefore the applicant could claim to be a victim of violation of their rights under the ECHR.[184] On the other hand, in *Big Brother Watch v UK*, the ECtHR, using the same 'Zakharov' test, held that the applicants could claim to be victims because they were potentially at risk of having their communications obtained by the intelligence services.[185]

4.2.1.2. Quality of Domestic Law in Cases Involving Secret Interception of Personal Data

The phrase 'in accordance with the law' in Article 8(2) means not only a simple existence in the domestic law of certain limitations to the enjoyment of rights, but it also presupposes that such laws are 'accessible' and 'foreseeable'.[186] The requirement of 'foreseeability' does not mean that an individual ought to be able to foresee when public authorities are likely to intercept their communications, so they can adapt their conduct accordingly.

---

[182] *Zakharov v Russia*, see n 27 above, Paragraph 170.
[183] *Zakharov*, see n 27 above, Paragraph 171.
[184] *Szabo and Vissy v Hungary*, see n 76 above, Paragraphs 38-39.
[185] *Big Brother Watch and Others v* UK, Judgment of 25 May 2021, Paragraphs 464, 467 (*'Big Brother Watch (2021)'*).
[186] *Malone v UK* see n 20 above, Paragraphs 67 and 70; *Amann v Switzerland*, see n 32 above, Paragraph 55.

There must be sufficiently clear provisions in the law, which would give people adequate indication as to the circumstances and conditions, when public authorities would be authorized to take secret surveillance measures.[187] The technology, used by public authorities, especially by executive bodies, for secret interception, constantly develops and continually becomes more sophisticated. It is therefore essential to have clear and detailed rules on secret interception measures.[188]

In *Zakharov v Russia* the ECtHR held that in cases related to secret surveillance, the lawfulness of the interference is closely related to the question of compliance with the 'necessity' test.[189] It therefore found it appropriate to examine 'in accordance with the law' component jointly with the 'necessary in democratic society' part of the test. The ECtHR thus came to the conclusion that in cases involving secret surveillance measures, apart from having accessibility and foreseeability features, the domestic law must ensure that the secret surveillance measures are applied only when adequate and effective safeguards and guarantees against abuse are in place.[190]

4.2.1.3. 'Weber requirements'

The ECtHR in its jurisprudence on secret interception cases developed the 'Weber requirements', which represent six main safeguards to be stipulated in the domestic law in order to forestall the State authorities exercising secret interception measures in an abusive manner.[191] It is called in this thesis after the *Weber and Saravia v Germany*[192] case, where the ECtHR generalized the previous case law[193] indicating the following main safeguards related to the quality of domestic law. The national law ought at least to stipulate:

1) the nature of offenses, which may give rise to an interception order;
2) a definition of the categories of people liable to have their communications intercepted;
3) a limit on the duration of interception;

---

[187] *Malone v UK* see n 20 above, Paragraph 67.
[188] *Big Brother Watch (2021)*, n 185 above, Paragraph 333.
[189] *Zakharov*, see n 27 above, Paragraph 236.
[190] *Zakharov*, see n 27 above, Paragraph 236.
[191] The ECtHR in *Big Brother Watch and Others v UK,* see n 50 above, in Paragraphs 280, 286, 289, and 292, referred to 'Weber requirements', indicated in the parties' submissions, as those safeguards or requirements on avoiding abuses of power were all analysed and outlined in its Judgement in the case of *Weber and Saravia v Germany*, see n 180 above, Paragraph 95. The Grand Chamber in 2021 has referred to those requirements as 'Weber criteria'. See *Big Brother Watch (2021)*, n 185 above, Paragraph 362.
[192] *Weber and Saravia v Germany*, see n 180 above, Paragraph 95.
[193] Such case law includes: *Huvig v France* (1990) Series A no.176-A, Paragraph 34; *Amann v Switzerland*, see n 32 above, Paragraph 76; *Valenzuela Contreras v Spain,* Judgment of 30 July 1998, Paragraph 46; and *Prado Bugallo v Spain,* Judgment of 18 February 2003, Paragraph 30.

4) the procedure to be followed for examining, using, and storing the data obtained;
5) the precautions to be taken while communicating the data to other parties; and
6) the circumstances in which intercepted data may or must be erased or destroyed.[194]

In 2019 in *Big Brother Watch v UK,* or 13 years after the *Weber* case, the ECtHR had an opportunity to add to the foregoing 'Weber requirements' some new safeguards, proposed by the applicants, such as 1) the requirement for objective evidence of reasonable suspicion in respect of persons for whom data was being sought; 2) prior independent judicial authorization of interception warrants; and 3) the subsequent notification of the surveillance subject.[195] The applicants, in that case, suggested that the technological development since the *Weber* case allowed public authorities to create detailed and intrusive profiles of intimate aspects of private lives by analysing patterns of communications on a bulk basis. The ECtHR's Chamber, however, having recognized those suggestions as possibly being pertinent for some other cases, has nevertheless decided that in that particular case of bulk interception of personal data, it did not consider it appropriate to add them to the list of 'Weber requirements'.[196]

This case was subsequently brought before the Grand Chamber of the ECtHR, and in 2021 the Grand Chamber reviewed the applicability of those minimum requirements to the bulk surveillance again.[197] The Grand Chamber stated that the first two of the six minimum safeguards were not readily applicable to a bulk interception regime.[198] As for the three additional requirements proposed by the applicants, the Grand Chamber determined that the first requirement of 'reasonable suspicion' was less pertinent in the bulk interception context rather than in respect of the targeted interception regime. Indeed, the purpose of bulk interception is a preventive one, whereas targeted interception is done in the context of an investigation of a specific target or an identifiable criminal offence.[199] The Grand Chamber further has adopted the second proposed additional requirement – an independent judicial authorization in order to minimize the risk of the bulk interception being abused.[200] It held that each stage of the bulk interception process ought to be subject to supervision by an independent authority.[201] The Grand Chamber however has dismissed the inclusion of the third proposed additional requirement – subsequent notification of the surveillance subject.

[194] The wording of these six safeguards is used from *Big Brother Watch (2021)*, n 185 above, Paragraph 335.
[195] *Big Brother Watch and Others v UK,* see n 50 above, Paragraphs 280, 294 and 316.
[196] *Big Brother Watch (2019),* see n 50 above, Paragraphs 316-320.
[197] *Big Brother Watch (2021)*, n 185 above, Paragraph 347.
[198] *Ibid.,* Paragraph 348.
[199] *Ibid.*
[200] *Ibid.,* Paragraphs 350-351.
[201] *Ibid.,* Paragraph 356.

It ruled that in those jurisdictions, which provide for an effective domestic remedy, subsequent notifications are redundant.[202] It further held that since bulk interception regime was usually used in respect of foreign intelligence gathering, and would thus target the communications of persons located outside of the territory of the State, the notification requirement would have had little, if no, practical effect.[203]

4.2.1.4. Bulk Data Surveillance

There is no legal definition of 'bulk' data surveillance or bulk data interception in the ECHR, CFREU[204] or any other binding international or regional human rights instrument. If 'bulk surveillance' is comparable to a 'mass surveillance', then it can be regarded as an opposite to a 'targeted surveillance' as explained by the 'Venice Commission' in its 2015 Report.[205] The ECtHR opposes these two types of surveillance against each other.[206] 'Mass' is different from 'bulk' in that it refers to a number of people targeted by the measures of surveillance. For instance, an entire population of a country or a substantial part thereof may comprise a 'mass'. 'Bulk' on the other hand is related to the data obtained or collected or intercepted through conducting surveillance measures, and such data represents large amount of information about large number of people, which is collected in an indiscriminate way. 'Bulk' surveillance can at some point become a 'mass' surveillance.

The ECtHR has considered a few cases related to the bulk interception of communications.[207] In the earliest of those cases – *Weber*, the ECtHR afforded wide margin of appreciation to the national authorities in evaluating how best to achieve the legitimate aim of protecting national security[208]. The ECtHR in that case expressly recognized that the national authorities enjoy a wide margin of appreciation necessary for the protection of national security.[209] At the same time, in *Rattvisa*, the ECtHR contended that the national authorities ought to be afforded narrower discretion in operating an interception regime, and employed the 'Weber requirements', which would minimize the abuse of power.[210]

---

[202] *Ibid.,* Paragraph 357.
[203] *Ibid.,* Paragraph 358.
[204] the Charter of Fundamental Rights of the EU adopted by the European Parliament, European Council and the Council on 7 December 2000 and entered into force together with the Treaty of Lisbon on 1 December 2009.
[205] Council of Europe's European Commission for Democracy through Law 'Report on the Democratic Oversight of Signals Intelligence Agencies', CDL-AD(2015)011, Paragraph 56.
[206] *Centrum for Rattvisa v Sweden,* Judgment of 25 May 2021, Paragraphs 257-261; *Big Brother Watch (2019),* see n 50 above, Paragraph 317.
[207] *Weber*, see n 180 above; *Liberty and Others v UK,* Judgment of 1 October 2008; *Big Brother Watch and Others v UK (2021)*, n 185 above; and *Rattvisa*, n 206 above.
[208] *Weber*, see n 180 above , Paragraph 137; *Liberty and Others v UK*, see n 207 above.
[209] *Weber*, see n 180 above, Paragraph 106.
[210] *Rattvisa*, n 206 above, Paragraph 256.

In *Big Brother Watch v UK (2019),* the ECtHR considered that the bulk interception could not be automatically assumed to constitute a greater intrusion into the private life of an individual than the targeted interception, which by its very nature can result in the acquisition and examination of a large number of their communications.[211] The Venice Commission in its 2015 Report noted that bulk interception could be crucial for security operations, which would enable security services to take a proactive approach to looking for unknown dangers rather than investigating known ones.[212]

The ECtHR echoed the argumentation of the Venice Commission by stating that in view of advancements in technology, which made it easier for terrorists and criminals to avoid identification on the Internet, the public authorities decisions to conduct bulk surveillance in order to identify unknown threats to national security, squarely fitted the rationale behind the application of the national margin of appreciation.[213] Nevertheless, all interception regimes – both bulk and targeted, can be potentially abused by the public authorities, especially when the national legislation cannot reflect a true discretion granted to the authorities to intercept personal data, and the ECtHR, in such cases, examines the 'Weber requirements'.[214]

Three additional safeguards to the 'Weber requirements' against the abuse of power, proposed by the applicants in *Big Brother Watch v UK (2019)*,[215] were initially dismissed by the ECtHR because in cases involving bulk interception, those proposed safeguards could contradict the very nature of secret surveillance conducted through bulk interception of data. First of all, bulk interception is by definition untargeted, and it will be impossible to render such operations if the law requires the existence of reasonable suspicion. Similarly, a subsequent notification of the subject of surveillance is impossible, as it presupposes that the interception is targeted. Secondly, the requirement of having prior judicial authorization for bulk surveillance was not considered in the case of *Big Brother Watch v UK (2019)*[216] as a mandatory requirement of being 'necessary in a democratic society', as there could be other, non-judicial, bodies, which would impartially consider any individual complaints on bulk interceptions. Moreover, there is always a threat of having an improper action by a dishonest, negligent or overzealous official in any system,[217] and the *Zakharov* case serves as an

[211] *Big Brother Watch (2019)*, see n 50 above, Paragraph 316.
[212] Venice Commission's 2015 Report, n 205 above, Paragraph 3.
[213] *Big Brother Watch (2019)*, see n 50 above, Paragraph 314.
[214] *Big Brother Watch (2019)*, see n 50 above, Paragraph 315; *Rattvisa*, n 206 above, Paragraph 261.
[215] See n 191 above concerning the *Big Brother Watch* case.
[216] *Big Brother Watch (2019)*, see n 50 above, Paragraph 316.
[217] *Big Brother Watch (2021)*, n 185 above, Paragraphs 317-319.

example, where prior judicial authorization has provided limited or no protection against abuse.[218]

In 2021, however, the Grand Chamber in *Big Brother Watch (2021)* has agreed to include the second proposed requirement – judicial authorization – for the bulk surveillance.[219] The ECtHR in that case has modified the 'Weber requirements' for the bulk surveillance proposing eight requirements, which the domestic law ought to clearly define:

1. the grounds on which bulk interception may be authorized;
2. the circumstances in which communications of an individual may be intercepted;
3. the procedure to be followed for granting authorization;
4. the procedures to be followed for selecting, examining, and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercepted material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.[220]

4.2.1.5. Communications Data

An analysis of bulk interception cases raises the issue of communications data (or metadata) as opposed to the content data. There is no internationally accepted legal definition of 'communication data', and the ECtHR has dealt with it only in a few cases.[221] While the 'content data' is information contained within the communication, the 'communication data' is information about such communication. For instance, communications data can describe how, when, and between which addresses the electronic communication is conducted.[222]

It is usually disputed by the States that the interception of the content data poses more threat to the private life of an individual than the communications data. Thus, in 2010 in *Uzun v Germany*, the ECtHR agreed with the responding State that the interception of

[218] *Zakharov*, see n 27 above.
[219] See *Big Brother Watch (2021)*, n 185 above, paragraphs 350-351.
[220] *Big Brother Watch (2021)*, n 185 above, Paragraph 361.
[221] In *Malone v UK*, see n 20 above, the ECtHR considered 'metering', i.e., an information on the telephone numbers collected by the public authorities from the telephone companies, as an information, which, if used unlawfully, could result in violation of individual's right to private life; *Uzun v Germany*, see n 25 above; *Big Brother Watch (2019)*, see n 50 above; and *Rattvisa*, n 206 above.
[222] *Rattvisa*, n 206 above, Paragraph 14.

communications represented a greater intrusion into the private life of the individual than the tracking of their vehicle via GPS.[223]

However, in 2019, in the *Big Brother Watch* case, the ECtHR was not persuaded by the respondent government that the acquisition of related communications data is necessarily less intrusive than the acquisition of content.[224] In that case, the respondent State – the UK had extensive legislation containing provisions on 'communications data', which was defined as consisting of three parts: 1) traffic data, 2) service use information; and 3) subscriber information. Separately, UK's domestic law defines 'related communications data' as a limited subset of 'communications data', which is obtained by or in connection with the interception, and which is related to the communication or the sender or recipient, or the intended recipient, of the communication.[225]

Communications data is a valuable resource for intelligence services. They can easily analyse it and find certain patterns in the behaviour of people, which could lead to planned terrorist attacks or to persons engaged in such attacks. In comparison to much of the content data, communications data is not encrypted. There could be situations when intelligence services spend much of their time on decryption, and the results thereof will give them no necessary information. In the case of 'communications data', on the other hand, the identities and the geographic location of the senders and recipients of communications can be determined. In case of bulk interception of communications data, the degree of intrusion into private life increases dramatically, and the intelligence services will be able to use many patterns to reveal intimate pictures of a person through the mapping of social networks, location tracking, Internet browsing tracking, and an overview of who that person communicated with.[226]

4.2.2. Surveillance in the Form of Using Retained Data

Personal data retained by public authorities can be obtained via secret interception of such data, or through an open acquisition in the way provided by law or otherwise[227]. Such an acquisition of personal information may take the form of a direct interception or collection from the individuals, or through data sharing or transferring from communications services providers.

---

[223] *Uzun v Germany*, see n 25 above, Paragraph 52.
[224] *Big Brother Watch (2019)*, see n 50 above, Paragraph 356.
[225] *Big Brother Watch (2019)*, see n 50 above, Paragraphs 64, 66 and 293.
[226] *Big Brother Watch (2019)*, see n 50 above, Paragraphs 353 and 356.
[227] In *S. and Marper v UK* the ECtHR found that the public authorities' power to retain personal information had been of a blanket and indiscriminate nature. See *S. and Marper v UK*, see n 4 above, Paragraph 125.

The ECtHR has found that the mere storing of data relating to the private life of individuals amounted to an interference with their right to private life.[228] In *S. and Marper v UK* the ECtHR held that in retaining personal data in order to determine if any private-life aspects were involved, it ought to give due regard to the context, in which the information was obtained, the scope and nature of such information, the way such records were used and processed and the results to be obtained from such information.[229] In that case, fingerprints, DNA profiles, and cellular samples were retained by public authorities in the context of criminal proceedings, but the ECtHR has distinguished fingerprints from DNA profiles and cellular samples by their nature, as the latter had stronger potential for future use, and consequently examined them separately.[230]

Cellular samples contain more sensitive and extensive personal information than fingerprints, and therefore their retention by public authorities *per se* ought to amount to interfering with the private lives of individuals.[231] Retention of DNA profiles may create interference with sensitive information, such as the ethnic origin of an individual, and such information ought to be accorded a heightened level of protection by the State in accordance with the Convention 108.[232] However, for the purposes of justification of retention of fingerprints, DNA profiles, and cellular samples, the ECtHR ought to examine them by using its standard formula of whether the interference was in accordance with the law, whether it pursued a legitimate aim, and whether it was necessary in a democratic society.[233]

The ECtHR, in the context of the retention of identification data, has indicated that some minimum safeguards concerning duration, storage, usage, access of third parties, procedures securing confidentiality, and procedures for destruction of data, ought to be in place.[234]

4.2.2.1. Purposes of Data Retention

Data retention is one of the forms of data processing,[235] and the purposes, for which personal data can be retained in criminal proceedings, are indicated in the EU Law

[228] *Leander v Sweden* (1987) Series A no.116, Paragraph 48.
[229] *S. and Marper v UK*, see n 4 above, Paragraph 67.
[230] *S. and Marper v UK*, see n 4 above, Paragraph 69.
[231] *S. and Marper v UK*, see n 4 above, Paragraph 73.
[232] *S. and Marper v UK*, see n 4 above, Paragraph 76; Article 6(1) of the Convention 108, see n 36 above.
[233] *S. and Marper v UK*, see n 4 above, Paragraph 86.
[234] *P.N. v Germany*, see n 34 above, Paragraph 62.
[235] Article 3(2) of the LED defines 'processing' as any operation or set of operations […], such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'. See Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 "On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution

Enforcement Directive (LED)[236] as follows: 'prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'[237] In *S. and Marper v UK*, the ECtHR found that the retention of personal data for the prevention and detection of crime in the law of the respondent State was formulated rather in general terms and could give rise to extensive interpretation.[238] The main principles of protection of personal information require data retention to be proportionate in relation to the purpose of data collection. The Convention 108 specifies that personal data must not be processed in a way incompatible with or be excessive in relation to legitimate purposes of such data processing, and must be preserved in a form, which would allow identifying individuals for no longer than required for the purposes of data retention.[239]

In *P.N. v Germany*, although the ECtHR held that the national law of the respondent State gave a relatively broad description of purposes for data retention, the established case law of that State provided for a sufficient degree of foreseeability of the law, which added to the quality of domestic law.[240] Where the ECtHR had concerns about the ambiguity of the legal basis for the collection of personal data, it would state that the question of whether the retention and use of data 'in accordance with the law' was closely related to the broader issue of whether the interference was 'necessary in a democratic society', and for that reason, the ECtHR did not think it was necessary to examine 'in accordance with the law' element.[241]

4.2.2.2. Duration of Data Retention

All three European instruments on data protection mentioned in this Chapter: Convention 108, GDPR, and LED, provide that the public authorities or third parties, which could eventually disclose the retained personal data to the public, must store and use personal data for as long as it is necessary for the purposes for which such data was obtained.[242] In *S. and Marper v UK*, the ECtHR stressed that the retention of personal data for an indefinite period of individuals, who were not convicted of any offence, can affect the presumption of innocence of those individuals, and such data retention can be especially harmful with

---

of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA" (Law Enforcement Directive – LED).

[236] See Law Enforcement Directive – LED, 235 above.

[237] Article 1(1) of the LED, n 235 above.

[238] *S. and Marper v UK*, n 4 above, Paragraph 99.

[239] Article 5(4)(b, c and e) of the Convention 108, n 36 above.

[240] *P.N. v Germany*, see n 34 above, Paragraphs 65-66.

[241] *S. and Marper v UK*, n 4 above, Paragraph 99; *Catt v UK*, see n 42 above, Paragraphs 106-107.

[242] Article 5(4)(e) of the Convention 108, n 36 above; Article 4(1)(e) of the LED, n 235 above; Article 5(1)(e) of the GDPR, n 38 above.

respect of minors.[243] In any way, blanket, indiscriminate retention with no indication of the duration of such retention of personal data of individuals, suspected but not convicted of offenses, fails to strike a fair balance between competing private and public interests.[244]

In *P.N. v Germany*, the ECtHR found no violation of Article 8 provision where the domestic law of the respondent State provided for a 5-year duration of retention of personal data of an adult offender, whose offenses were neither of minor nor of special significance.[245] In *M.K. v France*, a 25-year period of data retention, rather standard than a maximum one, was found to be practically tantamount to indefinite retention.[246]

4.2.2.3. Necessity and Proportionality of Data Retention

In *Catt v UK*, the personal data of the applicant, such as name, photograph, address, and date of birth, were retained by the public authorities under the title 'domestic extremism' due to the political opinions of the applicant and his participation in different demonstrations. He claimed that the retention of his personal data was not necessary within the meaning of Article 8(2) of the ECHR.[247] The legislation of the respondent State allowed for the retention of such personal data for the minimum period of six years and the subsequent revisions, which would lead to a deletion of personal data from the database. The ECtHR having considered that the domestic law contains certain ambiguities, such as a loose definition of 'domestic extremism' and a possibility for retaining personal data for indefinite period of time, decided, as in the case of *S. and Marper v UK*, to skip the issue of whether the interference with private life was in accordance with the law, and concentrate rather on the issue of necessity in a democratic society.[248]

A margin of appreciation in such cases is usually left to the competent authorities to assess whether there was a pressing social need for data retention, whether such data retention was proportionate to the legitimate aim pursued, and whether the reasons for data retention, given by the public authorities are relevant and sufficient.[249] In cases where impartial and independent domestic courts carefully examine the facts, and apply relevant human rights standards consistently with the ECHR in their case law, the ECtHR will not be

[243] *S. and Marper v UK*, n 4 above, Paragraphs 122 and 124.
[244] *Ibid*., *S. and Marper v UK*, Paragraph 125.
[245] *P.N. v Germany*, see n 34 above, Paragraphs 85.
[246] *M.K. v France*, see n 67 above, Paragraph 42.
[247] *Catt v UK*, see n 42 above, Paragraphs 12, 72 and 80.
[248] *Catt v UK*, see n 42 above, Paragraphs 105-107; *S. and Marper v UK*, n 4 above, Paragraph 99.
[249] *S. and Marper v UK*, n 4 above, Paragraphs 101-102.

in a position to disregard their assessments on merits, and will not make its own assessment instead.

However, in *Catt v* UK, the ECtHR found some compelling reasons to make its own assessment of the facts. It held that the political opinions of an individual represent a special category of personal data due to its high sensitivity, and such data therefore ought to be afforded a heightened level of protection.[250] The ECtHR in that case has employed an approach which it had used in cases involving covert surveillance. In those cases, it found that powers vested in the State were obscure, creating a risk of arbitrariness in the context of using more sophisticated technologies by public authorities.[251] The ECtHR found that there was a pressing need to *collect* the personal data of the applicant, but there was no pressing need to *retain* that personal data in the case of *Catt v UK*, and, consequently, found that the retention of personal data of the applicant was not absolutely necessary.[252]

4.2.2.4. Retention of Sensitive Data

Article 6 of the Convention 108 stipulates that special categories of personal data, such as genetic data, biometric data, data relating to offenses, criminal proceedings and convictions, data revealing ethnic or racial origin, political opinion, religious or other beliefs, health or sexual life of an individual, as a sensitive data, can be processed only if appropriate safeguards are enshrined in the law.[253]

The ECtHR has determined that such sensitive personal data must attract a heightened level of protection in the domestic law.[254] In *S. and Marper v UK*, the ECtHR contended that a DNA profile of an individual contains genetic information of the person, which is very important for both the person concerned and for their family. It has held that a cellular sample contains sensitive information about the health of an individual.[255] So, the processing of such information represents a more intrusive interference with private life than, e.g., information contained in fingerprints.[256] It is therefore in some cases such a difference between sensitive

[250] *Catt v UK*, see n 42 above, Paragraph 112.
[251] See *Zakharov v Russia*, see n 27 above, Paragraph 229; and *Szabo and Vissy v Hungary*, see n 76 above, Paragraph 68.
[252] *Catt v UK*, see n 42 above, Paragraphs 117, 119 and 124.
[253] Modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the CoE Committee of Ministers on 18 May 2018, CM/Inf(2018)15-final.
[254] *S. and Marper v UK*, n 4 above, Paragraph 76.
[255] *S. and Marper v UK*, n 4 above, Paragraphs 72 and 75.
[256] *P.N. v Germany*, see n 34 above, Paragraph 84.

and ‘ordinary’ personal data could be decisive when a violation of Article 8 provisions is found by the ECtHR.[257]

4.3. Conclusion

The right to privacy protected by Article 8 of ECHR stems from the Western idea of individual autonomy and personal development. Dignity is in the gist of their free exercise of rights and freedoms, particularly the right to privacy. The European human rights law framework perceives the right to privacy as an individual right or as a value, which is opposed to the social or community needs, and in each particular case the ECtHR engages in the balancing exercise attempting to determine whether or not the right to privacy overrides the common good or vice versa. In order to successfully fulfill such an exercise, the ECtHR in its jurisprudence employs certain techniques, which help it to determine the necessity and proportionality of measures taken by the States to interfere with private life.

The rapid development of surveillance technologies poses new threats and challenges to the informational self-determination of individuals, i.e., their privacy in terms of personal data protection. More sophisticated surveillance technologies are available for authorities to fulfill their functions in the field of combatting and preventing crimes and defending national security. The work of authorities becomes more efficient, and the common values, such as national security, are attained more effectively with the availability of such new surveillance technologies. The task of the ECtHR in such a situation becomes more of a standard-setter. It decides what the minimum legal requirements for carrying out surveillance in the Member States ought to be.

The ECtHR is hesitant to rapidly adopt new tests or widen minimum requirements when it comes to new surveillance measures, such as bulk interception of communications. The lack of thorough examination of domestic legislation of the majority of Member States prevents the ECtHR from setting new standards of human rights protection in respect of the right to privacy. The ECtHR is not able to determine what ought to be considered proportionate interference in the case of bulk surveillance. Neither the ECtHR readily uses a margin of appreciation doctrine in such cases, although it mentions that the manner in which the States use bulk surveillance must entail a narrower margin of appreciation afforded to the States by the ECtHR.

The dignitarian understanding of the right to privacy, where an individual freely develops their personality through controlling or deciding when, to whom and in what

[257] *Catt v UK*, see n 42 above.

circumstances to allow the use of their personal information, is leading the ECtHR through the complicated and time-consuming process of setting a myriad of rules and restrictions, which aim to protect the right to private life. Eventually, the ECtHR comes to a conclusion that an indiscriminate bulk interception of communications belonging to individuals per se is allowed and does not necessarily violate the right to privacy, which is premised on the human dignity. The ECtHR only gives individuals the right to develop reasonable suspicion that they probably are under secret surveillance, and subsequently seek the redress in local courts. And, if it eventually comes to the ECtHR to decide, it will employ its proportionality principle in order to determine, whether an indiscriminate bulk surveillance was necessary in particular circumstances, and was serving the common good – protecting national security or preventing the crime.

The ECtHR has very rarely considered the right to privacy as a common good or as a social need as opposed to some other individual freedoms, such as, e.g., freedom of expression. Perhaps, it is time to perceive the right to informational self-determination as a common good, as something, the protection of which would serve to the whole community. In the present-day reality, when secret bulk surveillance measures are not directly prohibited by the European human rights law, any interference with the right to privacy can be regarded as an interference into the right to privacy of many people. Such an approach may help the ECtHR in taking decisions in favour of protecting the right to privacy. The right to privacy in such case will be opposed to the social need for protecting national security or preventing crime not as an individual right versus public good, but, rather, as a common value versus another common value. This way, the ECtHR may constrain its earlier pattern of relying on the doctrine of margin of appreciation only in a small number of cases concerning Article 8 ECHR rights, if at all. This may pave the way for treating the right to privacy as a 'universalizable value' for all Member States in the context of data protection and surveillance. The ECtHR's approach is to accord wide margin of appreciation to the Member States if there is no 'European consensus', and, thus, in bulk surveillance cases the States have a wide margin of appreciation in choosing the type of conducting surveillance. However, Member States ought to provide adequate procedural safeguards – the 'Weber requirements' in order to operate the interception regime.

The next Chapter – Chapter 5 will discuss the EU legislation related to the right to privacy and data protection, where this thesis will explore why the right to personal data protection is separated from the right to privacy by the CFREU, and how the right to data protection can further change our perception of the right to privacy as the right of individual to control the use of information about them.

Chapter 5. EU Law Rules Regarding Data Protection and Privacy Rights

5.1. Introduction

On the territory of the European countries, the right to privacy as a human right is not only protected under the European Convention on Human Rights (ECHR)[1] framework, as has been explored earlier in Chapter 4, or under the national laws of the Member States, but is also subject to legal protection for the European Union (EU) Member States under EU Law. This Chapter will focus on supranational law, which is binding on the Member States.

The Charter of Fundamental Rights of the European Union (the CFREU)[2] contains Article 7, according to which everyone has the right to respect for their private and family life, home, and communications. While Chapter 4 of this thesis has examined the right to data protection as a subset of the right to private life because the right to data protection is not expressly mentioned in the text of the ECHR, an important difference in the case of the CFREU is that the drafters opted to proclaim the right to data protection as a separate fundamental right of a natural person in Article 8 CFREU.

Other main legislative acts of the EU on data protection which are analyzed in this Chapter are the Data Protection Directive of 1995 (DPD),[3] the General Data Protection Regulation of 2016 (GDPR),[4] and the Data Retention Directive of 2006 (DRD).[5]

This Chapter seeks to explore why the right to data protection has been carved out from the right to private life under EU law, and whether such separation of two rights is important in better understanding of privacy as a concept. Chapter 3 was devoted to the concepts of privacy as understood in the West along with their historical and modern

[1] Convention for the Protection of Human Rights and Fundamental Freedoms adopted by the Council of Europe on 4 November 1950 and entered into force on 3 September 1953.
[2] The CFREU was adopted by the European Parliament, European Council and the Council on 7 December 2000 and entered into force together with the Treaty of Lisbon on 1 December 2009.
[3] Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (1995) OJ L281/31 (DPD). The DPD was in force until 2018 when the GDPR came into legal force.
[4] Regulation (EU) 216/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), (2016) OJ L119/1.
[5] Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54 (DRD). The DRD was in force until 2014 when the Court of Justice of the EU declared it invalid in its case of *Digital Rights of Ireland*. See Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others,* Judgement of the GC dated 8 April 2014.

development, and this Chapter explores an approach taken by EU law on privacy. Early EU laws on data protection, such as the DPD clearly referred to the fundamental right to private life as an underlying principle of data protection. The current legislation – the GDPR – has changed references to the right to private life with references to the right to data protection as an underlying principle.

EU law rules and standards pertaining to data protection[6] are considered to have become a global standard of data protection in the world.[7] This Chapter explores the standards of data protection set by the EU in general, and in respect of transborder data flows in particular. One of the aims of this Chapter is to build on the earlier exploration of data protection laws of Tajikistan in Chapter 2, with a view to finding out how these could in the future better be aligned with the standards established by EU data protection law.

This Chapter is divided into three main sections. The first main section (Section 5.2.) is about fundamental rights to private life and data protection. It explains the evolution of fundamental rights in the EU legal framework, including some critical discussions with regard to whether fundamental rights are given precedence over market freedoms in the EU in the example of data protection.

The second main section (Section 5.3) examines main EU data protection laws. A separate sub-section is devoted to the theme of the extraterritorial application of data protection laws of the EU within Section 5.3, which explains the willingness of the EU to promote its values beyond the borders of the EU. According to Article 5(3) of the Treaty on European Union (TEU), the EU ought to promote its values, such as the promotion and protection of fundamental rights and freedoms to a wider world.[8] Extraterritoriality is an important feature of data protection legislation,[9] as it implies a desire of EU institutions, primarily the CJEU, to show the importance of fundamental rights protection when personal data is processed by foreign entities or transferred abroad.[10] Section 5.3. explores a recent

[6] The General Data Protection Regulation (GDPR) is the main instrument of EU secondary law on data protection. It entered into legal force in 2018 and was preceded by the Data Protection Directive of 1995 (DPD).
[7] See Michael Rustad and Thomas Koenig 'Towards a Global Data Privacy Standards' (2019) 71 Florida Law Review 365; Stefano Saluzzo 'The EU as a Global Standard-Setting Actor: The Case of Data Transfers to Third Countries' in E. Carpanelli and N. Lazzerini (eds.) *Use and Misuse of New Technologies* (Springer Nature Switzerland AG, 2019); Graham Greenleaf 'The Influence of the European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108' (2012) 2 International Data Privacy Law 68; Claes Granmar 'Global Applicability of the GDPR in Context' (2021) 3 International Data Privacy Law 225; Anu Bradford 'How the EU Became a Global Regulatory Power' in A. Bradford *The Brussels Effect* (OUP, 2020).
[8] See Treaty on European Union, OJEU, C 326/13.
[9] See Lee Bygrave *Data Privacy Law*: *An International Perspective* (UOP 2014) 199; Dan Jerker B. Svantesson 'Extraterritoriality and Targeting in EU Data Privacy Law: the Weak Spot Undermining the Regulation' (2015) 4 International Data Privacy Law 226, 228.
[10] See Case C-362/14 *Maximillian Schrems v Data Protection Commissioner,* Judgment of the GC dated 6 October 2015; Case C-311/18 *Data Protection Commissioner v Facebook and Maximillian Schrems,* Judgment

shift in highlighting the fundamental right to data protection instead of the right to private life by the CJEU. This Chapter discusses whether such a shift may lead us to conclude that the EU considers the right to data protection as a 'universal right', which would be respected in all parts of the world as it is done in the EU. In contrast to this, the right to private life may be understood differently even among the EU Member States. This right is hardly mentioned in the GDPR.

This Chapter thereafter examines the role of private companies in ensuring the right to data protection and their role in making data protection a universal right when adhering to the EU data protection laws as by adopting certain practices and following certain rules established by the GDPR. The Chapter subsequently discusses the so-called 'Brussels Effect'.[11] The EU market as one of the largest economies in the world is considered to be attractive for businesses from third countries, such as Tajikistan. If such businesses seek to sell their goods and services in the EU market, they must adhere to the EU standards of protecting personal data. Third countries thus are prompted to promote and adopt data protection rules and standards adequately protecting the rights of individuals during data processing.

The third main section (Section 5.4) shows how EU secondary laws in the area of data protection[12] have developed the concept of data protection as a separate fundamental right. The emergence of the right to data protection affects our understanding of the right to privacy. It will be seen that scholars have observed that the Court of Justice of the European Union (CJEU) failed so far to conceptualize the right to data protection as opposed to the right to private life. The Chapter examines this issue with a view to understanding what privacy is meant by contemporary EU data protection legislation.

