



FACULTY OF LAW

Lund University

Christopher Andersson

A Matter of Privacy

How the substantial rule of law ensures fundamental rights in a
digital era

LAGM01 Graduate Thesis

Graduate Thesis, Master of Laws program

30 higher education credits

Supervisor: Xavier Groussot

Semester of graduation: Period 1 spring semester 2021

Contents

SUMMARY	1
SAMMANFATTNING	2
PREFACE	3
ABBREVIATIONS	4
1 INTRODUCTION	5
1.1 Background	5
1.2 Purpose and legal issue	7
1.3 Methodology	11
1.4 Scope and Delimitation	13
1.5 Research on the subject	14
2 SETTING THE CONTEXT: SURVEILLANCE IN A DIGITAL ERA	15
2.1 Introduction	15
2.2 Surveillance used by national authorities and the relation to data	16
2.2.1 <i>Overview of electronic communications</i>	16
2.2.2 <i>Overview of surveillance</i>	18
2.2.3 <i>Data Processing</i>	20
2.3 Summary	21
3 DEFINING ‘RULE OF LAW’: RULE BOOKS AND RIGHTS	22
3.1 Introduction	22
3.2 Brief history	23
3.3 Formal and substantive rule of law	25
3.3.1 <i>Substantive rule of law in the EU</i>	27
3.3.2 <i>Issues</i>	28

3.4	Summary	30
4	THE OBJECT OF SUBSTANTIVE RULE OF LAW: FUNDAMENTAL RIGHTS	31
4.1	Introduction	31
4.2	Fundamental rights guaranteed under surveillance of communications	31
4.2.1	<i>Case-law from the ECtHR: the bare minimum</i>	32
4.3	Summary	37
5	DATA PRIVACY AT THE BEGINNING OF 2020'S: FROM SCHREMS II TO ENCROCHAT	38
5.1	Schrems II	38
5.1.1	<i>Introduction</i>	38
5.1.2	<i>Case facts</i>	38
5.1.3	<i>Judgement</i>	41
5.2	La Quadrature du net	46
5.2.1	<i>Introduction</i>	46
5.2.2	<i>Case facts</i>	47
5.2.3	<i>Judgment</i>	49
5.3	Prokuratuur	52
5.3.1	<i>Introduction</i>	52
5.3.2	<i>Case facts</i>	53
5.3.3	<i>Judgment</i>	53
5.4	The Affair of EncroChat	57
5.4.1	<i>Introduction and background</i>	57
5.4.2	<i>European Investigation Order</i>	58
5.4.3	<i>The lawfulness of the European Investigation Order</i>	59
6	SUBSTANTIVE RULE OF LAW: THE PROTECTOR OF FUNDAMENTAL RIGHTS	61
6.1	Introduction	61

6.2	Is Rule of Law ensuring fundamental rights?	61
6.3	Conclusion	65
	BIBLIOGRAPHY	66

Summary

In a world which is becoming more digital, electronic information is being transferred every second to all parts of the world, containing personal data. This electronic communication can be subject of surveillance by the public authorities – the capabilities of the public authorities were leaked already by Edward Snowden in 2013. On the other side of the surveillance are the fundamental rights, namely the rights to privacy, protection of personal data and a fair trial and an effective remedy.

The rule of law plays a vital part of ensuring fundamental rights, since a large objective of the rule of law is to constrain the public authorities from abusing their powers. This essay explores how the substantive rule of law, as developed by Ronald Dworkin, protects fundamental rights concerning surveillance by the public authorities. The conception of substantive rule of law does not only see rule of law as its formal attributes, such as correct promulgation and proper authorisation, but it also acknowledges that the rule of law entails substantive justice – that it captures and enforces moral rights recognised in positive law.

Three recent cases from the CJEU are objects in the thesis: *Schrems II*, *Quadrature du Net* and *Prokuratuur* as well as the EncroChat affair. The thesis summarises how the fundamental rights were construed by the CJEU in the three cases and thereafter applies the conception of substantive rule of law on the cases and the EncroChat affair.

The thesis finds that the substantive rule of law ensures fundamental rights and provides substantive justice in the cases *Schrems II*, *Quadrature du Net* and *Prokuratuur*. It further explains how substantive rule of law ensures fundamental rights in legal grey holes, so the power of public authorities is constrained. Lastly, it also finds that a substantive rule of law approach should not only be used by the CJEU in the future.

Sammanfattning

I en alltmer digital värld överförs elektronisk information varje sekund till alla delar av världen. Denna elektroniska information övervakas av stater och dess offentliga myndigheter, vars övervakningsförmåga läcktes redan 2013 av Edward Snowden. På andra sidan av detta fenomen finns grundläggande rättigheter, nämligen rätten till integritet, skydd av personuppgifter, en opartisk domstol och tillgång till ett effektivt rättsmedel.

Rättsstatsprincipen spelar en viktig roll för att säkerställa de grundläggande rättigheterna eftersom en stor del av den handlar om att hindra offentliga myndigheter från att missbruka sina befogenheter. Detta examensarbete utforskar hur den materiella rättsstatsprincipen – som har utvecklats av Ronald Dworkin – skyddar de grundläggande rättigheterna när offentliga myndigheter övervakar elektronisk kommunikation. Den materiella rättsstatsprincipen ser inte bara rättsstatsprincipen ur dess formella egenskaper, såsom korrekt utfärdande av lagar och korrekt auktorisation, men också att rättsstatsprincipen innebär en materiell rättvisa: att den fångar och verkställer moraliska rättigheter erkänd i positiv rätt.

Tre nya fall från EU-domstolen ligger i fokus för examensarbetet: *Schrems II*, *Quadrature du Net* och *Prokuratuur* samt EncroChat-affären. Examensarbetet sammanfattar hur de grundläggande rättigheterna tolkades av EU-domstolen i de tre fallen och tillämpar därefter konceptet materiell rättsstat i de tre fallen och i EncroChat-affären.

Examensarbetet finner att den materiella rättsstaten säkerställer grundläggande rättigheter och ger materiell rättvisa i fallen *Schrems II*, *Quadrature du Net* och *Prokuratuur*. Den förklarar vidare hur principen om materiell rättsstatsprincip säkerställer grundläggande rättigheter i legala gråa hål, så att myndigheternas makt begränsas. Slutligen finner den också att en materiell strategi inte endast bör användas av EU-domstolen i framtiden.

Preface

Inlämnandet av detta examensarbete markerar inte bara slutet på juristprogrammet, det markerar även slutet på min tid här i Lund. Jag vill därför tillägna förordet till min tid i Lund. Jag minns fortfarande när jag gick in i Pufendorfsalen för första gången en kall vinterdag januari 2016. På många sätt är jag samma person som kom ner 2016, på många sätt är jag även en helt ny människa. På det stora hela har jag otroligt många och tacka för att jag har kunnat utvecklas de här senaste 5,5 åren. Tack Utrikespolitiska föreningen för att ni lärt mig att det finns en värld utanför Lund. Tack Juridisk Publikation för alla nya vänner och för mitt funna språkintresse. Tack ACLU för all tid och framförallt Patrik Lindskoug för att jag har fått ha dig som chef. Tack Maksym, Sonja, Arina, Clara, Max för de kanske sex mest intensiva men mest lärorika månaderna med ELMC och framförallt ett stort tack till Xavier Groussot som under det senaste året har fått mig att se juridiken med helt nya ögon. Och naturligtvis tack till Carin, Annica, Charlotta, Maria och Kerstin för att jag fick se Lund från sin mest vackra sida.

Det är inte lätt att lämna Lund, men efter en så lång tid är det även dags för mig att testa mina vingar. Men några saker är säkra, och det är att tiden här inte hade varit densamma utan mina Lads och Tankers. Där har jag minnen tillräckligt för ett liv. Och till slut kommer kanske det största tacket, och det är till alla minnen från Östra Vallgatan 51 – på Malmö Nation. Jag hade idag inte varit samma person utan alla vänner jag fått och minnen vi skapat på Malmös, och för det är jag evigt tacksam. Jag vet att mitt hem alltid kommer vara nere i Falsterbo, bara en kilometer från Skanör – vid de gamla pärafiltens därhimma...

På återseende Lund.

Lund den 27 maj 2021

Christopher Andersson

Abbreviations

AG	Advocate General
CFR	Charter of Fundamental Rights of the European Union
CIA	Central Intelligence Agency (United States)
CJEU	Court of Justice of the European Union
CSI	Code de la sécurité intérieure
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EIO	European Investigation Order
E.O.	Executive Order
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FBI	Federal Bureau of Investigation (United States)
GDPR	General Data Protection Regulation
IPT	Investigatory Powers Tribunal
NSA	National Security Agency (United States)
OJ	Official Journal of the European Union
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

1 Introduction

“There were 5 Exabytes of information created between the dawn of civilization through 2003, but that much information is now created every 2 days.”¹

1.1 Background

With the explosion of data since common man started to use tele communications, the way of life has changed drastically from how it looked after the second world war. People are using computers, mobile phones, televisions, digital watches etc. to send information every second. It is private messages, public information, location data, health data as well as pictures and greetings to friends and family.

With the change in how information is communicated, surveillance by public authorities has naturally also changed from the way it was conducted before. No longer are agents needed to be out in the field in disguise, no longer are microphones needed to be planted in order to gather information secretly, and no longer do public authorities need to rely on neighbours to gather intelligence on subjects.

Today, public authorities gather information and intelligence from headquarters filled with electronic devices and communications, effectively gathering information for objectives of preventing and combatting crime and protecting national security. This was perhaps at least the perception the public had due to the cultural impact of action movies in late 90's and 2000's.²

¹ Eric Schmidt, a former CEO of Google, at Google Atmosphere Convention 2010, explaining how much data that are created in the 21st century.

² See Klaus Dodds 'Gender, Geopolitics, and Geosurveillance in "The Bourne Ultimatum"' (January 2011) Vol 101 No 1 Geographical Review pp. 100-102.

Although cultural perception was that public authorities had much power and extensive capabilities in digital surveillance, this was nevertheless confirmed in 2013, when Edward Snowden – a National Security Agency (NSA) whistle-blower – leaked capabilities of NSA to the world press. From then, the public understood the true capabilities of the public authorities and governments regarding surveillance of telecommunications.³

In the EU and other western countries, such as the USA, Canada, Australia, and New Zealand, public authorities have the capabilities to conduct surveillance, but often not the legal basis to conduct surveillance.⁴ In both common law traditions and civil law traditions (in civil law traditions especially after the second world war), the rule of law has quite a prominent place in constitutions as well as in the legal systems, in order to keep the authorities in check.⁵

As will be explained in Chapter 3, the concept of rule of law is often referred to in different laws, legal texts, case-law and doctrine, regardless of the legal system, and may at the first sight have substantial meaning to the description of the legal system. As an example, rule of law has a strong relationship to Union law and the EU. It functions both as a founding value as well as a value to be promoted by the Union.⁶ However, there is really no real definition of rule of law in the Treaties and is frequently a topic for debate.

Nevertheless, rule of law plays a significant role in the EU legal system. It is there to prevent governments from misusing power, to remind them that they also are subject to the law and not above the law, and in the end, it is there to protect our fundamental rights as citizens of the EU. This thesis will examine

³ See Ewen Macaskill & Gabriel Dance ‘NSA Files: Decoded’ *The Guardian* (London: 1 November 2013) <<https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>> accessed 20 May 2021.

⁴ See Dodds p. 100 and Chapter 4.

⁵ Laurent Pech ‘The Rule of law as a Constitutional Principle of the European Union’ (2009) Jean Monnet Working Paper Series 4/2009 pp. 22-35 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1463242>.

⁶ TEU, Article 2.

how rule of law functions as a protector of our fundamental rights in the dawn of the age of digitisation.

1.2 Purpose and legal issue

Naturally, rule of law plays a vital part in the protection of all fundamental rights. In the preamble to the Treaty on European Union (TEU) it is stated that the rule of law is a universal principle which functions as an inspiration to the Union. It is also already laid down in Article 2 TEU, where it is prescribed that the rule of law is a founding value of the EU.

The rule of law functions as a check on the state, to prevent it from misusing its powers against the individual. This is a part of the formal conception of the rule of law. Nevertheless, prominent scholars such as Ronald Dworkin and Paul Craig, has brought up the fact that rule of law has a substantive dimension as well. This concept of rule of law says that rule of law is not only there to tell whether a law has been correctly promulgated, but that a substantive justice within its meaning also exists. Substantive rule of law requires that the rule of law enforces the correct moral rights individuals have, so that they in the end receive the best substantive justice and have their fundamental rights ensured.

During this digital age, some fundamental rights have become particularly highlighted in connection to electronic telecommunications. In some way, all fundamental rights can be connected to digitalisation, but the right to privacy in Article 7 and the right to the protection of personal data in Article 8 of the Charter of Fundamental Rights of the European Union (CFR) have been particularly highlighted. These two rights have previously many times been the subject of court cases at the Court of Justice at the European Union (CJEU). Secondly, the right to a fair trial and an effective remedy in Article 47 of the CFR is also highlighted in cases concerning privacy. The purpose of this thesis is to understand if the EU is truly providing these fundamental

rights which are necessary in the digital age and use the substantive rule of law as a lantern to provide light on the issue.

In July 2020, the CJEU handed down *Facebook Ireland and Schrems (Schrems II)*, a case that concerned the transfer of personal data from the EU to the USA, in which the transferred data would be subject by the U.S. authorities and processed.⁷ In October 2020, the Court handed down *La Quadrature du Net* which regarded telecommunications surveillance by French and Belgian authorities in matters related to terrorism and national security.⁸ In March 2021, the Court handed down *Prokuratuur*. The case concerned the access to personal data by Estonian authorities, when they investigated a steal crime.⁹ Conclusively, these three Grand Chamber cases has sparked a legal debate because of the substance in the judgements, where EU privacy law has been a hot debate topic.¹⁰

What the three cases all have in common is that they concern interferences by public authorities with the right to privacy, the right to personal data, and to some extent the right to a fair trial and the right to a remedy.

The three mentioned cases will be subjects for this thesis and will be complemented with a fourth element – the affair of EncroChat. What differ the EncroChat affairs from *Schrems II*, *La Quadrature du Net*, and *Prokuratuur* is that it is not a case from the CJEU but refers to a hacking of a sophisticated software system used by criminals. It has also been the subject of large media attention and will hopefully be reviewed by the CJEU in the near future.¹¹ The EncroChat affair is interesting from several legal

⁷ Case C-311/18 *Facebook Ireland and Schrems* ECLI:EU:C:2020:559 (*Schrems II*).