5.2. The Right to Privacy under the EU Charter of Fundamental Rights

5.2.1. The Nature of EU law

In order to meaningfully examine the importance and the legal force of the rights to privacy and data protection as separate and intertwining fundamental rights within the EU, this thesis will briefly explain the special nature of EU law and its relationship to the national laws of the Member States.

---

of the GC dated 16 July 2020; Case C-131/12 *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez,* Judgment of the GC dated 13 May 2014.

[11] See A. Bradford *The Brussels Effect* (OUP, 2020).

[12] GDPR, DPD and the Data Retention Directive (DRD). Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54.

Among major subjects of international law, such as States and international organizations[13], the European Union represents a specific form of governance, which contains characteristics of a polity or a State on the one hand, and an international organization, on the other hand. There is a common agreement in the legal scholarship that the EU (or, previously, the European Communities – EC) represents a *sui generis* international organization, i.e., a special type of international organization, which contains the elements of both a federal State and an international organization.[14] EU law as a reflection of the special nature of the EU has certain elements which make that law enforceable on the territories of its Member States. It has a direct effect in the legal orders of the Member States and primacy over national legislation of the Member States.

'Direct effect' may be defined as a possibility of an EU norm to be directly invoked by individuals in domestic court proceedings.[15] The CJEU however implied that not all provisions of the Community (or now Union) law enjoyed direct effect. The Court had indicated several conditions for the Union legal act to be immediately applicable: legal norms must be clear and concise, unconditional, and would not require additional measures for implementation at the national level.[16]

The primacy of the law must be understood as supremacy[17] or precedence of the EU rules over the national rules of the Member States, which means that in case of a conflict of two sets of rules, the former must be applied, and the latter must be set aside. As in case of the direct effect, primacy is not expressly stated in the primary sources of EU law. Again, as in case of the judicial doctrine of direct effect, the CJEU took initiative to pronounce the principle of primacy of the then Community law over national law of the Member States in its *Costa v ENEL* judgment in 1964.[18]

---

[13] A state was always considered as primary subject of international law, whereas international organizations received confirmation of their international legal personality at a later stage, when the ICJ in its advisory opinion of 11 April 1949 confirmed that the UN is a subject of international law capable of possession of international rights and duties, and had the capacity to maintain its rights by bringing international claims. See *Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion* I.C.J. Reports 1949.

[14] See, eg, Armin von Bogdandy, 'Neither an International Organization, Nor a Nation State: the EU as a Supranational Federation', in *The Oxford Handbook of the European Union* (OUP 2012).

[15] See Bruno de Witte Chapter 12 'Direct Effect, Primacy and the Nature of the Legal Order' in Paul Craig and Grainne de Burca (eds.) *Evolution of EU Law* (OUP 2011).

[16] Case 26/62 *NV Algemene Transport en Expeditie Onderneming Van Gend en Loos v Nederlandse administratie der belastingen* [1963] ECR 1.

[17] Bruno de Witte considers 'primacy' and 'supremacy' as interchangeable terms in the English language literature. See Bruno de Witte 'Direct Effect, Primacy and the Nature of the Legal Order' in Paul Craig and Grainne de Burca *Evolution of EU Law* (OUP, 2011) p.323. Matej Avbelj, on the other hand, sees conceptual differences between these two terms. See Matej Avbelj 'Supremacy or Primacy of EU Law – (Why) Does It Matter?' (2011) 17 European Law Journal 744.

[18] Case 6/64 *Costa v ENEL* [1964] ECR 585.

There has been a debate about whether the 'primacy' principle was only inherent to the Community law, as after the division into supranational and international parts of EU law established by the Maastricht Treaty, where the Common Foreign and Security Policy (CFSP) lacked supranationalism, the CJEU, as observed by de Witte, has allegedly no opportunity to examine the primacy principle.[19] The CJEU did not examine this issue in an earlier case of *Van Gend en Loos*, because primacy, unlike direct effect, was unproblematic from the point of view of the Dutch court, due to the fact that the Dutch constitutional law enshrined primacy of a self-executing treaty provision over the conflicting national law.[20]

Legal norms of national law conflicting with the provisions of EU law must be disapplied even if such norms of national law were enacted after the EU law provisions.[21] The CJEU held that both the organs of the judiciary of the Member States as well as other State organs, including administrative authorities, who are in charge of the application, implementation, and enforcement of legal norms, ought to refrain from applying the conflicting norms of domestic legislation.[22]

The EU (and before that the European Communities) has emerged as a union or community of States pursuing certain economic goals, such as the free flow of goods, capital, and labour force. It is a political union where the Member States have developed and implemented the CFSP, and have established internal goals and values common for each of them. Such values serve as an integrative element within the EU. Moreover, they are subject to promotion by the EU in a wider world because such values are recognized as universal values as enshrined in the Preamble of the TEU.

Democracy, the rule of law, and respect for fundamental rights were initially mentioned as principles in the Preamble of the Maastricht Treaty and in the parts related to the CFSP[23] and development cooperation[24]. The Treaty of Lisbon has further added human dignity, equality, and respect for the rights of minorities, and renamed these principles as 'values'. Article 2 of the TEU proclaims the main EU values, on the basis of which the EU

[19] See Bruno de Witte n 17 above. In fact, the CJEU used the term 'primacy of Community law' even in 2009 in the case of *Krzysztof Filipiak*, where the Community law was subject to review: case C-314/08 *Krzysztof Filipiak v Dyrektor Izby Skarbowej Poznaniu*, CJEU Judgment of 10 December 2009. At the same time, in more recent cases (2016-2019) the CJEU made use of the term 'primacy of EU law': Case C-689/13 *Puligienica Facility Esco Spa (PFE) v Airgest Spa* [2016], Judgment of the GC dated 5 April 2016; Case C-378/17 *Minister for Justice and Equality, Commissioner of An Garda Siochana v Workplace Relations Commission* [2018] OJ 2019 C 44/3; and Case C-573/17 *Daniel Adam Poplavski v Openbaar Ministerie* [2019], Judgment of the GC dated 24 June 2019.
[20] See Bruno de Witte n 17 above.
[21] Case C-106/77 *AMMINISTRAZIONE DELLE FINANZE and Simmentahl S.p.A.,* Judgment of 9 March 1978.
[22] Case C-378/17 *Minister for Justice and Equality, Commissioner of An Garda Siochana v Workplace Relations Commission*, Judgment of 4 December 2018*,* Case C-573/17 *Daniel Adam Poplavski v Openbaar Ministerie* [2019], Judgment of the GC dated 24 June 2019.
[23] Article 11 TEU Maastricht Treaty
[24] Article 177(2) TEC.

is founded upon and operating: respect for human dignity, freedom, democracy, equality, rule of law and human rights. Such values, as mentioned earlier, are common for all Member States, where the main ideas of pluralism, non-discrimination, tolerance, justice, solidarity and gender equality prevail.

Member States are obliged to comply with and promote those values both within and outside of the EU. Such an obligation is enshrined in Article 7 of the TEU, under which Member States would refrain from committing or would act for not allowing serious breach of the EU values. The Council is entitled to suspend certain voting rights of the Member State in breach of complying with and promoting the EU values, and such a suspension may include voting rights in the Council. In addition to observing the EU values, Member States must promote them within the EU. Article 4(3) of the TEU imposes an obligation on the Member States to cooperate, and in full mutual respect help each other to carry out their tasks arising from the Treaty of Lisbon.

In addition to primary EU law, there are secondary sources of law, such as directives and regulations, which are adopted by the EU main institutions through ordinary and special legislative procedures. The EU secondary law, depending on the form of the legislative act (regulation or directive), is enacted or transposed within the national law of Member States differently. Directives become effective in a Member State through passing appropriate implementation measures, including passing national laws, which would take into account national peculiarities of the respective Member State. At the same time, regulations have direct effect on the territory of Member States, thus enhancing harmonization of laws within all Member States.

In the field of data protection, current General Data Protection Regulation (GDPR)[25] has harmonized the laws of all Member States and simultaneously entered into legal force on their territories. There are certain so-called 'opening clauses', which give some scope of discretion to the Member States on legislating data protection issues in some sensitive areas. The GDPR was preceded by the Data Protection Directive (DPD)[26], which could fully be enforced on the territory of the Member States only after its transposition, i.e., after Member States take implementing measures, such as enacting national data protection laws. These measures will be explored to a greater extent in Section 5.3 of this Chapter.

[25] GDPR, n 4 above.
[26] DPD, n 3 above.

5.2.2. Evolution of the Protection of Fundamental Rights and Human Dignity in EU Law

Human dignity is listed as the first value in the list of European values in Article 2 of the TEU and as a first fundamental right in Article 1 of the CFREU. It serves as a basis for other fundamental rights and is a cornerstone of most of the rights and freedoms enshrined in that instrument. It is a guiding principle for the external action of the EU within the CFSP[27] because the aim of the EU is *inter alia* to promote its values[28] beyond the boundaries of its Member States.

The CJEU has made a mention of human dignity in its case law even before the CFREU became part of the primary EU law and was bestowed a legally binding force.[29] The CFREU stipulates that human dignity is inviolable and must be respected and protected.[30] There are two aspects in the approach taken in the CFREU, which are important to discuss here: 1) since human dignity is inviolable, the question may arise whether it is an absolute right granted to individuals, and 2) while TEU uses the word 'respect' human dignity, as well as other EU values, the CFREU stipulates that the human dignity must be respected and protected. Thus, human dignity as a right is afforded negative protection by the Member States and the EU institutions from the interference of national or supranational institutions. Moreover, the CFREU secures positive obligations of those organs to provide meaningful protection from encroachments of third parties, including other individuals.[31]

The Explanations Related to the CFREU consider human dignity as part of the substance of fundamental rights, which must be respected even if the right is restricted.[32] AG Sanchez-Bordona calls the right to human dignity as absolute right, 'which cannot, per se, be balanced against other interests.'[33] The absolute nature of human dignity means that there must be no derogation from it, and it would trump other conflicting norms or rights,

[27] Article 21 TEU.
[28] Article 3 TEU.
[29] Case C-377/98 *Netherlands v Parliament and Council,* CJEU Judgment of 9 October 2001; Case C-36/02 *Omega Spielhallen und Automatenaufstellung v Oberburgermeisterin der Bundesstadt Bonn,* CJEU Judgment of 14 October 2004.
[30] Article 1 CFREU.
[31] AG Trstenjak considers that the CFREU affords the right to human dignity a positive protective function by stating that the right to "human dignity must not only be 'respected', but also 'protected". See Opinion of AG Trstenjak dated 22 September 2011 on Case C-411/10, Paragraph 112. Williams mentions that in general the obligation to promote EU values suggests a more positive and proactive human rights commitment by the EU institutions. See Andrew Williams 'Human Rights in the EU' in Damian Chalmer and Anthony Arnull *The Oxford Handbook of European Union Law* (OUP, 2015).
[32] Explanations Relating to the Charter of Fundamental Rights, OJEU, 2007/C 303/02, 14 December 2007.
[33] Opinion of AG Sanches-Bordona on case C-128/18, Opinion dated 30 April 2019, Paragraph 107.

which may be limited.[34] In *Omega*,[35] however, the CJEU has engaged in balancing one of the market freedoms – free movement of services – with the human dignity as a general value of the EU. Such a balancing exercise is facilitated by a proportionality test, which excludes the absolute nature of the right to human dignity under EU law.[36]

When exploring the protection of fundamental rights in the EU, it is important to bear in mind that initially the EU legal order was based only on market integration and did not contain a fundamental rights dimension. However, this has gradually changed, especially in response to concerns raised by the German Federal Constitutional Court ('BVerfG') in the *Solange* cases, where the supremacy of EU law was made conditional on respect for fundamental rights.[37]

The CJEU started invoking fundamental human rights; however, this was seen as being dictated by other reasons than the willingness of the CJEU to interpret the Community law as containing a bill of rights in the form of general principles common to the Member States.[38] The Member States were doubtful of the inherent aspiration of Community law to respect fundamental rights due to the above-mentioned absence of the formal bill of rights and democratically elected parliament at the Community level.[39] Thus, in *Solange I,* the BVerfG has made the primacy of the Community law conditional by checking the compatibility of Community law with the fundamental rights and freedoms enshrined in the national constitution.[40] The CJEU sought to impose the primacy of Community law by claiming that the respect and protection of fundamental rights were inherent to the Community legal order.[41] The CJEU has also stated that the fundamental rights as general principles stem not only from the common constitutional traditions of its Member States, but also from international human rights agreements, such as the ECHR, to which Members States were parties.[42]

---

[34] See Koen Lenaerts 'Exploring the Limits of the EU Charter of Fundamental Rights' [2012] 8 EuConst 375.
[35] Case C-36/02 *Omega Spielhallen und Automatenaufstellung v Oberburgermeisterin der Bundesstadt Bonn,* CJEU Judgment of 14 October 2004.
[36] See Dieter Grimm et al 'European Constitutionalism and the German Basic Law' in Anneli Albi and Samo Bardutzky *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law (National Reports)* (Asser Press 2019) at p.437. Grimm's main point was that in German Constitutional Law human dignity protection featured a much higher standard going above inviolable, whereas in CJEU case law it can be subject to balancing with market freedoms through the principle of proportionality.
[37] *Internationale Handelsgesellschaft* (29 May 1974) BVerfGE 37, 2712, 2 BvL 52/71 (*Solange I*) BVerfGE 73, 339 2 BvR 197/83 (*Solange II*).
[38] See Stijn Smismans 'The European Union's Fundamental Rights Myth' [2010] 1 JCMS 45.
[39] German Federal Constitutional Court has raised such doubts in its *Solange* case. See *Internationale Handelsgesellschaft* (29 May 1974) BVerfGE 37, 2712, 2 BvL 52/71 (*Solange I*).
[40] *Ibid.*
[41] Stijn Smismans 'The European Union's Fundamental Rights Myth' [2010] 1 JCMS 45, at p. 48.
[42] Case 4/73 *Nold v Commission*, Judgment of 14 May 1974.

The CFREU was adopted in 2000 and initially had non-binding force, and only with entry into force of the Treaty of Lisbon in 2009, the CFREU attained legally binding force. Under Article 6 TEU the rights, freedoms, and principles stipulated in the CFREU had the same legal value as TEU and TFEU,[43] i.e., it has acquired legal force of acts of primary EU laws, which could mean that the CFREU may serve as a European constitutional bill of rights.[44] The CFREU contains fifty rights, which include civil and political as well as economic and social rights.

For the completeness of the account, the present author deems it fitting to reiterate that there is an extensive critical discourse on the EU protection of fundamental rights, where it is pointed out that in the actual adjudication, the CJEU tends to promote market freedoms and economic values rather than fundamental rights. The origins of such an approach lie in the foundations of EU law in market integration. Albi argues that before the *Omega*[45] case in 2004, the CJEU had not given priority to the right to human dignity over market freedoms, such as freedom of services.[46] Smismans points to several human rights discourses, which assign fundamental rights as inherent in the European project basing them on a common European heritage. He contended that the CJEU "initiated a discourse on fundamental rights when national constitutional courts contested the principle of supremacy of Community law in the grounds that there were not enough guarantees that Community law would respect the fundamental rights guaranteed in national constitutions."[47]

Other authors have earlier pointed out double standards in the approach employed by the CJEU to fundamental rights – one standard for Community acts, another standard for the acts of the Member States. In the former, human rights are subordinate to and ought to be interpreted in the light of Community objectives. In the latter, human rights are presented as an additional hurdle for the validity of acts of national States.[48]

Albi expresses concern about the erosion of constitutional rights in EU law.[49] She points to the introduction of the CFREU in the European legal order, which as part of a

---

[43] In 2007 two main EU treaties were amended and restated: the Maastricht Treaty of 1992, now called the Treaty on European Union (TEU), and the Treaty of Rome (TEC), now called the Treaty on the Functioning of the European Union (TFEU).

[44] See Grainne de Burca 'After the EU Charter of Fundamental Rights: the Court of Justice as a Human Rights Adjudicator?' (2013) 20 Maastricht Journal of European and Comparative Law 168.

[45] Case C-36/02 *Omega Spielhallen und Automatenaufstellung v Oberburgermeisterin der Bundesstadt Bonn,* CJEU Judgment of 14 October 2004.

[46] Anneli Albi 'Erosion of Constitutional Rights in EU Law: A Call for Substantive Cooperative Constitutionalism' Part 1 [2015] 9/2 Vienna Journal of International Constitutional Law (ICL Journal) 151, p.159.

[47] Stijn Smismans 'The European Union's Fundamental Rights Myth' [2010] 1 JCMS 45.

[48] See Aidan O'Neill and Jason Coppel *The European Court of Justice Taking Rights Seriously?* (EUI, 1992), at p.31.

[49] Anneli Albi 'Erosion of Constitutional Rights in EU Law: A Call for Substantive Cooperative Constitutionalism' Part 2 [2015] 9/3 Vienna Journal of International Constitutional Law (ICL Journal) 291.

primary source of EU law initially uplifted hopes that the EU would acquire a more classical constitutional legal order rather than an economic type of constitutionalism.[50] However, after the *Melloni* case and Opinion 2/13 on Accession to the ECHR,[51] the CJEU came to consider the CFREU as another instrument for securing primacy, autonomy, effectiveness and uniform application of EU law, which would lead to lowering the standard of protection of national constitutional rights.[52]

In the field of data protection, whilst the present Chapter mainly demonstrates that EU instruments have had a positive impact on fundamental rights, it will be seen that the critical concerns have had some continued validity in relation to the Data Retention Directive, which will be explored in Section 5.3.2. below. The Data Retention Directive came to be subject to a large number of constitutional challenges in the Member States on the grounds of the introduction of blanket surveillance of electronic data, and was indeed eventually annulled by the CJEU.

5.2.3. The Relationship Between the CFREU and the ECHR, and the Added Value of the CFREU

5.2.3.1. Differences and Similarities in the Scope and Application of the CFREU and the ECHR

There are certain aspects that arise in respect of the importance, interpretation, and application of the CFREU by the CJEU and the Member States judiciary, and in respect of its usage by the EU in its external relations, which are important to outline in order to better understand the EU rules on data protection in comparison with the ECHR system.

The CFREU foresees some rights which are not initially envisaged by the ECHR, and currently are either covered more extensively by the CFREU or have no equivalent in the ECHR. Among those rights, which have no equivalent in the ECHR, the following groups of rights may be elucidated:

a) economic and social rights, such as the rights of workers (Article 27-31) to information and consultation within the undertaking, collective bargaining and action, access to placement services, protection from unjustified dismissal, and fair and just working conditions, as well as choose an occupation and engage in work and conduct a business (Articles 15-16);

[50] *Ibid,* p.297.
[51] Case C-399/11 *Melloni* [2013], Judgment of GC dated 26 February 2013; Opinion 2/13 of CJEU of 18 December 2014: Accession by the Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms.
[52] Albi n 46 above, p.297.

b) freedoms protecting family and children in connection with social and economic rights, such as prohibition of child work, family and professional life, social security, healthcare (Articles 32-35);
c) equality and non-discrimination (Articles 22, 24-26) ensuring cultural, religious and linguistic diversity, rights of the child and elderly and integration of disabled persons; and
d) other rights and freedoms, such as environmental and consumer protection (Articles 37-38).

Further, there are certain rights, which are contained in both the CFREU and the ECHR (including the protocols to the latter) and are covered more extensively under the CFREU.[53] These are the following:[54]

a) protection of personal data (Article 8);
b) right to marry and found a family (Article 9);
c) right to education (Article 14);
d) right not to be punished twice for the same crime (*ne bis in idem*) (Article 50).

The CFREU distinguishes the rights from principles, with the principles having more limited legal effect. Article 52(5) the CFREU indicates that principles can only be justiciable in the interpretation of legislative acts of the EU and acts of the Member States implementing EU law. The CFREU in comparison to the ECHR has its own specificities, which make its interpretation and application process different from the one of the ECHR. There are a few points to be explained in this regard.

First, the CFREU only applies within the scope of competence of EU law. This has been specified in Article 51(1) CFREU, whereby Member States are only bound by the provisions of the CFREU when they act in the scope of EU law; thus the scope of the CFREU application is not universal.[55]

Secondly, Article 52(1) CFREU sets out some limitations on the exercise of the rights and freedoms, declaring that such limitations must be provided by law, must be proportional and necessary to meet the goals of general interest recognized by the EU, including protection of rights and freedoms of others. It additionally seems relevant to mention that

[53] Here the author means that some rights, such as the right to personal data protection, are covered by the ECHR's protected right to private life, but since there are certain discrepancies in the scope of those two rights, the ECHR provides protection to a narrower range of aspects of personal data protection. For the differences between the right to private life and the right to data protection see the next Section of this Chapter.
[54] Explanations to CFREU enumerate the list of rights with the same meaning, but a wider scope than the ECHR. See Explanations Relating to the Charter of Fundamental Rights, OJEU, 2007/C 303/02, 14 December 2007, explanation to Article 52, Paragraph 3 CFREU.
[55] See Sionaidh Douglas-Scott 'The European Union and Human Rights after the Treaty of Lisbon' [2011] 4 HRLR 645.

whereas the ECHR provides specific grounds on the basis of which fundamental rights may be limited, CFREU refers to all goals of general interest recognized by the EU, i.e. that the grounds for limitation are much wider under the Charter.

Thirdly, Article 52(3) CFREU stipulates that those rights and freedoms, enshrined in the CFREU, which correspond to the rights guaranteed by the ECHR, shall be given at least the same scope and meaning as they are given in the ECHR. However, EU law may grant even more extensive protection to those rights. This essentially means that the rights and freedoms of absolute character under the ECHR shall be similarly treated as absolute rights under the CFREU.

Fourthly, there is a discussion that shapes our understanding of the importance of the CFREU as a human rights instrument. Such a discussion concerns the issue of whether the EU ought to accede to the ECHR. In 1996 the CJEU ruled that under the (then) Community law, the Community had no competence, express or implied, to accede to the ECHR, and in order to do so, it would bring about an amendment to the treaty.[56] The Treaty of Lisbon brought about such an amendment: Article 6(2) TEU obliges the EU in the future to accede to the ECHR. In 2014 the CJEU issued its Opinion 2/13 in respect of the draft agreement on accession of the EU to the ECHR.[57] The CJEU found that the draft agreement on accession was not compatible with TEU, mainly because it interfered with the autonomous nature of the European legal order, a conception, created and developed by the CJEU in its jurisprudence,[58] which could *inter alia* undermine the exclusive competence of the CJEU in interpretation, application of EU law and dispute resolution between the Member States.[59] Accession of the EU to the ECHR would have formalized the jurisdiction of the ECtHR over EU law giving rise to actions on challenging the EU legal instruments and measures directly before the ECtHR.[60]

Finally, the aim of the ECHR is to provide a basic floor of protection, in cases where the protection of freedoms and rights in the State has failed, whereas EU law, including the CFREU, is meant to create a uniform standard for all Member States. As discussed in Chapter 4, Subsection 4.1.3.4, the ECtHR in its jurisprudence employs the doctrine of margin

[56] Opinion 2/94 [1996] ECR-I-1759, paragraph 35.
[57] Opinion 2/13 of CJEU of 18 December 2014: Accession by the Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms.
[58] See ECJ, opinion 1/91, [1991], ECR I-6079; Joint cases C-402/05 and C-415/05 *Kadi and Al Barakaat International Foundation v Council and Commission*, CJEU, Judgment of 3 September 2008.
[59] For the importance and outcomes of the Court's opinion 2/13 see Christophe Hillion, Monica Claes and Sejla Imamovic (eds) *The EU Fundamental Rights Landscape After Opinion 2/13* (Maastricht Faculty of Law Working Paper 2016).
[60] Grainne de Burca Grainne de Burca 'The Evolution of the EU Human Rights Law' in Paul Craig and Grainne de Burca (Eds.) *The Evolution of EU Law* (Oxford Scholarship Online, 2021) 480, at p.488.

of appreciation, which is explicitly indicated in the text of the ECHR's Preamble.[61] The ECtHR does not act as a court of fourth instance. According to the principle of subsidiarity, the protection of human rights and fundamental freedoms is a primary responsibility of the States parties to the ECHR. The ECtHR in cases involving alleged violation of Article 8 of the ECHR rights may accord governments wide margin of appreciation when there is no 'European consensus' among the ECHR Member States. As Cameron points out:

> The ECHR is a minimum standard of rights protection (Article 53). It is complementary to the national mechanisms. Procedurally this is reinforced by the requirement that national remedies be exhausted before recourse is allowed to the ECtHR. Although the ECtHR frequently emphasises the subsidiarity principle, the task of the ECtHR is to determine in a concrete case whether the respondent state fulfills the minimum standards of the Convention.[62]

It may be argued that by incorporating the doctrine of margin of appreciation and the principle of subsidiarity into the fabric of the ECHR through adoption of Protocol No.15 in 2013, the Council of Europe has signaled its intention to defer to diverse values espoused by national authorities based on social, cultural and political differences.

In the absence of the 'European consensus', the ECtHR may be tending to accord wide margin of appreciation to the Member States. The CJEU, as it will be shown in Section 5.3 below, tends to protect EU market freedoms and promote the idea of a uniform and harmonized laws within the EU.

5.2.3.2. The CFREU References to the ECHR

The CFREU in its text makes a few references to ECHR. First, it mentions the ECHR in its Preamble, reflecting the idea of the CJEU that the fundamental rights enshrined in the CFREU result from the common constitutional traditions of the Member States and international agreements, such as the ECHR. As de Burca puts it, the CJEU, in *Stauder,*[63] *Internationale Handelsgesellschaft*[64] and *Nold,*[65] produced a new account of the

[61] Protocol No 15 amended the ECHR's Preamble and included the doctrine of 'margin of appreciation' and the principle of subsidiarity into the text of the ECHR. See Protocol No 15 Amending the Convention on the Protection of Human Rights and Fundamental Freedoms European dated 24 June 2013. Council of Europe Treaty Series – No 213.
[62] See Iain Cameron 'Competing Rights?' in Sybe de Vries, Ulf Bernitz and Stephen Weatherill (eds) *The Protection of Fundamental Rights in the EU after Lisbon* (Hart Publishing Ltd., 2013) 181-206, at 189.
[63] Case 29/69 *Stauder v City of Ulm*, Judgment of 12 November 1969.
[64] Case 11/70 *Internationale Handelsgeselschaft,* Judgment of 17 December 1970.
[65] Case 4/73 *Nold v Commission*, Judgment of 14 May 1974.

constitutional role of human rights in the EC legal order.[66] Fundamental rights inspired by international human rights treaties became part of the general principles of Community law.[67]

Secondly, Article 52(3) CFREU stipulates that the meaning and the scope of those rights and freedoms, which correspond to the rights guaranteed by the ECHR, ought to be the same as laid down in the ECHR. That provision was clearly intended to promote harmony between the provisions of the CFREU and the ECHR, giving room for developing a more extensive protection than is provided by the ECHR.[68] However, some authors noted that the CJEU has changed its approach to using the ECHR as a material source of EU law after the CFREU entered into legal force in 2009.[69] Before 2009[70] the CJEU extensively referred to the ECHR (and the ECtHR jurisprudence) in its case law while after 2009 the CJEU has dramatically reduced references to the ECHR or other international human rights instruments.[71]

Thirdly, Article 53 CFREU establishes that nothing in the CFREU must be interpreted as restricting or adversely affecting human rights as recognized by EU law and international law, and by international agreements including the ECHR, and by the Member States' constitutions. The CJEU however, as established in *Melloni,*[72] does not allow Member States to interpret Article 53 CFREU to elevate the human rights protection standards in the Member States to make them effectively higher than the EU human rights standards when the primacy, unity, and effectiveness of EU law risks being compromised. This is a fundamental difference between the ECHR and EU law, in that the ECHR allows a higher standard of protection under national law, whereas EU law prioritizes uniformity. Lenaerts further suggests that Article 53 CFREU, read in conjunction with Article 52(3) CFREU, preserves the constitutional autonomy of EU law, if, hypothetically, the ECtHR ever decides to lower the standard of protection below that guaranteed by the EU law; the

[66] Grainne de Burca, n 60 above.
[67] *Ibid.,* p.489.
[68] Grainne de Burca 'Human Rights in the EU' in Paul Craig and Grainne de Burca (Eds.) *EU Law. Text, Cases and Materials* (Fifth Edition, OUP, 2011) at pp.367 and 397-398.
[69] See Katja Ziegler 'Autonomy: From Myth to Reality – or Hubris on a Tightrope? EU Law, Human Rights and International Law' (2015) University of Leicester School of Law, Research Paper No 15-25; Grainne de Burca 'The Evolution of the EU Human Rights Law' in Paul Craig and Grainne de Burca (Eds.) *The Evolution of EU Law* (Oxford Scholarship Online, 2021) 480, at p.498.
[70] Starting with the *Nold* case in 1974. See n 65 above.
[71] It must be noted that the other international human rights instruments, such as the ICCPR or American Convention on Human Rights, have been referred to by the CJEU in its case law less extensively than ECHR even before 2009. See Ziegler, n 69 above, at p.26.
[72] C-399/11 *Stefano Melloni v Ministerio Fiscal,* CJEU Judgment of 26 February 2013.

CJEU will then be precluded from interpreting the provisions of the CFREU in a regressive manner.[73]

The above-mentioned provisions of Articles 52 and 53 CFREU could be regarded as an attempt to establish a formal institutional relationship between the two human rights systems, but Opinion 2/13 of the CJEU dramatically abrupted such endeavour.[74]

5.3. Secondary EU Legislation on Data Protection: The DPD, the DRD and the GDPR

The adherence of the EU to its values and fundamental rights on the one hand, and its focus on the attainment of market freedoms on the other hand, have found their reflection in the secondary legislation acts of the EU, such as the Data Protection Directive (DPD), which was in force in 1995 to 2018, the Data Retention Directive (DRD),[75] in force from 2006 to 2014, and the General Data Protection Regulation (GDPR),[76] in force since 2018.

5.3.1. The Data Protection Directive 95/46/EC of 1995 (DPD)

The Data Protection Directive (DPD) was an instrument for achieving the goals of an EU internal market. It was designed to foster closer economic relations between the Member States and by a common action to eliminate the barriers dividing Europe.[77] At the same time, such a goal of achieving a functioning internal market requires that the fundamental rights are safeguarded.[78] The DPD was adopted five years before a formal EU bill of rights, i.e., the CFREU, was declared, and therefore its wording reflecting the right to privacy was different from the one used in the CFREU later.

In some other instances, the DPD separated the notion of fundamental rights and privacy of individuals from each other, enumerating them as two separate values, which ought to be protected from certain infringements.[79] A collocation 'data protection' could be

[73] Koen Lenaerts 'Exploring the Limits of the EU Charter of the Fundamental Rights' (2012) 8 EuConst 375.
[74] See de Burca n 60 above, at p.496.
[75] Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54. It was found invalid by the CJEU's judgment in the *Digital Rights Ireland* case in 2014 (Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others,* Judgement of the GC dated 8 April 2014).
[76] There are also other EU directives, such as Directive 2000/31/EC on electronic commerce dated 8 June 2000, Directive 2002/58/EC (E-Privacy Directive) dated 12 July 2002, or Directive (EU) 2016/680 on data protection during criminal investigations dated 27 April 2016 etc., which are not part of this Chapter.
[77] See DPD, n 3 above, Paragraph 1.
[78] *Ibid.,* Paragraph 3.
[79] *Ibid.,* Paragraphs 33 and 34.

found in a few instances in the entire text of the DPD, where it mainly appeared in the context of an official in charge of data protection matters within a company (controller).[80]

Drafters of the DPD considered that the Member States provided a different level of protection of rights and freedom, specifically the right to privacy with regard to data processing.[81] Such differences in level of protection could prevent the transmission of personal data from the territory of one Member State to the territory of another Member State, which could be detrimental to economic activities and competition within the EU common market.[82]

When personal data was transferred from one Member State to another, a definition of 'cross-border' flow of data was used by the DPD.[83] A 'cross-border' transmission of personal data was one of the core issues regulated by the DPD. As directives have limited direct effect in the Member States, the latter were supposed to transpose provisions of the DPD into their national legislation in order to bring laws of different Member States on data protection closer to each other. The differences however remained, as the DPD did not harmonize data protection laws of the Member States to the maximum extent.[84]

It was crucial to define data protection law, which Member State would apply to each cross-border data processing. The DPD sought to resolve this issue by introducing a conflict of laws provision,[85] through which a Member State would apply its national data protection law, if data processing took place in the context of the activities of an establishment of the controller on the territory of that Member State.[86] In case the controller has many establishments on the territory of different Member States, the DPD prescribed that each such establishment of the controller had to comply with the laws of the country of its establishment, confirming that there could be different regimes of regulating data protection in different Member States.

Some authors raised questions about what exactly was the role of a conflict of laws provision within the DPD, and more importantly, how that provision related to the other parts of the directive.[87] The text of the DPD did not clearly resolve the conflict of laws issue

[80] *Ibid.,* Paragraphs 49 and 54, Article 16, Paragraph 2 and Article 20, Paragraph 2.
[81] *Ibid.,* Paragraph 7.
[82] *Ibid.*
[83] *Ibid.,* Paragraphs 5, 6 and 8.
[84] Such harmonization was achieved later when GDPR was introduced.
[85] Article 4 DPD is called 'National Law Applicable'.
[86] See Article 4(1)(a) DPD.
[87] See Lee Bygrave *Data Privacy Law: An International Perspective* (OUP, 2014), 199.

among Member States. That has changed relatively recently, as Svantesson notes, not least due to the Internet.[88] In 2012 the EU decided to revise its entire data protection regime.[89]

After Snowden revelations,[90] the issue of the use of personal data of EU residents by foreign, predominantly US-based controllers, has become even more important. The CJEU stepped in to resolve the problem of conflict of laws in its two judgments: *Google Spain*[91] and *Weltimmo.*[92] The CJEU has interpreted the term 'establishment' in Article 4(1)(a) DPD broadly enough to conclude that a more formalistic approach in defining 'establishment' would not serve the purpose of protecting the rights of EU data subjects.[93]

The current interpretation of the term 'establishment' is based on the understanding of the CJEU of this notion under the DPD. There are two main characteristics, which the Court has pointed out in the two above-mentioned cases:[94] 1) the processing carried out in the context of an establishment of a controller does not necessarily mean that such processing is carried out by or through such an establishment.[95] However, such processing must be 'inextricably linked' with the activity of the establishment of the controller in the Member State,[96] and 2) it is not necessary that an establishment is registered or present in any legal form on the territory of another Member State – only one representative in certain circumstances even with minimal activity could be sufficient to constitute stable arrangement, if they act with a sufficient degree of stability.[97]

Advocate General (AG) Villalon in his opinion in the *Weltimmo* case points to the dual nature of the conflict of laws provision in Article 4(1)(a): on the one hand, making reference to the interpretation of the CJEU in the *Google Spain* case, where the actual processing took place outside the EU, he suggested that the respective provision enabled the application of

---

[88] Dan Janker B. Svantesson "Article 4(1)(a) 'establishment of the controller in EU data privacy law – time to rein in this expanding concept?' (2016) 6 International Data Protection Law 210.

[89] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regards to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation), COM (2012) 11 final (Jan.25, 2012).

[90] In 2013 Edward Snowden, an employee of the NSA has disclosed information about the US secret surveillance programs, such as PRISM to the journalists. It was revealed that bulk of personal information, including sensitive information of EU citizens were extracted from such social media platforms as Facebook and Google, and used by the US Government for their purposes.

[91] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez,* EU:C:2014:317.

[92] Case C-203/14 *Weltimmo s.r.o. v Nemzeti Adatvedelmi es Informacioszabadsag Hatosag,* Judgment of 1 October 2015.

[93] 'Data subject' means an identified or identifiable natural person under Article 4(1) GDPR

[94] For more detailed review of *Google Spain and Weltimmo* cases see Diana Sancho 'The Concept of Establishment and Data Protection Law: Rethinking Establishment' (2017) 42 E L Rev 491; and Dan Janker Svantesson 'The CJEU's Weltimmo Data Privacy Ruling: Lost in the Data Privacy Turmoil, Yet So Very Important' (2016) 23 Maastricht Journal of European and Comparative Law 332

[95] See *Google Spain* n 91 above, para.52. This interpretation became a rule under GDPR Article 3(1): "…regardless of whether the processing takes place within the Union or not".

[96] *Google Spain* n 91 above, para.56

[97] See *Weltimmo* n 92 above, paras.29-30.

EU law through the law of one of the Member States, while, on the other hand, he contended that that provision had operated as a rule for determining the applicable law as between Member States.[98] Since the *Weltimmo* case was about an internal conflict of laws between two Member States, AG Villalon focused his further analysis on the latter characteristic of that provision, and did not understandably elaborate the former one. Villalon's suggestion concerning the application of EU law through the domestic law of one of the Member States may be taken as an existence of external conflict of laws, i.e., the conflict between EU law on the one hand, and third country law on the other hand.

The DPD used the term 'transfer' of personal data in respect of data flows from a Member State to a third country, i.e., outside the EU. This was supposedly considered by the DPD drafters to be even a greater issue than (an inter-EU) cross-border flow of personal data.[99] How data privacy would be protected, if a data processing breach, which could lead to a violation of privacy, happened outside the EU, but data subjects (i.e., individuals) residing within the EU, were affected by such violation? The DPD drafters attempted at extending the application of the DPD beyond EU borders.

In Article 4 (1)(c) DPD, the drafters have foreseen situations when a data controller has no legal presence in the territory of the EU Member States but nevertheless makes use of certain equipment located on the territory of a Member State. This has added more confusion rather than solved the problem. According to Svantesson, the DPD 'predates extensive cross-border Internet communication', and was mainly concerned with intra-EU data flows'.[100] The DPD, however, has set certain rules related to the trans-border flow of personal data in its Articles 25 and 26.[101]

A general rule stemming from those provisions of the DPD is that a transfer of personal data to third countries (i.e., outside the EU) would be prohibited unless such third countries provide an adequate level of data protection. There are two types of derogations foreseen in the DPD from that general rule. First, such an international transfer of personal data may be allowed even if there is no adequate level of protection provided in the country, but there are certain cases, when such a transfer shall be deemed legal. For instance, when a data subject gives their unambiguous consent to the data transfer, or when a transfer is necessary for

---

[98] Opinion of Advocate General Cruz Villalon in *Weltimmo s.r.o. v Nemzeti Adatvedelmi es Informacioszabadsag Hatosag,* (Case C-203/14), EU:C:2015:426, para.23.

[99] Not only DPD mentioned 'transfer' of personal data to third countries many times in its preamble (paragraphs 37, 56-58, 60 and 66), but it also devoted a separate chapter (Chapter IV) to regulate data transfer to third countries. See DPD, n 3 above, Articles 25-26.

[100] Dan Janker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on US Businesses' (2014) 50 Stan. J. Int'l. Law 53.

[101] For an overview of Articles 25 and 26 DPD, see Christopher Kuner 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 4 IDPL 235.

conclusion of contract between data subject and a controller.[102] Secondly, trans-border flow of personal data may be conducted in case the controllers provide an adequate safeguard in the appropriate contractual clauses to protect privacy and other fundamental rights.[103]

The European Commission has a decisive role in defining whether or not a third country in question puts in place internal legislation, which would provide an adequate level of protection.[104] Since the year 2000, adequacy decisions have been rendered in respect of only fifteen countries or territories.[105] The USA for more than two decades has had special arrangements with the EU, called 'Safe Harbour'[106] and 'Privacy Shield'.[107] These arrangements were later found invalid by the CJEU[108] as providing an inadequate level of protection of individuals' fundamental rights. This thesis will touch upon this issue later in the GDPR sub-section. In 2023, the European Commission adopted a new adequacy decision for the EU-US Data Privacy Framework.

The mass data collected and processed by private companies (controllers and processors) for their business purposes created an opportunity for the States to make use of such data for preventing and combatting crime. As the DPD obliged private controllers and processors to delete personal data after it had been processed and had served the purpose of its collection, the State authorities conducting crime investigations had limited possibilities to meaningfully use personal data in their activity. As Bignami puts it, the DPD was designed to regulate market actors, not the police.[109] The emergence of data retention law was initially seen as a necessary step for the States to exercise their powers of national security and law enforcement.[110]

---

[102] See DPD, n 3 above, Article 26(1).
[103] *Ibid.,* Article 26(2).
[104] *Ibid.,* Article 25.
[105] Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, United States of America and Uruguay. See: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed on 12 March 2024.
[106] EU Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), *Official Journal L 215 , 25/08/2000 P. 0007 – 0047.*
[107] EU Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), *OJ L 207, 1.8.2016, p. 1–112.*
[108] See Case C-362/14 *Maximillian Schrems v Data Protection Commissioner,* Judgment of the GC dated 6 October 2015 and Case C-311/18 *Data Protection Commissioner v Facebook and Maximillian Schrems,* Judgment of the GC dated 16 July 2020.
[109] Francesca Bignami 'Privacy and Law Enforcement in the European Union: The Data Retention Directive' (2007) 8 Chicago Journal of International Law 233, p.237.
[110] *Ibid.,* p.233.

5.3.2. The Data Retention Directive 2006/24/EC of 2006 (DRD)

Whilst EU measures have mostly advanced fundamental rights protection in the field of data protection, it is fitting to mention a problematic episode in this field as regards the Data Retention Directive (DRD). This Directive, which came to be widely contested through constitutional challenges in the Member States on the grounds of concerns about the introduction of bulk retention of electronic data, was eventually annulled by the CJEU. As discussed earlier in Section 5.1., the CJEU referred to fundamental rights stipulated in the CFREU as a basis for invalidating the DRD.

The Data Retention Directive was adopted in 2006 and was rendered invalid by the CJEU judgment in the *Digital Right Ireland*[111] case in 2014. Although the DRD is not valid for many years now, the present author believes it is important to explain the role it played in the development of the right to data protection and privacy.

As Albi points out, in the process of transposition of the DRD to national law, the Directive became regarded as an instrument for Orwellian surveillance by government agencies of people's lives, since law enforcement agencies had access to all necessary communication data specifically retained by the private controllers for the purposes of surveillance.[112] According to her, tens of thousands of people in Germany and Austria filed claims to the respective constitutional courts, and in a large number of States, challenges were brought by members of parliaments, data protection agencies, civil society groups, and other stakeholders.[113]

The DRD did not concern the content data, it was all about retention of metadata (or communication data), i.e., information about communication, such as time and place of sending or receiving communications, addressees or senders of those communications, frequency and timing of sending or receiving communications etc. Metadata has proved to be very useful for law enforcement agencies in their strive for the prevention of crimes and terrorist attacks. Security forces and police could easily track alleged terrorists by processing large amounts of metadata held by telecommunication companies.

By the time of the adoption of the DRD in the aftermath of terrorist attacks in the US in 2001 and the London bombings in 2005, it was a generally accepted understanding among the EU Member States that future terrorist attacks could be prevented through imposing

[111] C-594/12 *Digital Rights Ireland and Others,* Judgment of the GC dated 8 April 2014.
[112] Anneli Albi "The EU Data Retention Directive in Twenty-Eight Member States: An emblematic case study of blind spots, lost higher national standards and systemic flaws in autonomous EU human rights law and discourse" p.19. Unpublished paper, cited with the permission of the author.
[113] Albi, *ibid.*

comprehensive legislative framework for surveillance used by security forces as well as police.[114] The European policy focus has shifted from one of data protection to data retention, in order to ensure that the collected data is made available for the purposes of investigation of serious crimes.[115]

The DRD was drafted as an EU legislative act that would harmonize the laws of the Member States[116] because of legal and technical differences between national data retention laws, which were in place for the purposes of 'prevention, investigation, detection, and prosecution of criminal offenses'.[117] The DRD established that telephone and Internet service providers must collect and retain metadata, including emails and phone calls, for a period from six months up to two years.[118] The DRD, however, left discretion to Member States in determining cases that would justify access to retained data by law enforcement agencies.[119]

The DRD makes reference to the DPD specifying that it requires Member States to protect the rights and freedoms of individuals concerning their personal data processing, especially the right to privacy.[120] It makes reference to Article 8 ECHR containing the right to private life and correspondence. It specifically mentions a balancing mechanism foreseen by the ECHR: '[p]ublic authorities may interfere with the exercise of that right only in accordance with the law, and where necessary in a democratic society'.[121] Finally, the DRD declares that it respects fundamental rights enshrined in the CFREU, specifically the right to private life (Article 7) and the right to data protection (Article 8).[122] However, the main aim of the DRD was in contrast with the main goal of the DPD. The DPD was enacted to protect fundamental rights, particularly, the right to privacy, while the DRD was designed to harmonize the differing national laws of the Member States on data retention[123] because the DRD allowed Member States to adopt legislative measures to restrict their obligations under

[114] See Federico Fabbrini 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' (2015) 28 Harvard Human Rights Journal 65.
[115] Arianna Vedaschi and Valerio Lubello 'Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective' (2014) 20 Tilburg Law Review 14, p.18.
[116] See DRD, n 5 above, Article 1, Paragraph 1.
[117] See DRD, n 5 above, Recital 6.
[118] See DRD, n 5 above, Article 6.
[119] See DRD, n 5 above, Recital 1.
[120] *Ibid.*
[121] See DRD, n 5 above, Recital 9.
[122] See DRD, n 5 above, Recital 22.
[123] See Arianna Vedaschi and Valerio Lubello, n 115 above, p.18

the DRD for purposes of safeguarding national security, defense and fighting criminal offenses.[124]

The validity of the DRD was first challenged in the CJEU by Ireland, supported by the Slovak Republic in 2006 in the case of *Ireland v Parliament and Council.*[125] Ireland argued that almost the sole purpose of the Directive was to facilitate the investigation, detection, and prosecution of crime rather than harmonization of the internal market. The DRD, thus, would have been adopted under the then Third Pillar – the Area of Freedom, Security and Justice (AFSJ), not the then First Pillar – the European Communities, or economic, social and environmental policies.[126]

The Slovak Government brought up a fundamental rights discourse to the case by claiming that the DRD paved the way to extensive interference with the right of individuals to privacy and questioned whether such interference could be justified on economic grounds.[127] The CJEU rejected the claim of Ireland and did not examine the claims and arguments of the Slovak Government at all in its judgment of 2009. The CJEU thus focused on the protection of the single market rather than the protection of fundamental rights of individuals.[128]

The *Digital Rights Ireland*[129] judgment of the CJEU, which declared the DRD invalid as contrary to EU law, represents a milestone decision in the area of privacy rights in the digital age.[130] It was the second legal challenge to the DRD after the *Ireland v Parliament and Council* case mentioned above. Two national courts: the Austrian Constitutional Court on the request of individual petitioners (Mr. Seitlinger and more than 11,000 other individuals) and the High Court of Ireland on the request of an advocacy and lobbying group "Digital Rights Ireland" requested a preliminary ruling by the CJEU, so there were many petitions challenging the national laws of the Member States related to the implementation of the DRD before the national courts.[131]

The CJEU ruled that the DRD failed to provide sufficient safeguards for the protection of the right to privacy. It did not clearly define what data was to be retained, who could access it, and for what purposes it could be used. The CJEU was engaged in a balancing

[124] See Federico Fabbrini 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' (2016) 28 Harvard Human Rights Journal 66.
[125] Case C-301/06 *Ireland v Parliament and Council,* CJEU Judgment of 10 February 2009.
[126] *Ireland v Parliament and Council, ibid.* Paragraph 28.
[127] *Ireland v Parliament and Council, ibid.* Paragraph 34.
[128] See Anneli Albi, n 112 above, p.33.
[129] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others,* Judgment of the GC dated 8 April 2014.
[130] Federico Fabbrini, n 124 above.
[131] See for details Anneli Albi, n 112 above, p.34.

exercise of the right to privacy and data protection on the one side, and ensuring national security and crime prevention, on the other. It opened up fundamental questions regarding the acceptable limits of mass surveillance and the function of the right to privacy.[132]

The CJEU made references to the ECtHR while examining the proportionality of the measures stipulated in the DRD with the fundamental rights to private life and data protection. Some authors considered such an exercise by the CJEU as adopting a methodological approach of the ECtHR in *S. and Marper v UK.*[133] The CJEU held that the DRD met the first layer of proportionality analysis – the Court has found that generally retention of personal data is considered appropriate for the purposes of investigation of serious crimes.[134] The DRD, however, according to the CJEU, has not passed the second layer of proportionality analysis – a necessity test.[135] The CJEU has held that in respect of the necessity for the retention of personal data

> […]it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.[136]

As mentioned earlier, the DRD was widely contested in a large number of constitutional courts of the Member States[137] before it was eventually annulled by the CJEU in the second case.[138] The main reason for challenging the DRD is that it was widely regarded as a very far-reaching measure introducing mass-scale surveillance.

---

[132] See Andrew Roberts 'Privacy, Data Retention and Domination: *Digital Rights Ireland Ltd v Minister for Communications*' (2015) 78(3) Modern Law Review 522.
[133] *Ibid.*
[134] *Digital Rights Ireland and Others,* n 111 above, Paragraph 49.
[135] See more analysis on this in Federico Fabbrini, n 124 above.
[136] *Digital Rights Ireland and Others,* n 111 above, Paragraph 51.
[137] See Anneli Albi 'Erosion of Constitutional Rights in EU Law: A Call for Substantive Cooperative Constitutionalism' Part 1 [2015] 9/2 Vienna Journal of International Constitutional Law (ICL Journal) 151
[138] The first case, where CJEU examined DRD was *Ireland v Council.* In that case CJEU did not annul DRD. See Case C-301/06 *Ireland v Council,* Judgment of 10 February 2009.

5.3.3. The General Data Protection Regulation (EU) 216/679 of 2016 (GDPR)

5.3.3.1. General Overview

The General Data Protection Regulation of the EU (GDPR) as an instrument of EU law has harmonized the data protection legislation of the EU Member States and has a direct effect on their territories. The GDPR has emerged as a result of a number of different factors influencing the market of goods and services, as well as capital, in the EU. It was drafted with a view to protecting the fundamental rights of data subjects – individuals in the era of advanced technologies, such as the Internet. In its Preamble, paragraphs (1) and (2), the GDPR is clear that while being a fundamental right of natural persons, the right to data protection stems from the founding agreement of the EU – TFEU.[139] It further declares in the Preamble, paragraph (4), that the GDPR particularly respects the right to private life as recognized in the CFREU and enshrined in the Treaty of Lisbon.[140]

The GDPR sets a list of principles for data processing, which would be respected. In its Article 5, it reiterates two main principles: lawfulness and fairness of data processing, and adds one about transparency.[141] According to van der Sloot, 'transparency' has been one of the pillars of data processing even before, and the GDPR has transformed it from an obligation to notify general public about data processing into the right of individual data subject to be notified 'when a data leak has a potentially detrimental effect on his personal interests'.[142] Personal data must be processed only for legitimate purposes, and must not be processed further if it becomes incompatible with the initial purposes.[143] It must be relevant content-wise and in volume, and must be kept accurate and in the form necessary to identify individuals and for the period necessary for the purposes, for which such data was collected.[144]

Lawfulness of data protection comprises an express consent of the data subject to data processing or other legitimate grounds for data processing.[145] The lawfulness and

[139] In 2007 two main EU treaties were amended and restated: the Maastricht Treaty of 1992, now called Treaty on European Union (TEU), and the Treaty of Rome (TEC), now called the Treaty on the Functioning of the European Union (TFEU). Article 16(1) of the TFEU establishes that everyone has the right to the protection of personal data concerning them.
[140] *Ibid.*
[141] DPD refers mainly to lawful and fair data processing only. See DPD n 3 above, Recital 28, Article 6(1)(a).
[142] Bart van der Sloot 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 IDPL 307.
[143] GDPR, n 4 above, Article 5(1)(b).
[144] GDPR, n 4 above, Article 5(1)(c-e).
[145] Article 6(1)(b) GDPR enumerates those legal grounds: processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of

fairness of data processing will be examined in Section 5.4 later in the sub-section devoted to the comparison between the right to privacy and the right to data protection. Van der Sloot indicates that the GDPR emphasizes (i) increasingly detailed and specific obligations for data controllers, (ii) specific data processing rights of individuals, and (iii) an increased level of enforcement.[146]

The GDPR expressly ensures the right of individuals to erasure, which is called the right to be forgotten.[147] This right has been earlier pronounced by the CJEU in the *Google Spain* case.[148] Individuals have the right to obtain from the controller the erasure of their personal data, and the controllers, respectively, are obliged to erase such personal data without undue delay. Erasure takes place on certain legal grounds stipulated in the GDPR, such as if personal data is no longer necessary for data processing, or an individual withdraws their initial consent or objects to the data processing, etc.[149]

5.3.3.2. Extraterritorial Application of the GDPR

One of the most debated and controversial legal aspects of the GDPR is its extraterritorial application.[150] Under public international law, the State's sovereignty implies that the laws of the State apply within the territorial boundaries of that State. In transborder activity or events, the laws of one State may spread their application to the things, people, or events, which are initially supposed to be under the ambit of the laws of another State. A data protection law regulates activities mainly occurring in virtual reality, which is borderless. This poses certain challenges in the application of such laws. Bearing in mind that the GDPR was enacted to provide better protection of fundamental rights to private life and data protection, it may be of interest to explore how the application of the GDPR beyond the EU borders may influence perception of privacy both within and outside the EU.

There is a fair share of academic writings on both jurisdictional issues of data protection, and transborder flow of personal data.[151] A few attempts were made to build a

another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[146] Bart van der Sloot n 142 above, p.309.

[147] Article 17 GDPR. See GDPR n 4 above.

[148] See *Google Spain*, n 91 above.

[149] Article 17(1) GDPR. See GDPR n 4 above.

[150] See Lee Bygrave *Data Privacy Law*: *An International Perspective* (UOP 2014) 199; Dan Jerker B. Svantesson 'Extraterritoriality and Targeting in EU Data. Privacy Law: the Weak Spot Undermining the Regulation' (2015) 4 International Data Privacy Law 226, 228

[151] See e.g., Dan Janker B. Svantesson "Article 4(1)(a) 'establishment of the controller in EU data privacy law – time to rein in this expanding concept?' (2016) 6 International Data Protection Law 210; Paul de Hert and

nexus between those two aspects: jurisdiction and transfer of personal data abroad,[152] as those areas, although intertwined in the sense that the application of EU law may reach a latitude far beyond its territorial ambit, remain different in terms of their respective purpose, parties or stakeholders involved and, oddly enough, geographical application. The jurisdictional part of the GDPR is enshrined in its Article 3, called 'Territorial Scope', while the main provisions on the free flow of personal data abroad are stipulated in Articles 44-50 GDPR.

Article 3 GDPR consists of three paragraphs, where the last paragraph is related to the situations, when laws of the EU Member States apply by virtue of public international law, i.e., within the Member States diplomatic missions abroad or on board of the Member States ships or aircrafts.[153] That paragraph however shall remain out of the focus of this thesis, as there are no extensive debates on any legal controversy in respect of the territorial extension of the law within the diplomatic posts.[154]

First two paragraphs of Article 3 GDPR are designed to enshrine the territorial link of application of this legislative act to persons and a conduct. Such a link is mainly a twofold:

1) The GDPR is applicable to any processing of data of natural persons, when such processing is carried out in the context of an establishment of those who process personal data (processors), or those who determine the purposes and means of such data processing (controllers). Such an establishment must be located in the EU; or
2) The GDPR would be applicable to data processing carried out by the controllers and processors located outside of the EU, which takes place in respect of those natural persons, who happen to be in the EU at the time of such processing.

Michal Czerniawski 'Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context' (2016) 6 International Data Protection Law 230; Federico Fabrini and Edoardo Celeste 'The Right to be Forgotten in the Digital Age: the Challenges of Data Protection Beyond Borders' (2020) 21 German Law Journal 55; Stefano Saluzzo 'The Principle of Territoriality in EU Data Protection Law' in T.Natoli and A. Riccardi (eds), *Borders, Legal Spaces and Territories in Contemporary International Law* (Springer Nature Switzerland AG and G Giappichelli Editore 2019) 121.

[152] Christopher Kuner, Chapter 6 'Applicable Law, Extraterritoriality and Transborder Flows in Christopher Kuner *Transborder Data Flows and Data Privacy Law* (Oxford Scholarship Online 2013); Benjamine Greze, 'The Extraterritorial Enforcement of the GDPR: a Genuine Issue and the Quest for Alternatives' (2019) 9 International Data Protection Law 109; Paul de Hert and Michal Czerniawski 'Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context' (2016) 6 International Data Protection Law 230

[153] See Recital 25 GDPR and Chapter 3 of the EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)

[154] For a critical analysis of Article 3(3) GDPR, however, see Claire Jervis 'The Curious Case of Article 3(3) of the GDPR and its application to Diplomatic Missions [2020] 1 International Data Privacy Law 107.

The idea was thus to cover as many controllers and processors globally, as possible, and to protect personal data of as many natural persons as possible.[155] The European Data Protection Board[156] has even claimed that the GDPR protects non-EU nationals, who are not in the EU, even if the data processing takes place outside the EU, but the controller is located in the EU.[157] Such ambitious intentions, however, need a nuanced regulation in order to exclude legal uncertainties, which may lead to different interpretations of the GDPR by different stakeholders.

The transfer of personal data from the EU to third countries is given special attention in the GDPR. Article 45 envisages that such a transfer is possible if the European Commission decides that the third country ensures an adequate level of protection of personal data. In *Schrems I*, the CJEU has for the first time pronounced that an adequate level of protection of personal data in third countries would not necessarily mean an identical level of protection. It is enough to ensure protection essentially equivalent to that guaranteed within the EU.[158] The wording for this standard of 'essential equivalency' was then borrowed by the GDPR.[159]

Article 45 GDPR establishes that the European Commission, when rendering an adequacy decision, must make a proper assessment of the laws of third countries related to data protection, along with the laws related to public and national security, defense, criminal law, and the access of public authorities to personal data of individuals. The enforceability of the rights of data subjects, the implementation of the laws, and the existence and effective functioning of an independent supervisory authority, are also assessed by the European Commission. Moreover, such general concepts as the rule of law and the respect for human rights and fundamental freedoms, are subject to the assessment of the European Commission.[160]

---

[155] Within the drafting process of GDPR the Commission in its communication to the Parliament has stated that the EU data protection standards had to apply regardless of the geographical location of a company or its processing activity. See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, COM (2012) 09 final (25 Jan. 2012), p.10

[156] The European Data Protection Board is an independent body of the EU established by the GDPR to ensure the consistent application of the GDPR. See Articles 68-76 GDPR for more detailed information.

[157] See EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1 dated 12 November 2019, p. 9, as well as EDPB's predecessor – Article 29 Data Protection Working Party's Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, p. 7 made such assertion in respect of data processing through making use of the controller's equipment located in the EU

[158] See Case C-362/14 *Maximillian Schrems v Data Protection Commissioner,* Judgment of the GC dated 6 October 2015, Paragraphs 73-74. This case is called 'Schrems I' as there was a subsequent case in 2020, which is called 'Schrems II'. Schrems I abolished the 'Safe Harbour' arrangement, while the Schrems II judgment rendered the 'Privacy Shield' decision of the European Commission invalid.

[159] See GDPR, n 4 above, Recital 104, and Article 45.

[160] GDPR, n 4 above, Article 45, Paragraphs (2a) and (2b).

When such a decision of the European Commission is made, subject to periodic revisions, at least once in four years, personal data of those who reside in the EU,[161] is freely transferred to that third country, in respect of which a decision was made. No consent of data subjects is necessary for the free flow of personal data under such arrangements. Nor is there a need to ensure the existence and functioning of other safeguards. An adequacy decision by the European Commission may look like a *carte blanche* for the controllers and processors in the third country in question to process the personal data of those who are in the EU. In reality, such controllers and processors are under strict obligation to observe the laws on data protection of their own country, and such laws are effectively implemented. They comply with the EU standards of data protection through complying with the similar, or 'essentially equivalent' standards of their own country.

A long list of criteria for establishing whether or not the laws of third countries provide essentially equivalent protection of personal data, a wide range of factors affecting such a decision, and ambiguous concepts of the rule of law and the respect for human rights, which the European Commission assesses in respect of each third country, make it difficult for many countries to receive such a decision in the first place. As was mentioned earlier in the sub-section devoted to the DPD, only 15 countries received such a decision within the last 22 years.[162]

In the absence of an adequacy decision a transfer of personal data to third countries is still possible due to other legal grounds for transferring personal data outside the EU borders, such as binding corporate rules, standard data protection clauses adopted or approved by the European Commission, approved code of conduct and contractual clauses.[163] These safeguards reflect an obligation of controllers and processors in third countries, which are mainly private entities, while an adequacy decision mechanism is more directed at the governments of third countries to secure a mechanism and national legislation, which would guarantee an adequate level of protection of personal data.

The provisions of the GDPR on 'adequacy decisions' are similar to those of the DPD, albeit with certain differences. Adequacy decisions under the DPD linked to a concrete transfer or set of transfers.[164] Under the GPDR, on the other hand, the European Commission assesses the situation in a given country or territory more generally, paving the way for future

[161] GDPR technically does not use the term 'reside in EU' or 'EU residents'. Article 3, Paragraph 2 indicates that GDPR applies to the processing of personal data of data subjects, who are in the EU.
[162] See n 105 above.
[163] See Article 46 GDPR.
[164] Article 25, Paragraph 2 DPD reads: "The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations […]"

transfers to that country.[165] The first case under the GDPR, which challenged the adequacy decision of the European Commission, was the *Schrems II* judgment.[166] The CJEU in that case has found that the 'Privacy Shield' arrangement with the USA was contrary to the requirements of the CFREU, namely, the right to private life and the right to data protection, and therefore found that such arrangements reflected an inadequate level of protection of personal data in the United States.

The CJEU in *Schrems II* reiterated its finding in the *Schrems I* judgment that the term 'adequate level of protection' of personal data must be understood as requiring the third country to ensure a level of protection of fundamental rights and freedoms, which are 'essentially equivalent to those guaranteed within the EU by virtue of the GDPR read in the light of the CFREU.[167] The CJEU in that case went on to further declare that other than the adequacy decision safeguards, guaranteed by the GDPR, such as standard data protection clauses, must provide individuals a level of protection of their personal data essentially equivalent to that which is secured in the EU.[168]

This was an attempt to find a single standard of protection, which, in the opinion of some authors, is difficult to reconcile with the differentiated terms used in the GDPR for different types of safeguards.[169] Indeed, for adequacy decisions (Article 45), the GDPR uses the term 'adequate level of protection'; for other safeguards (Article 46) – 'appropriate safeguards', for derogation from adequacy decisions and other safeguards (Article 49) – 'suitable safeguards'. This creates a state of legal uncertainty on what the required standard of protection must be.[170]

Kuner mentions that in practice it is difficult to make decisions on a foreign regulatory system without political considerations, which may play a certain role.[171] In Roth's opinion, the *Schrems I* judgment, and, consequently, the GDPR, raises the standard of data protection higher from 'adequacy' to 'essential equivalence'.[172] This, according to him, is not likely to be achievable by most of the third countries.[173] The European

[165] See Article 45 GDPR.
[166] Case C-311/18 *Data Protection Commissioner v Facebook and Maximillian Schrems,* Judgment of the GC dated 16 July 2020 (*Schrems II*).
[167] See *Schrems II, Ibid.,* Paragraph 94.
[168] *Ibid.,* Paragraph 96.
[169] See Zuzanna Gulczinska 'A Certain Standard of Protection for International Transfers of Personal Data under the GDPR' (2021) 4 IDPL 360.
[170] *Ibid.,* p.366.
[171] See Christopher Kuner *Transborder Data Flows and Data Privacy Law* (OUP, 2013), 66.
[172] Paul Roth '*Adequate Level Of Data Protection* in Third Countries post Schrems and under the GDPR' (2017) 25 J.L. Inf & Sci. 49.
[173] *Ibid.,* p.63.

Commission itself made it clear that there would be certain priorities in choosing which countries the EU seeks to be engaged in a dialogue to pursue adequacy arrangements:

- the extent of the commercial relations and the existence of the free trade agreement with a third country;
- the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
- the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and
- the overall political relationship with the third country in question, particularly with respect to the promotion of common values at the international level.[174]

It is evident that commercial considerations play a crucial role in deciding with which country data protection arrangements could be built in the first place. This probably can explain why the GDPR, which was enacted a year later, has more references to the fundamental right to data protection than the right to private life.[175] Reference to the countries with cultural ties may suggest that the difference in perception of the right to private life may be explained or driven culturally in other parts of the world, while the right to data protection would bear less cultural burden, and thus be perceived as more of a universal right. The CJEU's implicit attempt to differentiate the right to data protection from the right to private life in one of the first cases under the GDPR – *Schrems II*,[176] discussed in Section 5.4.3. of this Chapter, as the technical right to data processing, serves as another evidence of the right to data protection to be treated as a universal right.

The early perception of data protection in the DPD was that the underlying value or principle of fair data processing was considered to be the right to privacy, which through many years served to build our perception of the right to private life as extending to the automatic processing of personal data. The enactment of the CFREU along with the Treaty of Lisbon in 2009, the CJEU case law (particularly, *Schrems I*) in the aftermath of the Snowden revelations in 2013, and now the text of the GDPR, which has entered into force in 2018, are gradually shifting the focus from the right to private life to the right to protection of personal data when it comes to the automatic data processing.

The CJEU has been conflating two rights as it has had to accommodate the narrative that the right to data protection, along with or separately from the right to private life, would

[174] See Communication from the Commission to the European Parliament and the Council 'Exchanging and Protecting Personal Data in a Globalised World' COM (2017) 7 final.
[175] There is only one clear reference to the right to private life in GDPR – Recital 4.
[176] See *Schrems II*, n 166 above.

be at stake. In order to fully switch to the right to data protection in the CJEU's reasonings, the Court needs to explicate the value of the right to data protection as opposed to the right to private life. This Chapter has sought to explore how the EU laws and the CJEU's jurisprudence, as well as legal scholarship, contributed to the understanding of the right to data protection as the main focus of personal data protection legislation.

To recall, Chapter 3 of the thesis has discussed the differences between the US and European perceptions of privacy, and how in Whitman's view it affected data protection in a transatlantic battle.[177] This thesis argues that the cultural differences indicated by Whitman will not play a decisive role in determining whether the US data protection legal regime provides adequate protection of the rights of individuals, as the primary right to be protected here will be the right to data protection, not the right to privacy.

The right to data protection is declared a fundamental right by the EU, and the task is to convince third countries not to perceive it as a culturally different value because it would be different from the right to private life. The EU may see it as an opportunity to promote data protection as a value, which is common to the whole international community.

5.4. The Right to Privacy as Compared to the Right to Data Protection in EU Law and in the ECHR

Chapter 4, on the basis of the ECtHR jurisprudence, has shown that the right to data protection may be regarded as a subset of the right to private life.[178] This is primarily due to several factors. At the time of the drafting and adoption of the ECHR in 1950, the protection of personal data was simply not on the agenda. Personal data protection has become relevant with the emergence and development of new technologies when it is possible to process data by automatic means. The ECHR is *a living instrument*,[179] which the ECtHR has been developing by changing and widening its interpretation to fit to the realities of modern-day society. The list of rights in the ECHR is supplemented not by introducing new human rights, but by expanding the scope of existing rights, such as the right to private life. The most important factor in defining data protection as a sub-section of the right to private life is the values protected by the right to data protection: the right to personal development, the right to determine the space and limits of personal interaction with society and the personal nature

[177] James Q. Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty", in "The Yale Law Journal", 2004, vol 113, p. 1157.
[178] See Chapter 4 'The ECHR: General Principles Relating to Surveillance, Data Protection and Privacy Rights' of this thesis.
[179] *Tyrer v. UK*, (1978) A26, Paragraph 31.

of data, that is, data is always associated with a specific person, and their dignity will be affected if such data is used without knowledge of the person or be misused otherwise.[180]

The EU Member States have been introducing their national legislation on the protection of personal data since the 1970s. Many constitutions of the Member States had already foreseen general protection of personal data. By the time the CFREU was adopted, the drafters of that document had decided to give the protection of personal data an independent meaning and elevate it to the rank of a separate fundamental right (Article 8 CFREU), along with the already "classic" right to private life (Article 7 CFREU). Advocate General Sharpston called the right to private life under the ECHR a 'classic' right in the context of comparing it with the right to data protection.[181]

Articles 7 and 8 CFREU are stipulated as follows:

> Article 7
>
> Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8
>
> Protection of personal data
>
> 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 of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Over the past 10-15 years a question has been raised in the doctrine as to why the CFREU provides for a separate fundamental right to the protection of personal data, along with the right to privacy. What is the difference between these rights and is this difference, if any, so significant that the right to the protection of personal data has the status of a fundamental right provided for and protected by the primary legal instruments of the EU?

[180] See Chapter 4 'The ECHR: General Principles Relating to Surveillance, Data Protection and Privacy Rights', pp.20-23.
[181] See Case C-92/09 and C-93/09 *Volker und Markus Schecke and Hartmut Eifert,* CJEU Judgment of 9 November 2010, Opinion of Advocate General Sharpston, para 71.

Before developing an analysis of the two rights enshrined in the CFREU, this Chapter will examine how 'personal data' is understood by data protection bodies of the EU.