⁸ Case C-511/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791.

⁹ Case C-746/18 *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* ECLI:EU:C:2021:152.

¹⁰ See Anupam Chander 'Is Data Localisation a Solution for Schrems II?' (September 2020) Volume 23 Issue 2 *Journal of International Economic Law* pp. 771-784 & Jack Maxwell & Joe Tomlinson 'Privacy Int'l v. Secretary of State for Foreign & Commonwealth Affairs and La Quadrature du Net v. Premier minister (C.J.E.U)' (June 2021) Volume 60 Issue 3 *International Legal Materials* pp. 464-520.

¹¹ See David James Smith 'The EncroChat Bust: how Police hacked the secret gangster messaging network' *The Times* (London, 11 April 2021) <<https://www.thetimes.co.uk/>

perspectives (as it concerns privacy infringements and sharing of personal data between Member States) and will therefore be complemented to the three cases in this thesis.

The above three cases and EncroChat affair impeaches the state power and the usage of surveillance of electronic communications. With the usage of data around the world every millisecond, it is necessary to examine the power public authorities have and their boundaries when it comes surveillance of electronic communications. Hence, the purpose of this essay is to examine if EU law actually provides protection from state interferences of the electronic communications for purposes of surveillance, e.g., in criminal proceedings or to protect national security.

An extraordinary trait with surveillance in the 2020's, is the rapid development it has made during the last 20 years. It can be quite difficult for the common man to understand the technological development surveillance has made, or even the capabilities the public authorities have. This concern was skillfully expressed by the European Court of Human Rights (ECtHR) in *Szabó and Vitty v Hungary*:

‘The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen[...], especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of

article/the-encrochat-bust-how-police-hacked-the-secret-gangster-messaging-network-mjvh3xlw> accessed 26 May 2021, Jacques Follorou & Martin Untersinger ‘Le réseau crypté EncroChat infiltré par les polices européennes : « C’est comme si nous étions à la table des criminels »’ *Le Monde* (Paris, 3 July 2020) <https://www.lemonde.fr/international/article/2020/07/03/c-est-comme-si-nous-etions-a-la-table-des-criminels-comment-les-polices-europeennes-ont-penetre-le-reseau-crypte-encrochat_6045024_3210.html> accessed 26 May 2021, and Johan Palm ‘Nytt läge efter Encrochat: ”Bruten tystnadskultur”’ *Svenska Dagbladet* (Stockholm, 26 March 2021) <<https://www.svd.se/nytt-lage-efter-encrochat-bruten-tystnadskultur>> accessed 26 May 2021.

surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights'.¹²

Thus, it is vital to examine if fundamental rights for the individual have developed at the same pace.

The first dimension of the thesis will look at is EU fundamental rights as given the CFR and the articles that concern interference by public authorities in surveillance matters: Primarily Articles 7, 8, and 52, and secondarily Article 47. Thus, the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) becomes highly relevant, due to the fact that the CFR must at the minimum provide the same level of protection as the ECHR for corresponding rights.¹³ The ECHR will therefore be used as a tool since Art. 7 of the Charter has a corresponding right in Art. 8 of the ECHR,¹⁴ Art. 8 of the Charter is reflected in Art. 8 of the ECHR,¹⁵ and Art. 47 of the Charter is based on Art. 13 and 6(1) of the ECHR.¹⁶

The second dimension of the thesis will focus on the rule of law and especially the substantive rule of law. It will be examined how the rule of law protects the fundamental rights given above. Rule of law is essential because its very existence is based on the aim to control the misuse of power from the ruler, the state and since surveillance of electronic communications is a severe infringement into the private lives of citizens (as well as non-citizens), the dimension of rule of law plays a vital role in controlling the misuse of government power and the surveillance of electronic communications. In the

¹² *Szabó and Vissy v. Hungary* App no 37138/14 (ECtHR, 12 January 2016) para. 68.

¹³ This is laid down by Art. 52(3) of the CFR.

¹⁴ Fundamental rights and the right to respect private and family life forms an integral part of general principle of EU law, Case C-136/79 *National Panasonic v Commission* ECLI:EU:1980:169 paras. 118.

¹⁵ See *Z v Finland* App no 22009/93, and the explanation of Article 8 CFR explains that it is based on Art. 8 ECHR.

¹⁶ This is explained in the description of the CFR.

end, the substantive rule of law will shine a light on whether EU actually provides fundamental rights in matters of surveillance.

Conclusively, the purpose of this essay is to understand if the EU fully provides fundamental rights in situations that relates to the surveillance of personal data, and examine if the rule of law guards the fundamental rights relating to privacy in EU law. Two questions will be answered by the thesis:

- How does the substantive rule of law ensure fundamental rights in situations when public authorities conduct surveillance of electronic communications?
- Should the CJEU take a substantive rule of law approach in future cases?

1.3 Methodology

The aim of legal doctrine in general and the legal-dogmatic method in particular, is to find *lex lata*, and for this thesis there will be no exception.¹⁷ This thesis will be using the legal-dogmatic method. For the legal-dogmatic method, the correct use of the sources of law needs to be used.¹⁸ For EU law, the Treaties sits at the top of the EU legal hierarchy, with the CFR which has the same value as the Treaties. Treaty provisions and other legal legislation must be construed in the light of the Charter.¹⁹ Naturally, from a constitutional perspective it is important to understand how Charter provisions should be construed which is the aim of the thesis.

A vital instrument will be case law by the CJEU. Since the Court has the exclusive right to interpret the Treaties, case law by the CJEU is vital to

¹⁷ Jan M. Smits 'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' (2015), Maastricht European Private Law Institute Working Paper 2015/06 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644088> accessed 21 May 2021.

¹⁸ Jan Kleineman 'Rättsdogmatisk metod' in Maria Nääv & Mauro Zamboni (eds) *Juridisk metodlära* (2nd edn, Studentlitteratur 2018) pp. 21-27.

¹⁹ Art. 6(1) TEU and Paul Craig & Gráinne de Búrca Gráinne *EU Law: Text, Cases, and Materials* (7th edn, Oxford University Press 2020) p. 147 P.

understand how Charter provisions should be interpreted.²⁰ Thus, the thesis will compare the recent judgements in *Schrems II*, *Quadrature du Net*, and *Prokuratuur* to see how the CJEU has interpreted *lex lata* and examine whether there have been any developments made for the relevant provisions of the CFR: Articles 7, 8, 47, and 52. As written earlier, the ECHR is also important to understand the minimum standards on the Charter, since Art. 52(3) of the Charter stipulates that corresponding rights in the ECHR should at the minimum provide the same right and freedom as the ECHR. The thesis will therefore also process case-law from the ECtHR to understand the scope of the rights of the ECHR.

The research questions, nonetheless, cannot be answered without a discussion on the rule of law. The primary objective of this thesis is not to find *lex lata*, but to find what role the substantive rule of law plays in protecting fundamental rights in surveillance matters. I will therefore have a discussion on the rule of law, what role it plays in general, and then defining substantive rule of law. The concept of rule of law will then be applied to the three cases of *Schrems II*, *La Quadrature du Net*, and *Prokuratuur* and the EncroChat affair. The application of the rule of law will be the analysis of the thesis.

Concerning the structure of the thesis, it follows a structure with the aim to make it as easy as possible to understand the context, the concepts and the rules. In Chapter 1, the introduction is given with background, purpose and legal issue but also more technical information such as the method, delimitation as well as existing research on the subject. Chapter 2 will set the surveillance context. It briefly explains surveillance in a historic context and then elaborates how surveillance is done this age with electronic communications. Chapter 3 discusses the rule of law from first a historical perspective and then by defining the substantial rule of law. At last, it quickly examines how rule of law is meant to function in the EU. Chapter 4 elaborates on the relevant fundamental rights and their minimum scope. Chapter 5 will

²⁰ These are vital since the ECJ has the right in preliminary rulings to interpret EU law, according to Art. 267 TFEU.

present the three cases *Schrems II*, *La Quadrature du Net* and *Prokuratuur* and the EncroChat affair. Chapter 5, the last chapter, will apply the substantive rule of law on the three cases and the EncroChat affair and examine if how the substantive rule of law protects fundamental rights. It will finish with answers to the research questions.

Last, concerning the reference system, I have followed Oxford University Standard for Citation of Legal Authorities (OSCOLA).²¹

1.4 Scope and Delimitation

To understand what rights and freedoms EU law provides in surveillance situations, the focus of this thesis will be on the three above named cases: *Schrems II*, *La Quadrature du Net*, and *Prokuratuur*. It therefore mainly focuses on two rights given in the Charter: the right to privacy and the right to protection of personal data but also the right to a fair trial and an effective remedy. Article 52 of the CFR, which describes when limitations and interferences of the fundamental rights, is highly relevant and will be analysed.

Concerning the three cases, I have chosen not to go into detail of the opinions of the Advocate Generals (AG), unless the CJEU has referred to the opinions or the AG have said something worth mentioning. This is in order to keep the thesis narrow and understandable for the reader. Regarding the material on rule of law, I have chosen what I have deemed to be relevant and will serve as a good foundation to the discussion of electronic communications surveillance. For substantive rule of law, I have mainly focused on the definition by Dworkin, but have also used the research by Craig as assistance.

²¹ ‘OSCOLA Oxford University Standard for the Citation of Legal Authorities’ Fourth Edition, Faculty of Law, University of Oxford.

1.5 Research on the subject

Research has been previously made on the right to privacy and protection of personal data. *Schrems*, the predecessor case to *Schrems II*, has widely been discussed in academic literature.²² However, the distinctive contribution this thesis will try to make, and what to my knowledge has not extensively been written on are mainly two dimensions.

The first dimension is the fact that *Schrems II*, *La Quadrature du Net*, and *Prokuratuur* are three relatively new cases, with *Schrems II* judgment published July 16th 2020, *La Quadrature du Net* published October 6th the same year, and *Prokuratuur* published March 2nd 2021. I.e. Not much time has passed since these three cases came out. The same goes with the EncroChat affair. It has still not been brought to the CJEU, but only national courts. The second dimension relates how rule of law is applied through the union and how substantive rule of law is applied practice. Although it is stated in preamble and in the beginning of the TEU, the principle is still not crystal clear. The concept of substantive rule of law has been discussed by many prominent legal scholars, and how it should function in theory. By applying it on the case-law from the CJEU, I hope to make a small academic contribution.

²² For discussion post *Schrems*, see Christopher Kuner ‘Reality and Illusion in EU Data Transfer Regulation Post *Schrems*’ (March 2019) Volume 18 Issue 4 German Law Journal pp. 881-918.

2 Setting the Context:

Surveillance in a digital era

2.1 Introduction

Surveillance has in some form always existed in modern history. Already in 1844, a scandal in the United Kingdom broke out when the public learnt that the government was opening letters, in the name of national security.²³ It has even been suggested that surveillance and information gathering was more far more intrusive in England before 1750 than today.²⁴ What is common, however, is that with new technology comes new types of surveillance with new discussions on what is morally right and wrong. In the first half of the 1900's, the *Metaxas dictatorship* in Greece used mass surveillance of all Greek citizens to control the state.²⁵ In *Estado Novo* in Portugal, the government had the ability to control all media and communication channels,²⁶ and during the Iron Curtain, the East German secret police *Stasi* employed a large pool of informants to gather information on citizens in East Germany. The Polish secret police *Śłużba Bezpieczeństwa* used wiretapping and microphones to gather intelligence, more or less on who they wanted to.²⁷

The point of the fleeting history brief is that surveillance by public authorities is not a new invention, but governments has used surveillance with the tools they have had available. Despite the fact that the majority of examples have

²³ David Vincent 'The Origins of Public Secrecy in Britain' (1991) Vol 1 Transactions of the Royal Historical Society pp. 229-248.

²⁴ Edward Higgs 'Further thoughts on the Information State in England...since 1500' in Kees Boersma et al. *Histories of State Surveillance in Europe and Beyond* (Routledge 2014) pp. 17-31.

²⁵ Minas Samatas 'A brief history of the anticommunist surveillance in Greece and its lasting impact' in Boersma pp. 49-54.

²⁶ Helena Machado & Catharina Frois 'Aspiring to modernization: Historical evolution and current trends of state surveillance in Portugal' in Boersma pp. 67-68.

²⁷ Ola Svenonius, Fredrika Björklund & Paweł Waszkiewicz 'Surveillance, lustration and the open society: Poland and Eastern Europe' in Boersma pp. 97-99.

been in more or less dictatorships, the NSA files leaked by Edward Snowden manifest that far-reaching advanced surveillance is not something reserved for dictatorships but used by advanced democracies as well.²⁸

The purpose of this Chapter is to first set the context of the surveillance used by the authorities. It will then proceed with defining the rule of law in context of surveillance in order to understand the next chapter, which will treat the fundamental rights in the chapter of surveillance.

2.2 Surveillance used by national authorities and the relation to data

2.2.1 Overview of electronic communications

Surveillance is conducted through many different ways, but for the sake of delimitation, I will focus on the types of surveillance made by public authorities in *Schrems II*, *La Quadrature du Net*, *Prokuratuur* and in the EncroChat cases. The method used by the public authorities in these cases is made through the surveillance of *electronic communications*, and thus the meaning of ‘data’ becomes highly relevant to understand the surveillance methods.

There is no single term for ‘data’. In Cambridge Dictionary, data is defined as ‘*information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer.*’²⁹ Data can be categorised as personal data, which provides information of character traits, preferences and geographical location of individuals. Data can also concern economic entities and objects, such as information on competitors, business strategies

²⁸ See Macaskill & Dance.

²⁹ Cambridge Dictionary ‘Data’ <<https://dictionary.cambridge.org/dictionary/english/data>> accessed 18 April 2021.

or business transactions. However, data in this thesis and in the CFR mainly focuses on personal data of individuals.³⁰

When personal data is topic for discussion, the term ‘big data’ also becomes relevant. Big data is used to describe the collection and utilisation of large masses of data. Big data often consist of different types of data, from various sources at a high speed. It is often processed by different algorithms and requires powerful processors and data transport technology. Big data can be described with three different ‘V’s: Velocity, Variety and Volume.³¹

Concerning data collection of personal data, there are different ways to gather these data. Personal data are not seldom provided to inter alia social networks and online shops. These online companies receive personal data such as postal address, email address, date of birth etc, but also pictures, videos, information on friends and relatives.³² Furthermore, the collection of personal data is not only collected by the entities which is on the opposite side of the customer, but also the intermediary, i.e., ‘*providers of electronic communications services*’.