5.4.1. Definition of 'Personal Data'

In 2007 within the EU data protection system the definition of 'personal data' was clarified by the main advisory data protection body of the EU – Article 29 Data Protection Working Party (Article 29WP). With the enactment of the GDPR in 2018, the role of the main data protection advisory body within the EU was transferred from Article 29WP to the European Data Protection Board – EDPB. In its Opinion 4/2007 'On the Concept of Personal Data', Article 29WP based its analysis of the concept of 'personal data' on four elements: 'any information', 'relating to', 'an identified or identifiable', and 'natural person'.[182]

Article 29WP maintains that 'any information' must mean that the concept of 'personal data' must be widely interpreted irrespective of the nature or content of the information.[183] Both subjective and objective information about a person could comprise 'personal data'. Another component – 'related to' plays a crucial role in defining the concept of 'personal information'. There are three independent sub-components to determine whether the information is related to a person: content, purpose, and result. The 'content' means when information is *about* a person, regardless of the purposes or results of processing such information. The 'purpose' element is considered when the data is used or likely to be used for the purposes of evaluating treating or influencing the status or behaviour of a person. Finally, 'result' entails situations when even if two previous elements are absent, data would be considered to 'relate' to an individual, because their use is likely to have an impact on certain rights or interests of the person.[184]

The third element highlighted by Article 29WP is 'identified or identifiable'. A person may be "identified' if, within a group of persons, they are distinguished from all other members of the group. Accordingly, a person may be 'identifiable', if although such a person has not been identified yet, it is possible to do it. This is normally achieved through obtaining and analysing specific pieces of information – 'identifiers', such as, e.g., location data, online identifier, or one or more factors specific to the physical, genetic, mental, economic, cultural, or social identity of such a person.[185]

---

[182] Article 29 Working Party, Opinion 4/2007 'On the Concept of Personal Data' adopted on 20 June 2007, 01248/07/EN WP 136.
[183] Schwartz and Solove call it 'expansive approach' by the EU, and criticize it for not distinguishing between 'identified' and 'identifiable'. See Paul Schwartz and Daniel Solove 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 NY University Law Review 1814.
[184] Opinion 4/2007, n 182 above, 10-11.
[185] Opinion 4/2007, n 182 above, 12.

The last, fourth, element of the concept of 'personal data' is a 'natural person', which means any human being, and generally excludes legal persons. This was confirmed by the ECtHR in *Bernh Larsen v Norway* case, where the Court refused to examine personal data issues as applied by the applicants – legal entities, and was open to do so only if individuals made a complaint.[186]

5.4.2. The Scope of Privacy and Data Protection

Kokott and Sobotta indicate that the jurisprudence of the CJEU justifiably considers privacy to be at the core of data protection.[187] They however show a few distinctions between privacy and data protection.[188] According to them, the scope of data protection is broader than the scope of privacy, because data protection concerns all information about identified or identifiable persons, while privacy does not necessarily include all that information.[189]

Similarly, Lynskey argues that the right to data protection provides individuals with more rights over more types of data than the right to privacy does.[190] From the jurisprudence of the CJEU, she makes an inference that the CJEU consistently conflates the rights to data protection and privacy during the period prior to and after the entry into force of the Lisbon Treaty.[191] She however explains two distinctions regarding the range of data falling within the scope of both rights: first, the notion of 'personal data' unlike the term 'privacy interference' is not context-related, and second, the concept of personal data besides identified persons covers identifiable persons.[192] According to her, the ECtHR endorses a broad interpretation of the right to privacy rather than incorporating the definition of 'personal data' into its Article 8 ECHR jurisprudence.

All of the above-mentioned authors seek to distinguish data protection from privacy not through the jurisprudence of the CJEU, because the CJEU has not offered much by way of explanation. Instead, they seek to do so through the jurisprudence of the ECtHR.[193] In the

---

[186] *Bernh Larsen Holding AS and Others v Norway* (2013) Judgment of the First Section dated 8 July 2013, Paragraph 107.
[187] Juliane Kokott and Christoph Sobotta 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 4 International Data Privacy Law 222.
[188] Kokott and Sobotta have used the terms 'privacy' and 'private life' to indicate the same meaning throughout the text of their article. *Ibid*.
[189] *Ibid.*, p.225.
[190] Orla Lynskey 'Deconstructing Data Protection: the "Added Value" of the Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569, p.573.
[191] *Ibid.,* p.574-575.
[192] *Ibid.,* p.583.
[193] It probably can be reasoned by the fact that the CJEU in its judgments, as well as the AGs, examine the right to private life and data protection through the prism of the ECtHR's jurisprudence, as the latter can offer some meaningful findings and interpretation. The CJEU's judgment in *Digital Rights Ireland,* case C-293/12 and 594/12, can be an example, where the CJEU made references to the relevant ECtHR case-law (Paragraphs

system, which designs and establishes a separate right to data protection, the main law interpreting body – the CJEU – in Lynskey's view, constantly conflates two rights and seems not to be in a position to explain how the right to data protection could be regarded a fundamental right.[194]

While the distinctions in the scope of the rights made by Kokott and Sobotta on the one hand, and Lynskey – on the other – may indeed exist, they still do not provide an answer to the question of why data protection must be regarded as a fundamental right of individuals. From those authors' point of view, the two rights are largely intertwined and they overlap, but they are distinct. However, such distinctions seem to be rather technical than substantive. The difference in the texts of Articles 7 and 8 CFREU suggests that the right to private life, unlike the right to data protection may be limited only on the basis of the general limitation provision contained in Article 52(1), as will be explained next.

Article 7 CFREU contains no special limitation. It only proclaims everyone's right to private life, while Article 8 CFREU provides for specific limitations to the right to data protection. Personal data may be processed only on legitimate bases, such as the individual's consent,[195] and may be rectified upon the individual's request.

At the same time, Article 8 CFREU provides for an additional safeguard for the protection of personal data – an independent data protection authority must be in place to exercise control over compliance. Kokott and Sobbota argue that the data protection right is affected when one of the safeguards, clearly indicated in the secondary legislation, has been breached.[196] Indeed, if personal data is processed without the consent of the individual or any other legitimate ground, then such data processing may be in conflict with the right to data protection. For the right to privacy to be interfered with, however, some other contextual features are necessary.

Kokott and Sobotta further discuss the *Rotaru case*,[197] where the right to private life has been interfered with. The ECtHR in that case stressed that the personal information in question went back a long time and was systematically collected and stored. In the opinion of Kokott and Sobotta, the ECtHR would (most probably) not find interference with the right

47, 54 and 55). AG Villalon also made use of the interpretation of the ECtHR in his Opinion in *Digital Rights Ireland.*

[194] See Orla Lynskey, n 190 above.

[195] In addition to the data subject's (individual's) consent, GDPR defines the following as legal grounds for data processing and data transfer: 1) EU Commission's decision on the adequacy of the data protection regime in third countries or international organization in case of data transfer (Article 45); 2) an agreement between states (Article 46, (2a); 3) binding corporate rules (Article 47); 4) Standard data protection clauses (Article 93); 5) Code of conduct of controllers and processors (Article 40); 6) Certification mechanism (Article 42); 7) Contractual clauses (Article 46 (3a).

[196] See Juliane Kokott and Christoph Sobotta, n 187 above, p.226.

[197] *Rotaru v Romania*, Judgment of the ECtHR dated 4 May 2000.

to private life if personal information was not stored for a long time and was not collected and stored systematically.[198]

Such a reasoning of Kokott and Sobbota, however, seems to be unconvincing. The ECtHR in *S and Marper* held that the mere retention of DNA profiles, cellular samples, and fingerprints was in itself sufficient to conclude that their retention interfered with the right to the private life of the individuals concerned.[199] The duration of such retention of data served as a variable in the balancing exercise, which the ECtHR employed in order to define whether or not the interference with the right to private life resulted in a violation of the right to private life. Data protection instruments, both domestic and regional, may determine the duration of data retention, and the task of the ECtHR is to examine the necessity and proportionality of such duration to the pressing social needs in each particular case. It is data protection laws, which are scrutinized by the ECtHR in order to examine the 'quality of law', according to which an alleged interference with private life takes place.[200]

Lynskey refers to the *Rundfunk*[201] case considered by the CJEU to show the difference in the scope of the two rights. She contends that the 'mere recording by an employer of data by the name relating to the remuneration paid to his employees'[202] cannot as such constitute an interference with private life as understood under the ECHR, while such recording constitutes 'data processing' and thus falls within the scope of data protection.[203] She compares the notions of 'privacy interest' with 'personal data',[204] although she admits the difficulty of comparing those two notions.[205] This thesis suggests that it makes sense to compare similar concepts that may be assessed using the same criterion. In this manner, the difference between the two rights are explored. Thus, the notion of 'privacy interest' is compared with the notion of 'data protection interest'.

Neither the EU secondary legislation on data protection, nor the jurisprudence of the CJEU, define or make clear references to 'data protection interest'. However, since the right to data protection is recognized as a fundamental right, there must be an interest, which is protected by that right. The DPD contained 13 references to the right to privacy as an underlying interest of data protection, while the GDPR has only once referred to the right to

---

[198] See Kokott and Sobotta n 187 above, at p.224.
[199] *S. and Marper v UK* (2008), Judgment of the Grand Chamber (GC) dated 4 December 2008, Paragraphs 75 and 85.
[200] For more on the 'quality of law' see Chapter 4 'The ECHR: the General Principles Relating to Surveillance, Data Protection and Privacy Rights' of this thesis.
[201] Joint Cases C-465/00, C- 138/01, C-139/01 *Österreichischer Rundfunk and Others*, Judgment of 20 May 2003.
[202] *Ibid.,* Paragraph 74.
[203] See Orla Lynskey n 190 above, at p. 585.
[204] See Orla Lynskey n 190 above.
[205] See Orla Lynskey n 190 above, at p. 583.

private and family life along with other fundamental rights, which the GDPR seeks to respect.[206] It seems that all references to the 'right to privacy' were replaced with references to the right to data protection in the GDPR.[207] This is one of the reasons why two rights were conflated by the CJEU, and this is why it is difficult to understand what the right to data protection actually is designed to protect. For the purposes of distinguishing between the right to private life and the right to data protection, can one assume that the right to data protection protects the data protection interest?

For Lynskey 'personal data' represents data protection interest. However, if the Court is to identify the interference with the right, it must show the interference with the underlying interest. In this author's view a data protection interest may be explained by the principles relating to the processing of personal data, such as lawfulness, fairness, and transparency of personal data processing. It is for this reason that this thesis will compare the privacy interest with the interest in lawful or fair processing of personal data.[208]

All principles of personal data processing are enshrined in Article 5 GDPR:

> Personal data shall be:
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; […]
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
> (d) accurate and, where necessary, kept up to date […].

Hypothetically, if interference with the right to data protection (instead of the right to private life) was to be determined, the Court (ECtHR or CJEU) would scrutinize the domestic laws and regional data protection instruments, such as the Convention 108,[209] the GDPR, the Law Enforcement Directive,[210] etc. The Court would find out that, e.g., according

[206] See GDPR n 4 above, Preamble, Paragraph 4.
[207] Van Der Sloot 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in Ronald Leenes, Rosamunde van Brakel Serge Guthwirth, Paul De Hert (eds) *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer International Publishing AG, 2017).
[208] At this stage the author does not discuss why data processing should be lawful, fair, and transparent, i.e., the author does not delve into the question of what value is at the core of the data protection right.
[209] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) dated 28 January 1981, amended later with Additional Protocol of 2001 (ETS 181), and, recently, modernized through Amending Protocol (CETS 221). Now, it is the Modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the CoE Committee of Ministers on 18 May 2018, CM/Inf(2018)15-final.
[210] Directive EU 216/680 of the European Parliament and of the Council of 27 April 2016 'On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, direction or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data' (LED), OJEU, L 119/89.

to Article 5 (1)(e) GDPR, personal data must be kept no longer than necessary for the purposes for which the personal data are processed, or even kept longer for some specified purposes, such as archiving for public interest and scientific or historical research. The Court (ECtHR or CJEU) would need to explain in each particular case whether the personal data is kept or retained no longer than necessary for the purposes of data processing, and such purposes may be different in each particular case, and the duration for achieving such purposes may vary from case to case. Thus, the context in the case of data protection equally plays an important role as much as it does in the case of the right to private life.

Returning to the *Rundfunk* case, the present author can see that the mere recording of names of employees and their salaries by the employer may trigger the right to data protection only if such recording is contrary to the principles of data processing, such as lawfulness. If such recording is done lawfully and it breaches no other principles of data processing, why would the issue of data protection emerge in the first place?

Bygrave uses the term 'data privacy' as meaning 'data protection'.[211] For him, the data privacy rights are usually expressed in terms of privacy, and sometimes in terms of autonomy and integrity.[212] The main goal of data privacy according to him is the protection of the privacy-related interests of an individual.[213] In some cases data privacy covers more aspects than the right to private life does, and in other cases – less. For him the term 'data protection' is problematic, as it fails to indicate central interest on the one hand, and may be misleading on the other hand, for it does not protect the data, but rather the individual.[214]

Rodotà sees the difference between the right to private life and the right to data protection in the type of protection granted by the respective right. In his view, the right to private life is a more classic negative right 'to be let alone', while the right to data protection is a positive right, which empowers individuals to take steps and develop their personality.[215] Article 8 CFREU, in his view, deals with the integrity of an 'electronic body' of the human, thus, data protection rights are related to dignity.[216] The present writer cannot agree with the delineation of two rights suggested by Rodotà, although the underlying value – human dignity – serves as the basis for both rights. As has been examined in Chapter 4, the right to private life under the ECHR has evolved to cover both negative and positive obligations of

[211] Lee Bygrave *Data Privacy Law: An International Perspective* (OUP, 2014).
[212] *Ibid.,* Chapter 1 'Data Privacy Law in Context', at p. 1.
[213] *Ibid.,* p.2.
[214] *Ibid.,* p.28.
[215] Stefan Rodotà 'Data Protection as a Fundamental Right' in Serge Gutwirth et al (eds) *Reinventing Data Protection* (Springer Science+Business Media B.V., 2009).
[216] *Ibid.*, p. 80.

State authorities.[217] The ECtHR's extensive jurisprudence indicates that both negative and positive rights are protected by Article 8 of the ECHR.[218]

5.4.3. The Essence of the Right to Data Protection

For the purposes of further distinguishing the two fundamental rights: the right to private life and the right to data protection, this Chapter engages in the discussion about the essence of fundamental rights. The problem of distinguishing the right to private life from the right to data protection experienced by the CJEU[219] is vividly evident in its attempts to find the incompatibility of certain data protection legal instruments or arrangements with the 'essence' of the fundamental rights. Article 52(1) CFREU, cited earlier, provides that any limitation to the enjoyment of fundamental rights must respect the 'essence' of those rights and freedoms.

In *Digital Rights Ireland,*[220] as it is observed in this Section, the CJEU found the DRD, which required telecommunications service providers to retain for up to two years all metadata (or communication data) from all EU citizens' emails, text messages, and telephone calls, and to provide these data to national security agencies for investigatory purposes, to be in violation of the fundamental rights to private life and data protection enshrined in the CFREU. In this context, the CJEU appeared as a proper constitutional court, which substantiated its stance on the grounds of its 'Bill of Rights', i.e., the CFREU.[221] However, as mentioned earlier in this Chapter (in Section 5.4.2. 'The Scope of Privacy and Data Protection') the CJEU failed to clearly distinguish privacy and data protection as two separate fundamental rights.

The CJEU, in this case, found no violation of the essence of the right to private life and the right to data protection but went on to find a violation of those rights by exercising a proportionality test. The essence of the right to privacy under Article 7 CFREU was untouched because the Data Retention Directive did not permit the acquisition of knowledge of the content of the communications as such.[222] Thus, in 2014 the CJEU considered that the

[217] See Matheu Leloup 'The Concept of Structural Human Rights in the European Convention on Human Rights' (2020) 20 Human Rights Law Review 480.
[218] See *Marckx v Belgium* (1979) Series A no 31; *Barbulescu v Romania ,* Judgment of the ECtHR dated 5 September 2017; *Craxy v Italy,* Judgment of the ECtHR dated 17 October 2003, Paragraphs 68-76; *Benediktsdottir v Iceland,* Decision of the ECtHR on admissibility dated 16 June 2009.
[219] See Orla Lynskey n 190 above, at p. 573.
[220] Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others,* Judgement of the GC dated 8 April 2014.
[221] See Arianna Vedaschi and Valerio Lubello, n 115 above.
[222] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Others,* Judgment of the GC dated 8 April 2014*,* Paragraph 39.

content data, as opposed to the metadata, could comprise the 'essence' of the right to privacy under the CFREU. In respect of Article 8 CFREU, the CJEU held that there was no violation of the essence of the fundamental right to data protection because the DRD had foreseen certain principles of data protection. The CJEU added that according to those principles the Member States had to ensure the appropriate technical and organizational measures against accidental or unlawful destruction, accidental loss, or alteration of the data.[223]

One year later, in *Schrems I,*[224] the CJEU by its judgment invalidated the decision of the European Commission, known as the 'Safe Harbour Decision',[225] which allowed for personal data transfer from the EU to the United States of America, assuming that the data protection regime complied with by the US organizations ensured an adequate level of protection in respect of the transferred personal data. The Court held that the right to private life under Article 7 CFREU was not merely violated, but seriously deprived of its essence as enshrined in Article 52(1) CFREU by the legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications.[226]

In the earlier CJEU case law, i.e., before the adoption of the CFREU, the Court used the term 'substance' of fundamental rights,[227] which in Article 52(1) CFREU was converted into the 'essence' of fundamental rights.[228] There is a debate in the literature on what the essence of the rights means, and how the essence or the core of the fundamental rights is explained.[229] The notion of the core or substance or essence of the rights is known to some of the European constitutional orders. The most prominent one is the German Basic Law,[230] which in Article 19(2) stipulates that in no case may the essence of a basic right be affected. Such a constitutional limitation clause containing the reference to the essence of the rights was then adopted by some other countries, such as Estonia, Hungary, Portugal, Poland,

---

[223] *Ibid.,* Paragraph 40.
[224] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner,* Judgment of the GC dated 6 October 2015. This case is called 'Schrems I' as there was a subsequent case in 2020, which is called 'Schrems II'. Schrems I abolished the 'Safe Harbour' arrangement, while the Schrems II judgment rendered the 'Privacy Shield' decision of the European Commission invalid.
[225] Decision 2000/520 of the European Commission*, OJ L 215, 25.8.2000.*
[226] *Schrems I,* n 224 above, Paragraph 94.
[227] Case 4/73 *Nold v Commission*, Judgment of 14 May 1974, *Hauer v Land Rheinland-Pfalz*, Judgment of 13 December 1979, paras 23, 30; Case 265/87, *Schräder v Hauptzollamt Gronau*, Judgment of the 5th Chamber dated 15 July 1989.
[228] Maja Brkan 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (2018) 14 EuConst at p.333.
[229] See Orlando Scarcello 'Preserving the 'Essence' of Fundamental Rights under Article 52(1) of the Charter: A Sisyphean Task?' (2020) 16 EuConst 647; Maja Brkan 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (2018) 14 EuConst 332; Koen Lenaerts 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779; Takis Tridimas and Giulia Gentile 'The Essence of Rights: An Unreliable Boundary?' (2019) 20 German Law Journal 794.
[230] Grundgesetz 1949 [GG] [Basic Law] translation at http://www.gesetze-im-internet.de/englisch_gg/index.html

Romania, the Slovak Republic, Spain, and Switzerland.[231] Other European countries had no constitutional provision on the essence of the rights in the context of the limitation clause to the fundamental rights and freedoms, so it remains debatable whether recognition of the notion of 'essence' in the CFREU is seen as emerging from the commonality of constitutional traditions of all EU State Members.[232]

In *Schrems I* the CJEU found the interference with the essence of the right to privacy through *a contrario* reasoning from Digital Rights Ireland.[233] It may be inferred from the Court's judgment that the content of communication, not their metadata, constitutes the core or the essence of the protected right – the right to privacy. Thus, the Court pronounced the breach of the essence of the fundamental right to privacy because the US mass online surveillance programmes granted access not only to communication data (metadata) but to the actual content of the communications.

This has been justifiably criticized, as the communication data taken as a whole can draw an exact portrait and compile a comprehensive profile of the individual, while the content might not really give any clue about the author or their private life.[234] The ECtHR in *Big Brother Watch* reiterated that the interception of the communication data or metadata is not less intrusive than the acquisition of the content data.[235]

The present writer has analysed the ECtHR case law on surveillance in Chapter 4 of the thesis and has shown that in 2010[236] the ECtHR had a similar position to the CJEU's interpretation, but changed it in 2019 – 2021 in two cases.[237] This shows the difference in the approach to treating content data and communications data by the ECtHR and the CJEU. Such an inconsistency in the ECHR and EU rules may create uncertainty and a lack of clarity for third countries about standards of data protection in the European legal space.

Returning to the *Schrems I* case, Brkan is of the opinion that the CJEU deliberately avoided proper engagement in the proportionality test because it was unclear what the

[231] For more information on this see Takis Tridimas and Giulia Gentile 'The Essence of Rights: An Unreliable Boundary?' (2019) 20 German Law Journal 794 and Maja Brkan 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (2018) 14 EuConst 332.
[232] Brkan n 228 above, p.344.
[233] *Ibid.,* p.354.
[234] *Ibid.* See also Maria Tzanou '*Schrems I and Schrems II*: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' in Federico Fabbrini et al (eds) *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart Publishing, 2021).
[235] *Big Brother Watch and Others v* UK, Judgment of the ECtHR dated 25 May 2021, Paragraph 363.
[236] In the case of Uzun v Germany the ECtHR held that GPS surveillance is actually less interfering with private life than other measures of surveillance such as acoustical and visual. See *Uzun v Germany,* Judgment of the ECtHR dated 2 December 2010, Paragraph 52.
[237] *Big Brother Watch and Others v* UK*,* Judgment of the ECtHR dated 4 February 2019; *Centrum for Rattvisa v Sweden,* Judgment of the ECtHR dated 4 February 2019; *Big Brother Watch and Others v* UK, Judgment of the ECtHR dated 25 May 2021.

legitimate objectives for the interference with the right to privacy were.[238] The interference with the rights of EU data subjects could be justified by the interests of national security. However, it was the US national security, which had to be opposed to the rights holders within the EU. Thus, Brkan explains the approach of the CJEU not to engage in employing the proportionality test for practical reasons: it is difficult to apply the proportionality test where interference with privacy takes place in the country.[239] This, however, does not give the answer to the question of what the essence of fundamental rights is.

Lenaerts infers from *Schrems I* that the concept of the 'essence of a fundamental right' implies that each fundamental right has a 'hard nucleus', which is absolute and may not be subject to limitations.[240] He further suggests that a measure, which compromises the essence of a fundamental right, must automatically be regarded as disproportionate. He contends that the CJEU first must examine whether the measure in question respects the essence of the fundamental rights, and must only be engaged in performing a proportionality assessment if the first question is answered in the affirmative.[241]

It remains however unclear how the Court would explain the essence of each fundamental right. If it is a matter of a scale, i.e., the more severe or the more comprehensive measure is used to interfere with the right or the more important or vital the interest protected by the right appears, the more likely would the Court find the interference with the essence of the fundamental rights.[242] However, this means that even when answering to the first question (whether the measure compromises the essence of the rights), the Court would effectively employ the proportionality test, so there is no way to find the measure in question to be automatically disproportionate.[243]

Brkan proposes a two-step methodology to define the essence of the right: (1) whether the interference affects the very existence of the right, and (2) whether there are overriding legal reasons for interference.[244] The first step is to show whether the limitation undermines the existence of the right, and the second is to see if it is impossible to identify any overriding reason. Scarcello argues for the first step, contending that every time the right is outweighed, it would cease to exist for the rights holders at least in the minimal sense.[245]

---

[238] Brkan, n 228 above, p.354.
[239] *Ibid.*
[240] Koen Lenaerts 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779.
[241] *Ibid.,* at p. 787.
[242] See Orlando Scarcello 'Preserving the 'Essence' of Fundamental Rights under Article 52(1) of the Charter: A Sisyphean Task?' (2020) 16 EuConst 647.
[243] *Ibid.,* p.652.
[244] Brkan n 228 above, pp.359-367.
[245] Scarcello, n 242 above, p. 653.

For the second step, he claimed that some of the limitations could be regarded as overriding legal reasons, but others (such as the rights of others or general interests) would not.[246]

The discussion in the legal scholarship on the difference between the right to private life and the right to data protection is far from being finished. The tendency to interpret the right to data protection as a more technical right as opposed to the right to private life does not add to the argument for the right to data protection as a fundamental right. Can a technical right be a fundamental right? Apparently, this dilemma does not allow the Court to clearly distinguish between these two rights in its jurisprudence. In *Schrems II*, the CJEU tried to carefully outline the reason for the emergence of the right to data protection alongside, or even separately from, the protection of privacy in the following manner:

> Thus, access to a natural person's personal data with a view to its retention or use affects the fundamental right to respect for private life guaranteed in Article 7 of the Charter, which concerns any information relating to an identified or identifiable individual. Such processing of data also falls within the scope of Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article.[247]

The quoted wording of the CJEU judgment suggests that the right to data protection can indeed be seen as a more technical right for it concerns only the processing of personal data. It is suggested that the reasons why and for what purposes personal data is accessed could not be regarded as part of the right to data protection. It is attributed by the Court to the concern protected by the fundamental right to private life. In the above-mentioned case, the CJEU avoids naming the right to data protection as a 'fundamental' right along with the right to private life, which may be seen as the Court's vision of the right to data protection as a technical right.

5.5. Conclusion

The adherence of the EU to common market freedoms on the one hand, and to the fundamental human rights, on the other hand, poses certain challenges in formulating what exact values the EU are promoting in the wider world. Since the processing of personal data

[246] *Ibid.,* p. 654.
[247] Case C-311/18 *Data Protection Commissioner v Facebook and Maximillian Schrems,* Judgment of the GC dated 16 July 2020, Paragraph 170.

became automatized, and private economic entities found themselves collecting, storing, and using the personal data of a large number of individuals, the healthy development of the common market of the EU became possible with the free flow of personal data within such a common market.

The EU reacted by adopting common rules of data processing among Member States declaring that such rules reflected in the DPD were introduced for the sake of good functioning of a common market and in order to ensure the protection of the fundamental rights of individuals in the EU. At the time when it was the European Community, it was not inspired by the protection and promotion of human rights. After decades of the establishment of the EC, human rights and freedoms protected by its Member States have become part of EU law by announcing that human rights are part of the general principles of EU law, which stem from common constitutional legal orders and traditions of Member States, as well as from international human rights law instruments, such as the ECHR.

It was crucial to convince all Member States to adopt a unified set of rules for data protection by explaining that there was a need to protect the fundamental rights of individuals. At the time of drafting and adopting the DPD (1992-1995), the ECHR as a human rights instrument, legally binding Member States separately from their EU obligations, has guided the drafters of the DPD. The jurisprudence of the ECtHR suggests that the right to data protection is a subset of the right to private life, and the DPD drafters seemed to accept that perception. Thus, the DPD contained numerous references to the right to privacy.

Transposition of the DPD provisions into the national legislation of the Member States did not achieve a full harmonization of data protection laws within the EU, since even among Member States there was a different perception of privacy, and the main issue under the DPD, in the light of the free flow of personal data within the EU, was a resolution of conflict of laws of the Member States.

The EU has enacted the CFREU as a primary source of EU law, and together with the Treaty of Lisbon has elevated the right to data protection to a separate fundamental right. The Chapter showed that the CJEU after that appeared to conflate the right to privacy and the right to data protection in its jurisprudence. Many scholars sought to identify the differences between the two rights, but it remained unclear why the right to data protection became a fundamental right.

The GDPR has harmonized data protection laws of the Member States on the premise that it is currently the right to data protection, not the right to privacy, which is given a primary focus. The right to data protection is undoubtedly intertwined with the right to

privacy, and shifting the focus from one to another in such a powerful instrument as the GDPR, which may apply far beyond the territory of the EU, indicates the willingness of the EU to present the right to data protection as a universal right, which would not be affected anyhow by possible cultural differences in other parts of the world.[248]

The right to data protection is presented currently as a fundamental human right, although it is rather a technical right, which concerns certain rules of fair and transparent data processing. One of the contributions of this thesis to the literature is that the right to data protection is to be considered a technical right as opposed to the right to privacy which concerns deeper human values, such as dignity and freedom.

The values of the EU common market are in line with the right to data protection and vice versa, and, allegedly, such common market values, as well as the right to data protection, may be attractive to third countries. For ensuring the free transfer of personal data abroad, the adequacy decisions of the European Commission play a crucial role. The more countries with large economies enter into adequacy arrangements with the EU, the better is for the development of the EU internal market. Cultural differences in accepting the rules, essentially equivalent to the GDPR, might hamper the plans of third countries to adhere to the values proclaimed by the EU.

Chapter 4 of this thesis has explored that under the ECHR the cultural, economic, and political differences among different States are taken into account by the ECtHR when it examines cases involving the right to privacy and data protection issues because the right to data protection forms a part of the right to private life. The EU law takes a different approach by declaring a technical right to data protection as a fundamental right for the purposes of promoting it within the third countries as a value that is free from cultural or other implications.

[248] In Chapter 3 'The Concept of Privacy' the author examined the cultural differences in the perception of privacy in different continents, in the example of the USA and Europe.

Chapter 6: Lessons that Tajikistan Could Learn from the ECHR and the GDPR

6.1. Possible Areas of Tajik Surveillance and Data Protection Laws where More Advanced Protection Could be Provided in the Light of the Standards Set by the ECHR and the GDPR

6.1.1. The ECHR Standards and Tajik Surveillance Laws

Chapter 4 of this thesis has examined the European Court of Human Rights (ECtHR) case law on privacy and surveillance issues. The ECtHR has established a 'Weber requirements',[1] which consist of six minimum procedural requirements that must be enshrined in the domestic law of the Member States of the European Convention on Human Rights (ECHR)[2] in respect of the targeted surveillance measures,[3] and eight minimum requirements applicable to the cases of bulk surveillance.[4] It is not the intention of this thesis to make a comparison between the Tajikistan surveillance laws and the ECtHR jurisprudence. However, it is an attempt to understand what lessons Tajikistan could learn in order to improve its laws in the light of the standards set by the ECtHR in this area of law.

In *Klass v Germany*, the ECtHR held that the mere existence of the laws on surveillance may create a threat to the freedom of communication between individuals, and thus may be considered as an interference by the authorities with the private life of individuals.[5] Chapter 2 (Tajikistan Laws Related to Privacy and Data Protection Issues)

[1] Named after the ECtHR case *Weber and Saravia v Germany*, Admissibility Decision of 29 June 2006. The ECtHR in 2021 has referred to those requirements as 'Weber criteria'. See *Big Brother Watch and Others v* UK, Judgment of 25 May 2021, Paragraph 361 (*'Big Brother Watch (2021)'*).

[2] Convention for the Protection of Human Rights and Fundamental Freedoms adopted by the Council of Europe on 4 November 1950 and entered into force on 3 September 1953.

[3] *Weber and Saravia v Germany*, Admissibility Decision of 29 June 2006, Paragraph 95. Those six requirements include 1) the nature of offenses, which may give rise to conducting surveillance measures; 2) the definition of the categories of people to have their communications intercepted; 3) a limit on the duration of interception of communications; 4) the procedure to be followed for examining, using and storing the data obtained; 5) the precautions to be taken when communicating the data to other parties; and 6) the circumstances in which recordings may or must be erased or destroyed.

[4] *Big Brother Watch and Others v* UK, Judgment of 25 May 2021, Paragraph 361. Eight requirements in bulk surveillance are the following: 1) the grounds on which bulk interception may be authorized; 2) the circumstances in which an individual's communications may be intercepted; 3) the procedure to be followed for granting authorization; 4) the procedures to be followed for selecting, examining and using intercept materials; 5) the precautions to be taken when communicating the material to other parties; 6) the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed; 7) the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; and 8) the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

[5] *Klass and Others v Germany* (1978) Series A no 28, Paragraph 41.

emphasized that due to its Soviet legacy, Tajikistan has a legal system very similar to some other former Soviet States, especially Russia, and that the Tajik legal scholarship is primarily informed by the Soviet and post-Soviet, particularly, Russian, legal thought. Tajik laws related to criminal proceedings and to the detection and investigation of crimes are almost identical to Russian laws, with some deviations and particularities.[6] Since Russia was a party to the ECHR[7], there were a few cases against Russia examined by the ECtHR in respect of privacy and data protection. In one of the cases (*Zakharov v Russia*), the ECtHR examined the laws of the Russian Federation related to crime detection and investigation, particularly, the laws related to surveillance.[8] By examining the ECtHR assessment of Russian laws,[9] the thesis seeks to ascertain to understand how Tajikistan laws meet the standards set by the ECtHR, and to what extent the Tajik surveillance laws need improvement from the human rights law perspective.

6.1.1.1. Quality of Law in Targeted Surveillance

As examined in Chapter 4 above, the ECtHR in its 'well-established'[10] case law determines that the domestic law ought to be of a certain quality: it must be accessible to the person concerned and its effects ought to be foreseeable.[11] The law must be sufficiently clear and adequately indicate the circumstances and conditions under which authorities may conduct surveillance.[12] The law must indicate the scope of any discretion and the manner of its exercise by the authorities with sufficient clarity, which gives protection to individuals against arbitrary interferences.[13]

---

[6] There is no comparative legal analysis of the Russian and Tajik laws on the detection and investigation of crimes in the legal literature, but some Tajik authors make references to the Russian scholarship in an attempt to discuss Tajik law problematics. See Chapter 2 for more details.
[7] Russia ceased to be a party to the ECHR on 16 November 2022. See Press Release issued by the Registrar of the ECHR on 16 September 2022, ECHR 286 (2022).
[8] *Zakharov v Russia,* Judgment of the ECtHR dated 4 December 2015.
[9] In Chapter 4 (General Principles Relating to Surveillance, Data Protection and Privacy Rights under ECHR) the author examined the case law of the ECtHR on surveillance issues in general, while in this Chapter, Tajikistan laws on surveillance can be reviewed in light of those findings introduced by the ECtHR on the standards of human rights protection in the surveillance cases.
[10] The word 'well-established' is used by the ECtHR in *Zakharov v Russia* in respect of the case law on privacy and data protection: *Rotaru v Romania* (2000) ECHR 2000-V, *S and Marper vs UK,* Judgment of 4 December 2008, and *Kennedy v United Kingdom,* Judgment of the ECtHR dated 18 August 2010. See *Zakharov v Russia*, n 8 above, Paragraph 228.
[11] *Ibid.*
[12] *Zakharov v Russia,* Judgment of the ECtHR dated 4 December 2015, Paragraph 229; *Big Bagrother Watch v UK* (2021), Paragraph 333.
[13] *Zakharov v Russia,* Judgment of the ECtHR dated 4 December 2015, Paragraph 230; *Big Brother Watch v UK,* Judgment of 25 May 2021, Paragraph 333.

The Law of the Republic of Tajikistan 'On Crime Detection and Investigation' (the CDI),[14] and the Criminal Procedure Code (the CPC),[15] mainly regulate surveillance issues.[16] Both laws are publicly accessible – they were published in the official journal of the Tajik Parliament,[17] so the first criterion of the quality of law, i.e., its accessibility to the persons concerned, is met. In respect of the 'foreseeability' of the effects of the law, the ECtHR held that in the context of surveillance, this term cannot be the same as in many other fields.[18] It does not mean that the person concerned must be able to foresee the likeliness of interception of their communications by the authorities so that such a person can adapt their conduct accordingly. However, the risk of arbitrariness is present in cases where law enforcement bodies exercise their power in secret.[19]

In *Zakharov v Russia*, the ECtHR examined the requirement of 'foreseeability' together with the 'necessity' because in cases where the ECtHR examines domestic legislation permitting secret surveillance, the lawfulness of the interference is closely related to the question of 'necessity'.[20] The quality of secret surveillance law is scrutinized from the viewpoint of whether it is necessary in a democratic society.[21] The law must ensure that secret surveillance measures are applied only when the law provides adequate and effective safeguards and guarantees against abuse.[22] Under the CDI wiretapping of telephone conversations and other communications is allowed only in relation to persons suspected or accused of committing a grave or especially grave crime, as well as in relation to persons who may have information about these crimes.[23] Grave crimes are defined by the Criminal Code of the Republic of Tajikistan as those committed intentionally and which are punishable by five to twelve years of imprisonment; especially grave crimes – by more than twelve years of imprisonment.[24]

---

[14] Law of the Republic of Tajikistan (RT) "On Crime Detection and Investigation", No 352 dated 2 March 2011.
[15] Criminal Procedure Code of the RT dated 3 December 2009, No 12.
[16] Other laws, such as the Law of the RT 'On National Security Bodies' dated 6 March 2008, No 443, or the Law of the Republic of Tajikistan 'On Electric Communication' dated 10 May 2002, No 56, also contain some provisions related to surveillance.
[17] Bulletin of Majlisi Oli of the RT.
[18] See n 12 above.
[19] *Ibid.*
[20] See *Zakharov v Russia*, n 8 above, Paragraph 236. The requirement of 'necessity' or 'necessary in a democratic society' has been discussed in Chapter 4.
[21] See Schabas W. *The European Convention on Human Rights Commentary* (OSAIL 2015), p.406.
[22] See *Zakharov v Russia*, n 8 above.
[23] The CDI, Article 8(5). See n 14 above.
[24] The Criminal Code of the RT of 1998, Article 18. Here, CDI actually is more 'liberal' in comparison to its Russian counterpart, which includes also crimes of medium severity, which are punishable by minimum 3 years of imprisonment, into the list of crimes, which may trigger secret surveillance measures by authorities. See *Zakharov v Russia*, n 8 above, Paragraph 244.

The ECtHR requires that domestic law ought to provide sufficient detail on the nature of the crimes, and it expressed concern that Russian law allows 'secret interception of communications in respect of a very wide range of crimes, including for example, […] pickpocketing'.[25] Indication of a detailed nature of the crime in domestic law is the first requirement out of six 'Weber requirements', established by the ECtHR in 2006.[26] Likewise, CDI does not give further details of the nature of criminal offenses other than referring to grave and especially grave crimes. Under the second 'Weber requirement', the law ought to clearly define the categories of people liable to have their communications intercepted.[27] However, the CDI stipulates that secret surveillance measures could be taken in respect of any person who may have information about such crimes,[28] and the ECtHR expressed its concern that similar Russian domestic law provisions do not give any clear guidance on who exactly falls under this category.[29]

The third 'Weber requirement' establishes a limit to the duration of interception of communications.[30] According to the CDI, surveillance measures can be granted by a judge for a period of up to 6 months unless otherwise provided in the judicial resolution. The judge can prolong that term after examining new documents and data.[31] The CDI is silent about cases and grounds for termination of surveillance measures. This, in the opinion of the ECtHR, means that domestic law (Russian law) does not provide sufficient guarantees against arbitrary interference.[32]

The ECtHR criticized the urgency procedure under Russian law, which is identical to the CDI provisions on conducting surveillance without prior judicial approval.[33] Under the CDI, in urgent cases that may lead to the commission of a grave or especially grave crime, or where there is information about events or actions that pose a threat to the public, state, military, economic, information, or environmental security of the State, surveillance measure can be conducted without prior judicial authorization. In such a case, the judge ought to be notified within 24 hours. Within 48 hours from the start of the operational-search measure, the law enforcement bodies conducting surveillance must receive judicial authorization or discontinue surveillance.[34] This may leave the authorities an unlimited

[25] See *Zakharov v Russia*, n 8 above, Paragraph 244.
[26] See *Weber and Saravia v Germany*, n 3 above, Paragraph 95.
[27] *Ibid.*
[28] See n 23 above.
[29] See *Iordachi and Others v Moldova*, Judgment of the ECtHR dated 14 September 2009, Paragraph 44; *Zakharov v Russia*, n 8 above, Paragraph 245.
[30] See n 26 above.
[31] Article 9(5) of the CDI, n 14 above.
[32] See *Zakharov v Russia*, n 8 above, Paragraph 252.
[33] *Ibid.,* Paragraph 266.
[34] See the CDI, n 14 above, Article 8(3).

degree of discretion in determining the situation in which it is justified to use a non-judicial urgent procedure. The judge has no power to assess the justification of the use of urgent procedures or to decide the fate of the materials obtained during 48 hours of surveillance.[35]

Under the CDI, as under Russian law, judicial supervision of the surveillance measures is limited to giving initial authorization. Subsequent supervision is entrusted to non-judicial bodies, such as prosecutors.[36] The ECtHR requires that such an organ is independent of the executive bodies, e.g., when it is composed of members of parliament.[37] The Prosecutor General is appointed by the President of the Republic of Tajikistan (RT) upon the approval of the Parliament. Local prosecutors are appointed directly by the Prosecutor General.[38]

The ECtHR was critical of the role of Russian prosecutors in supervising surveillance measures. The Russian law envisages broad and diversified functions for the prosecutors, and supervision of criminal investigations is just one of them. It was not addressed properly and in detail in the law. The mixture of different roles by the prosecution bodies, i.e., their power to grant approvals for conducting surveillance measures on the one hand, and their supervisory function, on the other, raised doubts about their independence.[39] This critique can further apply to the Tajik law provisions on the prosecution bodies.

However, unlike Russian law on prosecutors, the Tajik law provides more specificity in the functions of prosecutors related to the supervision of crime detection and investigation procedures. Tajik prosecutors may request necessary information and documentation from the law enforcement bodies conducting surveillance measures on the progress of conducting those measures and have the authority to annul any unsubstantiated or unlawful decisions made by the officials (investigators, etc.) conducting surveillance.[40]

The ECtHR has found that the supervision by the prosecutors over the operations of national security bodies in Russia is limited in that it can only be meaningfully triggered following an individual complaint. Individuals are not notified about surveillance measures taken in respect of them, so it is unlikely that such a complaint would be lodged. National security bodies thus in fact avoid any prosecution scrutiny of their surveillance operations.[41]

---

[35] See *Zakharov v Russia*, n 8 above, Paragraph 266.
[36] See Article 31 of the Constitutional Law of the RT "On Prosecution Bodies of the Republic of Tajikistan" No 102 dated 15 July 2005.
[37] *Klass and Others v Germany,* n 5 above, Paragraphs 21 and 56; *Weber and Saravia v Germany*, n 3 above, Paragraphs 24-25 and 117.
[38] The Law of the Republic of Tajikistan 'On National Security Bodies' No 857 dated 30 January 2008, Articles 14 and 16.
[39] See *Zakharov v Russia*, n 8 above, Paragraph 280.
[40] See n 38 above, Articles 30-31.
[41] See *Zakharov v Russia*, n 8 above, Paragraph 281.

ECtHR thus has found that the prosecutors' supervision of the secret surveillance measures was not effective in practice.[42]

In respect of subsequent notification of interception of communications, the ECtHR assessed the laws of the Member States to the ECHR through the lens of the 'necessity' test. Not receiving any subsequent notification by individuals *per se* does not contradict the notion of 'necessary in a democratic society' as it is the very absence of knowledge of surveillance that ensures the efficacy of the interference.[43] As soon as it becomes possible to provide subsequent notification, without any harm to the purposes of the restrictive measures, information must be provided to the persons concerned.[44] In some instances, the ECtHR has found that the absence of subsequent notifications is incompatible with the ECHR.[45] In *Kennedy v UK,* the ECtHR has found that the absence of such a requirement is compatible with the ECHR because in the UK any person who suspects that they have been subject to secret surveillance measures can apply to the independent tribunal.[46]

Laws in Tajikistan do not provide for the subsequent notification requirement, so the persons concerned are unlikely to learn that they have ever been subject to secret surveillance. The effectiveness of any remedies, which individuals may resort to, is available only to persons who have information about the interception of their communications. Similarly, the ECtHR found the Russian laws as not providing for an effective judicial remedy against secret surveillance measures where no criminal proceedings were initiated against the persons concerned.[47] It stated that '[b]y depriving the subject of interception of the effective possibility of challenging interceptions retrospectively, Russian law thus eschews an important safeguard against the improper use of secret surveillance measures.'[48]

6.1.1.2. Quality of Law in Bulk Surveillance

Tajik law does not expressly and in detail regulate the bulk interception of communications of individuals and the safeguards against any possible abuse of power of those exercising such surveillance measures. There are however some provisions within the

[42] *Ibid.,* Paragraph 284.
[43] *Ibid.,* Paragraph 287.
[44] See *Klass v Germany*, n 5 above, Paragraph 58.
[45] See *Association for the European Integration and Human Rights and Ekimdzhiev v Bulgaria*, Judgment of the ECtHR dated 30 January 2008 and *Dumitru Popescu v Romania,* Judgment of the ECtHR dated 14 December 2006
[46] *Kennedy v United Kingdom,* Judgment of the ECtHR dated 18 August 2010.
[47] See *Zakharov v Russia*, n 8 above, Paragraph 298.
[48] *Ibid.,* Paragraph 300.

CDI, the CPC, the Law on Communication, the Law on national security bodies, and other legal acts, which may create the basis for bulk surveillance measures in Tajikistan.

In 2020, the Government of Tajikistan introduced a State system of identification of all mobile telecommunication devices (MTDs) through a procedure of registration of MTDs in a single database (the Procedure).[49] Every mobile phone, tablet, or any other device with a mobile telecommunication module (SIM card) must be registered with the State system of identification of such devices. The system is intended for the creation of a unified database containing information on the International Mobile Equipment Identifier (IMEI)[50] of all MTDs used, imported for sale or personal use, or produced in the territory of Tajikistan.[51] All switched-on MTDs with a functioning SIM card on the territory of Tajikistan are automatically registered with the system in the first three months of the trial. Individuals, who import MTDs, must register them and for these purposes must provide information about the device (its IMEI), copies of their passports, and their tax-payer identification numbers.[52] The database of all MTDs in Tajikistan shall be managed and processed by a private processor. However, the authorized State organ in the field of communications in Tajikistan ought to be considered as the controller of the database.[53]

The controller of the MTD database on a contractual basis integrates the database with other information systems or databases and can request from mobile operators the necessary technical information, including data on the operation of an MTD and activities performed by an MTD in real-time, as well as at regular intervals within the framework of the system operation.[54] The national security authority in Tajikistan, in order to suppress crimes in the field of information security, is provided with remote access to the system.[55] Lastly, the Procedure provides that in the interests of ensuring the security and defense of the State during the conduct of particularly important socio-political events, the system operator (processor), at the request of law enforcement agencies, forcibly suspends and resumes the operation of MTDs.[56]

The Procedure ranks lower than the CDI and the CPC in the Tajik system of legal normative acts, so, in case of any discrepancy between the Procedure and the laws, the latter

[49] The Government of Tajikistan passed Resolution No 208 dated 31 March 2020 'On the Procedure of Registration of Mobile Communication Devices and Defining Functions of the State System of Identification of Mobile Communication Devices', which approved the 'Procedure'.
[50] IMEI is a serial number consisting of 15 digits and allocated by GSMA. IMEI is available in all mobile telecommunications that support the operation of SIM cards. See the Procedure, n 49 above, Paragraph 1.
[51] See the Procedure, n 49 above, Paragraph 2.
[52] *Ibid.,* Paragraph 35.
[53] *Ibid.,* Paragraph 4.
[54] *Ibid.,* Paragraphs 51 and 55.
[55] *Ibid.,* Paragraph 56.
[56] *Ibid.,* Paragraph 57.

must apply.[57] The provisions of the Procedure explained above may be in contradiction with the standards of protection of the right to private life established by the ECtHR. If the national security authority is given remote access to the MTDs database, will this be contrary to the CDI and the CPC provisions on the need for judicial authorization?

The law on national security[58] is clear that the national security authorities of Tajikistan upon judicial authorization may request from legal entities and individuals, which provide postal and telecommunication services, providing access to special equipment for taking information from communication channels, as well as creating other conditions necessary for the national security bodies in Tajikistan to conduct crime detection and investigation. The Procedure, on the other hand, contains provisions that may render the statutory provisions requiring prior judicial authorization for secret surveillance ineffective. The vast majority of MTDs are registered with the database automatically, which means that the controller (Ministry of Communications) and the processor (a private company) will have access to the personal data of millions of individuals without receiving their express consent for the processing of their data. The ability of the national security authority to remotely access such databases may circumvent the authorization procedure. According to the ECtHR, such a system is particularly prone to abuse.[59]

The Procedure implies that some personal information, such as name and passport details, which include the address, marital status, taxpayer identification number, and the blood group of the entire adult population in Tajikistan, may become accessible to the national security authority.[60] All this information, coupled with the communication data (or metadata), such as time, length, duration, addressees, frequency of communications, geolocation of the MTD, the movement of the MTDs, and similar data, may become accessible by the national security authority without necessary judicial authorization.[61]

In Tajikistan, bulk surveillance can be conducted by the national security authority in respect of all kinds of communications: between MTD holders within the territory of Tajikistan, and between them and individuals outside Tajikistan. This is not in line with the ECtHR's perception of bulk surveillance, which is seen as a measure used by security forces only in respect of transborder communications.[62]

[57] According to Article 9 of the Law of the RT 'On Legal Normative Acts', No 1414 dated 30 May 2017, the laws and codes ought to have priority over resolutions of the Government of Tajikistan.
[58] The Law of the Republic of Tajikistan 'On National Security Bodies' No 857 dated 30 January 2008.
[59] See *Zakharov v Russia*, n 8 above, Paragraph 270.
[60] See the Procedure, n 49 above, Paragraph 56.
[61] *Ibid.*
[62] *Ibid*.

The ECtHR held that targeted and bulk surveillance measures differed in several aspects. Firstly, bulk interception is usually applied to the trans-border flow of communications, where the purpose of bulk interception is to monitor the communications of persons outside the territory of the surveilling State, which could not be monitored by other forms of surveillance.[63] Secondly, the purposes of targeted and bulk monitoring of communications are different. According to the ECtHR, targeted interception is in most cases used to investigate crimes, while bulk interception of communications is directed at early detection and investigation of cyber-attacks, counter-espionage, and counter-terrorism.[64]

The ECtHR does not consider bulk surveillance measures *per se* incompatible with the ECHR. However, the Court has adopted and further developed the 'Weber requirements' in respect of bulk interception of communications.[65] Under the previous sub-section called 'Quality of Law in Targeted Surveillance', this Chapter has examined Tajik law provisions through the lens of the first three 'Weber requirements' applicable to targeted surveillance. All six requirements were applied by the ECtHR to bulk surveillance measures in the *Weber* case.[66] The ECtHR has further developed 'Weber requirements' in the period between the *Weber* case of 2006 and the *Big Brother Watch (2021)*, the period during which technology has developed significantly, which led to changes in the way of communication between people. People increasingly live their lives online accumulating an enormous amount of data through their electronic communications, which are significantly different in nature and quality to those generated in times of the *Weber* case.[67]

In the *Big Brother Watch (2021)* case, the ECtHR revised the 'Weber requirements' in relation to bulk surveillance measures. For the ECtHR this time it was clear that the first two requirements were not readily applicable to a bulk interception regime. To reiterate, targeted surveillance is usually employed for investigation purposes in respect of the crimes already committed, while bulk interception of communications is primarily used for crime prevention purposes,[68] so the ECtHR has developed a separate set of criteria, which included some of the initial 'Weber requirements'. In total, the ECtHR defined eight 'Weber requirements' applicable to the bulk interception regime in the domestic law of the Member States.[69]

---

[63] See *Big Brother Watch (2021),* n 4 above, Paragraph 344. The ECtHR makes references to the German and Swedish laws, which foresee bulk surveillance only to monitor foreign communications outside the territory of those States.
[64] *Ibid.,* Paragraph 345.
[65] See n 1 above.
[66] See *Weber and Saravia v Germany*, n 3 above.
[67] *Big Brother Watch (2021),* n 4 above*,* Paragraph 341.
[68] *Ibid.,* Paragraph 348.
[69] All those eight criteria have been explained and analysed in Chapter 4 of the thesis.

The legal provision within the CDI permitting the wiretapping of communication concerns the content of the intercepted communications, as it uses the word 'listening' as wiretapping.[70] As opposed to the content data, the communication data can be intercepted by a national security authority without receiving judicial authorization for such surveillance measures. In Chapter 2 this thesis has emphasized the lack of conceptualization of the right to private life and data protection within the Tajik scholarship, which has led to confusion about the right to private life and the right to access information in the Law on Data Protection of the Republic of Tajikistan (Law on DP).[71] According to the Law on DP, any State body exercising their functions prescribed by law can process the personal data of individuals without receiving their consent.[72] Granting free access to MTDs empowers national security authorities to track all incoming and outgoing communications, including their timing, length, and frequency, associated with identified individuals. Furthermore, it allows for the monitoring of the movement of these individuals, including their typical routes, destinations, visited places, and regular interactions with other MTD users. The ECtHR in *Uzun v Germany* noted that the surveillance by GPS allowed authorities to collect and store data determining the whereabouts and movements of the individual, which in the ECtHR's view amounted to interference.[73] This type of surveillance is not regulated by Tajik law and the first 'Weber requirement' of having grounds for authorizing bulk interception is thus not met in Tajik law.

Bulk interception of communication through remote access to the MTDs database gives the national security authority the power to abuse its right to monitor those communications because there is no legal provision which would set a mandatory requirement of receiving judicial authorization for interception of communication data. The ECtHR in the *Big Brother Watch (2021)* case confirmed that the acquisition of communication data was not necessarily less intrusive than the acquisition of content,[74] and therefore the bulk interception of communications must be subject to independent authorization.[75]

Contrary to the 'Weber requirements', Tajik law does not prescribe the circumstances in which communication data can be intercepted, and procedures to be followed for granting authorization and using or storing the intercepted data. The ECtHR held that the use of bulk

[70] See the CDI, n 14 above, Article 8(5).
[71] See Chapter 2, Section 2.6 'Personal Data Protection Law in Tajikistan'.
[72] See The Law of the Republic of Tajikistan "On Personal Data Protection", No 1537, dated 3 August 2018, Article 12.
[73] *Uzun v Germany,* Judgment of 2 December 2010, Paragraphs 51-52.
[74] See *Big Brother Watch (2021),* n 4 above, Paragraph 363.
[75] *Ibid.,* Paragraph 350.

surveillance can be compatible with the ECHR only in case of the most significant threats if it is strictly necessary for the safeguarding of democratic institutions and for the obtaining of vital intelligence.[76] Murray and Fussey suggest that only threats that themselves threaten a democratic society could justify bulk surveillance measures.[77]

The Procedure makes only one reference to the purposes of suppression of crimes in the field of information security as a legal ground for conducting bulk surveillance by the national security authority.[78] Tajik Criminal Code contains seven different articles on the crimes against information security, which are mainly about cyber security, and only one of them can be considered a grave crime – illegal acquisition or interception of data from computers, conducted repeatedly, or by an organized group or resulted in the death of a person.[79] In respect of the other crimes, the national security authority is even not authorized to conduct interception of communications, as those crimes are considered to be non-grave and the maximum punishment for those does not exceed four years of imprisonment.

Laws authorizing mass surveillance in the form of access to personal data, which is inferred from combined categories of communication data, will be deemed to breach the proportionality principle under the standards established by the ECtHR.[80]

The legal provisions in the Tajik law related to bulk surveillance measures do not thus squarely comply with the standards set by the ECtHR jurisprudence.

6.1.2. The EU GDPR Standards and Tajik Data Protection Law

Having explored the lessons that Tajikistan could learn from ECHR, this thesis will next turn to explore perspectives from the European Union (EU) General Data Protection Regulation (GDPR),[81] thus moving away from crimes and bulk surveillance mainly by the State institutions, to exploring general data protection where the role of the State and private operators is important.

This thesis has indicated the main GDPR standards for the protection of personal data in Chapter 5: lawfulness, fairness, and transparency.[82] These three principles are named

[76] *Szabo and Vissy v Hungary,* Judgment of 6 June 2016, Paragraph 73.
[77] Daragh Murrey and Pete Fussey 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Approach to Bulk Monitoring of Communication Data' (2019) 52(1) Israel Law Review 31.
[78] See the Procedure, n 49 above, Paragraph 56.
[79] See the Criminal Code, n 24 above, Article 301(4)
[80] See Martin Sheinin 'Towards Evidence-based Discussion on Surveillance: A Rejoinder to Richard A. Epstein' (2016) 12 European Constitutional Law Review 341.
[81] General Data Protection Regulation of 2016 (Regulation (EU) 216/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), (2016) OJ L119/1).
[82] Those standards are called principles of data processing in Article 5(1)(a) GDPR. See GDPR, *ibid*.

as core principles of data processing by the European Data Protection Supervisor (EDPS).[83] Lawfulness means that there ought to be legal grounds for processing personal data. Such legal grounds ought to be clearly indicated in the law accessible to people. As De Hert and Gutwirth put it, data protection laws do not protect individuals from data processing, but from unlawful and disproportionate data processing.[84] Personal data can only be processed for specifically indicated, express, and legitimate purposes, and may be further processed only for the purposes and under the conditions specified in the law.[85]

6.1.2.1. Lawfulness of data processing

Tajikistan Law on DP foresees three lawful grounds for processing personal data:

1) when a data subject gives their consent for data processing;
2) when the data processing is carried out by the State organs implementing their public functions; and
3) when constitutional rights and freedoms of individuals ought to be protected.[86]

The first ground, i.e., the consent of the data subject is a primary legal ground in Tajikistan for data processing, and the other two grounds are mentioned in the Law on DP as the exceptions to the primary ground.[87] Those two exceptions are effectively granting wide discretion to the State organs to process the personal data of people without having received their consent.

First of all, State organs have a wide range of functions, which makes it possible for them to carry out data processing as something intrinsic to their activity. Since the law does not prescribe obtaining the consent of a person to the processing of their data by State organs, the latter will not treat the processing of personal data as something that requires special care and accuracy. Since the law does not outline in detail in what specific cases and for what specific purposes the collection and processing of personal data by State organs are allowed, they will be able to use the accumulated and retained personal data for almost any purpose, justifying this by the need to perform their functions.

---

[83] See EDPS Opinion 8/2016 'On Coherent Enforcement of Fundamental Rights in the Age of Big Data' dated 23 September 2016.
[84] See Paul De Hert, Serge Gutwirth et al (eds) *Reinventing Data Protection* (Springer Science+Business Media B.V., 2009), p.3.
[85] *Ibid.,* p.4.
[86] The Law on DP, n 72 above, Articles 8 and 12.
[87] The Law on DP (Article 8) establishes that data processing is carried out upon an individual's consent, except for the cases indicated in Article 9. It must be a typo because the exceptions to that main rule are actually contained in Article 12, not Article 9. Article 12 is called 'Collecting and processing personal data without the consent of a data subject'. Article 9, on the other hand, is devoted to the issues of access to personal data.

Within the EU, in addition to the GDPR, another law regulating data protection issues is the Regulation on Data Protection by the EU Institutions (the Regulation).[88] According to the Regulation, the EU institutions may lawfully process personal data under one of the five different legal grounds:[89]

1) processing is necessary for performing a task in the public interest or in the exercise of official authority vested in the EU institution;
2) processing is necessary for compliance with the legal obligation of the controller;
3) processing is necessary for performing the contract to which the data subject is a party;
4) the data subject has given their consent for one or several purposes; and
5) processing is necessary in order to protect the vital interests of the data subject or other persons.

All these five grounds are reflected in the GDPR.[90] The Regulation and the GDPR foresee a wide range of legal grounds for data processing with a view to having more detailed, express, and specific rules, which data controllers will need to comply with in order to minimize the possibility of abuse. The more detailed a rule is, the less room for the abuse the controller or processor will have. The Regulation and the GDPR prohibit the processing of special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, and an individual's sex life or sexual orientation.[91]

There are specific and clear instances or legal grounds referred to in the EU law as exceptions to the processing of special categories of personal data by the controllers, public or private ones. An individual's explicit consent for processing their sensitive personal data is one of the main exceptional legal grounds for such data processing. Since Tajikistan Law on DP allows it, all above mentioned sensitive data can be processed by the Tajik State organs without receiving the consent of data subjects. Only biometric data is mentioned in the Tajikistan Law on DP as a category of data, which requires special treatment.[92]

[88] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 'On the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data', (21.11.2018) OJEU, L 295/39.
[89] *Ibid.*, Article 5 (Lawfulness of processing).
[90] Article 6 GDPR contains similar grounds applicable to private controllers and processors and foresees one more legal ground: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. See GDPR n 81 above.
[91] Article 10 of the Regulation and Article 9 GDPR.
[92] See Law on DP, Article 17.

Tajikistan State organs as data controllers will have to obtain the consent of data subjects for the processing of biometric data, except for the long list of cases, which would exempt the State from receiving any consent from individuals. Such exceptional cases include cases when criminal prosecution and justice must be exercised, judicial acts must be enforced, as well as in cases provided for by the legislation of the Republic of Tajikistan on defense, security, crime detection and investigation, countering terrorism, extremism, corruption and legalization (laundering) of proceeds from criminal activity, financing of terrorism and financing the proliferation of weapons of mass destruction, enforcement of criminal sentences, acquisition and termination of citizenship of the Republic of Tajikistan and the laws on public service.

The third legal ground for processing personal data, which is indicated in Tajikistan Law on DP, and emerges as a second exception to the main legal ground (the consent of the data subject), is when State organs seek to protect human rights.[93] This is again a very vague and indeterminate provision, which gives public authorities the possibility to process the personal information of individuals under the auspices of human rights protection. Human rights can be civil and political as well as economic, social, and cultural. They can be individual or collective. There is a large catalog of rights and freedoms, and the State organs in exercising their public functions always deal with human rights. Again, the State organs in reality may always find an excuse for processing personal data by referring to human rights protection. The Regulation and the GDPR refer to the 'vital interests of the data subject of other persons', which is quite indeterminate in nature, but nevertheless is narrower in meaning than the Tajik law's generic reference to human rights.

Chapter 2 of this thesis has explained the Tajik legal thought in respect of data protection and privacy issues as focusing on the role of the State not as a possible human rights violator, but as a protector of human rights. Individuals are seen as the main perpetrators and violators of the right to private life, and the role of the State bodies is to establish a system that would provide safeguards to the privacy of individuals from possible encroachments of other individuals. Such safeguards include possible penalties to those private parties, which violate data protection and privacy laws in Tajikistan.

The Law on DP clearly reflects such observation. All privately owned data controllers and processors must receive the consent of the data subjects in order to be able to process their personal data, while State organs – controllers and processors are free from

[93] The Law on DP, Article 12 refers to the constitutional rights of a human and a citizen.

such obligation. They can process any personal data just because they exercise their statutory functions, or because they protect data subjects' constitutional rights and freedoms.

The MTDs database is processed by a private processor. However, it is controlled by the State organ (the data controller). Since the Law on DP prescribes that only State organs may collect and use personal data without the consent of data subjects, it ought to be considered unlawful for a private processor to collect and use the personal information without receiving prior consent of each of the MDTs holders. Initially, all MTDs in the territory of Tajikistan were automatically registered with the database, which means that no separate and express consent from any of the data subjects, whose MTDs were in use in Tajikistan, could have been received for the purposes of data processing.

6.1.2.2. Fairness and Transparency of Data Processing

The principle of fairness in data processing is not expressly defined by the GDPR or the Regulation. The fair processing of personal data includes different rights and to a considerable extent concerned with transparency.[94] Clifford and Ausloos divide the fairness principle into procedural fairness and fair balancing elements.[95]

The individuals must be informed about the fact that their personal data is collected, and they ought to know for what purposes and to what extent such personal data will be processed. They ought to be made aware of risks, rules, safeguards, and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. The personal data ought to be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum.[96]

Data controllers must provide information to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Controllers ought to always be able to provide information on their identity and contact details, the purposes and legal basis for data processing, recipients and third countries, where personal data is planned to be transmitted.[97]

[94] Roger Bronsword 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' in Gutwirth S., et al. *Reinventing Data Protection?* (Springer 2009), p.83.
[95] Damien Clifford and Jef Ausloos 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130.
[96] GDPR, Paragraph 39.
[97] GDPR, Articles 12-14.

Tajikistan Law on DP lays out those three core principles: lawfulness, fairness, and transparency, but does not specify what they mean.[98] There are no other references to these three principles elsewhere in the text of that law. In addition to them, the Law on DP further mentions observance of human rights and freedoms, the confidentiality of data under restricted use, equality of the rights of data subjects, controllers, and processors, and providing security for individuals, society, and the State.

Observance of human rights is an attractive narrative, which is meant to give the impression that the law is about protecting human rights and freedoms. As was noted earlier, the Law on DP gives the right to the State organs, exercising the functions of the data controller, to collect and process personal data without receiving data subjects' consent, *inter alia*, for the purposes of protecting human rights and freedoms. Taking into account the main focus of the Law on DP, which is about granting or having access to personal information by other individuals,[99] it is evident that the Law on DP is not directed at protecting the rights of individuals *viz-a-viz* the State. The observance of human rights is used as a legal ground for the State to avoid the situation where the consent of individuals for processing their data is mandatory.

The Law on DP, however, foresees some provisions which are in line with the fairness and transparency of data processing. The collection and processing of personal data must be limited to the achievement of specific, predetermined, and legitimate purposes. It is not allowed to process personal data that is incompatible with the purposes of its collection. The content and scope of the collected and processed personal data must comply with the stated purposes of collection and processing.[100]

When collecting and processing personal data, the accuracy of personal data, their sufficiency, and, if necessary, their significance in relation to the purposes of collecting and processing personal data, must be ensured. The processor must take the necessary measures to clarify incomplete or inaccurate data.[101]

The data subject must be notified about the data collected about them, they must be provided with access to the data concerning them, and they have the right to demand the correction of inaccurate or misleading data.[102]

Reverting to the issue of creating and using the database of the MTDs introduced by the Procedure, this thesis poses a question of whether all personal data contained in the

[98] The Law on DP, Article 4.
[99] See Chapter 2, where the author analyzed the Law on DP, and revealed its focus was not on the protection of the right to privacy, but on securing the right to receive information.
[100] The Law on DP, Article 8.
[101] *Ibid.*
[102] *Ibid.*

MTDs and inferred from MTDs and the SIM cards used by the particular MTDs, can be said to be processed in a fair and transparent way. The purpose of collecting and processing the personal data of the MTD holders is not clearly announced in the Procedure.

It is implied that after the initial automatic registration of all MTDs within the prescribed trial period of three months plus six months thereafter, all remaining MTDs will be registered for a certain State fee.[103] However, what do data subjects receive in exchange for paying the State fee? The Procedure gives no express and clear guidance on this. It is implied that in case the MTD is not registered with the database within the prescribed time, the holder of the MTD will not be able to use the services of any Tajikistan telecommunication services providers: Internet or cellular communication services. Can this be regarded as a fair purpose for collecting and processing personal data?

All telecommunication services providers in Tajikistan provide their services to the data subjects on a contractual basis, for which purposes they already collect and use the personal data of their customers, such as passport details, so there is no further reason for the data subjects to provide their personal data to another data controller and/or processor to be able to make use of the telecommunication services they are already paying for. The Procedure thus gives no indication that the data processing by the private entity operating the database and by the data controller – the State organ will be fair or transparent.

To summarize the Section 6.1 findings, this thesis submits that the laws on privacy and data protection in Tajikistan do not to the fullest extent reflect the standards established by the EU data protection law as well as the human rights law standards set by the ECtHR. In the field of detection and investigation of crimes, Tajikistan laws lack a clear mechanism for judicial authorization and review in case of the use of bulk surveillance. The competence of the national security authority is not defined in detail and the law allows the State organs to conduct surveillance without receiving prerequisite judicial authorization. Most of the 'Weber requirements' set by the ECtHR's jurisprudence in respect of the domestic laws of the ECHR Member States are absent in the CDI.

Tajikistan Law on DP does not provide sufficient safeguards in respect of data processing. It is designed not to protect individuals from the State data controllers. On the contrary, the law gives the State organs almost unlimited powers to collect and use the personal data of individuals without their consent for almost any purpose.

The laws in Tajikistan are reflecting the Tajik legal thought on the right to private life and data protection: State organs cannot be seen as perpetrators, as they aim to protect

[103] See the Procedure, n 49 above, Paragraphs 13, 15, 29, and 49.

individuals from other individuals, who may interfere with their private lives. The government uses a human rights protection narrative in order to be able to process personal data without any constraint. Private data processors and controllers are put in an unequal situation compared to the State controllers because the only lawful ground for them to collect and process personal data is receiving the consent of the data subject. Private entities in Tajikistan are deprived by the law of processing the personal data of their customers on the basis of performing their contract or other bases, which are deemed to be a standard legal provision in EU law.

6.2. The Case Study of Tajikistan: the 'Brussels Effect' or Legal Transplants?

The questions of why Tajikistan needs data protection law and how it ought to be shaped lead to the discussion of whether Tajikistan data protection laws may be seen as legal transplants.

More generally, a broader question that needs to be explored in relation to the possible adaptation of Tajik laws to ECHR and EU law is how to conceptualise the legal nature and conceptual basis of the adaptation. In the sections that follow, the so-called 'Brussels Effect' and the broader discourse regarding legal transplants will be explored to this end in relation to Tajikistan, which is a third country.