Electronic communications services are those services provided through remuneration. The services offered are the transfer of electronic signals on electronic communications networks. In a clearer way, these are providers of internet access, interpersonal communications services such as number-based interpersonal services (voice calls) and number independent interpersonal services, and services of the conveyance of signals.³³

³⁰ Bruno Lasserre & Andreas Mundt ‘Competition Law and Big Data: The Enforcers’ View’ (2017) Vol 4 No 1 Italian Antitrust Review pp. 87-103.

³¹ Ibid. See also Gil Press ‘12 Big Data Definitions: What's Yours?’ *Forbes* (3 September 2014) <<https://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/>>.

³² Lasserre & Mundt pp. 89-90.

³³ Art. 2(4)-(7) Directive 2018/1972 establishing the European Electronic Communications Code.

Conclusively, there are many entities involved when electronic transmissions are sent through the e.g., internet. There is a high chance that by only downloading this thesis, electronic signals have been sent to the other side of the Atlantic Ocean. How does the authorities then conduct the surveillance?

2.2.2 Overview of surveillance

Public authorities have different ways of conducting surveillance of electronic data. This sub-chapter will shortly elucidate the surveillance used in *Schrems II*, *La Quadrature du Net*, *Prokuratuur*, and in EncroChat. Chapter 4 will explain in detail how the public authorities conducted their surveillance.

Public authorities from EU Member States conducting surveillance of electronic communications data were not the issue in *Schrems II*, but U.S. authorities. Namely, surveillance were conducted by the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA), which could receive access to personal data under two espionage programs: PRISM and UPSTREAM.³⁴

The PRISM program gave NSA the tool to collect data such as search history, email content, file transfers and live chats. In other words, the program facilitated surveillance on live communication as well as stored communication. The PRISM program also allowed intelligence services, such as NSA, to directly access servers of companies participating in the PRISM program, e.g. Facebook,³⁵ which was the object of *Schrems II*.³⁶ UPSTREAM was the other surveillance program used by U.S. authorities to conduct surveillance on electronic communications and was the object questionable program in the *Schrems II* judgement. Through the UPSTREAM surveillance, NSA was able to conduct bulk interception on the Transatlantic

³⁴ See Chapter 5.1.2.

³⁵ Facebook is a social media platform.

³⁶ Glenn Greenwald & Ewen MacAskill 'NSA PRISM program taps in to user data of Apple, Google and others' *The Guardian* (London, 7 June 2013) <<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>> accessed 12 May 2021.

communications cables.³⁷ This meant that NSA was able to conduct live surveillance of all electronic traffic in those cables, such as emails, chats and web-browsing traffic.³⁸

La Quadrature du Net and Others was actually three joined cases, two from France and one from Belgium. The first case (C-511/18) concerned French legislation which forced electronic communication providers to implement automatic data processing practices what would automatically detect links to potential terrorist threats. The second case (C-512/18) concerned French legislation that obliged a general and indiscriminate retention of communications by electronic communications providers. The third case (C-520/18) concerned Belgian legislation that required providers of electronic communications to retain data transferred on the network.³⁹

Prokuratuur did not concern surveillance by intelligence agencies or for the objective of terrorist threat or national security as in the two other cases, but it related to how investigating authorities in a criminal proceeding had obtained pre-trial personal data on the individual charged with the criminal acts, from a provider of electronic communications.⁴⁰

Conclusively, surveillance can be made by public authorities in many different ways, processing both live communications as in *Schrems II* and processing already retained data as in *Prokuratuur*. It can also be processed by other actors, such as providers of electronic communications services, at

³⁷ The Transatlantic communications cables are cables where data transfer across the Atlantic. To understand more on how the internet and electronic communications work, see the short documentary Cleo Abram (producer) 'How Does the Internet Work? - Glad You Asked S1' (Vox, 8 January 2020) <<https://www.youtube.com/watch?v=TNQsmPf24go>>.

³⁸ See Ashley Gorsky & Patrick Toomey 'Unprecedented and Unlawful: The NSA's 'Upstream' surveillance' American Civil Liberties Union (26 September 2016) <<https://www.aclu.org/blog/national-security/privacy-and-surveillance/unprecedented-and-unlawful-nsas-upstream>> accessed 3 May 2021

³⁹ Global Freedom of Expression 'The Cases of Privacy International, La Quadrature du Net and Others' Columbia University <<https://globalfreedomofexpression.columbia.edu/cases/the-cases-of-privacy-international-la-quadrature-du-net-and-others/>> accessed 7 May 2021.

⁴⁰ *Prokuratuur* paras. 16-17.

the request of public authorities, which was the case in *La Quadrature du Net*. Surveillance is also conducted on different bases, ranging from national security and terrorist threats (*Schrems II & La Quadrature du Net*) to relatively minor crimes (*Prokuratuur*). The question that needs to be asked is how public authorities are constrained from abusing these powerful tools and what role rule of law plays in this constraint.

2.2.3 Data Processing

To understand the context, it is also vital to understand the act of processing data. Data processing includes many different operations, such as “flow of data through the CPU and memory to output devices”, “formatting or transformation of output”, and “the conversion of raw data to machine-readable form”.⁴¹

Data processing in this thesis, will concern the type of processing which has been made by public authorities in the cases of *Schrems II*, *Quadrature du Net*, and *Prokuratuur* as well as in the EncroChat affair. Processing is defined in the GDPR as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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;”.⁴² It is this definition which the CJEU also uses, and notes that the GDPR does not distinguish between processing operations which are made within the European Union and in a third-country. It also goes as far as saying that merely the transferring of personal data from an EU member state to a third country in itself constitutes processing of personal data.⁴³

⁴¹ Encyclopedia Britannica Academic edition ‘data processing’ accessed May 10th 2021.

⁴² GDPR Article 4(2).

⁴³ *Schrems II*, paras. 82-83.

2.3 Summary

To summarise the chapter, it is quite clear that surveillance by the authorities is not a new phenomenon. It has constantly been conducted by the state and always adapted to the technology which has existed at the time. As the world is currently transferring into the digital age new type of technology is available to the authorities.

As can be seen in Chapter 2.2, the authorities today have many different types of capabilities in conducting surveillance. They can process communications live, meaning they see data operations at the same time they are conducted meaning they will always be at the same pace as the communicator. The data they can access is also quite extensive, unless it is ‘secret’ as in the EncroChat affair (although the Police actually managed to process all data in 2020). This could be done e.g., through tapping electronic cables, which the NSA did, or through automatic data processing practices. It can also be made through already retained data. In all three cases data had already been retained by different undertakings through national legislation. Through the capacities of the authorities extends even more since they can request the data after an investigation is already open.

Obviously, authorities also have rules and legislation to follow when they conduct these types of surveillances – they are constrained and cannot conduct surveillance when they wish to on whom they wish to. This is because surveillance in almost any given situation interferences with fundamental rights. Chapter 4 will furthermore explain how the fundamental rights are affected. Next chapter, however, will explore what role the rule of law plays in these situations.

3 Defining ‘rule of law’: Rule books and rights

3.1 Introduction

The idea of rule of law was already central to legal thought in the 4th century B.C., when Aristotle separated the rule of law from ‘that of any individual’. Around 2,200 years later, the French philosopher Montesquieu developed a doctrine of rule of law, which has since influenced Western liberal thought. In short, the meaning of this rule of law is that the mere creation of laws, the enforcement of the laws, and their relationships are themselves legally regulated so that no one is above the law. This means that governments and their bodies are subject to laws as much as ordinary citizens are.⁴⁴

Rule of law in the EU has a prominent place. It is already given in the preamble to TEU that the next step of European integration has drawn its inspiration from the inheritances of Europe, ‘*which have developed universal values of...the rule of law*’.⁴⁵ Furthermore, in order to construct the future of Europe, the Member States have to confirm ‘*their attachment to...the rule of law*’.⁴⁶ It is one of the founding values of the Union⁴⁷ and shall be promoted⁴⁸ by the Union. The CFR even says that the Union is based on the ‘principle’ rule of law.⁴⁹ Naturally, respecting the rule of law and being committed to promoting it are two conditions to join the EU.⁵⁰

⁴⁴ Choi, Naomi *Rule of law: political philosophy* Encyclopedia Britannica.

⁴⁵ TEU Preamble para 3.

⁴⁶ TEU Preamble para 5.

⁴⁷ TEU Art. 2.

⁴⁸ TEU Art. 3(1) states that its values should be ‘promoted’.

⁴⁹ CFR Preamble para 2.

⁵⁰ TEU Art. 49(1).

Ensuring the rule of law shall not only be task for the judiciary, the CJEU has held that EU institutions must review their compatibility with the Treaties and general principles of law.⁵¹ However, rule of law has many different dimensions and meanings. The next subchapters will expand on these different dimensions and concepts.

3.2 Brief history

Rule of law has a special relationship to the EU. It was in Europe it was incepted. The UK – a former EU member – the concept was developed by Locke and provided an example to Montesquieu and later served as an inspiration to the Federalist papers. In the Anglo-American world, the rule of law is far from having one steady definition.⁵² At the end of the 19th century, the concept of rule of law was developed by A. V. Dicey, who developed principles on the rule of law.

The first principle being ‘*no man is punishable or can be lawfully made to suffer in body or goods except for a distinct breach of law established in the ordinary legal manner before the ordinary courts of the land. In this sense the rule of law is contrasted with every system of government based on the exercise by persons in authority of wide, arbitrary, or discretionary powers of constraint*’. This first principle related to the fact that guilt should only be decided through the ordinary trial process. The second principle relates to the equality: ‘*every man, whatever be his rank or condition, is subject to the ordinary law of the realm and amenable to the jurisdiction of the ordinary tribunals*’. This principle related to equal access to remedy.⁵³ The first two principles essentially says that actions should be governed by legal norms, equal subjection to the law as well as access to the legal system. In order to

⁵¹ See e.g. Case C-583/11 P *Inuit Tapiriit Kanatami and Others v Parliament and Council*

⁵² Richard H Fallon, Jr, “The Rule of Law” as a Concept in Constitutional Discourse’ (January 1997) Vol 97 No 1 Columbia Law Review pp. 1-56.

⁵³ Constitution Committee, *Relations Between the Executive, the Judiciary and Parliament* (HL 2006-07) ‘Appendix 5: Paper by Professor Paul Craig, The Rule of Law’.

comply with the rule of law, the government must be able to have basis for its actions, which is by the legal system deemed as relevant.⁵⁴

On the continent, the *Grundgesetz* emerged with the *Rechtsstaat* with both formal and substantive components.⁵⁵ The *Rechtsstaat principle* means that public power is constrained by law, following the dark age of Nazi rule with horrendous human rights violations. Following this, the meaning and the scope of the *Rechtsstaat* was greatly expanded in the 1949 *Grundgesetz*.⁵⁶ In the formal sense, it encompasses the principles of legality, legal certainty, proportionality and judicial review. For its substantive part, is that the principle of protecting fundamental rights.⁵⁷

In France, it is agreed that the *Etat de droit* should be described by Giscard d'Estaing, saying 'When each authority, from the modest to the highest, acts under the control of a judge who insures that this authority respects the entirety of formal and substantive rules to which it is subjected, the *Etat de droit* emerges.'⁵⁸ In other words, it could be perceived that France is an *Etat de droit* since all public authorities must act under the control of a judge that can ensure that authorities respect formal and substantive rules in the Constitution.⁵⁹

How shall the rule of law be defined in the EU? Many of the older EU States do not have 'rule of law' in the national constitutions. However, where it is not explicitly mentioned, it is often said to be a part of a principle in the constitution. Nevertheless, a majority of the new countries explicitly refer to rule of law – a trend after the cold war. A common trait is that rule of law is

⁵⁴ Paul Craig 'Formal and Substantive Conceptions of the Rule of Law: an Analytical Framework' (1997) *Public Law* p. 467.

⁵⁵ The concept of formal and substantive rule of law will be discussed in the following subchapter.

⁵⁶ Pech pp. 32-33.

⁵⁷ Pech p. 34.

⁵⁸ Translation by Laurent Pech who cites Jacques Chevallier *L'Etat de droit* (Montchrestien, 2nd ed. 1994), p. 128.

⁵⁹ Pech p. 40.

exactly not defined by courts or constitutions. Regardless of the national legal systems, it is often left to scholars and judges to find out what rule of law is.⁶⁰

3.3 Formal and substantive rule of law

As described in the previous subchapter, formal and substantive components existed in Germany due to both *Grundgesetz* and *Rechtsstaat*, where it in its formal sense concerned the principles of legality, legal certainty, proportionality and judicial review, and in its substantive sense the fundamental rights. In France, even Giscard d'Estaing stated that the *Etat de droit* can only emerge once both formal and substantive rule of law are respected. Needless to say, formal and substantive rule of law need to be distinct from each other.

When it comes to the distinction between formal and substantive rule of law, the formal components such as proportionality, non-retroactivity, access to courts and fundamental rights protection serves the substantive values such as human dignity, individual autonomy and social justice. I.e., the gravity put on the rule of law has led to the legitimisation of the instrumentalization of the state, which is supposed to serve the individual as well as protect the rights. This also means, inter alia, that individuals must be able to challenge public authorities for fundamental rights violations.⁶¹

To be more precise, formal conceptions of the rule law concerns how the law was promulgated, i.e., if was properly authorised by the correct person and in a correct manner, how clear the norm is (in order to have legal certainty), and the temporal dimension of the rule. Formal conceptions, nonetheless, does not aim to analyse the actual substances of the rule itself. If the rule itself is good or bad does, in the formal conception, not matter.⁶²

⁶⁰ Pech pp. 42–43.

⁶¹ Pech p. 44.

⁶² Craig p. 467.