6.2.0.1. The 'Brussels Effect'

Anu Bradford coined the term 'Brussels Effect', explaining that only large economies, such as the EU, can become sources of global standards.[104] According to her, the EU sets certain standards in different spheres of legal regulation, such as environment or data protection, which are de facto followed globally.[105] The EU data protection laws, specifically GDPR, establish rules and regulations, which are enshrined in the legislation of third countries. Chapter V of the GDPR is devoted to the transfer of personal data to third countries, and according to that chapter, one of the legitimate means of transferring personal data from the EU to third countries is a so-called 'adequacy decision' mechanism. As we mentioned in Chapter 5 of the thesis, the European Commission after examining the relevant

[104] Anu Bradford 'The Brussels Effect' in Bradford A. *The Brussels Effect* (OUP, 2020), p.26.
[105] See Anu Bradford 'The Brussels Effect' (2012) 107 Nw. U.L. Rev. 1 and Bradford A. *The Brussels Effect* (OUP, 2020).

data protection laws[106] of a third country may decide that the data protection regime in that third country adequately protects the fundamental rights and freedoms of individuals, namely the right to data protection during the processing of personal data.

The significance extends beyond market size to encompass regulatory capacity, stringent standards, inelastic targets, and non-divisibility, all of which Anu Bradford highlighted as essential elements of the 'Brussels Effect'.[107] In simpler words, if businesses, i.e., controllers and processors, originating in Tajikistan, seeks to enter the EU market of goods, services, and capital, and offer and trade goods and services in the EU, the domestic data protection laws of such businesses' country of origin, i.e., Tajikistan, ought to be in line with the high standards of data protection set by the GDPR.

Analysis of Tajikistan law on data protection, which is provided in Chapter 2 of this thesis, and the areas of Tajik law to be improved in the light of the GDPR as discussed in Section 6.1 above, leads to an understanding that the Tajikistan data protection law of 2018 was not necessarily designed and drafted with a view to fully complying with the standards set by the GDPR. The present author has not made empirical research on whether there is a significant demand for Tajik businesses to enter the EU market. However, since the domestic law on data protection does not adequately guarantee protection for individuals while processing their data, and since that law has been dormant since its enactment, it becomes obvious that there is no urgency for Tajik businesses to have in place the domestic legislation, which would be in line with high standards of data protection set by the EU. Otherwise, there would have been at least a discussion among different stakeholders about the need to improve the Law on DP and other legal instruments to comply with the GDPR standards.

As discussed in Chapter 2 and Section 6.1 of this Chapter, Tajik legal thought on the right to privacy has influenced the content and the shape of Tajikistan data protection law with the lamentable consequence that it does not provide adequate protection to individuals – data subjects, as understood by the EU data protection legislation. The legislation on electronic trade (or commerce) in Tajikistan was adopted for the first time only in 2022 and has not yet been tested.[108] It contains no specific provisions for data protection.

---

[106] Article 45, paragraph 2(a) GDPR specifies that the Commission while making relevant decisions in respect of the third country's laws shall take into account 'the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred'.

[107] Anu Bradford, n 104 above.

[108] The Law of the Republic of Tajikistan "On Electronic Trade" dared 24 December 2022, No 1921.

For the 'Brussels Effect' to happen in respect of Tajikistan data protection laws, at least two principal factors must be in place: 1) an increased demand among Tajik businesses to offer and export goods and services to the EU market, and 2) emergence of a debate among legal scholars on the concept of privacy in Tajikistan. The first factor depends on the economic growth of the country and its exporting capacity, while the second factor may be in place when all spheres of life, in which personal data is processed automatically, need more detailed legal regulation. At present, neither of those two factors exists.

6.2.0.2. Legal Transplants

Another way to conceptualize the possible voluntary adaptation of legal norms by third countries is through the perspective of the discourse on legal transplants. Transplantation of law is understood as a movement of legal norms and rules from one jurisdiction to another through law-making or legal reform.[109] The notion of 'Legal transplants' was first used by Kahn-Freund[110] and conceptualized by Watson[111] in the 1970s. Since then, this concept has evolved through a well-known debate about its possibility and impossibility as well as its relation to society and culture.[112] For Watson, the development of the law is free from any social, political, and cultural factors, and legal transplantation is an easy exercise because most changes in most jurisdictions emerge as a result of legal borrowing from other jurisdictions.[113] On the other hand, Legrand in his seminal work 'The Impossibility of Legal Transplants' disagrees with Watson, arguing that transplantation of law or legal rules is impossible since different jurisdictions reflecting different cultures and contexts cannot provide the same meaning to the legal concepts and rules borrowed from the donating jurisdiction.[114] Both views were criticized for the lack of empirical evidence and for being radical.[115]

Some authors interpret legal literature on legal transplants as a reaction to the functionalist-positivist views of the law, i.e., to a collection of legal norms produced by power-holders in response to the social need with the mechanism in place to enforce those

[109] See Tatiana Kyselova 'The Concept of Legal Transplant' (2008).
[110] Otto Kahn-Freund 'On Uses and Misuses of Comparative Law', (1974) 37 Modern Law Review 1.
[111] Watson A. *Legal Transplants: An Approach to Comparative Law* (Scottish Academic Press, 1974; American ed. University Press of Virginia, 1974).
[112] See Andrew Harding 'The Legal Transplants Debate: Getting Beyond the Impasse?' in Breda V. (ed.) *Legal Transplants in East Asia and Oceania* (CUP, 2019) p.13.
[113] See Alan Watson, n 111 above and Alan Watson 'Aspects of Reception of Law' (1996) 44 Am. J. Comp. L. 335, 335.
[114] Pierre Legrand 'The Impossibility of Legal Transplants' (1997) 4 Maastricht Journal of European and Comparative Law 111. For a more recent discussion see Glanert S., Mercescu A., and Samuel G. *Rethinking Comparative Law* (2021, Edward Elgar Publishing Limited).
[115] See Harding, n 112 above.

norms.[116] In their view, the research on legal transplants represented a challenge to that account of law, because many legal systems borrow legal norms regularly irrespective of economic, social, political, and cultural barriers that separate the world's legal systems.[117]

Legal transplants can have advantages and disadvantages. The main advantage, according to Corrin, is that the transplanted law has been already drafted and scrutinized in a donor country through a legislative process.[118] In a developing country such as Tajikistan, with limited resources and legislative know-how in a particular field of law, a ready-made law can be regarded as a better way of introducing new legislation.

Having similar laws in different jurisdictions, like in donor and receiving States, can be advantageous for trade.[119] The main disadvantage, however, of the legal transplants is that they do not originate from the borrowing or receiving jurisdiction, which may lead to the problem of fitting the law or legal rules into the existing system and the context, in which those legal rules ought to be applied in the receiving country.[120] Corrin interpreted Kahn-Freund's account of legal transplantation in a way that the success of transplants depends on the type of the laws, where public laws are unlikely to succeed due to cultural differences in different jurisdictions.[121] Harding suggests that some laws have a potentially more complex relation to culture than other laws, and for this reason, some laws are easy to transplant and others are not.[122]

In the 1990s, the legal scholarship on legal transplants shifted its focus to EU harmonization and post-Soviet and East European reform processes, where technical assistance agencies from the European States consolidated their efforts on judicial and legislative reforms.[123] In the field of business law and commercial law, a large number of legal experts from Europe were involved in drafting and consulting formerly socialist countries.[124] They acted on the premise that the newly emerged market-oriented economies in Eastern Europe and the CIS had no time to carefully craft naturally homemade and culturally aware legislation. Waelde and Gunderson echoing Watson's account of legal transplants, discussed the 1990s approach as follows:

---

[116] Michele Graziadei 'Legal Transplants and the Frontiers of Legal Knowledge' (2009) 10 Theoretical Inquiries in Law 693, at 696.
[117] *Ibid.,* pp.697-698.
[118] Jennifer Corrin 'Transplant Shock: The Hazard of Introducing Statutes of General Application' in Breda V. (ed.) *Legal Transplants in East Asia and Oceania* (CUP, 2019) p.34.
[119] *Ibid.,* p.35.
[120] *Ibid.,* p.36.
[121] See Corrin, n 118 above, p.36. Corrin refers to Kahn-Freund, see n 110 above, pp.5-6.
[122] See Harding, n 112 above, p.22.
[123] See more on this Toby Goldbach 'Why Legal Transplants' (2019) 15 Annual Review of Law and Science 583, at p 587.
[124] Daniel Berkowitz, Katharina Pistor and Jean-Francois Richard 'The Transplant Effect' (2003) 51 The American Journal of Comparative Law 163, at p.164.

> [W]ith regard to the legislation of a more technical, less political character (as traditional core contract law) it makes sense not to try to reinvent the wheel; indeed, it may seem that 'technical' or 'formal' rules, i.e., those that do not have a strong linkage with the prevailing social and political beliefs, interests and institutions, can be transplanted quite easily.[125]

Knieper expresses concern that a first wave of Western economic and legal advice to the East European and CIS countries on the market economy in the early 1990s mainly concerned the privatization of State enterprises, liberalization of trade and financial markets, deregulation of the economy, and restricting the State to fiscal discipline; the Adam Smithian 'invisible hand' of the market will do the rest.[126] After the 'shock therapy' reforms turned into a social disaster, those Western advisors – 'shock therapists' – changed their minds and started insisting on the role of the State institutions, a secure legal environment, and social protection.[127]

Influenced by a transition into a market-oriented economy and democratic governance, Tajikistan 'imported' public and private laws from the West. Dupre points out that

> [a]rguably, law importation was one of the main characteristics of these transitions: in order to become liberal democracies, post-communist countries imported the institutions and the law of the democracies of the West. […] [a]s a result, post-communist countries faced a double process of transition: one at the economic level, the other at the political level.[128]

Institution building became one of the necessary prerequisites for legal reforms. Technical assistance rendered by Western development agencies included creating, staffing and financing new institutions, which were not associated with the Soviet legacy.[129] For example, in Tajikistan, the Council of Justice was established in 1999[130] as a new and unknown to the Soviet system organ. It was an attempt to enhance judicial independence from the Ministry of Justice, which was in charge of the administrative and financial matters

---

[125] See Thomas Waelde and James Gunderson 'Legislative Reform in Transition Economies: Western Transplants – A Short-Cut to Social Market Economy Status?' (1994) 43 International and Comparative Law Quarterly 347, at pp. 368-369.
[126] Rolf Knieper 'Pulls and Pushes of Legal Reform in Post-Communist States' (2010) 2 Hague Journal on the Rule of Law 111, at p.113.
[127] *Ibid.,* p.114.
[128] Dupre C. *Importing the Law in Post-Communist Transitions: The Hungarian Constitutional Court and the Right to Human Dignity* (Hart Publishing, 2003) 192, at p.11 and 16.
[129] *Ibid.,* p.117.
[130] The Council of Justice was established by the Presidential Decree 'On Establishment of the Council of Justice of the Republic of Tajikistan' dated 14 December 1999, No 48.

of the courts and judge nomination procedures as well as judge training programmes. All those competencies were transferred to the Council of Justice; it was virtually a spin-off of an entire department with the staff from the Ministry of Justice.

Different development agencies immediately started supporting the newly established organ by providing their technical assistance. In 2016 the Council of Justice was dissolved and all its staff was transferred to the Supreme Court and the High Economic Court.[131] Knieper suggests that in most cases the development agencies and donor countries ought to work with the existing institutions and try to reorient them.[132] This is an example of a transplanted public law in the Tajik legal system, which did not last long.

This author during many years of practicing law in Tajikistan has experienced the effects of the application of the transplanted laws related to business and economic activity. A few selected examples of legal reforms in Tajikistan involving foreign or international technical assistance are: 1) State registration of companies has been transferred from the competence of the Ministry of Justice to the Tax Committee in 2009,[133] 2) pledge and mortgage rights registration was entrusted to the Ministry of Justice in 2005-2008,[134] and 3) the mortgage registration and other types of immovable rights registration became the competence of the Land Committee in 2018.[135]

The first example concerns international technical assistance to Tajikistan in the field of opening and liquidating businesses, and was designed to simplify the procedure of registration and deregistration of companies. The Tax Committee performs a dual function: (1) acts as a regulator, registering companies and any amendments in the register, and (2) acts as a fiscal authority that collects taxes. Ideally, these two different functions must not affect or depend on each other; however, the reality is that before making changes to the State register in connection with a change in the shareholding structure of the company, the Tax Committee requires the company to pay all taxes, both corporate and related to a specific transaction, as a result of which there was a change in the composition of the company's

[131] the Presidential Decree 'On Liquidation of the Council of Justice of the Republic of Tajikistan' dated 9 June 2016, No 698.
[132] See Rolf Knieper, n 126 above, p.117.
[133] The Law on "State Registration of Legal Entities and Individual Entrepreneurs" dated 19 May 2009, No 508.
[134] The Law on "Pledge of Movable Property" dated 1 March 2005, No 93; the Law "Mortgage" dated 20 March 2008, No 364.
[135] In 2015 the Government of Tajikistan adopted the Resolution 'On the Issues of Maintaining the Unified System of State Registration of Immovable Property and Immovable Property Rights' dated 2 July 2015, No 432 introducing a new state register for mortgages, and in 2018 the Law of the Republic of Tajikistan 'On State Registration of Immovable Property and the Rights to Immovable Property' was amended to introduce the mentioned reform.

shareholders. Without paying taxes, registration does not occur. The previous procedure for registering companies did not depend on paying taxes.

The second example is related to software that a foreign development agency has installed in the computing systems of the Ministry of Justice providing necessary hardware for pledge and mortgage registration. Technical assistance included basic training for the staff in the Ministry of Justice on the exploitation of the pledge and mortgage register. However, it did not include any IT staff specialist, who could maintain the system. As a result, in a few years after launching the register, the software and hardware malfunctioned, and for some time there were no means or the capacity to register pledges or mortgages.

In the third example, the focus shifts to staff training, specifically emphasising legal training this time. The Land Committee registers a mortgage as a security for five years but the law does not prescribe this limitation. The staff dealing with the registration matters simply refers to the period in which a debtor/borrower must perform its main obligations secured by a mortgage. Erroneous reading of the law by the staff of the Land Committee may limit the creditor's right to enforce the mortgage.

The above-mentioned examples concern public laws, which are technical, i.e., they all regulate different business registers and do not affect cultural or societal norms in Tajikistan. Those laws survived some amendments and modifications, but are working in a way, which was not probably envisaged initially by the development agencies that brought those laws to Tajikistan. So, even if a transplanted law has little relation to the culture, it may not serve the purpose to the fullest extent due to many other factors mentioned in those examples. Harding points out that the main problem is a vivid tendency of the technical assistance to transplant laws with no regard for the societal context in the receiving States.[136] In Chapter 2, this thesis has referred to a Tajik author who elucidated the Tax Code of Tajikistan as emblematic of a transplanted legal framework, formally characterized as resembling a Roman legal tradition while substantively resembling an Anglo-Saxon legal tradition.[137]

Chapter 2 of this thesis has explained the Soviet legacy of contemporary Tajik law. On the one hand, Tajikistan was part of the Union of the Soviet Socialist Republics (USSR), and its laws were part of the USSR laws, which were not transplanted from any other jurisdiction and were a product of a socialist idea of governing the society. On the other

[136] See Harding, n 112 above, p.25.
[137] See Chapter 2, Section 2.2.2 'Tajik Legal System After Gaining Independence (1991-2024)'. Specifically, see A. Kholiqzoda 'Nazare ba tabiati huquqii "qonuni milli" va vizhagihoi on' [The view on the nature of the "national law" and its peculiarities] (2018) 2 Davlatshinosi va Huquqi Inson [State Science and Human Rights] 10.

hand, Soviet law was introduced in Tajikistan as a new legal order irrespective of any cultural, social, or other considerations. Soviet law, in this respect, was neither a transplant nor an autochthonous set of legal rules. The post-Soviet Tajikistan law currently represents mainly the Soviet legal idea in the context, which is different from the Soviet times. Tajikistan law is currently a set of legal rules reflecting a mixture of Soviet, to a lesser extent, pre-Soviet, and Western culture due to the massive 'importation' of Western laws.

The CDI and the Law on DP thus represent different sources of origin. The CDI is a product of post-Soviet legal thought inherited by Russia, Tajikistan, and some other post-Soviet States. Although formally CDI could be regarded as a legal transplant from Russia, it nevertheless reflects the Soviet legacy of considering an individual not as a right-bearer, but rather as a duty holder. The Law on DP, on the other hand, represents a mixture of legal norms, which reflect Soviet and post-Soviet legal thought, and which are adapted to the Tajik legal system from different jurisdictions of liberal democracies. In some parts, the Law on DP contains legal provisions similar to GDPR, and in other parts, it reflects a post-Soviet approach to personal information as information of an individual to be protected from access by other individuals. As a result, the Law on DP, while still not tested in practice, cannot provide meaningful regulation of data processing and cannot ensure full protection of the privacy of data subjects.

6.3. Internal Perspectives for Tajikistan: why Tajikistan Ought to Develop its Data Privacy Laws

6.3.0.1. Law on Crime Detection and Investigation (CDI)

In Section 6.1 above this thesis has discussed the shortcomings of the Tajik laws related to State surveillance and data protection in the light of the standards set by the ECHR and the GDPR, respectively. In this Section, the thesis discusses whether Tajikistan needs to change its domestic laws on State surveillance. The compatibility of the CDI provisions with the 'Weber Requirements' as established in the ECtHR cases of *Zakharov v Russia,*[138] and *Big Brother Watch (2021)*[139] can be a basis for improving Tajikistan laws on State surveillance.

Within the frame of the universal periodic review conducted by the UN Human Rights Council, the human rights situation in Tajikistan has been subject to review three

[138] *Zakharov v Russia*, Judgment of the ECtHR dated 4 December 2015.
[139] *Big Brother Watch and Others v* UK, Judgment of 25 May 2021, ECHR.

times so far.[140] In the last cycle of review, the Council's working group has presented its report in 2022 and recommended that Tajikistan secure guarantees against interference with individual privacy in the context of the CDI.[141] This recommendation appeared due to the governmental resolution establishing the State-owned Unified Commutation Centre (UCC) in 2015,[142] according to which all international incoming and outcoming phone calls, as well as Internet traffic, must go through such a switching centre – the UCC. As a result, the government has access to all phone calls and communications coming in or outgoing from Tajikistan. The recommendation of the working group of the Human Rights Council is of a general nature and does not specify in detail which provisions of the CDI ought to be subject to change.

For the purposes of this thesis, as explained in Chapter 4, the present author chose to analyze the right to private life as secured by the ECHR and the jurisprudence of the ECtHR, which provide a comprehensive evaluation of the right to private life in the context of State surveillance. Such a choice of discussing the ECHR is based on the ground that the ECtHR has examined cases against the Russian Federation, and as explained in Chapter 2 of the thesis, Tajikistan laws are similar to the Russian laws due to their common Soviet legacy. Therefore, it was important to examine the ECtHR case law in order to be able to provide meaningful insight into the areas of Tajikistan law on State surveillance, which need to be improved.[143] In order to comply with its international human rights law obligations, it is therefore important for Tajikistan to consider the revision of the CDI and other instruments,[144] which allow State surveillance, in the light of the standards set by the ECHR and the ECtHR.

6.3.0.2. Law on Data Protection (Law on DP)

The answer to the question of whether and why the Law on DP ought to be changed or improved is more complicated than the question of whether the CDI ought to be improved. The CDI was mainly discussed through the lens of international human rights law, which sets certain standards to be followed by the States. On the other hand, the Law on DP was

[140] There were three cycles of the universal periodic reviews of Tajikistan's human rights situations so far: in 2011, 2016 and 2022. See: https://www.ohchr.org/en/hr-bodies/upr/tj-index.
[141] See UN Human Rights Council 'Report of the Working Group on the Universal Periodic Review. Tajikistan', A/HRC/49/12 dated 6 January 2022. Recommendation 123.160.
[142] The Resolution of the Government of the Republic of Tajikistan 'On the Unified Commutation Centre of Electric Communications' dated 30 December 2015, No 765.
[143] In *Zakharov v Russia,* the ECtHR scrutinized the Russian law on Crime Detection and Investigation, which is almost identical to the CDI. See n 138 above.
[144] 'Other instruments' are the mentioned UCC resolution, and the MTD's Procedure discussed in Section 6.1 of this Chapter.

scrutinized through a market freedoms instrument of the EU, which is announced to have been enacted to protect the fundamental rights of individuals.

The critique of the law proposed by this thesis concerns fundamental questions. The problem with the law is not so much that it does not fully or fairly regulate the processing of personal data. The main problem of the Law on DP is the lack of a theoretical foundation and the lack of conceptualization of the right to privacy and personal data in Tajik legal science. Burdened with a Soviet approach to privacy issues, the Tajik legislator created a tool not to protect the personal data of an individual, but to use this data for State purposes without restrictions.

This thesis has emphasised that the Law on DP is dormant.[145] It was adopted in 2018 without any noticeable public discussion, and the draft law was not developed by the Tajik law-making institutions. Unfortunately, this author does not have access to official documents that could cover the entire process of the formation of the law from the moment it was drafted to its adoption by the Tajik legislature.

With the rapid development of advanced technologies through which the government can easily interfere with the private life of individuals, coupled with globalization processes, which may involve a massive transborder transfer of personal data, Tajikistan needs to domestically protect the privacy of individuals. The debate among legal scholars in Tajikistan is necessary in order to challenge the understanding of the right to privacy that has been established since Soviet times. The result of such a discussion may lead to a change in the Tajik point of view on the relationship between the State and the individual in matters related to protecting privacy. The individual must have a sufficient set of guarantees for the protection of his private life from encroachments by the State itself, and not just from the interference of third parties.

The Law on DP can be changed formally in the form of a technical legal transplant without shifts in the legal consciousness of Tajik science. However, in this case, it seems that such a formal law in its new form will remain on paper and will not be implemented in practice. Moreover, without a theoretical basis for the protection of privacy and personal data, this thesis assumes that even a well-modified law will only work in favor of the State as a self-proclaimed guarantor of human rights and freedoms in Tajikistan.

In addition to scientific debate, it is further necessary to try in practice to implement some of the rights of individuals to the protection of privacy or the protection of personal data in the courts. Tajikistan is not a country with a common law system, and therefore

[145] See Chapter 2, Section 2.6 of the thesis, and relevant part of Section 6.1 of the present Chapter.

possible court decisions will not be regarded as a precedent. Moreover, access to judicial decisions in Tajikistan is still not guaranteed to researchers, lawyers, and other interested non-State actors. However, despite this, any possible litigation will allow the parties to the process to cover the main problems of the implementation of the law in the media or otherwise. Higher courts in Tajikistan, such as the Supreme Court and the High Economic Court, can summarize the practice of considering cases on the protection of personal data and adopt appropriate explanatory rulings that can be published to the general public.

6.4. Discussion of Tajik Data Privacy Laws in View of Controversies Between the ECHR and EU Law Approach to Privacy and Data Protection

The analysis of the CDI and the Law on DP, as well as other legal acts of the Republic of Tajikistan provided in Section 6.1 above, was made in the light of the standards set by the ECHR and the GDPR, as interpreted and applied by the respective Courts – the ECtHR and the CJEU. Chapters 4 and 5 of the thesis, in addition to introducing the above-mentioned judicial bodies' approach to the right to private life and data protection, also revealed certain controversies and differences in dealing with privacy and data protection issues.

If Tajikistan is to improve its domestic laws in the light of the standards set by the ECHR and EU law, such as the GDPR or the Charter of Fundamental Rights of the European Union (CFREU),[146] it has to be taken into account that the mentioned legal instruments and their application by the respective Courts are not free from flaws or controversies, which are subject to scientific discussion among European scholars as highlighted in Chapters 4 and 5 of the thesis respectively.

6.4.0.1. *ECHR and CDI*

The right to the protection of personal information or data is part of the right to private life according to the ECtHR jurisprudence.[147] In a few cases of State surveillance, the ECtHR has examined and applied where necessary its doctrine of margin of appreciation.[148] Some Russian authors even criticized the approach of the ECtHR in bulk

[146] the Charter for Fundamental Rights of the EU adopted by the European Parliament, European Council and the Council on 7 December 2000 and has entered into force together with the Treaty of Lisbon on 1 December 2009.

[147] See *López Ribalda and Others v. Spain*, Judgment of 17 October 2019 ; *Segerstedt-Wiberg and Other v Sweden,* Judgment of 6 September 2006; *Z v Finland,* Judgment of 25 February 1997; *Uzun v Germany,* Judgment of 2 December 2010; *S and Marper vs UK* Judgment of 4 December 2008; *Lozovyye v Russia,* Judgment of 24 July 2018; and *B v France* (1992) Series A no 232C.

[148] See *Zakharov v Russia,* Judgment of the ECtHR dated 4 December 2015; *Big Brother Watch and Others v* UK, Judgment of 25 May 2021; *Big Brother Watch and Others v UK*, (2019) ECHR; *Weber and Saravia v*

surveillance cases. According to Rusinova, the ECtHR approach in two recent cases of bulk surveillance – *Rattvisa (2019)* and *Big Brother Watch (2019)* may give 'permission' to the States for conducting mass surveillance, as the ECtHR has acknowledged that mass surveillance *per se* does not violate the ECHR.[149] She argues that since the case of *Weber and Saravia v. Germany* (2006), the ECtHR has developed progressive case law in surveillance cases, but in the two cases cited above in 2019, the ECtHR halted its progressive approach.[150]

The present author disagrees with the above-mentioned Russian scholar that the case law of the ECtHR was progressive and then suddenly was on halt due to two surveillance cases. The ECtHR in *Big Brother Watch (2019)* explicitly referred to the *Weber* case claiming that the ECtHR in the *Weber* case (2006) accepted that the bulk surveillance regime did not *per se* violate the ECHR. Thus, the findings and conclusions of the ECtHR in *Big Brother Watch (2019)* were in line with the reasoning of *Weber* (2006).[151]

However, it is notable that the critique provided by the above-mentioned Russian author implies the doctrine of margin of appreciation employed by the ECtHR in surveillance cases. Another Russian author criticizes different approaches taken by the ECtHR in different surveillance cases.[152] He argues that in *Szabo and Vissy v Hungary,*[153] the ECtHR established that there ought to be a judicial or other independent administrative authorization for conducting surveillance, but in *Big Brother Watch (2019)*, the ECtHR ignores that requirement in respect of the UK because some elements allegedly demonstrate that the executive power does not abuse its right to conduct surveillance.[154] He does not mention that the ECtHR takes into consideration the extensive post-authorization scrutiny of the surveillance measures provided in the UK though. The above-mentioned critique offered by the Russian authors, fair or not, indicates how different the approach of the ECtHR could be in similar cases.

The above-mentioned Russian scholars did not mention that the ECtHR affords a wide margin of appreciation to the States in deciding what type of interception regime is necessary (targeted or bulk) to protect national security, but the discretion given to them in

---

Germany, Admissibility Decision of 29 June 2006; *Kennedy v UK,* Judgment of the ECtHR dated 18 August 2010; and *Centrum for Rattvisa v Sweden,* Judgment of 25 May 2021.

[149] Vera Rusinova 'A European Perspective on Privacy and Mass Surveillance at the Crossroads' (2019) Higher School of Economics Research Paper No. WP BRP/87/LAW/2019.

[150] *Ibid.,* p.5.

[151] See *Big Brother Watch and Others v UK*, (2019) ECHR, Paragraph 314.

[152] Tigran Oganisyan 'Pravo na Zaschitu Personal'nykh Dannykh: Istoricheskiy Aspekt i Sovremennaya Kontseptualizatsiya v Epokhu Big Data' [The Personal Data Protection Right: Historical Aspect and Modern Concept in the Era of Big Data] (2020) 2 Journal of Foreign Legislation and Comparative Law 48.

[153] *Szabo and Vissy v Hungary,* Judgment of 6 June 2016.

[154] Tigran Oganisyan, n 152 above, p.58.

operating an interception regime must necessarily be narrower.[155] For the Tajik scholars, who are mainly accustomed to reading their Russian counterparts, the ECtHR jurisprudence, although available in the Russian language, might look at times incoherent, and not give clear guidance on how to improve domestic laws on crime detection and investigation. Moreover, erroneous interpretations of the ECtHR jurisprudence offered by some authors can be perceived as human rights law standards established in Europe, according to which the right to privacy as a general rule can be limited for national security purposes.

6.4.0.2. *GDPR and the Law on DP*

This thesis has discussed the EU approach to privacy and data protection in Chapter 5. In order for the Tajikistan Law on DP to develop and reach the level of personal data protection established by the GDPR, in addition to formal borrowing and 'importing' the legal provisions of the GDPR to the legislation of the Republic of Tajikistan, this thesis suggests that there is a need to conceptualize the right to data protection and the right to privacy. At the same time, since this thesis considers the possibility of improving the legislation of the Republic of Tajikistan in the light of the high standards set by the ECHR and EU law, it is necessary to take into account the problems and inconsistencies pertaining to these systems.

The elevation of the right to data protection to the rank of fundamental rights caused confusion. The CJEU after the enactment of the CFREU conflated the right to data protection with the right to private life in its jurisprudence.[156] Designed to promote EU market freedoms, the EU data protection laws at the same time enshrined initially the right to private life and later, the right to data protection, as a main value of the data protection laws in the EU.[157]

The CJEU in its jurisprudence used to give preference to market rights when they conflicted with fundamental human rights, but in the *Omega* case,[158] the CJEU decided in favour of the fundamental right to dignity.

---

[155] See *Big Brother Watch and Others v UK*, (2019) ECHR, Paragraph 315.
[156] See Orla Lynskey 'Deconstructing Data Protection: the "Added Value" of the Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569.
[157] See Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (1995) OJ L281/31; and Regulation of EU 216/679 dated 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[158] Case C-36/02 *Omega* [2004] ECR I-9609.

Tajik legal scholarship needs to conceptualize the right to data protection if Tajikistan Law on DP is to be improved in the light of the GDPR standards. Tajik scholars consider data protection as part of the right to private life,[159] although there is almost no solid legal scholarship examining data protection and the right to privacy in Tajikistan. As the discussion in Chapter 5 revealed, there is no consensus on defining the right to data protection as opposed to the right to private life among European scholars.[160] Different approaches to the right to data protection taken by the ECHR and the CFREU may lead to confusion among Tajik scholars.

This thesis in Chapter 5 has proposed its vision of the right to data protection if it has to be separated from the right to private life. The right to data protection is more of a technical right of an individual – data subject, according to which the personal data of the data subject can be processed only lawfully, transparently, and in a fair manner. The recognition of the right to data protection in EU law as a fundamental right must not mislead a Tajik reader. Tajik Constitution implies the right to data protection, as discussed in Chapter 2 of the thesis, so there is a legal basis for the Tajik scholarship to evolve the concept of data protection as part of the right to private life or as a separate constitutional right.

6.5. Conclusion

This thesis suggests that the laws of the Republic of Tajikistan concerning data protection and privacy could be improved in the light of the standards established by the ECHR and EU law. As the entire thesis has discussed mainly two bodies of laws: laws on surveillance and data protection laws, the current Chapter is devoted to the need to improve the legislation of the Republic of Tajikistan in two main areas: crime detection and investigation and the law on personal data.

The CDI and other laws related to surveillance issues in Tajikistan lack the necessary safeguards against arbitrary surveillance measures conducted by State authorities, especially in the context of bulk surveillance. The ECtHR jurisprudence is a useful tool for the Tajik drafters, legislators, lawyers, scholars, and other readers to address certain deficiencies in the CDI. Since CDI is almost identical to its Russian counterpart, and since the ECtHR has scrutinized the Russian law on crime detection and investigation, it makes it easier for the

[159] See, e.g., K. Kurbanov 'Ponyatiye Chastnoy Zhizni v Grazhdanskom Prave' [The Concept of Private Life in Civil Law] (2016) 16 Hayoti Huquqi [Legal Life 132].
[160] See, in particular, Orla Lynskey, n 156 above; Juliane Kokott and Christoph Sobotta 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 4 International Data Privacy Law 222.

Tajik readers to discuss the problems of protection of private life and personal data in the light of the ECHR requirements.

The Law on DP in its current form is deficient, as it does not provide any meaningful idea of personal data protection while automatic processing of personal data. It does not give an individual safeguard against the arbitrary use of their personal data by State organs and State-owned businesses. It does not provide private businesses with the necessary tools to conduct their businesses using the personal data of individuals, and as a result, private companies will be de facto in a constant state of breaching the Law on DP.

In order to improve the law or adopt the new one, which would protect data subjects on the one hand, and ensure the smooth functioning of private businesses processing personal data, it is not enough to only borrow legal provisions from GDPR into the Tajik legal system. It is essential to create a theoretical basis and conceptualize the right to data protection and the right to privacy in the Tajik legal thought. In this respect a wider discussion of the concept of privacy and data protection in Tajikistan is welcome. A stereotypic post-Soviet concept of privacy guiding Tajik scholars ought to be challenged with a view to discussing the concept of privacy, which informs contemporary privacy standards established by the ECHR and EU law, bearing in mind the controversies inherent to those legal instruments.

Chapter 7. Conclusions

This thesis has explored how the legislation of the Republic of Tajikistan concerning privacy and data protection has evolved, and has identified areas that would benefit from further development or improvement in line with the standards set by the European Union (EU) data protection law and the case law of the European Court of Human Rights (ECtHR) regarding the right to private life. By suggesting that Tajik legal scholarship ought to re-evaluate the concept of privacy in the light of contemporary concepts, which inform data protection laws in the EU, the thesis contends that such a reassessment would enhance the safeguarding of human rights within Tajikistan's surveillance and data protection laws.

The main findings of this thesis are threefold. Firstly, it has elucidated how Tajik legal scholarship conceptualizes privacy and data protection laws in Tajikistan, delving into its Soviet heritage, and contrasting it with notions of privacy and data protection which inform contemporary data protection laws in Europe. Secondly, this thesis has explored how contemporary conceptions of privacy in Europe influence the jurisprudence of the European Court of Human Rights and EU data protection law, including the Charter of Fundamental Rights of EU (CFREU)[1] and the General Data Protection Regulation (GDPR).[2] The thesis has concentrated on the privacy and data protection standards set forth by the European Convention on Human Rights (ECHR)[3] and EU law, as interpreted and applied by their respective courts. The thesis has elucidated differences between these legal systems, with the ECtHR adopting a nuanced approach to privacy rights that considers political, economic, and cultural contexts within Council of Europe Member States, while the Court of Justice of the EU (CJEU) prioritizes market freedoms within the EU and applies harmonized EU data protection laws to the greatest possible extent across all Member States. The third set of findings has addressed the scope of surveillance and data protection laws in Tajikistan, suggesting areas for re-evaluation and improvement to better safeguard human rights in accordance with ECHR and EU data protection standards. In addition to presenting three primary sets of findings, this thesis has elucidated the feasibility of Tajikistan adopting the data protection standards outlined in the GDPR and other EU data protection laws. This

[1] The CFREU was adopted by the European Parliament, European Council and the Council on 7 December 2000 and entered into force together with the Treaty of Lisbon on 1 December 2009.
[2] Regulation (EU) 216/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), (2016) OJ L119/1, is applied since 24 May 2018.
[3] Convention for the Protection of Human Rights and Fundamental Freedoms adopted by the Council of Europe on 4 November 1950 and entered into force on 3 September 1953.

evaluation has encompassed exploring the mechanisms suggested by the GDPR for ensuring the extraterritorial application of its standards beyond the EU borders. Moreover, the thesis has engaged in a discussion on adopting standards of privacy and data protection by Tajikistan as a legal transplants from a foreign jurisdiction into the Tajik legal system.