This is where substantive rule of law differs. The concept of substantive rule of law says that rule of law indeed has formal attributes, as defined in the paragraph above, but that itself has bigger purpose – that rights can actually be derived from the rule of law itself.⁶³

The prominent American jurist Ronald Dworkin did a thorough account of substantive rule of law and divided the formal and substantive rule of law by calling the formal rule of law ‘the “rule book” conception’ and the substantive rule of law ‘the “rights” conception’. He defined the rights conception as the following:

“It assumes that citizens have moral rights and duties with respect to one another, and political rights against the state as a whole. It insists that these moral and political rights be recognized in positive law, so that they may be enforced upon the demand of individual citizens through courts or other judicial institutions of the familiar type, so far as this is practicable. The rule of law on this conception is the ideal of rule by an accurate public conception of individual rights. It does not distinguish, as the rule book conception does, between the rule of law and substantive justice; on the contrary it requires, as part of the ideal of law, that the rules in the book capture and enforce moral rights.”⁶⁴

This has further been explained by the fact that in a democracy, the people have a moral right that the courts actually enforce the rights the legislature has enacted. If it is clear which rights the legislature has granted them, it is also clear which rights they have a moral right to receive in the judiciary. Substantive rule of law does not separate substantive justice from rule of law.

⁶³ Craig, p. 467

⁶⁴ Ronald Dworkin *A Matter of Principle* (Harvard University Press 1985), pp. 11-12.

It requires that the rule of law enforces the correct moral rights, and in the end, if the Court enforces what they believe is the best substantive justice.⁶⁵

3.3.1 Substantive rule of law in the EU

The notion on ‘substantive rule of law’ as something that ensures that fundamental rights can be found in EU case-law from the CJEU. It has developed two sorts of lines concerning substantive rule of law. The first line derives from the case *Portuguese Judges*, in which the CJEU extended the use of Article 19 TEU and has now become competent to rule on matters which used to be a part of the national competences.⁶⁶ The second line, deriving from the case *LM*, exists in the context of mutual recognition and the European Arrest Warrant (EAW), by examining the independence and impartiality of the judicial authorities issuing the EAW.⁶⁷

Through *Portuguese judges*, the independence of the judicial system was highlighted in the context of preliminary proceedings in Article 267 TFEU. Any national organ being a court or tribunal, must exercise its functions completely autonomously, without being constrained by other hierarchy or subject to any other body so it is protected against external intervention pressure which might affect the impartiality of the body. The Court essentially extended the meaning of rule of law to the dimension of other Member States to protect fundamental rights.⁶⁸

LM concerned the fundamental right to a fair trial and regarded the European Arrest Warrant. The Applicant opposed his surrender since he believed that there were systemic deficiencies which would affect the independence of the judiciary in the trial and his right to a fair trial. The Court assessed as a first

⁶⁵ Craig, pp. 477-479.

⁶⁶ Case C-64/14 *Associação Sindical dos Juizes Portugueses (Portuguese Judges)*.

⁶⁷ Xavier Groussot & Johan Lindholm ‘General Principles: Taking Rights Seriously and Waving the Rule-of-Law-stick in the European Union’ (2019) Lund University Legal Research Paper 1/2019 p. 14 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3361668> accessed 20 May 2021 & Case C-216/18 PPU *Minister for Justice and Equality (Deficiencies in the system of justice) (LM)*.

⁶⁸ *Portuguese judges* para. 43 & Groussot & Lindholm pp. 7 & 16.

step that the independence of the judiciaries must be assessed on whether systemic or generalised deficiencies at the judiciary existed. The main assessment was made on the so-called external and internal independence of the national judicial system. The external aspect is that the Court is able to fill its function autonomously without any hierarchical constraints or other body so that it is protected against external intervention. The internal aspect is linked to the impartiality of the court, so both parties have an equal distance from the court during the proceedings as well as their respective interests.⁶⁹ The assessment must also take into account the fact that when a Member State has been the subject for procedure in the Commission and the Council for assessing that there is a risk of breaching the values in Article 2 TEU. i.e., the rule of law.⁷⁰

Conclusively, the CJEU has through these two cases adopted a human-rights-based approach concerning the independence of judiciary and is almost touching upon the substantive rule of law which was discussed by Dworkin.⁷¹ Then it must be asked how this would relate to fundamental rights in surveillance matters.

3.3.2 Issues

How formal and substantive rule of law in the EU relates to surveillance, has several dimensions. The rule of law relates to the idea that state power, such as the ability to mass surveillance, is constrained. Surveillance can be legal in a strict sense, but still breach rule of law. The protection of privacy is deeply rooted in the idea of rule of law, since the idea is to constrain the arbitrary discretion of state power – something that the substantive rule of law does.⁷² A broad discretion may increase the risk of abuse of power.⁷³

⁶⁹ *LM* paras. 62-66 and Groussot & Lindholm p. 17.

⁷⁰ *LM* paras. 69 and Groussot & Lindholm p. 17.

⁷¹ Groussot & Lindholm p. 19.

⁷² Lisa M Austin 'Surveillance and the rule of law' (July 2015) Vol 13 No 2 *Surveillance and Society*, see also Lisa M Austin 'Getting Past Privacy? Surveillance, the Charter, and the Rule of Law' (June 2014) Vol 27 No 3 *Canadian Journal of Law and Society* 27, p. 383 and Craig, p. 486.

⁷³ Austin 'Getting Past Privacy? Surveillance, the Charter, and the Rule of Law' p. 387.

Across the Atlantic, there have been discussions about legal ‘black holes’ and legal ‘grey holes’.⁷⁴ Legal black holes are laws that ‘either explicitly exempt [...] the executive from the requirements of the rule of law or explicitly exclude [...] judicial review of executive action.’⁷⁵ Grey holes exist when ‘there are some legal constraints on executive action [...] but the constraints are so insubstantial that they pretty well permit government to do as it pleases.’⁷⁶ What is interesting is the notion of legal ‘grey holes’ – laws that *prima facie* seem to comport with rule of law, but actually do not.⁷⁷

For legal grey holes, substantive rule of law may play a vital role in order to ensure fundamental rights for the individual. Laws that allow the authorities in advance who might exercise the judgement over the exception brings the problem in defining the exception. Exceptions are difficult to specify and will therefore be left to future actors to decide what constitutes as a valid exception. Open-ended exceptions and its standards must be subject for review, if the review becomes sufficiently low, grey holes will appear.⁷⁸ Grey holes, however, may play a part in emergencies or e.g security emergencies. Where law decides that authorities may stop with procedural requirements because there are good causes for the stop, the good cause will serve as a justification in circumstances of emergency.⁷⁹ Nevertheless, the concept of substantive rule of law can prevent ‘bad’ grey holes from emerging since they are there to serve the best substantive justice.

⁷⁴ ‘Legal black hole’ was coined by Johan Steyn, see Johan Steyn ‘Guantanamo Bay: The Legal Black Hole’ (January 2004) Vol 53 No 1 The International and Comparative Law Quarterly pp. 1-15., and ‘legal grey hole’ was coined by David Dyzenhaus, see David Dyzenhaus *The Constitution of Law: Legality in a time of emergency* (Cambridge University Press 2006) p. 3.

⁷⁵ Dyzenhaus p. 3.

⁷⁶ Ibid. p. 42.

⁷⁷ Adrian Vermeule ‘Our Schmittian Administrative Law’ (February 2009) Vol 122 No 4 Harvard Law Review p. 1102.

⁷⁸ Ibid. p. 1104.

⁷⁹ Ibid. pp. 1105-1106.

3.4 Summary

As has been explained above, the rule of law has a long history on the European continent, with different expressions in different constitutions and legal systems. In old legal systems as UK, Germany and France rule of law have been important principles, and also been expressed in formal and substantive conceptions. The American jurist Dworkin examined the rule of law by dividing them in two conceptions: the formal rule of law as the “rule book” conception and the substantive rule of law as the “rights” conception. The “rights” conception is important since it looks on whether the law itself is good or not – and not only if the formal requirements have been fulfilled, It requires the formal rule of law to actually capture and enforce moral rights in order to bring substantive justice.

By then examining how the CJEU has enforced the rule of law in case-law it is clear that the CJEU has extended the application of the rule of law and seen it as a fundamental right, thus applying a human-rights-approach to define and protect judicial impartiality and independence (i.e. the rule of law). Last, rule of law issues were raised, particularly the issues of legal black and grey holes, and how the substantive rule of law could prevent legal grey holes.

Now that the substantive rule of law has been established as the part that guarantees fundamental rights, the next chapter will discuss the fundamental rights related to privacy and surveillance.

4 The object of substantive rule of law: fundamental rights

4.1 Introduction

It is important to remember the context in which the EU was founded. 2,000 years of conducting war with neighbours lead to the two most bloodshed events of history: the two world wars. After the horrors of the second world war, it was understood what capabilities humans have and how horrific mankind can be. It is not strange that it was after the second world war that the Universal Declaration of Human Rights was drafted, and it is not strange that it was after the second world war that the ECHR was drafted, and that the peace project European Coal and Steel Community was founded.

Fundamental rights are one of the most important components of the EU, which is demonstrated by the CFR and the judgements of the CJEU. This Chapter will examine the fundamental rights which are subject to surveillance matters and which will be the object of the substantive rule of law in Chapter 6.

4.2 Fundamental rights guaranteed under surveillance of communications

What goes hand in hand with data laws are the opposite of that spectrum, which is privacy rights. Privacy rights are derived from first the EU Charter on Fundamental Rights, namely Article 7, respect for private and family life and Article 8, Protection of personal data. What is also *prima facie* topical in *Schrems II* and *Quadrature du Net* is Article 47, the right to a fair trial and an effective remedy. I will also argue that this right is topical in *Prokuratuur*

even if the CJEU does not mention it. Last, Article 52 of the Charter is topical, since it lays down the conditions to when a right or freedom is limited.

The rights from the Charter can also be found in secondary law. In the GDPR, Data Protection Directive, the Electronic Commerce Directive, and the ePrivacy Directive there are all references to the above-mentioned CFR provisions.

4.2.1 Case-law from the ECtHR: the bare minimum

Article 52(3) provides that corresponding Articles in CFR to rights and freedoms in the ECHR, the *‘meaning and scope of those rights shall be the same as those laid down by the said Convention.’* Furthermore, importantly, this shall not prevent Union law to give a wider protection than the ECHR. In other words, the ECHR provides the bare minimum.

Article 7 CFR correspond to those rights given in Article 8 ECHR which gives:⁸⁰

- ‘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 the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.’⁸¹*

One could also believe that Article 8 CFR would have a separate corresponding the in the ECHR, but the case is that it does not correspond to

⁸⁰ Explanations (*) Relating to the Charter of Fundamental Rights

⁸¹ In the explanation is also given that in order to keep up with technology developments, ‘correspondence’ has been changed to ‘communications’.

a right in the ECHR, but it is *based on, inter alia*, on the above Article 8 of the ECHR.⁸² In order to find the bare minimum, it shall be investigated how what scope the ECtHR gives the rights.

In *Hambardzumyan v. Armenia* the Head of the Department Against Organised Crime in Armenia had sought the authorisation to carry out surveillance of Ms Hambardzumyan, who allegedly was accepting bribes in the prison she was working at. The District Court authorised the conduct of video and audio recordings for a month.⁸³ Ms Hambardzumyan had complained *inter alia* that she was denied a fair since the court had admitted recordings which were unlawfully obtained under her unlawful secret surveillance.⁸⁴

The Court noted that although Art. 6 ECHR does not set any rules on the admissibility of evidence – this is a matter for national law. Regard must instead be given on whether the rights of the defence were respected, particularly if she could challenge the authenticity of the evidence.⁸⁵ Furthermore, in deciding if the proceedings as a whole were unfair, the weight of public interest of the investigation and the punishment for the particular offence must be weighed against the individual interest that the evidence was gathered unlawfully.⁸⁶

The applicant had also raised the issue of covert surveillance in the initiation proceedings. The Court agreed with the government which had said that the courts did not deal with the complaint concerning the Applicant's right to respect for private life and not necessary in a democratic society. The Court therefore concluded that raising the issue of surveillance before courts that

⁸² Article 7 CFR, besides Article 8 ECHR, is also 'based' on Art. 286 Treaty Establishing the European Community (current Article 16 TFEU and Article 39 TEU) and Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

⁸³ *Hambardzumyan v. Armenia* paras. 6–9.

⁸⁴ *Ibid.* paras. 69 & 71–72.

⁸⁵ *Ibid.* paras. 73 & 75.

⁸⁶ *Ibid.* para. 76.

are viewing the merits of a criminal case against the applicant cannot be seen as effective remedy in respect of her complaints under art. 8 of the ECHR.⁸⁷

The case *Big Brother Watch and other V United Kingdom* concerned the PRISM programme – same as in *Schrems II* – after media reports from whistle-blower Edward Snowden. The leaked information from Mr Snowden also contained information about the UK surveillance programme TEMPORA, in which the GCHQ could access electronic traffic between the US and UK in the fiberoptic cables. ‘*GCHQ is able to access not only metadata but also the content of emails, Facebook entries and website histories.*’⁸⁸

One of the applicants had complained under Article 6 ECHR, saying that the limitations inherent in the Investigatory Powers Tribunal (IPT)⁸⁹ proceedings, saying the proceedings were disproportionate and ‘impaired the very essence of their right to a fair trial.’⁹⁰ The Court however, argued that Art. 6 ECHR was inapplicable, since the complaint of the complaints was ill-founded.⁹¹ However, the Court also reasoned that to ensure efficacy of the surveillance regime, and how important that is to combat terrorism and serious crime, the restrictions on the procedural rights were both necessary and proportionate and therefore did it did not breach the very essence of the right enshrined in Article 6 ECHR.⁹²

In *Centrum för Rättvisa v Sweden*, Centrum för Rättvisa, a Swedish foundation, had brought proceedings against Sweden on the matter of signal intelligence, saying that Swedish legislation and practice breaches Article 8 of the ECHR.⁹³ Namely, under certain conditions, the intelligence services

⁸⁷ *Hambardzumyan v. Armenia* para. 40, 42–44.

⁸⁸ *Big Brother Watch and others v United Kingdom*, para. 2.

⁸⁹ Investigatory Powers Tribunal, a special court established for wrongful interference under the Regulations of Investigatory Act 2000.

⁹⁰ *Big Brother Watch and others v United Kingdom*, para. 501.

⁹¹ *Ibid.* para. 508.

⁹² *Ibid.* para. 509–510.