7.1. Conceptualization of Privacy in Tajikistan

The study has shown that the Tajik conceptualization of private life as such has not been completely formed. This thesis has found that Tajik legal scholarship defines the right to privacy differently from Western legal literature. This is due to the Soviet past of Tajikistan where the right to private life as a constitutional human right was not fully recognized. The Soviet era in Tajikistan was characterized by totalitarianism and anti-liberalism, founded on collectivist principles that opposed individualism. Chapter 2 thus has explained Tajikistan's Soviet past, and that it plays a role in the development of legal science in Tajikistan. Soviet legal science did not treat the right to private life as a constitutional right. It simply reflected the Soviet view of the personal lives of citizens from the point of view of civil law. Therefore, Tajik scientists in post-Soviet times have not paid much attention to the right to private life, except from the point of view of civil law. From the Tajik legal scholarship perspective, the right to privacy is mainly considered the right of an individual to receive protection from the State against interference by third parties. The State and its bodies are not considered violators of the right to privacy. On the contrary, the State is seen as a protector and guarantor of the right to private life. It has been argued that such an approach to privacy limits the scope of protection of the private life of individuals from government encroachments.

The thesis has pointed out the insufficient amount of literature regarding the Tajik concept of privacy. It has been indicated that only a few works of several Tajik authors in this area have been available for use.[4] All those works have been devoted to the right to privacy not as one of the constitutional human rights, but as a category regulated by civil law, which is characteristic of the Soviet approach to the protection of personal life. The thesis has shown that in the Soviet Union, legal science studied the right to a person's private life as a civil law phenomenon and did not study the right to private life as a human right, since the word 'private' had a negative connotation in a socialist society. Thus, this thesis has considered Tajik legal thought in relation to private life as post-Soviet legal thought, since it reflects precisely the Soviet approach to private or personal life.

[4] See n 10 of the Introduction, where references to few articles of Tajik legal scholars on the concept of privacy are made.

In contrast to human rights legislation, civil law regulates horizontal relations; that is, relations between equally situated subjects, such as individuals. The role of the State in such relations comes down to the role of a regulator or the role of a body that creates conditions for the exercise by individuals of their rights, including the right to private life. In the eyes of civil law scholars, the State is meant to punish violators of the right to privacy. Thus, the State itself is not considered by Tajik and post-Soviet legal thought as a possible violator of the right to private life. The thesis has further argued that such conceptualization of private life in Tajikistan has left its mark on the legislation of the Republic of Tajikistan in the field of data protection. As a result, the idea of protecting privacy through the protection of personal data was embodied in Tajikistan with the addition of the post-Soviet understanding of the personal life of an individual. The thesis has argued that since the post-Soviet concept of privacy differs from the Western concepts, Tajikistan's data protection legislation represents a hybrid of Western and Soviet values.

It has been shown through the thesis that the idea of protecting a person from interference from third parties and from the State was not properly implemented in the Law on Personal Data Protection (Law on DP)[5]. This piece of legislation contains elements that are typical of other laws that deal with the protection of information, including personal information. By denying a person access to another individual's personal data, this law protects an individual's personal information. However, the concepts of privacy which inform data protection laws in the EU are aimed at something different. Their task is to provide a person with the opportunity to find out not about the personal data of other people, but about their own personal data – whether it is processed by anyone, to what extent, and for what purposes it is subject to processing.[6] An individual is given the right to decide for himself/herself whether it is worth further providing his/her data for processing, whether it is worth changing the data or erasing it in the database controlled by third parties or the State. The difference between the Tajik and Western concepts of privacy explains why the Tajik law has in practice been dormant.

7.2. Western Concepts of Privacy

The thesis has shown in Chapter 3 how Western concepts of privacy are different from the Tajik concept. The thesis has explained the basic concepts of privacy that have arisen and have been developed in the West. It has been shown that the Western concepts of privacy, which inform the contemporary data protection laws in Europe, have been

[5] The Law of the Republic of Tajikistan 'On the Protection of Personal Data', No 1537, dated 3 August 2018.
[6] See Westin A., *Privacy and Freedom* (New York: Atheneum, 1967), p.5.

developed from the European tradition of protection of dignity, personal development, and informational self-determination of individuals.[7] It was formulated by an American scholar – Westin[8] – as a claim of individuals to define what information about them could be made available to others.[9] European approaches to the concept of privacy and data protection stem from the idea that the individual's right to privacy must be protected from both governmental and third-party intrusion. It is submitted that there are also differences between American and European conceptions of privacy, as explained by Whitman, stemming from the differences in legal culture and mentality.[10]

The delineation of the concept of privacy, which informs contemporary data protection laws in Europe, has led to the identification of the gaps and deficiencies of Tajik surveillance and data protection laws through an examination of the standards of privacy and data protection established in Europe. The examination of two European legal systems – the European Convention on Human Rights and EU law on data protection – has brought about a clear picture of where deficiencies in Tajik law on surveillance and data protection lie. The thesis has shown those two European legal systems in separate chapters, Chapter 4 and Chapter 5, before identifying the gaps and deficiencies of Taik law, which thereafter have been reflected in Chapter 6.

7.3. The ECHR Approach to the Right to Privacy and Data Protection

The examination of Article 8 of the ECHR in Chapter 4 has shown that the European concept of privacy is enshrined in the ECHR as a concept that comprises a wide range of privacy interests to be protected by the governments of the States, signatories to the ECHR. Thereafter, the assessment of the ECtHR's jurisprudence has confirmed that the right to data protection is an integral part of the right to private life, to be protected both when the government directly interferes with privacy and when third parties violate the privacy of individuals. Examination of the case law on surveillance issues has shown the ECtHR's established standards of protection of individuals from State surveillance, especially in bulk surveillance cases, i.e. in cases when large amounts of personal data, predominantly

[7] It must be noted that the thesis makes reference mainly to the German concept of dignity and self-development. See Lee Bygrave 'Privacy and Data Protection in an International Perspective' (2010) 56 Scandinavian Studies in Law 165, at p.170; Rouvroy A. and Poullet Y. 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth S., Poullet Y., De Hert P., de Terwngne C., Nouwt S. (eds.) *Reinventing Data Protection?* (Springer, 2009) 45.

[8] According to Lisa Austin, Westin endorses informational self-determination as a concept of privacy. See Lisa Austin 'Re-reading Westin' (2019) 20 Theoretical Inquiries in Law 53, at p.63;

[9] Westin A., n 6 above.

[10] This thesis, in Section 3.2 of Chapter 3, makes references to James Q. Whitman "The Two Western Cultures of Privacy: Dignity versus Liberty", in "The Yale Law Journal", 2004, vol 113, p. 1151 - 1221.

communications data, are subject to surveillance. It has been explained that the ECtHR's jurisprudence has been evolving, and since 2019 the interception of communications data, i.e. data about the time, frequency, addresses, and place of transmitting data, ought to be considered as not less intrusive in comparison to interception of content data.[11]

The study of the case law of the ECtHR on surveillance has subsequently identified what standards of privacy and data protection must be established by national legislation of the States, signatories to the ECHR. Those standards, which have come to be referred to as 'Weber requirements', mainly concern procedural law safeguards while conducting surveillance by law enforcement agencies, and have been used by the ECtHR in several cases, including the case of *Zakharov v Russia*[12] where the Russian law on crime detection and investigation similar to the Tajik law has been scrutinized. The ECtHR jurisprudence on the right to private life, discussed in Chapter 4, has thereafter shown that, as part of the development of the right to privacy, an individual's personal data must be protected in as detailed a manner as possible by national legislation. At the same time, the thesis has shown that the ECtHR uses the doctrine of margin of appreciation in surveillance cases. It has been shown that the States have wide discretion with respect to choosing the type of interception regime for bulk surveillance, but there is a narrower margin of appreciation in operating such a system. The ECtHR thus in general decides that the national authorities of the Member State are better positioned to judge certain surveillance cases if the procedural 'Weber requirements' are in place within the domestic law of the Member States.[13]

7.4. The EU Approach to Privacy and Data Protection

Chapter 5 has discussed EU legislation on data protection, both past and present, as well as judgments of the CJEU. The literature review on the EU privacy and data protection laws has indicated that although the right to data protection is a fundamental right as stipulated in the EU primary law, specifically in the CFREU,[14] and is separate from another fundamental right – the right to private life, it is not yet fully conceptualized by the European legal scholarship as a separate fundamental right. Scholars in Europe have discussed the differences between the two fundamental rights from the perspective of the scope of those rights.[15] However, there is not much literature on the differences in the essence of these two

[11] See *Big Brother Watch and Others v* UK, Judgment of 4 February 2019, Paragraph 356.
[12] *Zakharov v Russia,* Judgment of 4 December 2015.
[13] *Big Brother Watch and Others v* UK, Judgment of 25 May 2021, Paragraphs 347.
[14] The CFREU was adopted by the European Parliament, European Council, and the Council on 7 December 2000 and entered into force together with the Treaty of Lisbon on 1 December 2009.
[15] See Juliane Kokott and Christoph Sobotta 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 4 International Data Privacy Law 222; Orla Lynskey

fundamental rights. Moreover, an analysis of the case law in this thesis has shown that the CJEU does not offer clear and substantiated insight into the differences between the right to private life and the right to data protection.

Subsequently, the CJEU's evolving case law on data protection has indicated that the Court emphasizes the importance of the protection of the fundamental rights of individuals when the privacy of their personal data is at stake.[16] In this way, a separate EU legislative act – Data Retention Directive (DRD)[17] – was invalidated by the CJEU as being contrary to the fundamental rights to private life and data protection.[18] Similarly, the European Commission's adequacy decision in respect of the data protection regime in the United States of America (Privacy Shield) was invalidated.[19] At the same time, the CJEU in many instances has prioritized market freedoms over fundamental rights of individuals.[20] The origins of such an approach lie in the foundations of EU law in market integration. This thesis argues that the GDPR is thus a result of the efforts to harmonise and unify the data protection laws of the EU Member States with a view to having a unified approach within the EU to freely flowing personal data within the EU market and to protecting individuals from unlawful and unfair practices of processing their personal data outside the EU.

The thesis has explicated the main standards of data protection provided by the GDPR as those stemming from the main principles of data protection: lawfulness and fairness of data processing. The GDPR provides several lawful grounds for data processing by the public and private entities – controllers and processors. Such lawful grounds, apart from receiving the consent of individuals for processing of their personal data, also include several other grounds, which help the controllers and processors to carry out their business

---

'Deconstructing Data Protection: the 'Added Value' of the Right to Data Protection in the EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569; Van Der Sloot 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in Ronald Leenes, Rosamunde van Brakel Serge Guthwirth, Paul De Hert (eds) *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer International Publishing AG, 2017).

[16] See Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others,* Judgement of the GC dated 8 April 2014; *Schrems v Data Protection Commissioner,* Judgment of the GC dated 6 October 2015; Case C-311/18 *Data Protection Commissioner v Facebook and Maximillian Schrems,* Judgment of the GC dated 16 July 2020; and Case C-131/12 *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez,* Judgment of the GC dated 13 May 2014.

[17] Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54 (DRD).

[18] Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others,* Judgement of the GC dated 8 April 2014;

[19] Case C-311/18 *Data Protection Commissioner v Facebook and Maximillian Schrems,* Judgment of the GC dated 16 July 2020.

[20] See Anneli Albi 'Erosion of Constitutional Rights in EU Law: A Call for Substantive Cooperative Constitutionalism' Part 1 [2015] 9/2 Vienna Journal of International Constitutional Law (ICL Journal) 151, p.159; and Stijn Smismans 'The European Union's Fundamental Rights Myth' [2010] 1 JCMS 45.

or other activity without unnecessary interruptions or delays. For instance, when the controller processes personal data in the context of the performance of contractual duties, or in compliance with the legal obligation to which the controller is subject, or when processing personal data is necessary to protect the interests of the individual or even public interest.[21]

The thesis has thereafter shown that the evolution of data protection legislation within the EU reflects a shifting landscape of technological advancements, global market influences, and evolving legal frameworks. Initially established in the mid-1990s with the Data Protection Directive (DPD),[22] the EU has sought to regulate cross-border data flows and protect the personal data of its residents, particularly in the light of the dominance of US companies in utilizing such data for commercial purposes. The recognition of personal data protection as a fundamental right within the EU became more pronounced with the entry into force of the Charter of Fundamental Rights of the EU (CFREU) in 2009. This recognition culminated in the enactment of the General Data Protection Regulation (GDPR) in 2018, which replaced the right to private life with the right to personal data protection as the foundational principle guiding data protection laws in the EU.[23] The CJEU's judgment in the *Schrems II*[24] case indicated the importance of both the CFREU's provisions on personal data protection and the GDPR's requirements, emphasizing the EU's commitment to safeguarding personal data both within and outside its borders.

7.5. Differences Between the ECHR and EU Law Approaches to Privacy and Data Protection

This thesis has shown that there is a certain gap in knowledge regarding the difference between the right to personal data protection and the right to privacy. The thesis has explored the discussion of this issue in Chapters 4 and 5 herein. According to the jurisprudence of the ECtHR, the right to the protection of personal data is part of the protection of the right to private life established by Article 8 of the ECHR.[25] However, EU

[21] See Article 6 of the GDPR. Regulation (EU) 216/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), (2016) OJ L119/1, is applied since 24 May 2018.
[22] Directive 95/46/EC of the European Parliament and of the European Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (1995) OJ L281/31 (DPD).
[23] GDPR makes references to the right to data protection, but not to the right to private life, as was the case with the DPD. The only instance when GDPR refers to the right to private life in in Paragraph (4) of the GDPR Preamble, when the right to private life along with other fundamental rights is juxtaposed as a possible limitation to the right to data protection.
[24] Case C-311/18 *Data Protection Commissioner v Facebook and Maximillian Schrems,* Judgment of the GC dated 16 July 2020 (*Schrems II*).
[25] See *López Ribalda and Others v. Spain,* Judgment of 17 October 2019; *Segerstedt-Wiberg and Other v Sweden,* Judgment of 6 September 2006; *Z v Finland*, Judgment of 25 February 1997; *Uzun v Germany,* Judgment of 2 December 2010; *S and Marper vs UK*, Judgment of 4 December 2008.

legislation has elevated the right to personal data protection to an independent fundamental right, distinct from the right to private life. In this regard, a natural question arose: what is the difference between these two rights? The CJEU has conflated these two rights in its jurisprudence so far, thereby adding more questions than providing answers.[26]

Through a study of literature, as well as EU legislation on the protection of personal data and jurisprudence of the CJEU, this thesis has shown that although these two rights – the right to privacy and the right to data protection – are strongly interrelated and interdependent, there are still differences between them.[27] The thesis has argued that the right to personal data protection is more technical, although it has been elevated to the rank of fundamental rights by the EU. It has been explained that the technical component of this right is expressed in the interest that is protected by this right. In the case of the right to private life, human dignity and freedom are protected. However, the right to the protection of personal data is about compliance with technical requirements for the collection and processing of personal data, such as the lawfulness of data collection and processing, fairness, and transparency of this process. In essence, the process of automatic data processing ought to be structured in such a way that it is easy for an individual – the data subject – to make decisions regarding the fate of their personal data. For an individual it must be clear what particular information will be subject to processing; for what purposes such information will be used; for how long his/her personal information will be processed; whether his or her personal information could be transferred to other controllers, including those established abroad; whether his/her personal information will be erased after serving the purpose for which it was collected and used; and whether the individual will be able to demand erasure or modification of his/her personal information. All these mentioned principles of fair and lawful processing of personal data provide more guarantees that the individual's personal data will not be used against his/her will or interests.

As the thesis has shown, the modern concept of the right to privacy implies the ability of a person to independently decide the fate of their personal data, thus developing a personality, including the informational self-determination of the individual. The concept of the right to the protection of personal data, as argued in the thesis, establishes ways to implement the informational self-determination of the individual, i.e., it establishes

[26] See Section 5.4.2 'The Scope of Privacy and Data Protection' within Chapter 5 of the thesis. More specifically, see Orla Lynskey, n 189 in Chapter 5.
[27] The differences between the right to private life and the right to data protection were discussed in Subsection 5.4.2 of Chapter 5 of the thesis. Specifically, see Kokott and Sobotta n 186 and Lynskey n 188-190 in Chapter 5 of the thesis.

procedural rules such as the lawfulness, fairness, and transparency of data processing. With the help of these rules and procedures, an individual is able to more easily exercise their right to informational self-determination.

The study in this thesis has contributed to the debate as to why the EU law, unlike the ECHR, elevates the right to the protection of personal data into a separate independent right along with the right to private life. Since the EU was initially created as an organization pursuing economic goals, and human rights were not central, the issues of the single market and market freedoms were placed at the forefront of EU law, applied by the CJEU.[28]

7.6. The Scope of the Laws on Surveillance and Data Protection in Tajikistan in the Light of the Standards Established by the ECHR and EU Law

After having explored the standards of data protection established by ECtHR case law and by the EU data protection law, the thesis has reverted its attention to privacy and data protection laws of the Republic of Tajikistan. Two main laws – the Law on Crime Detection and Investigation (CDI) and the Law on Personal Data Protection which have been discussed in Chapter 2 of the thesis – have then been scrutinized in Chapter 6 in the light of the standards of privacy and data protection established by the ECHR and EU law. The CDI has been explained through the prism of human rights law protection as interpreted and applied by the ECtHR in surveillance cases. The other law – Law on DP – has been elucidated from the perspective of the standards set by the GDPR.

The first main theme of inquiry has related exclusively to the activities of law enforcement agencies, that is, to the relationship between the State and the individual, in which the State is the exclusive controller, and the other main theme of inquiry has related to the direct protection of personal data when carrying out economic or other activities in which controllers and/or processors may act as government agencies and private companies.

7.6.1. The Analysis of Tajik Surveillance Laws in the Light of ECtHR Case Law

The analysis of the Law on Crime Detection and Investigation of the Republic of Tajikistan has shown that it has certain provisions which are not in line with the 'Weber requirements' established by the ECtHR. In the case of *Zakharov v Russia,*[29] the ECtHR examined the Russian Law on Crime Detection and Investigation for its compliance with the

[28] Discussion on the issue of prioritizing market freedoms over fundamental rights are indicated in Section 5.2.2 of Chapter 5. Specifically see Albi, n 45 and Smismans, n 46 in Chapter 5 of the thesis.
[29] *Zakharov v Russia,* n 12 above.

standards for the protection of private life that the ECtHR itself established in its jurisprudence. Since the CDI is similar to Russian law, the ECtHR's findings in the *Zakharov* case may also be useful for Tajikistan to improve legislation in the field of surveillance. The 'Weber requirements', established by the ECtHR case law,[30] could be considered by Tajik legislators as valuable standards to make specific changes and amendments to the existing legislation of the Republic of Tajikistan in the field of criminal law, criminal procedure, and crime detection and investigation by law enforcement agencies.

This thesis proposes to define in more detail the range of crimes committed, in relation to which the law may allow law enforcement agencies to carry out operational investigative activities related to surveillance. With regard to Tajik legislation, it is appropriate to define the range of crimes depending on their types and nature. It is not enough to simply indicate that all grave and especially grave crimes[31] fall under this category since two main criteria for determining this range of crimes are the intent and the severity of punishment.

However, law enforcement bodies seeking a Tajik court sanction for surveillance, among other things, indicate the information about threats to the public, state, military, economic, information, or environmental security of the Republic of Tajikistan.[32] This means that not all grave and especially grave crimes must automatically fall within the category of crimes that would be subject to surveillance. This thesis proposes that the law clearly defines who would become subject to surveillance. The CDI specifies that surveillance may be carried out on any person who may have information about a crime being committed.[33] This thesis argues that this provision of the CDI gives wide discretion to law enforcement bodies to decide what person may have some relevant information that could be used for the purposes of crime investigation. Law enforcement bodies are guided by an assumption, and this may give them the possibility to abuse their power. On the other hand, an individual feels insecure, because they do not know when and whether they may become subject to surveillance.

This thesis proposes that law enforcement bodies must provide evidence suggesting that an individual, in fact, possesses useful information in order to receive judicial approval for conducting surveillance measures. No assumption or speculation about such an

[30] See *Weber and Saravia v Germany,* Decision on admissibility of 29 June 2006, Paragraph 95; *Big Brother Watch and Others v UK,* Judgment of 4 February 2019, in Paragraphs 280, 286, 289, and 292.
[31] Under Tajik criminal law, crimes are classified into four categories: minor gravity, moderate gravity, grave, and especially grave crimes. See Article 18 of the Criminal Code of the Republic of Tajikistan of 21 May 1998.
[32] CDI, Article 8(2)(3).
[33] Ibid., Article 8(5).

individual's alleged possession of the information must be sufficient for the Tajik court to grant approval for conducting surveillance. Further proposal of this thesis concerns the improvement of the CDI in the light of the standards established by the ECtHR ('Weber requirements') in respect of the duration of surveillance. The Tajik court's authorization to conduct surveillance in Tajikistan cannot exceed six months.[34] However, the CDI allows this period to be extended but does not indicate how long this extension can last, and how many times the court in Tajikistan can extend the period of surveillance. It is proposed to indicate more specifically for what period the court authorization in Tajikistan could be extended, for example, for a period of no more than one month, and it is also proposed to establish that it would be permissible to make such an extension only once.

The thesis has shown that in Tajikistan in urgent cases law enforcement agencies can carry out surveillance without prior court authorization. The CDI in such cases obliges the investigative authorities to provide the national court with information about surveillance *post factum* within 48 hours in order to obtain an appropriate court ruling, or otherwise the surveillance is terminated. At the same time, the law does not oblige the court to verify the legality of the surveillance carried out during those 48 hours. This, according to the ECtHR in the *Zakharov* case, violates the right of individuals to private life. In this regard, this thesis proposes that the legislation of Tajikistan is in need of amendments in order to ensure the protection of the right to privacy by introducing judicial control over the lawfulness of the use of surveillance measures in urgent cases. This could be expressed both in granting the right to individuals to challenge the legality of measures being taken or taken and in the obligation of the prosecutor's office to go to court with an appropriate resolution. Furthermore, the court in Tajikistan itself can, simultaneously with the question of the need to authorize surveillance, consider the question of the legitimacy of such measures. In cases where surveillance ends after 48 hours and law enforcement agencies do not apply to the court for the appropriate authorization, it is possible to provide for the obligation of such investigative agencies to provide all necessary materials to the court to consider the issue of the lawfulness of their use.

A study of the jurisprudence of the ECtHR in cases of bulk surveillance has shown that a person cannot accurately foresee circumstances when they may become the object of covert surveillance.[35] This thesis defines 'bulk surveillance' as representing an indiscriminate and large-scale collection and use of communications data by intelligence and

[34] Ibid., Article 9(5).
[35] See *Big Brother Watch and Others v* UK, Judgment of 4 February 2019, Paragraph 333.

law enforcement agencies for the detection and prevention of crimes. Bulk covert surveillance is carried out mainly on communications data. An individual is still able to control the content of his or her messages, that is, what he or she says or writes in messages, his or her thoughts, and his or her position on various issues of life. At the same time, an individual has practically no control regarding communications data.

Communications data or metadata determines how a person moves, what places he or she visits, where he or she spends the night, with whom at what time and how often he or she communicates on the phone, who he or she texts or calls, at what time this mainly happens. Communications data is also about where he or she shops, at what bank he or she opens his or her account, where he or she works, and how much time he or she spends at work and outside of it. Through the processing of communications data, the controllers and processors may know how often an individual meets with his or her friends or just acquaintances, in what places such meetings take place, and much more.

An individual can limit the ability to collect their communications data by using anonymizers, by limiting the use of cookies, or periodically deleting their Internet browsing history. However, all this does not guarantee complete privacy on the one hand, and significantly limits an individual's ability to live a full life without constant surveillance: meeting friends, making purchases, etc., on the other hand. Therefore, the thesis elucidates that data protection laws are intended to define the boundaries of the acceptable use of communications data in order to fully protect the personal data of the individual.

Chapters 4 and 6 of this thesis have explored the question of the lawfulness of bulk surveillance. According to the jurisprudence of the ECtHR, bulk surveillance as such does not violate the right to private life, but the country's legislation must have clear guarantees for the protection of the right to private life during bulk surveillance. There is a certain gap in the legislation of the Republic of Tajikistan regarding the regulation of bulk surveillance measures. It is proposed to make certain changes and amendments to the existing legislative acts of the Republic of Tajikistan regulating issues of operational investigative activities, as well as the activities of national security bodies and the prosecutor's office, in order to define in clearer terms the following:

- what 'bulk surveillance' is and how it differs from 'targeted surveillance';
- which agencies, other than national security agencies, can conduct bulk surveillance;

- in what specific cases bulk surveillance is permissible – a list of crimes to be prevented with the use of bulk surveillance;
- if bulk surveillance can be allowed on the territory of the Republic of Tajikistan or if it is permissible only in relation to cross-border crimes;
- a comprehensive list of the values protected by the chosen measure – bulk surveillance – such as national security;
- whether or not bulk surveillance is carried out to investigate a crime that has already been committed or whether it is permissible only in relation to the prevention of a crime in progress; and
- the procedure for obtaining preliminary court authorization to conduct bulk surveillance, as well as the procedure for challenging the legitimacy of this measure both by individuals and by the prosecutor's office.

All normative legal acts that are subordinate to the laws, including the Mobile Telecommunication Devices Registration Procedure,[36] ought to be brought in line with legislative acts regulating the activities of national security agencies and crime detection and investigation in order to eliminate the possibility of bulk surveillance without court authorization in Tajikistan. For these purposes, the thesis proposes to exclude the possibility of law enforcement agencies, and, primarily, national security agencies, to automatically connect to various information systems and databases controlled by private companies.

Improving the legislation of the Republic of Tajikistan in the light of the standards established by the jurisprudence of the ECtHR would significantly increase the protection of the right to private life of individuals in Tajikistan. However, the experience of another legal system in Europe, namely EU law on data protection, can also be a valuable source for the further development of the legislation of the Republic of Tajikistan, especially since EU law differently considers the place of the right to personal data protection in its system of protection of fundamental rights and freedoms.

7.6.2. The Analysis of Tajik Law on Data Protection in the Light of the Standards Established by EU Law

The thesis has argued that the EU data protection laws provide detailed regulation of the collection and processing of personal data so that a person feels his/her privacy is secured. The more guarantees the law on data protection provides to an individual, the better

[36] The Procedure of Registration of Mobile Communication Devices and Defining Functions of the State System of Identification of Mobile Communication Devices, approved by the Resolution of the Government of Tajikistan No 208 dated 31 March 2020.

the individual's private life is protected. The EU data protection legislation stipulates that data processing must take place in a lawful manner, taking into account the principle of fair and transparent data processing. The thesis has shown that data protection laws would enable a person to decide for himself/herself whether to allow third parties to process their personal data, or to demand changes or erasure of data from the third-party database.

The thesis has shown Tajik laws on data protection related to the area of private and public entities conducting their economic activities in Tajikistan. Specifically, the examination of the Law on DP carried out in Chapter 2 has shown the reflection of the Tajik concept of privacy in the provisions of this law. The thesis has argued that this law is aimed not so much at protecting an individual's personal data from encroachments of the State, but rather at controlling the process of collecting and using personal data by the State. The State has the right to collect and process personal data without an individual's consent in cases where government bodies process personal data while carrying out their governmental functions or where the State acts to protect the rights of third parties. In other words, the State is able to always process the personal data of individuals without seeking their consent.

The convergence between the GDPR standards and Tajik data protection legislation has been elucidated within this thesis, shifting the focus from state-centric surveillance to encompass broader data protection concerns involving both public and private entities. The European Data Protection Supervisor has identified three core principles underpinning GDPR: lawfulness, fairness, and transparency, emphasizing the necessity of legal justification for data processing, explicit consent for specified purposes, and transparent processing practices.[37] In Tajikistan, the Law on Data Protection, as shown by the thesis, delineates three lawful grounds for data processing: individual consent, processing by State organs in public functions, and protection of constitutional rights. However, the study has shown that the primacy of individual consent is circumvented by exceptions, granting broad discretion to State organs for data processing without consent. This lack of explicit consent requirements allows State organs to utilize personal data for various purposes without adequate safeguards.

In contrast, the GDPR provides more nuanced legal grounds for data processing, emphasising public interest, legal obligations, contractual necessity, individual consent, and protection of vital interests. Detailed provisions aim to minimize abuse by controllers or

[37] See EDPS Opinion 8/2016 'On Coherent Enforcement of Fundamental Rights in the Age of Big Data' dated 23 September 2016.

processors, including prohibitions on processing sensitive personal data without explicit consent.

While Tajikistan's data protection law mentions fairness and transparency principles, it lacks specific definitions or elaborations. It has been argued that, unlike the EU law's emphasis on procedural fairness and transparent processing, Tajik legislation remains vague, focusing more on safeguarding human rights as a justification for State data processing. This approach grants State organs wide latitude in data collection and processing without explicit consent, diverging thus from EU law standards. Furthermore, Tajikistan's data protection framework lacks robust safeguards against data processing abuses, prioritizing State interests over individual privacy. Private entities face unequal treatment compared to State organs, as they are restricted to processing personal data solely with individual consent, contrary to EU norms allowing various legal bases for data processing.

The thesis has pointed out that Tajikistan's data protection laws fail to meet EU standards and fail to provide adequate safeguards against state-centric data processing abuses. It has been argued that the legal framework reflects a narrative where State organs are portrayed as protectors rather than potential violators of individual privacy rights, resulting in unequal treatment between State and private data controllers.

Another recommendation is that the forthcoming data protection law in Tajikistan needs to establish a mechanism for addressing potential breaches of data privacy. An independent authority comprising data protection professionals ought to be established to oversee the enforcement of the law and safeguard the fundamental rights of data subjects. Tajikistan will require a greater number of professionals in the field of data protection, both within the competent data protection authority and within private enterprises acting as controllers and processors.

The new legislation need to mandate scenarios in which controllers or processors are obliged to appoint or contract a data protection officer. The primary responsibility of these officers must involve monitoring data processing activities within their respective organizations and providing guidance to ensure compliance with data protection regulations. Currently, there is a shortage of qualified professionals in Tajikistan with relevant training or education in data protection. Integrating data protection law into university curricula in Tajikistan and offering short courses tailored for legal professionals and practitioners would facilitate the correct implementation of data protection laws. Such courses could include

certification procedures for data protection officers and individual entrepreneurs, enabling them to serve as data protection officers on a contractual basis.

7.6.3. A Suggestion to Reconceptualise Privacy in Tajik Scholarship

This thesis advocates for the initiation of a discourse surrounding the notion of privacy within Tajikistan. In order to align the legislative framework of the Republic of Tajikistan with the data protection standards set forth by EU law and the European Convention on Human Rights, a fundamental reconceptualization of the right to privacy within Tajikistan is indispensable. Existing data protection laws, rooted partially in post-Soviet conceptions of personal life, are inadequate in meeting contemporary requirements for safeguarding personal data and are largely dormant in practice. This thesis seeks to catalyse Tajik legal discourse toward engaging in a dialogue concerning the formation of the concept of privacy within Tajikistan.

There is a dearth of scholarly literature addressing the right to privacy and the right to protection of personal data in Tajikistan. The thesis calls upon Tajik academics to delve into inquiries regarding the definition of privacy within Tajik law, human rights law perspectives, Tajik constitutional law, and data protection frameworks. Deliberations on these matters contribute to the evolution of the right to privacy in Tajikistan, distinct from the outdated post-Soviet conception, and reflective of contemporary Tajik realities. This reimagined notion of privacy need not mirror the conventional Western concepts entirely. What is paramount is that the Tajik conceptualization serves as a compass for the enactment of effective legislation aimed at protecting human rights, particularly safeguarding the right to private life in modern Tajikistan.

The thesis claims that the absence of a renewed conceptualization of privacy impedes the effective implementation of new laws designed to protect personal data in Tajikistan. Conceptualizing privacy helps legislators in appropriately prioritizing concerns when enacting laws and regulations pertaining to data protection, facilitating judicial interpretation, and enhancing the awareness of individuals about their rights and obligations. Consequently, legislation pertaining to data protection stands a greater chance of being applied more frequently and accurately in practice.

The legislative landscape of the Republic of Tajikistan concerning data protection could be improved through the lens of standards delineated by the jurisprudence of the European Court of Human Rights and EU legislation, contingent upon the establishment of a robust theoretical framework. This necessitates a reassessment of the concept of privacy

by Tajik legal scholarship, ensuring that Tajikistan's legislation mirrors the scholarly discourse within Tajikistan regarding private life and provides substantive protection to the right to privacy of individuals within the ambit of automated processing of personal data by both private and public entities.

7.6.4. 'Brussels Effect' and the Need for a Nuanced Approach to Legal Transplants

As Tajikistan is not a party to any association agreement with the EU, the extraterritorial application of the GDPR has also been part of the research. The thesis has found that apart from the jurisdictional clause within the GDPR, which covers data processing by controllers and processors established outside the EU,[38] the GDPR also provides for an 'adequacy decision' mechanism, which allows the European Commission to make decisions on the compatibility of legal data protection regime in third countries with the standards established by the GDPR, such as the 'Privacy Shield' with the USA mentioned earlier.[39] In the absence of such a decision, controllers and processors in third countries may still process the personal information of the EU residents, if certain data protection safeguards, such as binding corporate rules or standard data protection clauses are in place.[40] This thesis has discussed whether Tajikistan would be willing to adopt data protection standards established by the GDPR for the purposes of accessing the EU market of goods, services, and capital by Tajik businesses. The findings around the 'Brussels Effect' have been elucidated in Chapters 5 and 6 of the thesis.[41] Subsequently, the thesis has explained how the GDPR could be regarded as an 'imported law' to Tajikistan, which fits into the post-Soviet legal and political context. Chapter 6 has engaged in the discussion on legal transplants and their possibility or impossibility in general and in relation to the contemporary Tajik legal system in particular.[42]

This thesis acknowledges the presence of surveillance and data protection laws in Tajikistan that have been transplanted from other legal systems. It has shown that Tajikistan's current legal framework, shaped by its Soviet history, is a mosaic of legal elements borrowed not only from post-Soviet States but also from Western legal systems. Particularly

[38] See Article 3 of the GDPR.
[39] Article 45 of the GDPR.
[40] Article 46 of the GDPR.
[41] On the discourse on the extraterritorial application of GDPR and the 'Brussels effect' see Chapter 5, Subsection 5.3.3.2 'Extraterritorial Application of the GDPR', and Chapter 6, Subsection 6.2.0.1. Specifically, see n 149 in Chapter 5, and n 104 in Chapter 6 of the thesis for the literature used.
[42] On the 'Legal Transplants' and 'Imported Law', the thesis has engaged in the legal discourse in Chapter 6. Specifically, see the literature used in n 109-128 in Subsection 6.2.0.2 in Chapter 6.

noteworthy is the transplantation of laws governing market-oriented economic activities from Western legal systems over the past three decades.

However, the thesis has contended that the mere replication of Western standards is insufficient for ensuring the effectiveness of data protection laws in Tajikistan. It has emphasized the necessity for a theoretical reconceptualization of privacy. The revised data protection legislation must establish explicit safeguards against State surveillance and grant private controllers and processors enhanced legal authority to manage the personal data of individuals. Simultaneously, these laws need to prevent government institutions from accessing databases managed by private controllers and processors without proper authorization.

The thesis argues that the GDPR, as applied by the CJEU, could be considered more as a technical law, which provides a unified technical procedure for data processing. Such procedure involves clear rules on the lawfulness and fairness of data processing by controllers and processors. From this perspective, Tajikistan can adopt those standards of data protection established by the GDPR and revise its data protection laws with a view to having a robust legal instrument, which will help protecting fundamental rights on the one hand, and enable private and public businesses to conduct their economic operations smoothly, on the other hand.

Bibliography

Books:

Albi, A. The EU Data Retention Directive in Twenty-Eight Member States: An emblematic case study of blind spots, lost higher national standards and systemic flaws in autonomous EU human rights law and discourse (unpublished, used with the permission of the author)

Altman, I. The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding (Brooks/Cole Publishing, 1975)

Bradford, A. The Brussels Effect (OUP 2020)

Bygrave, L. Data Privacy Law: An International Perspective (OUP 2014) 199

Chalmers, D., Davies, G. and Monti, G. European Union Law (Cambridge University Press 2019)

Chalmers, D. and Arnull, A. The Oxford Handbook of the European Union Law (Oxford University Press 2018)

Conwey, G. The Limits of Legal Reasoning and the European Court of Justice (CUP 2012)

Cremona, M. and Scott, J. EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law (Oxford University Press 2019)

De Hert, P., Gutwirth, S. et al (eds). Reinventing Data Protection (Springer Science+Business Media B.V., 2009)

Dupre, C. Importing the Law in Post-Communist Transitions: The Hungarian Constitutional Court and the Right to Human Dignity (Hart Publishing, 2003) 192

Dzehtsiarou, K. European Consensus and the Legitimacy of the European Court of Human Rights (CUP, 2015), 229

Eeckhout, P. EU External Relations Law (Oxford University Press 2011);

Gayurov, S. Lichnoe informatsionnoe pravo grazhdan : problemy grazhdansko-pravovogo regulirovaniya v Respublike Tadzhikistan [Personal Information Right of Citizens: Problems of civil law regulation in the Republic of Tajikistan] (Moskva [Moscow], 2010) 371

Glanert, S., Mercescu A., and Samuel G. Rethinking Comparative Law (2021, Edward Elgar Publishing Limited)

Grogan, J. An EU-Centric Account of the Rule of Law (University of Oxford 2016)

Horspool, M. and Humphreys, M. European Union Law (Oxford University Press 2012);

Hillion, C., Claes M. and Imamovic, S. (eds). The EU Fundamental Rights Landscape After Opinion 2/13 (Maastricht Faculty of Law Working Paper 2016)

Joseph, S. and Castan, M. The International Covenant on Civil and Political Rights (Cases, Materials and Commentary) (OSAIL 3rd ed. 2013)

Kaczorowska-Ireland, A. European Union Law (Routledge-Cavendish 2012)

Kuner, C. Transborder Data Flow and Data Privacy, (Oxford University Press 2013);

Marx, K. and Engels F. The Civil War in France (English edition of 1871. Marc Harris, 2010)

Müllerson, R. International Law, Rights and Politics (Developments in Eastern Europe and the CIS), (Routledge, 1994)

Nissenbaum, H. Privacy in Context: Technology, Policy and the Integrity of Social Life (Stanford University Press, 2010)

O'Neill, A. and Coppel, J. The European Court of Justice Taking Rights Seriously? (EUI, 1992)

Regan, P. Legislating Privacy: Technology, Social Values, and Public Policy (University of North Carolina Press, 1995)

Romanovskiy, G.B. Pravo na neprikosnovennost chastnoy zhizni [The Right to Inviolability of Private Life] (MZ-Press, 2001)

Rössler, B. The Value of Privacy (Polity Press, 2005)

Shamolov, A.A. (ed.) Majmuai Konstitutsiyahoi Tojikiston [The Compilation of the Constitutions of Tajikistan] (Instituti Falsafa, Siyosatshinosi va Hukuki Akademiyai Ilmhoi Jemherii Tojikiston [The Institute of Philosophy, Political Science and Law of the Tajik Academy of Sciences], 2015) 633

Schutze, R. European Union Law, 2nd ed. (CUP 2018)

Schabas, W. The European Convention on Human Rights Commentary (OSAIL 2015);

Shumilov, A. Novaya redaktsiya operativno-rozasknogo zakona Rossii: otkrytyi proyekt [New Redaction of the Crime Detection and Investigation Law of Russia: Open Draft] (Moskva [Moscow], 2004) 33

Strömholm, S. Right of Privacy and Rights of the Personality: A Comparative Survey (Nordic Conference on Privacy organized by the International Commission of Jurists, Stockholm, 1967)

van der Sloot, B. and Broeders, D. (eds.). Exploring the Boundaries of Big Data (Amsterdam University Press 2016)

von Bogdandy, A. Neither an International Organization, Nor a Nation State: the EU as a Supranational Federation, (The Oxford Handbook of the European Union, OUP 2012)

Watson, A. Legal Transplants: An Approach to Comparative Law (Scottish Academic Press, 1974; American ed. University Press of Virginia, 1974)

Xenos, D. The Positive Obligations of the State under the European Convention of Human Rights (Oxon: Routledge 2012) 231

Chapters in Books:

Bhat, P. 'Doctrinal Legal Research as a Means of Synthesising Facts, Thoughts and Legal Principles' in Bhat, P. Idea and Methods of Legal Research (OUP, 2019) 148

Bognetti, G. 'The Concept of Human Dignity in European and US Constitutionalism' in Georg Nolte (ed) European and US Constitutionalism (CUP 2005)

Bradford, A. 'How the EU Became a Global Regulatory Power' in A. Bradford The Brussels Effect (OUP, 2020)

Bronsword, R. 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality' in Gutwirth, S. et al. Reinventing Data Protection? (Springer 2009), p.83

Celeste, E. and Fabbrini, F. 'EU Data Protection Law Between Extraterritoriality and Sovereignty' in Fabbrini F., Celeste E. and Quinn J (eds.) Data Protection Beyond Borders: Transatlantic Perspective on Extraterritoriality and Sovereignty (Hart, 2021)

Cameron, I. 'Competing Rights?' in de Vries, S., Bernitz, U. and Weatherill, S. (eds). The Protection of Fundamental Rights in the EU after Lisbon (Hart Publishing Ltd., 2013) 181-206

Claes, M. 'The Primacy of EU Law in European and National Law' in Chalmers D. and Arnull A. (eds.) The Oxford Handbook of European Union Law (OUP 2015)

Craig P. 'Integration, Democracy and Legitimacy' in Craig, P. and de Burca, G. (eds). The Evolution of EU Law (OUP 2011) 13-40

Corrin, J. 'Transplant Shock: The Hazard of Introducing Statutes of General Application' in Breda V. (ed.) Legal Transplants in East Asia and Oceania (CUP, 2019) p.34

de Burca, G. 'The Evolution of the EU Human Rights Law' in Craig, P and de Burca, G. (Eds.) The Evolution of EU Law (Oxford Scholarship Online, 2021) 480

de Burca, G. 'Human Rights in the EU' in Craig, P. and de Burca, G. (Eds.) EU Law. Text, Cases and Materials (Fifth Edition, OUP, 2011)

De Witte, B. Chapter 12 'Direct Effect, Primacy and the Nature of the Legal Order' in Paul Craig and Grainne de Burca (eds.) Evolution of EU Law (OUP 2011)

Dobinson, I. and Jones, F. 'Legal Research as Qualitative Research' in McConville, M. and Chui, H.W. (eds.) Research Methods for Law (Edinburgh University Press, 2017), p.21.

Gierke, Deutsches Privatrecht, vol.1 1895 (Systematisches Handbuch der Deutschen Rechtswissenschaft, ed. by Binding, part II.3.I)

Grimm, D. et al 'European Constitutionalism and the German Basic Law' in Albi, A. and Bardutzky, S. National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law (National Reports) (Asser Press 2019)

Grimm, D. 'Types of Constitutions' in Rosenfeld M. and Sajo A. (eds) Comparative Constitutional Law (OUP, 2012), p.98-132

Harding, A. 'The Legal Transplants Debate: Getting Beyond the Impasse?' in Breda V. (ed.) Legal Transplants in East Asia and Oceania (CUP, 2019) p.13

Hogan, G. 'The Influence of the continental constitutional tradition on the drafting of the Constitution' in Ruane, B., Barniville, D. and O'Callaghan, J. (eds), Law and Government: A Tribute to Rory Brady (Round Hall 2014) p. 162-164

Hughes, K. 'The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse' in Roessler, B. and Mokrosinska, D. (eds). Social Dimensions of Privacy: Interdisciplinary Perspectives (CUP, 2015) 225

Hutchinson, T. 'Doctrinal Research' in Watkins, D. (ed.) Research Methods in Law (2nd ed., Routledge, 2017), p.13.

Kant, E. 'Metaphysics of Morals', section 38 of the Doctrine of Virtue

Kohler, 'Das Autorrecht' in Iherings Jahrbücher, XVIII, new series VI

Kuner, C. Chapter 6 'Applicable Law, Extraterritoriality and Transborder Flows in Christopher Kuner Transborder Data Flows and Data Privacy Law (Oxford Scholarship Online 2013)

Kuner, C. Chapter 6 'Applicable Law, Extraterritoriality and Transborder Flows in Christopher Kuner Transborder Data Flows and Data Privacy Law (Oxford Scholarship Online 2013)

Lucarelli, S. & Manners, I., (Eds.), Values and Principles in European Union Foreign Policy (London: Routledge 2006)

Nissenbaum, H. 'Privacy and Common Good: Revisited' in Roessler, B. and Mokrosinska, D. (eds.) Social Dimensions of Privacy: Interdisciplinary Perspectives (CUP 2015) 278

Nolte, G. 'Introduction – European and US Constitutionalism: Comparing Essential Elements' in Georg Nolte (ed) European and US Constitutionalism (CUP 2005)

Peto, A. & Manners, I. 'The European Union and the value of gender equality'

Regan, P. 'Privacy and Common Good: Revisited' in Roessler, B. and Mokrosinska, D. (eds.). Social Dimensions of Privacy: Interdisciplinary Perspectives (CUP 2015) 50

Rodotà, S. 'Data Protection as a Fundamental Right' in Serge Gutwirth et al (eds) Reinventing Data Protection (Springer Science+Business Media B.V., 2009)

Rouvroy, A. and Poullet, Y. 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth, S., Poullet, Y., De Hert, P., de Terwngne, C., Nouwt, S. (eds.) Reinventing Data Protection? (Springer, 2009) 45

Saluzzo, S. 'The Principle of Territoriality in EU Data Protection Law' in Natoli, T. and Riccardi, A. (eds). Borders, Legal Spaces and Territories in Contemporary International Law (Springer Nature Switzerland AG and G Giappichelli Editore 2019) 121

Saluzzo, S. 'The EU as a Global Standard-Setting Actor: The Case of Data Transfers to Third Countries' in Carpanelli, E. and Lazzerini, N. (eds.) Use and Misuse of New Technologies (Springer Nature Switzerland AG, 2019)

Schutz, R. Chapter 2 'Constitutional Nature: A Federation of States' in 'European Union Law', (Cambridge University Press, 2018, 2nd Edition)

Solove, D. 'The Meaning and Value of Privacy' in Beate Roessler and Dorota Mokrosinska (eds) Social Dimensions of Privacy: Interdisciplinary Perspectives (CUP, 2015) 71

Tzanou, M. 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' in Fabbrini, F. et al (eds). Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty (Hart Publishing, 2021)

van der Sloot 'Legal Fundamentalism: is data protection really a fundamental right?' in Leenes, R., van Brakel, R., Guthwirth, S., De Hert, P. (eds.). Data Protection and Privacy: (In)visibilities and Infrastructures (Springer International Publishing AG, 2017)

van Rossem, JW. 'EU at Crossroads: A Constitutional Inquiry into the Way International Law is Received within the European Legal Order' in Cannizzaro, E. et al. International Law as Law of the European Union (BRILL 2011)

Williams, A. 'Human Rights in the EU' in Damian Chalmer and Anthony Arnull The Oxford Handbook of European Union Law (OUP, 2015)

Articles in Academic Journals

Albi, A. 'Erosion of Constitutional Rights in EU Law: A Call for Substantive Cooperative Constitutionalism' Part 1 [2015] 9/2 Vienna Journal of International Constitutional Law (ICL Journal) 151

Albi, A. 'Erosion of Constitutional Rights in EU Law: A Call for Substantive Cooperative Constitutionalism' Part 2 [2015] 9/3 Vienna Journal of International Constitutional Law (ICL Journal) 291

Albrecht, J.P. 'How the GDPR will Change the World' (2016) 2 European Data Protection Law Review 287

Alexy, R. 'On Constitutional Rights to Protection' (2009) 3 Legisprudence 1

Arai, Y. 'Margin of Appreciation Doctrine in the Jurisprudence of Article 8 of the European Convention on Human Rights' (1998) 1 Netherlands Quarterly of Human Rights 16, p.41

Austin, L. 'Re-reading Westin' (2019) 20 Theoretical Inquiries in Law 53

Berkowitz, D., Pistor, K. and Richard, J-F. (2003) 51 The American Journal of Comparative Law 163

BeVier, L. 'Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection' (1995) 4 William & Mary Bill of Rights Journal 455

Bignami, F. 'Privacy and Law Enforcement in the European Union: The Data Retention Directive' (2007) 8 Chicago Journal of International Law 233

Bougiakiotis, E. 'The enforcement of the Google Spain case' (2016) 24 International Journal of Law and Information Technology 311

Bowring, B. 'Russia and Human Rights: Incompatible Opposites?' (2009) 1 Goettingen Journal of International Law 257

Bradford, A. 'The Brussels Effect' (2012) 107 Nw. U. L. Rev. 1

Brems, E. 'Positive Subsidiarity and its Implications for the Margin of Appreciation Doctrine' (2019) 3 Netherlands Quarterly of Human Rights 37, p.210

Brkan, M. 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (2018) 14 EuConst

Byalt V.S., Demidov A.V. ‘Razdeleniye vlastey v istorii polotiko-pravovoy mysli Rossii’ [Separation of Powers in the Historical and Legal Thought of Russia] (2017) 1 (47) Leningradskiy Yuridicheskiy Zhurnal [Leningrad Legal Journal] 35

Bygrave, L. ‘Privacy and Data Protection in an International Perspective’ (2010) 56 Scandinavian Studies in Law 165

Chernichenko, S. ‘Perspektivy razvitiya mezhdunarodnykh standartov v oblasti obespecheniya prava na neprikosnovennost chastnoy zhizni’ [The perspectives of development of international standards in the field of securing the right to inviolability of private life in Pravo Grazhdan na informatsiyu i zaschita neprikosnovennosti chastnoy zhizni (Sbornik nauchnykh trudov) [Rights of Citizens to Information and Protection of the Inviolability of Private Life (Compilation of scientific works)] (Part I, Novgorod, 1999)

Çınar, O. ‘The Current case-law of the European Court of Human Rights on privacy: challenges in the digital age’ (2021) The International Journal of Human Rights 25:1

Clifford, D. and Ausloos, J. ‘Data Protection and the Role of Fairness’ (2018) 37 Yearbook of European Law 130

Cram, I. ‘Protocol 15 and Articles 10 and 11 ECHR – the Partial Triumph of Political Incumbency Past Brighton?’ (2018) 67 (3) International and Comparative Law Quarterly 477-503

Cohen, J. ‘What Privacy is For’ (2013) 126 Harvard Law Review 1904

Cohen, J. ‘Turning Privacy Inside Out’ (2019) 20 Theoretical Inquiries in Law 1

de Burca, G. ‘The European Court of Justice and the International Legal Order After Kadi’ (2010) Harvard ILJ vol.51, 1

de Burca, G. ‘After the EU Charter of Fundamental Rights: the Court of Justice as a Human Rights Adjudicator?’ (2013) 20 Maastricht Journal of European and Comparative Law 16;

de Hert, P. ‘Data Protection’s Future Without Democratic Bright Line Rules: Co-Existing with Technologies in Europe after Breyer’, [2017] 3 European Data Protection Law Review 20

de Hert, P. and Czerniawski, M. ‘Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context’ (2016) 6 International Data Protection Law 230

de Hert, P. and Gutwirth, S. et al (eds.). Reinventing Data Protection (Springer Science+Business Media B.V., 2009), p.3

Damann, U. and Simitis, S. EG-Datenschutzrechtlinie (Nomos Verlagsgesellschaft 1997)

Desmond, A. 'The Private Life of Family Matters: Curtailing Human Rights Protection for Migrants under Article 8 of the ECHR?' (2018) 1 European Journal of International Law 29

Dhont, J.X. 'Schrems II: The EU Adequacy Regime in Existential Crisis' (2019) 26 Maastricht Journal of European and Comparative Law 597

Diez, T. 'Normative Power as Hegemony' (2013) 48 Cooperation and Conflict 194

Diggelmann, O. and Cleis, M. 'How the Right to Privacy became a Human Right' (2014) 14 Human Rights Law Review 441

Dinorshoev, A. 'Sravnitelno-pravovoy analiz zakrepleniya prav I svobod cheloveka I grazhdanina v Konstitutsiyakh Rossiyskoy Federatsii i Respubliki Tadjikistan' [Legal comparative analysis of rights and freedoms of an individual and a citizen in the Constitutions of the Russian Federation and the Republic of Tajikistan] (2014) 2 Hayoti Huquqi [Legal Life 47]

Docksey, C. and Hijmans, H. 'The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law' (2019) 5 European Data Protection Law Review 300

Douglas-Scott, S. 'The European Union and Human Rights after the Treaty of Lisbon' [2011] 4 HRLR 645

Dworkin, R. 'A New Philosophy of International Law' (2013) 41 Philosophy and Public Affairs 1

Eberle, E. 'Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview' (2012) 33 Liverpool Law Review 201

Elliott, D. 'Data Protection is More than Privacy' (2019) 1 European Data Protection Law Review 13

Fabbrini, F. and Celeste, E. 'The Right to be Forgotten in the Digital Age: the Challenges of Data Protection Beyond Borders' (2020) 21 German Law Journal 55

Fabbrini, F. 'Human Rights in the Digital Age: the ECJ in the Data Retention Case and its Lessons for Privacy and Surveillance in the US' (2015) 28 Harvard Human Rights Journal 882

Fabbrini, F. 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' (2015) 28 Harvard Human Rights Journal 65

Faizulloev, A. ‘Ta’rikhi tashakkul va rushdi zuhuroty ‘malumoti shakhsi’ dar qonunguzorii Jumhurii Tojikiston va digar davlatho: tahlili qonunguzori va nazariyavi’ [History of formation and development of ‘personal data’ in the legislation of the Republic of Tajikistan and other states: legislative and theoretical analysis] (2022) 5 Vestnik TNU [Bulletin of TNU] 231

Faizulloev, A. ‘Ba’ze munosibathoi jam’iyatie, ki vobasta ba giriftan va korkardi ma’lumoti shkhsi paido meshavand: Tahlili tabiati huquqi [Some social relations, which appears in connection with collection of and processing personal data: analysis of legal nature] (2022) 6 Vestnik TNU [Bulletin of TNU] 233

Follesdal, A and Hix, S. ‘Why There Is a Democratic Deficit: A Response to Majone and Moravcsik’ [2006] 44 JComMarSt 533

Gavison, R. ‘Privacy and the Limits of Law’ (1980) 89 Yale Law Journal 421

Gerards, J. ‘Margin of Appreciation and Incrementalism in the Case Law of the European Court of Human Rights’ (2018) 18 Human Rights Law Review 495

Glanert S., Mercescu A., and Samuel G. Rethinking Comparative Law (2021, Edward Elgar Publishing Limited)

Goldbach, T. ‘Why Legal Transplants’ (2019) 15 Annual Review of Law and Science 583

Granmar, C. ‘Global Applicability of the GDPR in Context’ (2021) 3 International Data Privacy Law 225

Graziadei, M. ‘Legal Transplants and the Frontiers of Legal Knowledge’ (2009) 10 Theoretical Inquiries in Law 693

Greenleaf, G. ‘The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108?’ (2012) 12 University of Edinburg School of Law

Greer, S. ‘The Interpretation of the European Convention of Human Rights: Universal Principle or Margin of Appreciation’ (2010) 3 UCL Human Rights Review 1

Greze, B. ‘The Extraterritorial Enforcement of the GDPR: a Genuine Issue and the Quest for Alternatives’ (2019) 9 International Data Protection Law 109

Gulczinska, Z. ‘A Certain Standard of Protection for International Transfers of Personal Data under the GDPR’ (2021) 4 IDPL 360

Hartley, T. ‘Federalism, Courts and Legal Systems: The Emerging Constitution of the European Community’ [1986] American Journal of Comparative Law 229

Hughes, K. ‘A Behavioural Understanding of Privacy and its Implications for Privacy Law’ (2012) 75 MLR 806

Jacoby, N. ‘Redefining the Right to be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States’ (2007) 35 Georgia Journal of International and Comparative Law 433

Jarvis Thompson, J. ‘Right to Privacy’ (1975) 4 Philosophy and Public Affairs 295

Jervis, C. ‘The Curious Case of Article 3(3) of the GDPR and its Application to Diplomatic Missions [2020] 1 International Data Privacy Law 107

Kahn-Freund, O. ‘On Uses and Misuses of Comparative Law’, (1974) 37 Modern Law Review 1

Kamolov, Sh. ‘Mutobiqati sanadhoi baynalmillali ba Konstitutsiyai Jumhurii Tojikiston’ [Conformity of international acts to the Constitution of the Republic of Tajikistan] (2013) 3 Hayoti Huquqi [Legal Life] 52

Kholiqzoda, A. ‘Nazare ba tabiati huquqii “qonuni milli” va vizhagihoi on’ [The view on the nature of the “national law” and its peculiarities] (2018) 2 Davlatshinosi va Huquqi Inson [State Science and Human Rights] 5

Klatt, M. ‘Positive Obligations under European Convention on Human Rights’ (2011) 71 Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV) 691

Knieper, R. ‘Pulls and Pushes of Legal Reform in Post-Communist States’ (2010) 2 Hague Journal on the Rule of Law 111

Kokott, J. and Sobotta, C. ‘The Distinction Between Privacy and Data Protection in the Jurisprudence CJEU and ECtHR” (2013) 3 International Data Privacy Law, 222-228

Koskenniemi, M. ‘The Politics of International Law’ (1990) 1 EJIL 4

Kuner, C. ‘Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law’ (2015) 4 IDPL 235

Kuner, C. ‘Reality and Illusion in EU Data Transfer Regulation Post Schrems’ (2016) 18 German Law Journal 881

Kunets, A. ‘Nauchnye podkhody k ponimaniyu konstitutsionnogo prava na lichnuyu zhizn’ [Scientific Approaches to Understanding Constitutional Right to Personal Life] (2018) 60 Trud, Profsoyuzy, Obschestvo [Labour, Trade Unions, Society] 20

Kurbonov, K. ‘Pravo na chastnuyu zhizn v sisteme lichnykh neimuschestvennykh prav’ [The right to private life in the system of non-proprietary rights] (2019) 3 Hayoti Huquqi [Legal Life] 128

Kurbanov, K. ‘Pravo na neprikosnovennost chastnoy zhizni kak lichnoe neimuschestvennoe pravo’ [The Right to Inviolability of Private Life as a personal non-proprietary right] (2013) 4 Hayoti Huquqi [Legal Life] 58

Kurbanov, K. ‘Stanovlenie teoriy prava na chastnuyu zhizn’ [Formation of the Theory of the Right to Private Life] (2018) 4 Hayoti Huquqi [Legal Life] 220

Kurbanov, K. ‘Problemy sovershenstvovaniya grazhdansko-pravovogo regulirovaniya osuschestvleniya i zaschity prava na chastnuyu zhizn’ [Problems of Improvement of Civil Legal Regulation of Implementation and Protection of the Right to Private Life] (2020) 1 Davlatshinosi va Huquqi Inson [State Science and Human Rights] 45

Kurbanov, K. ‘Ponyatiye Chastnoy Zhizni v Grazhdanskom Prave’ [The Concept of Private Life in Civil Law] (2016) 16 Hayoti Huquqi [Legal Life] 132

Kyselova, T. ‘The Concept of Legal Transplant’ (2008)

Laima Janciute ‘Data protection and the construction of collective redress in Europe: exploring challenges and opportunities’ (2019) 9 International Data Protection Law 2;

Laudati, L. ‘Summaries of EU Courts Decisions Relating to Data Protection 2000-2015’ (2016) European Anti Fraud Office

Legrand, P. ‘The Impossibility of Legal Transplants’ (1997) 4 Maastricht Journal of European and Comparative Law 111

Leloup, M. ‘The Concept of Structural Human Rights in the European Convention on Human Rights’ (2020) 20 Human Rights Law Review 480

Lemmens, K. ‘The Margin of Appreciation in the ECtHR’s Case-Law’ (2018) 20 European Journal of Law Reform 2-3, p.78

Lenaerts, K. ‘The Principle of Democracy in the Case Law of the European Court of Justice’ [2013] 62 ICLQ

Lenaerts, K. ‘Limits on Limitations: The Essence of Fundamental Rights in the EU’ (2019) 20 German Law Journal 779

Lenaerts, K. ‘Exploring the Limits of the EU Charter of Fundamental Rights’ (2012) 8 EuConst 375

Lynskey, O. ‘Deconstructing Data Protection: the “Added Value” of the Right to Data Protection in the EU Legal Order’ (2014) 63 International and Comparative Law Quarterly 569

Ma, Y. ‘Relational Privacy : Where the East and West Could Meet’ (2019) 56 ASIS&T 196

Manners, I. ‘Normative Power Europe: A contradiction in terms?’ (2002) 40 Journal of Common Markets Studies 235

Manners, I. ‘Normative Power Europe Reconsidered: Beyond the Crossroads’ (2006) 13 Journal of European Public Study 182

Marks, S. ‘The European Convention on Human Rights and Its Democratic Society’ (1995) 1 British Yearbook of International Law 66

Marwick, A. and Boyd, D. ‘Networked Privacy: How teenagers negotiate context in social media’ (2014) 16/7 New Media & Society 1051

McCrudden, C. ‘Human Dignity and Judicial Interpretation of Human Rights’ (2008) 19 EJIL 655

McGoldrick, D. ‘A Defence of the Margin of Appreciation and an Argument for its Application by the Human Rights Committee’ (2016) 65 International and Comparative Law Quarterly 21

Minow, M. ‘Archetypal Legal Scholarship – A Field Guide’ (2013) 63(1) Journal of Legal Education 65

Murray, A. ‘Data Transfers” Between EU and UK post Brexit?’ (2017) 7 International Data Privacy Law 149

Murray, D. and Fussey, P. ‘Bulk Surveillance in the Digital Age: Rethinking the Human Rights Approach to Bulk Monitoring of Communication Data’ (2019) 52(1) Israel Law Review 31, Any Bradford ‘The Brussels Effect’ (2012) 107 Nw. U.L. Rev. 1

Nazarov, A. and Davlatzoda, K. ‘Istifodai tekhnologiyai raqami dar fa’oliyati operative-justujui’ [Use of Digital Technology in the Crime-Detection Operations] (2022) 4 Payomi Donishgohi Millii Tojikiston [Bulletin of the Tajik National University] 207

Nissenbaum, H. ‘Privacy as Contextual Integrity’ (2004) 79 Washington Law Review 119

Ntouvas, I. ‘Exporting Personal Data to EU-based International Organizations under the GDPR’ (2019) 9 International Data Privacy Law 272

Oganisyan, T. ‘Pravo na Zaschitu Personal’nykh Dannykh: Istoricheskiy Aspekt i Sovremennaya Kontseptualizatsiya v Epokhu Big Data’ (2020) 2 Journal of Foreign Legislation and Comparative Law 48 (Tigran Oganesyan ‘The Personal Data Protection Right: Historical Aspect and Modern Concept in the Era of Big Data’ (2020) 2 Journal of Foreign Legislation and Comparative Law 48)

Padova, Y. ‘Is the Right to be Forgotten a Universal, Regional or “Glocal” Right’ (2019) 9 International Data Privacy Law 15

Prosser, W. ‘Privacy’ (1960) 48 California Law Review 383

Purtova, N. ‘Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law Review’ (2018) 10 Law, Innovation and Technology 1

Qodirzoda, D., Shodiev, B. ‘Asosho va sharthoi guzaronidani chorabinii operativii gush kardani suhbathoi telefoni’ [Grounds and conditions of conducting surveillance measures of tapping telephone conversations] (2020) 6 Vestnik TNU [Bulletin of TNU] 256

Rao, N. ‘On the Use and Abuse of Dignity in Constitutional Law’ (2007) 14 Columbia Journal of European Law 201

Richards, N. ‘The Dangers of Surveillance’ (2013) 126 Harvard Law Review 1934

Roberts, A. ‘Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications’ (2015) 78(3) Modern Law Review 522

Roth, P. ‘Adequate Level Of Data Protection in Third Countries post Schrems and under the GDPR’ (2017) 25 J.L. Inf & Sci. 49

Rusinova, V. ‘A European Perspective on Privacy and Mass Surveillance at the Crossroads’ (2019) Higher School of Economics Research Paper No. WP BRP/87/LAW/2019

Rustad, M. and Koenig, T. ‘Towards a Global Data Privacy Standards’ (2019) 71 Florida Law Review 365

Sancho, D. ‘The Concept of Establishment and Data Protection Law: Rethinking Establishment’ (2017) 42 E L Rev 491

Scarcello, O. ‘Preserving the ‘Essence’ of Fundamental Rights under Article 52(1) of the Charter: A Sisyphean Task?’ (2020) 16 EuConst 647

Schwartz, P. and Solove, D. ‘The PII Problem: Privacy and a New Concept of Personally Identifiable Information’ (2011) NY University Law Review 86

Scott, J. ‘Extraterritoriality and territorial extension in EU law’ (2014) 62 American Journal of Comparative Law 87

Scott , J. ‘The New EU Extraterritoriality’ (2014) 51 Common Market Law Review 1343

Sheinin, M. ‘Towards Evidence-based Discussion on Surveillance: A Rejoinder to Richard A. Epstein’ (2016) 12 European Constitutional Law Review 341

Shokulova, S. ‘Tadjikistan v Svete Konstitutsii 1994 goda’ [Tajikistan in the Light of the Constitution of 1994] (2014) 2 Hayoti Huquqi [Legal Life] 20

Simitis, S. ‘Reviewing Privacy in an Information Society’ (1987) 135 University of Pennsylvania Law Review

Simitis, S. ‘Privacy – An Endless Debate’ (2010) 98 California Law Review 1989

Smismans, S. ‘The European Union’s Fundamental Rights Myth’ [2010] 1 JCMS

Solove, D. ‘Taxonomy of Privacy’ (2006) 154 University of Pennsylvania Law Review 477

Svantesson, D.J.B. “Article 4(1)(a) ‘establishment of the controller in EU data privacy law – time to rein in this expanding concept?’ (2016) 6 International Data Protection Law 210

Svantesson, D.J.B. ‘The CJEU’s Weltimmo Data Privacy Ruling: Lost in the Data Privacy Turmoil, Yet So Very Important’ (2016) 23 Maastricht Journal of European and Comparative Law 332

Svantesson, D.J.B. ‘The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on US Businesses’ (2014) 50 Stan. J. Int’l. Law 53

Svantesson, D.J.B. ‘Extraterritoriality and Targeting in EU Data Privacy Law: the Weak Spot Undermining the Regulation’ (2015) 4 International Data Privacy Law 226

Snyder, T. ‘Developing Privacy Rights in Nineteenth-Century Germany: A Choice Between Dignity and Liberty?’ (2018) 58 American Journal of Legal History 188

Tagainazarov, Sh. and Babadzhanov, I. ‘K teorii lichnykh neimuschestvennykh prav’ [On the Theory of Personal Non-proprietary Rights] (2018) 4 Hayoti Huquqi [Legal Life] 209

Tagainazarov, Sh. and Kurbanov, K. ‘Sovremennye podkhody k probleme instituta prava na chastnuyu zhizn v grazhdanskom prave’ [Contemporary Approaches to the Problem of the Concept of the Right to Private Life in Civil Law] (2018) 4 Hayoti Huquqi [Legal Life] 214

Tridimas, T. and Gentile, G. ‘The Essence of Rights: An Unreliable Boundary?’ (2019) 20 German Law Journal 794

van der Sloot, B. ‘Privacy as Personality Right: Why the ECtHR’s Focus on Ulterior Interest Might Prove Indispensable in the Age of “Big Data”’ (2015) 31 Utrecht Journal of International and European Law 25

van der Sloot, B. ‘Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation’ (2014) 4 IDPL 307

Vedaschi, A. and Lubello, V. ‘Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective’ (2014) 20 Tilburg Law Review 14

Vila, M. ‘Subsidiarity, Margin of Appreciation and International Adjudication within a Cooperative Conception of Human Rights’ (2017) 15(2) International Journal of Constitutional Law 393

Viljanen, J. ‘State Obligations to Protect the Right to Respect for the Private Life under Article 8 of the ECHR and the Challenge of the Internet’

Wagner, J. ‘The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?’ (2018) 8 International Data Protection Law 318

Waelde, T. and Gunderson, J. ‘Legislative Reform in Transition Economies: Western Transplants – A Short-Cut to Social Market Economy Status?’ (1994) 43 International and Comparative Law Quarterly 347

Warren, S. and Brandeis, L. in “The Right to Privacy” in “Harvard Law Review”, vol.4, 15 December 1890

Watson A. Legal Transplants: An Approach to Comparative Law (Scottish Academic Press, 1974; American ed. University Press of Virginia, 1974)

Weiler, J. ‘The Transformation of Europe’ [1991] The Yale Law Journal 2414

Whitman, J. Q. “The Two Western Cultures of Privacy: Dignity versus Liberty” (2004) 113 The Yale Law Journal 1151

Woods, A. ‘Litigating Data Sovereignty’ (2018) 128 The Yale Law Journal 328

Xenos, D. The Positive Obligations of the State under the European Convention of Human Rights (Oxon: Routledge 2012) 231

Ziegler, K. ‘Autonomy: From Myth to Reality – or Hubris on a Tightrope? EU Law, Human Rights and International Law’ (2015) University of Leicester School of Law, Research Paper No 15-25