⁹³ *Centrum för Rättvisa v. Sweden*

may collect (intercepting, processing, and analysing) electronic signals that are sent through satellites, radio links and cables (i.e. all things over internet and phones).⁹⁴

The Court then describes minimum safeguards that needs to be set out in law to prevent the abuse of power by public authorities:

*‘a description of the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of the measures; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed’.*⁹⁵

Regarding what is ‘necessary in a democratic society’, in Court replied that

*‘the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.’*⁹⁶

In *Szabó and Vissy v Hungary* the Court once again stated that any interference under art 8 § 2 can be justified if it is necessary in a democratic

⁹⁴ Centrum för Rättvisa v. Sweden paras. 7–9 & and 12–15.

⁹⁵ Centrum för Rättvisa v. Sweden para. 103, referring to *Roman Zakharov* para. 231.

⁹⁶ Centrum för Rättvisa v. Sweden para. 104, referring to *Roman Zakharov* para. 232.

society to pursue legitimate aims under art 8 § 2. Regarding the aim to safeguard national security, the Court repeated the minimum safeguards which were set out above.⁹⁷ When the state balances the interest of protecting its national security, through measures of secret surveillance nature, against the right to respect for the private life of the individual, national authorities have a certain high margin of appreciation of choosing the means. The Court nevertheless says: *‘a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse’*. The assessment should be made on the circumstances of the case: the nature, scope and duration of measures, competences of authorities to execute and supervise measures, and remedies provided under national law.⁹⁸

The applicants had argued that it did not meet the foreseeability requirement of article 8 § 2 since it did not give sufficient guarantees against abuse and arbitrariness.⁹⁹ In the context of surveillance, foreseeability does not mean that an individual should be able to foresee when the individual concerned shall not be able to foresee when the authorities may intercept his or her communications. Furthermore, it is necessary to have detailed rules on interception of telephone conversations, especially since the technology to use for this are becoming more sophisticated.¹⁰⁰ In matters of fundamental rights it would not be rule of law (‘one of the basic principles of a democratic society enshrined in the Convention’) for a discretion which is granted to authorities to be expressed in the sense of ‘unfettered power’.¹⁰¹

⁹⁷ Szabó and Vissy v Hungary paras. 54–56.

⁹⁸ Ibid. para. 57.

⁹⁹ Ibid. para. 61.

¹⁰⁰ Ibid. para. 64.

¹⁰¹ Ibid. para. 66.

4.3 Summary

To summarise, the right to privacy, the right to the protection of personal data as well as the right to a fair trial and effective remedy have all been scrutinised and a quite high level of protection. It is obvious, however, that the right to privacy and the right to the protection of personal data are not absolute rights. They can be interfered with what is deemed as necessary in a democratic society when pursuing certain objectives, such as national security. It is also quite clear that the rights function as a check on the authorities, in order to prevent the authorities from abusing their power.

Before examining how substantive rule of law protects these fundamental rights, it shall be examined how the CJEU have applied them in three recent cases and how they correlate to the current affair of EncroChat.

5 Data Privacy at the beginning of 2020's: From Schrems II to Encrochat

5.1 Schrems II

5.1.1 Introduction

As written in chapter 2.3.2, *Schrems II* concerned personal data leaving the Union to the U.S. which under two espionage programs, *PRISM* and *UPSTREAM* and the so-called Privacy Shield Decision from the Commission. Even though that the surveillance was made by extraterritorial authorities, the CJEU still found that the rights and freedoms laid down by the Charter were applicable and therefore made no distinction on public authorities in EU Member States and U.S. public authorities.

5.1.2 Case facts

Schrems II regarded the Privacy Shield Decision¹⁰² (PSD) from the Commission. In the primary case, *Schrems*¹⁰³, the Court had declared Commission Decision 2000/520/EC¹⁰⁴ invalid, since the CJEU did not find that the decision provided a sufficient protection in the EU-US Privacy shield. The decision concerned safe harbour privacy principles and related frequently asked questions by the U.S. Department of Commerce. Following the

¹⁰² Commission Implementing Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

¹⁰³ Case C-362/14 *Schrems* EU:C:2015:650

¹⁰⁴ Commission Decision 2000/520/EC 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.

judgment in *Schrems*, the Commission corrected the flaws of the decision and adopted the so-called Privacy Shield Decision.¹⁰⁵

In its assessment, the Commission had explained in the PSD how an adequate level of protection exists in the context of the EU-US Privacy shield.¹⁰⁶ According to Art. 1 of the PSD the U.S. would ensure an ‘*adequate level of protection of personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield.*’ The principles would may be limited to *inter alia* necessary extent of national security, public interest, or law enforcement requirements.¹⁰⁷

In the main proceedings, Mr Schrems, an Austrian national, had been a user of the social network Facebook, a product of Facebook Inc. All EU users of Facebook had to agree on terms with a subsidiary of Facebook Inc: Facebook Ireland. Some or all of the personal data of the users of Facebook Irelands were transferred to servers of Facebook Inc. in the U.S., where it also was processed.¹⁰⁸

In June 2013, Mr Schrems had filed a complaint with the Commissioner, requesting that Facebook Ireland be prohibited to transferring his personal data to the United States, since the United States did not ensure sufficient protection of personal data against surveillance activities from the public authorities.¹⁰⁹ The High Court, following the judgement from the CJEU in *Schrems*, annulled the rejection of Mr Schrem’s complaint and referred back the decision to the Commissioner. Facebook Ireland stated that the data

¹⁰⁵ *Schrems II* paras. 42-43.

¹⁰⁶ *Ibid.* para. 45, paras. 68, 69, 76, 77, 109, 112, 113, 114, 115, 116, 120, 136, and 140 in the PSD.

¹⁰⁷ *Schrems II* paras. 46-47.

¹⁰⁸ *Ibid.* paras. 50-51.

¹⁰⁹ *Ibid.* paras. 51-53.

transferred to Facebook Inc. followed the SCC Decision¹¹⁰, in which the Commissioner asked Mr Schrems to reformulate the complaint.¹¹¹

In the reformulated complaint, Mr Schrems claimed that U.S. law requires Facebook Inc to make the personal data available to certain law enforcement authorities, such as the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA). Mr Schrems argued that since the data was used in the context of different monitoring programmes incompatible with Articles 7, 8, and 47 of the Charter, the data transfers to the U.S. were not justified under the SCC Decision. He thus asked the Commissioner to prohibit or suspend the transfer of his personal data to Facebook Inc. in the United States.¹¹²

Since the reformulated complaint of Mr Schrems raised the issue of the validity of the SCC Decision, the Commissioner brought an action before the High Court. The High Court referred to a judgement given on 3 October 2017 in which the referring court is obliged to consider all facts presented to it and that the U.S. authorities' intelligence activities on personal data transferred to the U.S. from the EU is based on, inter alia, Section 702 of the Foreign Intelligence Surveillance Act (FISA, U.S. law) and on Executive Order (E.O. U.S. federal directive) 12333.¹¹³

Section 702 of the FISA gives the Attorney General and the Director of the National intelligence the permit to authorise (following an approval from the Foreign Intelligence Surveillance Court, FISC) the surveillance of non-U.S. citizens outside the U.S. in order to obtain 'foreign intelligence information', providing the basis for the PRISM and UPSTREAM surveillance programmes, in which the NSA, FBI, and CIA receives access to personal data of non-US nationals.¹¹⁴

¹¹⁰ Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 as amended by Commission Implementing Decision (EU) 2016/2297.

¹¹¹ *Schrems II* para 54.

¹¹² *Ibid.* para. 55.

¹¹³ *Ibid.* paras. 57-60.

¹¹⁴ *Ibid.* paras. 61-62.

The referring court also found that E.O. 12333 gives the NSA the permit to access, collect and retain data from underwater cables on the floor of the Atlantic, before arriving to the U.S. The referring court emphasised that non-U.S. persons are only covered by PPD-28, which states that intelligence activities should be ‘tailored as feasible’. It therefore considered that the U.S. carried out mass processing of personal data without guaranteeing the rights given in Arts. 7 and 8 of the Charter.¹¹⁵

5.1.3 Judgement

The relation to GDPR and Article 4(2) TEU

The first question the referring court asked whether Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR in conjunction with Article 4(2) TEU applies to data which is transferred to a third country when that same data is liable to be processed by authorities for purposes of public security, defence and state security.¹¹⁶ The CJEU concluded that Article 4(2) TEU was irrelevant since national security remains the sole responsibility of EU Member States.¹¹⁷

Regarding processing of personal data, the CJEU concluded that the GDPR does not distinguish operations that takes place within the European Union and those outside. It also said that the GDPR “subjects transfers of personal data to third countries” and has specific rules for such transfers in its fifth chapter.¹¹⁸ A transfer, such as the one in the proceeding, cannot fall outside the scope of the GDPR if that personal data will be processed by the public authorities of a third country, for the purposes of public security, defence and state security, since it is ‘*patent from the very wording of Article 45(2)(a)*’ of the GDPR that no processing by a third country for the purposes of public security, defence and state security excludes the transfer.¹¹⁹

¹¹⁵ *Schrems II* paras 63–64.

¹¹⁶ *Ibid.* para 80.

¹¹⁷ *Ibid.* para 81.

¹¹⁸ *Ibid.* para 82.

¹¹⁹ *Ibid.* paras 87-88.

The level of protection provided

The referring court also asked the CJEU to clarify the level of protection which is required by the GDPR when personal data transfers to a third country.¹²⁰

The CJEU replied that the third country does not have to provide an identical level of protection given in the EU, but an *adequate level of protection* (as given in recital 104 GDPR). This means a level of protection which is essentially equivalent to the one given in the EU, ‘*by virtue of the regulation, read in the light of the Charter*’.¹²¹

In the absence of an adequacy level of protection, safeguards must be taken by the controller or processor to compensate for the lack of adequacy level of protection.¹²² In those cases, appropriate guarantees must give a level of protection essentially equivalent to that given in the EU.¹²³ Article 46(1) of the GDPR says that data subjects must be given ‘*appropriate safeguards, enforceable rights and effective legal remedies*.’ The assessment must take into account the contractual clauses between the controller or processor in the EU and the recipient in the third country concerned. Also, concerning the access to personal data of public authorities in that country, relevant aspects of the legal systems.¹²⁴ Regarding the ECHR, the CJEU stated that since the ECHR does not constitute a legal instrument which is formally a part of EU law, the examination shall be made in the light of EU law.¹²⁵

The SCC Decision in light the CFR

The referring court asked about the validity of the SCC Decision in light of Articles 7, 8 and 47 CFR.¹²⁶

¹²⁰ *Schrems II* para. 90.

¹²¹ *Ibid.* para 94. The Court also referred, by analogy, to *Schrems* para. 73.

¹²² Art. 108 GDPR

¹²³ *Schrems II* paras. 95-96.

¹²⁴ *Ibid.* paras. 103-104.

¹²⁵ *Ibid.* paras. 98-99.

¹²⁶ *Ibid.* para. 122.

As stated earlier, in the absence of an adequacy decision, transfer of personal data is permitted if the controller or processor has provided appropriate safeguards and that enforceable data subject rights and effective legal remedies exist. It is not stated in the provisions, however, that all the safeguards must necessarily be provided for in a Commission decision.¹²⁷ It is the controller or processor in the European Union that needs to provide (given the absence of a Commission adequacy decision) the appropriate safeguards.¹²⁸

The nature of the contracts cannot bind the public authorities of the third country – GDPR¹²⁹ interpreted in the light of Articles 7, 8 and 47 of the Charter requires that the level of protection is not undermined and therefore need to support the guarantees given in the clauses. In other words, depending on the prevailing position in the third country, the controller might be needed to adopt supplementary measures to ensure the compliance of that level of protection.¹³⁰ The validity depends on whether the said Articles in light of Article 7, 8 and 47 of the Charter make it possible to ensure compliance with the level of protection required by EU law and that the breach of those rules has the consequence that transfer is suspended or prohibited.¹³¹

Clause 5 in the annex to the SCC decision states that mandatory requirements that do not go beyond what is necessary in a democratic society are not in contradiction with those standard data protection clauses, as long as the aim is to safeguard, *inter alia*, national security, defence and public security. Measures that go beyond what is necessary, are breaches of those clauses.¹³²

Transfer of data to third country and the CFR

¹²⁷ *Schrems II* para. 127.

¹²⁸ *Ibid.* para. 131.

¹²⁹ Article 44, 46(1) and 46(2)(c).

¹³⁰ *Schrems II* para. 132–133.

¹³¹ *Ibid.* para. 137.

¹³² *Ibid.* para. 141.

By the fourth, fifth and tenth question the referring court wished to know if the transfer to the third country of the personal data pursuant to standard data protection clauses in the SCC Decision annex breached the rights enshrined in Articles 7, 8 and 47 of the Charter, and in particular if the introduction of the ombudsperson in Annex III in the Privacy Shield.¹³³

The Court stated that it would examine if the Privacy Shield Decision complied with the GDPR in the light of the Charter and highlighted that the U.S. must ensure a level of protection which is essentially equivalent to the EU-level.¹³⁴ The Commission had found that the U.S. did ensure an adequate level of protection for personal. The PSD, however, prescribed that the principles may be limited in interest of national security, public interest, or law enforcement requirements. More particularly, the personal data can be accessed by the U.S. authorities through the PRISM and UPSTREAM surveillance programs.¹³⁵

The Court underscored that processing of data that related to the respect of personal life under Art. 7 CFR, which concerns any information that relates to an identified individual, also falls within the scope of Article 8 CFR.¹³⁶

The communication of personal data to a third party, e.g., a public authority, interferes with Art. 7 CFR, regardless how the data will be used. The same is when that data is only possessed by such authorities, regardless of its sensitivity.¹³⁷ However, the rights in Article 7 and Article 8 are not absolute, *'but must be considered in relation to their function in society'*.¹³⁸ Under Article 8(2) of the Charter, personal data must inter alia be processed *'for specified purposes and [...] some other legitimate basis laid down by law.'*¹³⁹

¹³³ *Schrems II* para. 150.

¹³⁴ *Ibid.* paras. 161–162, the Court also referred to *Schrems* para. 67 & 96.

¹³⁵ *Schrems II* paras. 163–165, and Section 702 of the FISA and E.O. 12333.

¹³⁶ See *Schrems II* para. 170.

¹³⁷ See *Ibid.* para. 171.

¹³⁸ See *Ibid.* para. 172.

¹³⁹ *Ibid.* para. 173.

Nevertheless, any limitation on the rights must be subject to the principle of proportionality.¹⁴⁰ Furthermore, limitations of fundamental rights must have a legal basis, which means interference and scope of limitation is permitted by law.¹⁴¹ In addition, the legislation must lay down clear and precise rules of the scope and application as well as the safeguards. Specifically, it must indicate the circumstances of the conditions so that the ‘*interference is limited to what is strictly necessary.*’¹⁴²

Since the FISA does not give any limitation on its power¹⁴³, the CJEU agreed with AG Saugmandsgaard Øe,¹⁴⁴ that the articles do not ensure a level of protection which is essentially equivalent to what is guaranteed by the CFR. The Articles do neither define the scope of the limitation nor give clear and precise rules on the scope nor impose minimum safeguards.¹⁴⁵ In addition, the Presidential Policy Directive 28 (PPD-28)¹⁴⁶ does not grant data subjects ‘actionable rights’ before courts against U.S. authorities and does therefore not ensure a protection level which is essentially equivalent to that in the CFR.¹⁴⁷ Conclusively, neither FISA nor E.O. 12333 in conjunction with PPD-28 does correlate to minimum safeguards from the principle of proportionality and i.e. cannot be seen as being limited to what is strictly necessary.¹⁴⁸

Regarding Art. 47 CFR, the Court stated that ‘*the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law.*’ Hence, if no legislation provides

¹⁴⁰ *Schrems II* para. 174 and Art. 52 of the CFR: ‘...limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.’

¹⁴¹ *Schrems II* para. 175, the Court also referred to *Opinion 1/15* (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, para. 139 and the case-law cited.

¹⁴² *Schrems II* para. 176, the Court also referred to *Opinion 1/15* paras. 140-141 and the case-law cited.

¹⁴³ Section 702 FISA.

¹⁴⁴ In paras. 291, 292 and 297 of Opinion of AG Saugmandsgaard Øe *Schrems II* ECLI:EU:C:2019:1145.

¹⁴⁵ *Schrems II* para. 180.

¹⁴⁶ The PPD-28 applies on all activities involving the collection and use of foreign intelligence information.

¹⁴⁷ *Schrems II* para. 181.

¹⁴⁸ *Ibid.* para. 184.

individuals the possibility to pursue legal remedy concerning his or her personal data, the very essence of the fundamental right to effective judicial protection is not respected.¹⁴⁹

The introduction of a Privacy Shield Ombudsperson cannot remedy the deficiencies in connection with the judicial protection of the personal data. Since the surveillance programs (Under Section 702 of the FISA and E.O. 12333) does not grant data subjects rights which can be used in courts against U.S. authorities, and therefore do the subjects not have the right to an effective remedy.¹⁵⁰ One condition of Article 47 is that individuals must be able to bring legal action in front of an independent and impartial court in order to have access to their personal data, obtain the rectification or erasure of the data in question.¹⁵¹ The CJEU also found that the independence of the Ombudsperson is not guaranteed since the office is appointed by the Secretary of the State and forms a part of the U.S. State Department.¹⁵²

5.2 La Quadrature du net

5.2.1 Introduction

The Quadrature du net-judgment was handed down from the CJEU October 6th 2020 and is three joined cases, two cases from France and one from Belgium. What the three cases have in common is that they concern surveillance in the name of public and national security, especially the combat against terrorism. The surveillance used by the authorities in the case, were *inter alia* a general and indiscriminate retention of traffic and data, real-time access to data, and an automated analysis of data.

¹⁴⁹ *Schrems II* para. 187, which also referred to *Schrems* paragraph 95.

¹⁵⁰ *Schrems II* paras. 190 & 192.

¹⁵¹ *Ibid.* para. 194.

¹⁵² *Ibid.* para. 195.

5.2.2 Case facts

C-511/18 La Quadrature du Net and Others

La Quadrature du Net, French Data Network, the Fédération des fournisseurs d'accès à Internet associatifs and Igwan.net brought actions before the Conseil d'État¹⁵³ seeking to annul three decrees¹⁵⁴ since they infringed the French Constitution, the ECHR and Directives 2000/31 ('e-Commerce Directive')¹⁵⁵ and 2002/58 ('ePrivacy Directive'),¹⁵⁶ in light of Arts. 7, 8 and 47 CFR.¹⁵⁷

Article L. 851-3 of the Code de la sécurité intérieure (Internal Security Code, CSI) require electronic communications operators as well as technical service providers to implement automated data processing practices on their networks, which would detect plausible terrorist threats.¹⁵⁸ The referring Court also explained that national legislation which required providers of electronic communications services to indiscriminately retain traffic and local data, fell within the scope of Art. 15(1) ePrivacy Directive.¹⁵⁹

Case C-512/18 French Data Network and Others

The second French case concerned a challenge by the French Data Network, La Quadrature du Net and the Fédération des fournisseurs d'accès à Internet associatifs which sought to annul the rejection decision in which the Prime Minister failed to reply on their application of repealing Article R. 10-13 of the code des postes et des communications électroniques (Post and Electronic Communications Code, CPCE) and Decree No 2011-219, on the ground that

¹⁵³ French administrative supreme court.

¹⁵⁴ Decrees No 2015-1185, No 2015-1211, No 2015-1639 and No 2016-57.

¹⁵⁵ Directive 2000/31/EC on certain legal aspects on information society services, in particular electronic commerce, in the Internal Market.

¹⁵⁶ Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

¹⁵⁷ *La Quadrature du Net*, para. 56.

¹⁵⁸ *Ibid.* para. 57.

¹⁵⁹ *Ibid.* para. 58.

those legislative texts breached Article 15(1) of the ePrivacy Directive in light of Articles 7, 8 and 11 CFR.¹⁶⁰

The obligation of general and indiscriminate retention of communications data by providers of electronic communications services, laid down in Articles R. 10-13 CPCE allows judicial authority to access data relating to communications before an individual is suspected of a criminal offence. Article 6(11) of loi pour la confiance dans l'économie numérique (Law to promote trust in the digital economy, LCEN) and Decree 2011-219 imposes an obligation to hold and retain only data relating to the creation of content. The referring court considered it not to fall within the scope of the ePrivacy Directive but falls within the scope of the e-Commerce Directive.¹⁶¹ It was also the view of the referring court notices that Article 15(1) and (2) of the e-Commerce Directive does not prohibit in principle on retaining data relating to the creation of content, and therefore it asked if the e-Commerce Directive.¹⁶²

Case C-520/18 Ordre des barreaux francophone and germanophone and Others

In the single Belgian case, actions had been brought by the Ordre des barreaux francophones et Germanophone, the Académie Fiscale ASBL and UA, the Liga voor Mensenrechten ASBL, the Ligue des Sroits de l'Homme ASBL, and VZ, WY and XX before the Cour constitutionnelle,¹⁶³ seeking to annul the Law of 29 May 2016. It was argued that the law infringed Articles 5, 6 to 11, 14, 15, 17 and 18 ECHR, Articles 7, 8, 11 and 47 and Article 52(1) CFR, as well as the principles of legal certainty, proportionality and self-determination in relation to information and Article 5(4) TEU.¹⁶⁴

¹⁶⁰ *La Quadrature du Net*, para. 69.

¹⁶¹ *Ibid.* paras 70-71.

¹⁶² Articles 12, 14 and 15.

¹⁶³ The Constitutional Court of Belgium.

¹⁶⁴ *La Quadrature du Net*, para. 74.

The applicants argued that the Law of 29 May 2016 was not strictly necessary and did not give adequate guarantees of protection. Furthermore, they contended that the personality profiles may be misused by competent authorities since no appropriate level of security and protection of the data exists. The referring court contended that the objective pursued was not only to combat terrorism and child pornography, but also to use data in a wide variety of situations in criminal investigations. Last, the judicial authorities and the intelligence and security services may be given access to retained data.¹⁶⁵

5.2.3 Judgment

The Court stated already in the beginning of the judgment that Article 4(2) TEU does not make the ePrivacy Directive inapplicable, since Article 15(1) expressly mentions the objective of safeguarding national security.¹⁶⁶ Article 1(1) Directive 2002/58 aims to harmonise national provisions so an equivalent level of protection of fundamental rights across the EU exists, in regards to the processing of personal data. However, Article 1(3) excludes State activities in areas such as criminal law, public security, defence and State security.¹⁶⁷ The ePrivacy extends not only to legislative measures which oblige providers of electronic communications services to retain traffic and location data, but also rules that says that providers have to grant the competent national authorities access to the data in question.¹⁶⁸

The pure fact that measure is made to protect national security within the meaning of Article 4(2) TEU, cannot have the consequence that EU law is disapplied. Furthermore, ‘activities’ within the meaning of article 15(1) ePrivacy Directive, cannot be extended to the activities of providers of electronic communications services, only because legislation require them to retain traffic and location data, or require them to grant authorities the access

¹⁶⁵ *La Quadrature du Net*, paras. 75–77.

¹⁶⁶ *Ibid.* para. 87.

¹⁶⁷ *Ibid.* para. 91–92, the Court also referred to Case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:788 para 32.

¹⁶⁸ *La Quadrature du Net*, para. 96.

to that data.¹⁶⁹ They fall within the scope of the ePrivacy Directive since the data is processed by providers of electronic communications services, including the processing operations which are made because of Law of 29 May 2016.¹⁷⁰

It is apparent from the recitals the ePrivacy Directive that the rights set out in Art. 7 and 8 CFR are ensured.¹⁷¹ Nevertheless, Article 15(1) of the ePrivacy Directive permits Member States to make exemptions from the principles laid down in Article 5 ePrivacy Directive, and restrict the rights if they are ‘...*necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.*’¹⁷²

The retention of traffic and location data constitutes itself a derogation from the prohibition in the ePrivacy Directive, and as well, is an interference with the fundamental rights Art. 7 and 8 of the Charter – whether or not the data later has been used.¹⁷³ Legislation which requires the retention of personal data must meet the objective criteria that establishes a connection between the data retained and its pursued objective for retaining that data.¹⁷⁴

Automated analysis of traffic and location data

From CSI, it is clear that automatic analysis of data means screening of all data retained by providers of electronic communications services and must be considered done on the behalf of public authorities and contains general and indiscriminate processing of data. National legislation which allows this type of data processing, interferes with Articles 7 and 8 CFR.¹⁷⁵ This type of interfering is quite serious, as it is general and indiscriminatory and covers

¹⁶⁹ *La Quadrature du Net*, paras. 96–99, see also case-law cited.

¹⁷⁰ *La Quadrature du Net*, para. 101.

¹⁷¹ *Ibid.* para. 106.

¹⁷² *Ibid.* para. 110.

¹⁷³ *Ibid.* para. 115, its referrals & para. 116.

¹⁷⁴ *La Quadrature du Net*, para. 133.

¹⁷⁵ *Ibid.* para. 170 & 173.

the data of users of the electronic communications systems. This is further strengthened by the mere fact that automated analysis may reveal the nature of online information. Last, it applied on users who are not even linked with potential terrorist activities.¹⁷⁶

Legislation allowing this type of interference ‘...cannot be limited to requiring that the authorities’ access to such data should correspond to the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use...’¹⁷⁷ When it comes to serious interferences – general and indiscriminate retention of traffic and location data and automatic analysis – can only be justified in situations when national security is seriously threatened, and that threat is genuine and present or foreseeable. The retention should also be limited to what is strictly necessary. In order to guarantee that the measure itself is limited to what is strictly necessary, it is necessary that the authorising decision is subject for effective review, by either a court or an independent administrative body.¹⁷⁸

Real-time collection of traffic and location data

The CSI allows real-time collection of traffic and location data if a person has previously been linked to a terrorist threat, as well as persons in his or her social circle, if substantial grounds exist for helping the authorities in the case.¹⁷⁹ As with automated analysis of traffic and location data, legislation that allows real-time collection of traffic and location data also infringes with Articles 8 and 9 CFR. Furthermore, these interferences are serious in nature, since national authorities have the possibility to track the movements of the users’ mobile telephones. The interference is also more serious when the real-time collection includes the traffic data.¹⁸⁰

¹⁷⁶ *La Quadrature du Net*, para. 174.

¹⁷⁷ *Ibid.* para. 176.

¹⁷⁸ *Ibid.* paras. 177-179.

¹⁷⁹ *Ibid.* para. 183.

¹⁸⁰ *Ibid.* paras. 185-187.

A decision authorising the real-time collection of traffic and location data must have objective criteria as a ground in national legislation and particularly define the circumstances and conditions when such authorization may be given and only persons with a link to the objective of combating terrorism. Last, the decision must also be subject to a review by a court or an independent administrative body. The real-time collection must be strictly necessary.¹⁸¹

Last, the Court held that the competent national authorities which collect real-time traffic and location data must notify the person surveilled, following national legislation. This shall be done to the extent that the notification will not jeopardise the investigation. The Court stated that the notification is a right given under Art. 7 and 8 of the Charter, but also to have that data rectified or erased as well as avail themselves under Article 47 of the Charter.¹⁸²

5.3 Prokuratuur

5.3.1 Introduction

Prokuratuur is the latest of the three cases and was handed down by the CJEU on March 2nd 2021. In relation to the two former grand chamber cases, the surveillance of the individual in question had committed a minor crime and thus is interesting by the fact from a rule of law perspective. It asks the question whether public authorities can conduct surveillance (even if it is done on already retained data) in cases when national or State security is not threatened.

¹⁸¹ *La Quadrature du Net*, para. 189.

¹⁸² *Ibid.* para. 190, see also references given in the paragraph.

5.3.2 Case facts

The Viru Maakohus¹⁸³ imposed a two-year custodial sentence on H.K. for thefts of goods and cash, using the bank card of another person, and violent acts against persons in the court proceedings concerning her. The value of the stolen goods ranged from EUR 3 to EUR 40 and value of the stolen cash ranged from EUR 5,20 to EUR 2.100. In addition, H.K. the value of the bank card use was EUR 3.941,82.¹⁸⁴ The reports on which the Viru Maakohus had relied upon, were made on basis of data from electronic communications. These data had been obtained by the investigating authority during the pre-trial procedure from a provider of electronic telecommunications services, after following the necessary judicial steps in the Estonian Code of Criminal Procedure.¹⁸⁵

H.K. appealed to the Riigikohus¹⁸⁶ contending that the reports based on the electronic data obtained by the providers of electronic communications were inadmissible, and that the legal provisions of paragraph 111 of the Law on electronic communications breaches Article 15(1) of the ePrivacy Directive in light of Articles 7, 8 and 11 and 52(1) of the Charter. The referring court thus asked if data in Article 15(1) of Directive 2002/58 should be restricted to combating serious crime, regardless of the period in which state authorities have sought access to the data.¹⁸⁷

5.3.3 Judgment

The CJEU stated that access to traffic and location data for the purposes of prevention, investigation, detection and prosecution of criminal offences granted to public authorities, must have been retained in a way that is consistent with Article 15(1) ePrivacy Directive.¹⁸⁸ It reminded of its reason

¹⁸³ The Court of First Instance in Viru, Estonia.

¹⁸⁴ *Prokuratuur*, para. 16.

¹⁸⁵ *Ibid.* para. 17.

¹⁸⁶ Supreme Court of Estonia.

¹⁸⁷ *Prokuratuur*, para. 19-21

¹⁸⁸ *Ibid.* para. 29 (In this para the CJEU referred to *Quadrature du Net* para 167).

in *la Quadrature du Net* that Article 15(1) ePrivacy Directive in light of Articles 7, 8 and 11 and 52(1) CFR forbids legislative measures that allows general and indiscriminate continuing possession of traffic and location data. Public authorities having access to data retained by providers of electronic communications services may only be justified by the public interest objective, for which the specific service providers has retained the data.¹⁸⁹

I.e., Member States may justify the limitation on rights inter alia in Arts 5, 6, and 9 ePrivacy Directive in proportion to the seriousness of the interference entailed by such a limitation as well as in proportion to the public interest. The objective of preventing, investigating, detecting and prosecuting criminal offences, in line with the principle of proportionality does not entail of any criminal offences. Only actions to combat serious crime and measures to prevent threats to public security can justify interferences with Article 7 and 8 CFR. Only non-serious interference with those fundamental rights may be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences such as in the case of *Prokuratuur*.¹⁹⁰

Regarding what constitutes as ‘serious interference’, data that does not ascertain the date, time, duration and recipients of the communications made by an individual, cannot give much information on the private lives of the individual, and cannot therefore be classified as serious.¹⁹¹ On the other hand, access to a set of traffic or location data may allow precise conclusions on private lives of the individuals whose data has been retained. These could include habits of everyday life, permanent or temporary residence, movements and social environments.¹⁹² Under the principle of proportionality, derogations from and limitations on the principle of personal data must be so far as it is only strictly necessary. The national authorities

¹⁸⁹ *Prokuratuur* para. 31, and also *Quadrature du Net* paras. 166 & 168.

¹⁹⁰ *Prokuratuur* para. 33, and also *Quadrature du Net* paras. 131, 140 & 146.

¹⁹¹ *Prokuratuur* para. 34, and also *Quadrature du Net* paras. 157 & 158.

¹⁹² *Prokuratuur* para. 36, and also *Quadrature du Net* para. 117.

must i.e. assess whether the data in question is strictly necessary for the purposes of the investigation in question.¹⁹³

Even access to a limited quantity of traffic or location data or for a short period may provide precise information on the private life of the individual. When the authorisation of access to the data is given by the court or competent independent authority, the assessment of the seriousness of the interference shall be done on the risk of interfering with the private life.¹⁹⁴

Does the evidence contravene EU law?

When deciding if evidence and information should be excluded because it contravenes EU law, regard must be given to the adversarial principle and the right to a fair trial “*entailed by the admissibility of such information and evidence.*”¹⁹⁵ The principle of effectiveness therefore requires national courts to disregard information and evidence gathered in breach of EU law, in the context of criminal proceedings.¹⁹⁶

Conclusively, the Court said that Article 15(1) ePrivacy Directive precludes national legislation that allows public authorities to access traffic or location data that may help the prevention, investigation, detection and prosecution of criminal offences, since the data can be used to draw up precise conclusions of the private life of the individual. The exception would be procedures and proceedings that combat serious crime or prevent serious threats to public security, regardless of the period, quantity, or nature of the data.¹⁹⁷

To satisfy the principle of proportionality when providers of electronic communications services grant authorities access to data, the national legislation allowing the grant must lay down clear and precise rules of the

¹⁹³ *Prokuratuur* para. 38, and also *Quadrature du Net* para 130.

¹⁹⁴ *Ibid.* para 40.

¹⁹⁵ *Prokuratuur* para. 44

¹⁹⁶ *Ibid.* para. 44, and also *Quadrature du Net* para. 226–227.

¹⁹⁷ *Ibid.* para. 45.

scope and application of the measure in question, as well as minimum safeguards. Through this, the risk of abuse decreases.¹⁹⁸

A general access to all retained data, regardless of link with the intended purpose, cannot be limited to what is strictly necessary. Such access to data can only be granted for the purpose of fighting crime, regarding data of individuals who are suspected of planning, committing or having committed a serious crime. In other situations, however, when it concerns national security, defence or public security, access may be granted if the data effectively contribute to combatting those activities.¹⁹⁹

The right to a fair trial

In these circumstances it is also of essentiality that the retained data is subject to prior review by a court or an independent administrative body. This means that this organ which executes the review has all the powers and provide all necessary guarantees as well is able to strike balance between the interests of the investigation and the fundamental rights at hand.²⁰⁰

Furthermore, if the review is carried out by an independent administrative body it must be free from any external influence.²⁰¹ That means that authority must be a third party in relation to the authority which requests access to the data in question. This way, the review can be carried out objectively, impartially and free from external influence. The AG points out in 126 that this authority reviewing, cannot be involved in the criminal investigation in question and has a “neutral stance vis-à-vis the parties to the criminal proceedings.”²⁰² The Court concluded that this was not the case of a public prosecutor’s office who is investigating crime.²⁰³

¹⁹⁸ *Prokuratuur* para. 48.

¹⁹⁹ *Ibid.* para. 50 and also *Quadrature du Net* para. 188.

²⁰⁰ *Prokuratuur* paras. 51-52, and also *Quadrature du Net* para. 189.

²⁰¹ *Prokuratuur* para. 53 and see case-law cited.

²⁰² *Prokuratuur* para. 54.

²⁰³ *Ibid.* para. 55-57.

5.4 The Affair of EncroChat

5.4.1 *Introduction and background*

This fourth part of the third chapter is different from the three previous parts in the way that does not concern a case from the CJEU. One might hope that it eventually will arrive at the CJEU sometime in the near future, but at the moment of writing this thesis, the issue of EncroChat is currently spread around at national courts in the EU.

An EncroChat phone was a phone that was disguised as an Android²⁰⁴ telephone but does not function as a normal one. By pressing a secret sequence of buttons, the telephone opens a software system called EncroChat. Each EncroChat device has its own nickname, and through that way, users become more or less anonymous. The software allows the users send text messages and pictures to other users of EncroChat. The unique function of EncroChat was perhaps not the disguise within the phone, but its ‘brilliant form of end-to-end encryption’. The messages sent was also the deletion of incriminating data.²⁰⁵

In early 2020, officers and prosecutors from France and Netherlands had formed a so-called joint investigation team called Operation Emma, in which the French police believed they would be able to hack into the EncroChat system. An important of the EncroChat system before its hacking was its alleged use, that no one used it for legitimate purposes. In mid-March the same year, the French police had developed a mechanism which would enable them to collect data from EncroChat telephones.²⁰⁶

More detailed, the French police had conceived an update which would be sent to all EncroChat telephones through a server in Roubaix, France. This

²⁰⁴ Android is an operative system used by many different mobile telephones.

²⁰⁵ Smith.

²⁰⁶ Smith.

update would entail a hidden function in all EncroChat telephone, which would allow the gathering of all data in two stages. The first stage would be the historical collection of existing data on every device, *inter alia*, contacts, usernames, and messages. The historical collection would only collect data from one week back, since the application itself was set to burn its data after one week on most of the devices. The second step would entail the daily collection of messages, which would continue to the point that the application was used and undetected. The French Police launched its collection operation April 1st 2020 and continued to mid-June.²⁰⁷

5.4.2 European Investigation Order

In the case of EncroChat, the EIO²⁰⁸ become highly relevant. A European Investigation order may be issued in order to obtain evidence which is already in possession of authorities in the executing Member State.²⁰⁹ The objective of the EIO initiative is to incept a single, efficient and flexible way to obtain evidence located in another Member State for criminal proceedings.²¹⁰

Articles 30 and 31 of the EIO concerns the interception of telecommunications. Article 31 concerns the situation when authorities of one Member State intercepts telecommunications in its state, but the communication address of the subject of the interception is on another Member State, and that Member State does not need to provide technical assistance for the inception. In those cases, the intercepting Member State has a duty to notify the other Member State of the interception. It is argued that

²⁰⁷ Smith.

²⁰⁸ Directive 2014/41/EU regarding the European Investigation Order in criminal matters.

²⁰⁹ Article 1 EIO. 'Executing State' is defined in Article 2(b) as '*...the Member State executing the EIO, in which the investigate measure is to be carried out...*'

²¹⁰ European Data Protection Supervisor 'Opinion on Directive regarding the European Investigation Order in criminal matters' Opinion of the European Data Protection Supervisor para 17.

this notification is not a recognition for an investigation measure, but a reflection of respect of the sovereignty of the other Member State.²¹¹

After the French authorities had intercepted the EncroChat server, authorities from other states issued EIOs, requesting the data obtained from EncroChat devices that were geo-located in their respective states. The data which had been collected by the French were transferred to Europol, categorised on where it the data had been geo-located, and after that transferred to relevant authorities depending on where the data had been collected.²¹² This could be done after the authorities had issued a so-called EIO.²¹³ How did the gathering of personal data relate to EIO and fundamental rights?

5.4.3 The lawfulness of the European Investigation Order

In the preamble to the EIO, it is given that the Directive shall not affect in modifying the obligation to respect fundamental rights in the CFR. The area of security and justice is furthermore based on the mutual confidence and presumption that the fellow Member State complies with fundamental rights. The EIO even specifies that everyone has the right to the protection of personal data concerning them.²¹⁴ The obligation to not breach fundamental rights is necessary according to the EIO:²¹⁵

“...if there are substantial grounds for believing that the execution of an investigative measure indicated in the EIO would result in a breach of a fundamental right of the person concerned and that the executing

²¹¹ José Eduardo Guerra & Christine Janssens ‘Legal and Practical Challenges in the Application of the European Investigation Order’ (2019) Issue 1 EUCRIM pp. 46-53.

²¹² Tom Schofield ‘A Riddle, wrapped in a mystery, inside an enigma’ (5 March 2021) No5 Barristers Chambers <<https://www.no5.com/media/publications/a-riddle-wrapped-in-a-mystery-inside-an-enigma/>> accessed 22 June 2021.

²¹³ See Polisen *Stor europeisk insats mot grovt kriminella* (2 July 2020) Polisen <<https://polisen.se/aktuellt/nyheter/2020/juni/stor-europeisk-insats-mot-grovt-kriminella/>> accessed 22 June 2021.

²¹⁴ EIO, preamble paras. 18-19 & 40.

²¹⁵ EIO, preamble para. 19.

State would disregard its obligations concerning the protection of fundamental rights recognised in the Charter, the execution of the EIO should be refused.”

Also, the European Data Protection Supervisor stated in its opinion²¹⁶ that since personal data will be processed and exchanged by different Member States, the data is protected by fundamental rights according to Article 16 TFEU and Article 8 CFR. Exchange of personal data between Member States are particularly sensitive since personal data will be processed in different jurisdictions where technical frameworks are not the same. Consequently, this will impact the legal certainty – national laws differ from Member State to Member State and might differ from what the subjects are used to. In these cases, greater efforts are required to ensure the compliance with EU legislation on data protection.²¹⁷ It should however be noted that the EDPS recommended that evidence gathered under the EIO should only be for prevention, investigation, detection, and prosecution of crime.²¹⁸

²¹⁶ The opinion was referred to in the preamble of the EIO para. 46.

²¹⁷ European Data Protection Supervisor paras. 20 & 30-31.

²¹⁸ European Data Protection Supervisor paras. 43-44.

6 Substantive Rule of Law: The Protector of Fundamental Rights

6.1 Introduction

As explained in Chapter 3, rule of law has a strong correlation with the protection of fundamental rights. This is because fundamental rights exist to codify the rights the individual has against the state or other powerful entities.²¹⁹ More importantly, substantive rule of law is the ideal of rule and does not distinguish between rule of law and substantive justice. This Chapter will serve as a discussion on how the substantial rule of law protects the fundamental rights.

6.2 Is Rule of Law ensuring fundamental rights?

As written in Chapter 3, substantive rule of law does not see substantive justice as something different from rule of law, but substantive rule of law requires the rule of law to capture and enforce what is morally right. It requires that the rule of law enforces the correct moral rights, and in the end, the best substantive justice.

By looking at the cases, it is prima facie clear that the formal dimension of rule of law exists in all three cases and the EncroChat affair. In *Schrems II* the enormous capabilities of the U.S. authorities under *PRISM* and *UPSTREAM*, were constrained by formal rule of law to hold back the authorities from

²¹⁹ Horizontal nature of CFR.

abusing their power. In order to conduct surveillance, an approval was needed from the Attorney General and the Director of the National Intelligence – following an approval from the FISC – and therefore a clear procedure existed according to the formal dimension of rule of law. Furthermore, the approval from a court or independent body is vital in matters like these. In *La Quadrature du Net* it was clarified by the CJEU that the mere fact that surveillance measures were made to protect national security, was not a valid reason to disapply EU law and thus fundamental rights. One of the constraints in this case was the fact that an automated analysis of traffic and location data needed an authorising decision from a court or independent body. Thus, it was subject for effective review. In *Prokuratuur*, it was clear by the CJEU that even access to a limited quantity of traffic or location data – even for a short period – may provide personal and sensitive information of the individual. In these circumstances, the authorisation must be assessed on the basis of the seriousness of the interference of the private sphere.

What role did then substantive rule of law play? Did it even play a role in protecting the fundamental rights? The fundamental rights to privacy, protection of personal data, and a fair trial and effective remedy are moral rights individuals have. *La Quadrature du Net* concerned both automated analysis of traffic and location data which was made on the behalf of the authorities. This automated processing was furthermore indiscriminate and general and thus, the Court reasoned, the interferences with Articles 7 and 8 of the CFR were serious. The CJEU acknowledged that this could only be justified when a genuine and present or foreseeable threat against national security existed. These constraints on the public authorities are derived from the substantive rule of law. The fundamental rights, the moral rights from the substantive rule of law, exists in order to prevent the authorities to abuse their power.

In *Prokuratuur* the CJEU found that legislation that allows public authorities to access traffic or location data could only be justified when the objective was to prevent serious crime or threats to the public security. Since the crimes

in *Prokuratuur* were neither serious or threatened the public security, the CJEU found that the authorities had abused their powers, effectively interfering with the fundamental rights to privacy and protection of personal data. Even though Articles 5, 6 and 9 of the ePrivacy Directive could be interpreted to allowing the interference in the name of public interest, the CJEU still found a way that upheld the fundamental rights and substantive justice.

However, as seen in all three cases, public authorities – subject to the principle of proportionality – are allowed to make interferences in the name of national security. Fundamental rights could be seriously undermined if no checks existed in these cases, and a legal black hole would appear. As however explained by the CJEU, formal conditions act as safeguards so that public authorities still are constrained. In *La Quadrature du Net* the CJEU explained that the threat had to be genuine and present or foreseeable, and thus prima facie has safeguards.

What if, however, if the safeguards are easy to go around? If it is easy for public authorities to conduct surveillance, e.g., automated analysis of traffic and location data (i.e. general and indiscriminate processing of data) as in *La Quadrature du Net*, or processing of retained data and live processing on the Transatlantic communications cables as in *Schrems II*, in the name of national security, there are signs of a so-called legal grey hole. That would mean that on the mere look on the law, the public authorities would be constrained from conducting these types of surveillance, but easy to circumvent only by justifying the surveillance with national security.

In cases such as these, the substantive rule of law plays a vital role. Since the concept of substantive rule of law means that the individuals also receive the best substantive justice, a court could look at these cases and assess that the public authorities have interfered with the fundamental rights to an unacceptable limit – which the CJEU did in *Prokuratuur*. Hence, it is vital with a court or independent authority that can scrutinise the validity of such

surveillance and make the assessment to what is necessary in a democratic society in the interests of national security and public safety.

However, an important component to this is that individuals have access to remedy and a fair trial. This is why the fundamental rights given in Article 47 of the CFR are necessary for the substantive rule of law. This was also the case of *Schrems II* and *Prokuratuur* where the CJEU found that the safeguards for the surveillance were not acceptable since the national provisions did not provide the right to a fair trial and an access to effective remedy. The impartiality dimension of the rule of law had earlier been developed in *Portuguese Judges* and *LM*, which shows that the CJEU understands that the rights enshrined in Article 47 of the CFR are moral rights the individuals have and concerns the very essence of the substantive rule of law.

In the case with EncroChat, no safeguards existed in regard to the data which was collected by the French. Furthermore, in many national cases in the EU, the data was used as evidence by the Courts. How would then the substantive rule of law ensure the fundamental rights in a case at the CJEU, concerning the EncroChat material?

By taking a substantive rule of law approach in a future case concerning EncroChat material, the CJEU would continue on its reasoning from *Schrems II*, *La Quadrature du Net* and *Prokuratuur*, and enforcing moral rights the individuals are entitled to and deliver substantive justice. As was explained in *La Quadrature du Net*, the automated analysis of traffic and location data, which is general and indiscriminate, can be justified when a genuine and present or foreseeable threat against national security exist – which was not the case of EncroChat. Furthermore, if the French police got the data unlawfully, the very essence of right to privacy would have been breached. It can be said that these constraints are derived from the substantive rule of law.

Interestingly, concerning the EncroChat affair, the authorities did not use the means they had previously used in the three cases. This time, they hacked a

company which questions the very legality of the operation. The fundamental right of protection of personal data concerning individuals was not only expressed in the CFR, but also specified in the EIO. The EIO further explained that if a substantial ground existed for believing that a breach of fundamental rights would happen when an EIO was executed – the execution should be refused.

However, the police did succeed with capturing criminals who were guilty of serious crime – crime that harm the society as a whole. This is an important argument against using only the substantive rule of law approach in future cases.

6.3 Conclusion

The answer to the first research question (How does the substantive rule of law ensure fundamental rights in situations when public authorities conduct surveillance of electronic communications?) is that the substantive rule of law protects fundamental rights to privacy, protection of personal data, and a fair trial and effective remedy by prohibiting the public authorities to abuse the power they have received. The CJEU uses the substantive justice derived from the substantive rule of law in order to ensure the fundamental rights.

The answer to the second research question (Should the CJEU take a substantive rule of law approach in future cases?) is that it probably would be against the good of society if the CJEU not *only* took a substantive rule of law approach in future cases. In the case with EncroChat, it can be argued that it was in the interest of the society that the police breached the fundamental rights derived from the substantive rule of law since so many criminals were detained and convicted.

Bibliography

Primary sources

EU legislation (primary law)

Charter of Fundamental Rights of the European Union [2012] OJ C 326/02

Consolidated Version of The Treaty on European Union [2012] OJ C 326/13

Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47

EU legislation (secondary law)

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

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects on information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L 178/1

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) Text with EEA relevance [2018] OJ L 321/36

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

Commission Decision 2000/520/EC 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 [2000] OJ L 215/7

Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46, as amended by Commission Implementing Decision (EU) 2016/2297 [2016] OJ L 39/5

CJEU

Case C-136/79 *National Panasonic v Commission* ECLI:EU:1980:169

Case C-583/11 P *Inuit Tapiriit Kanatami and Others v Parliament and Council* ECLI:EU:C:2013:625

Case C-64/14 *Associação Sindical dos Juízes Portugueses (Portuguese Judges)* ECLI:EU:C:2018:117

Case C-362/14 *Schrems* ECLI:EU:C:2015:650

Case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:788

Case C-216/18 PPU *Minister for Justice and Equality (Deficiencies in the system of justice) (LM)* ECLI:EU:C:2018:586

Case C-311/18 *Facebook Ireland and Schrems* ECLI:EU:C:2020:559

Case C-511/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791

Case C-746/18 *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)* ECLI:EU:C:2021:152

Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, ECLI:EU:C:2017:592

Opinion of AG Saugmandsgaard Øe *Schrems II* ECLI:EU:C:2019:1145

Other EU documents

Explanations (*) Relating to the Charter of Fundamental Rights [2007] OJ C 303/17

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 [2016] L 207/1

European Data Protection Supervisor 'Opinion on Directive regarding the European Investigation Order in criminal matters' (5 October 2010) Opinion of the European Data Protection Supervisor

ECtHR

Z v. Finland App no 22009/93 (25 February 1997)

Hambardzumyan v. Armenia App no 43478/11 (5 December 2019)

Szabó and Vitsy v. Hungary App no 37138/14 (12 January 2016)

Big Brother Watch and Others v. the United Kingdom Apps nos 58170/13, 62322/14 and 24960/15 (4 September 2013)

Roman Zakharov v. Russia App no 47143/06 (4 December 2015)

U.S. Legislation

Foreign Intelligence Surveillance Act of 1978 § 50 U.S.C.

Secondary sources

United Kingdom

Constitution Committee, Relations Between the Executive, the Judiciary and Parliament (HL 2006-07) ‘Appendix 5: Paper by Professor Paul Craig, The Rule of Law’

Electronic Sources

Gorsky A & Toomey P, ‘Unprecedented and Unlawful: The NSA’s ‘Upstream’ surveillance’ American Civil Liberties Union (26 September 2016) <<https://www.aclu.org/blog/national-security/privacy-and-surveillance/unprecedented-and-unlawful-nsas-upstream>> accessed 3 May 2021

Schofield T, ‘A Riddle, wrapped in a mystery, inside an enigma’ (5 March 2021) No5 Barristers Chambers <<https://www.no5.com/media/publications/a-riddle-wrapped-in-a-mystery-inside-an-enigma/>> accessed 22 June 2021

Encyclopedias & Dictionaries

Cambridge Dictionary ‘Data’ <<https://dictionary.cambridge.org/dictionary/english/data>> accessed 18 April 2021.

The Editors of Encyclopedia Britannica ‘data processing’ *Encyclopedia Britannica* <<https://www.britannica.com/technology/data-processing>> accessed May 10th 2021.

Choi, Naomi 'Rule of law: political philosophy' *Encyclopedia Britannica*
May 15th 2021.

Books

Craig P & de Búrca, G 'EU Law: Text, Cases, and Materials' (7th edn, Oxford University Press 2020)

Craig P 'Formal and Substantive Conceptions of the Rule of Law: an Analytical Framework' in Bellamy, Richard (Ed) *The Rule of Law and the Separation of Powers* (1997) *Public Law* (Routledge 2005)

Dyzenhaus D, 'The Constitution of Law: Legality in a time of emergency' (Cambridge University Press 2006)

Dworkin R, 'A Matter of Principle' (Harvard University Press 1985)

Higgs H, 'Further thoughts on the Information State in England...since 1500' in (eds) Boersma K et al., *Histories of State Surveillance in Europe and Beyond* (Routledge 2014).

Machado H & Frois C, 'Aspiring to modernization: Historical evolution and current trends of state surveillance in Portugal' in (eds) Boersma K et al., *Histories of State Surveillance in Europe and Beyond* (Routledge 2014).

Samatas M, 'A brief history of the anticommunist surveillance in Greece and its lasting impact' in (eds) Boersma K et al., *Histories of State Surveillance in Europe and Beyond* (Routledge 2014).

Svenonius O, Björklund F & Waszkiewicz P 'Surveillance, lustration and the open society: Poland and Eastern Europe' in (eds) Boersma K et al., *Histories of State Surveillance in Europe and Beyond* (Routledge 2014).

Kleineman J, 'Rättsdogmatisk metod' in Maria Nääv & Mauro Zamboni (eds) *Juridisk metodlära* (2nd edn, Studentlitteratur 2018).

Law Journals

Lisa M Austin 'Getting Past Privacy? Surveillance, the Charter, and the Rule of Law' (June 2014) Vol 27 No 3 *Canadian Journal of Law and Society* 27 pp. 381-398.

Austin LM 'Surveillance and the rule of law' (July 2015) Vol 13 No 2 *Surveillance and Society*

Dodds K, 'Gender, Geopolitics, and Geosurveillance in "The Bourne Ultimatum"' (January 2011) Vol 101 No 1 *Geographical Review*, pp. 88-105

Chander A, 'Is Data Localisation a Solution for Schrems II?' (September 2020) Volume 23 Issue 2 *Journal of International Economic Law* pp. 771-784

Fallon Jr RH, "'The Rule of Law" as a Concept in Constitutional Discourse' (January 1997) Vol 97 No 1 *Columbia Law Review* pp. 1-56.

Kuner, C 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (March 2019) Volume 18 Issue 4 *German Law Journal* pp. 881-918.

Lasserre B & Mundt A 'Competition Law and Big Data: The Enforcers' View' (2017) Vol 4 No 1 *Italian Antitrust Review* pp. 87-103.

Maxwell J & Tomlinson J 'Privacy Int'l v. Secretary of State for Foreign & Commonwealth Affairs and La Quadrature du Net v. Premier minister (C.J.E.U)' (June 2021) Volume 60 Issue 3 *International Legal Materials* pp. 464-520.

Steyn J, 'Guantanamo Bay: The Legal Black Hole' (January 2004) Vol 53 No 1 *The International and Comparative Law Quarterly* pp. 1-15

Vincent D, 'The Origins of Public Secrecy in Britain' (1991) Vol 1 Transactions of the Royal Historical Society' pp. 229–248

Vermeule A, 'Our Schmittian Administrative Law' (February 2009) Vol 122 No 4 Harvard Law Review pp. 1095-1149.

Other Journals

Guerra JE & Janssens C, 'Legal and Practical Challenges in the Application of the European Investigation Order' (2019) Issue 1 EUCRIM pp. 46-53.

Media

Cleo Abram (producer) 'How Does the Internet Work? - Glad You Asked S1' (Vox, 8 January 2020) <<https://www.youtube.com/watch?v=TNQsmPf24go>>

Newspapers

Follorou J & Untersinger M, 'Le reseau crypté EncroChat infiltré par les polices européennes : « C'est comme si nous étions à la table des criminels »' *Le Monde* (Paris, 3 July 2020) <https://www.lemonde.fr/international/article/2020/07/03/c-est-comme-si-nous-etions-a-la-table-des-criminels-comment-les-polices-europeennes-ont-penetre-le-reseau-crypte-encrochat_6045024_3210.html> accessed 26 May 2021

Greenwald G & MacAskill E, 'NSA PRISM program taps in to user data of Apple, Google and others' *The Guardian* (London, 7 June 2013) <<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>> accessed 12 May 2021.

Macaskill E & Dance G 'NSA Files: Decoded' *The Guardian* (London: 1 November 2013) <<https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>> accessed 20 May 2021

Palm J ‘Nytt läge efter Encrochat: ”Bruten tystnadskultur”’ *Svenska Dagbladet* (Stockholm, 26 March 2021) <<https://www.svd.se/nytt-lage-efter-encrochat-bruten-tystnadskultur>> accessed 26 May 2021

Smith DJ, ‘The EncroChat Bust: how Police hacked the secret gangster messaging network’ *The Times* (London, 11 April 2021) <<https://www.thetimes.co.uk/article/the-encrochat-bust-how-police-hacked-the-secret-gangster-messaging-network-mjvh3xlxw>> accessed 26 May 2021

Working papers

Laurent P ‘The Rule of law as a Constitutional Principle of the European Union’ (2009) Jean Monnet Working Paper Series 4/2009 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1463242>

Groussot X & Lindholm J, ‘General Principles: Taking Rights Seriously and Waving the Rule-of-Law-stick in the European Union’ (2019) Lund University Legal Research Paper 1/2019 p. 14 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3361668> accessed 20 May 2021.

Smits, JM ‘What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research’ (2015), Maastricht European Private Law Institute Working Paper 2015/06 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644088> accessed 21 May 2021

Hillion C, ‘Overseeing the rule of law in the European Union’ (January 2016) No 1 *European Policy Analysis* Swedish Institute for European Studies <https://www.sieps.se/en/publications/2016/overseeing-the-rule-of-law-in-the-european-union-legal-mandate-and-means-20161epa/Sieps_2016_1_epa?> accessed 17 May 2021