‘It takes one to know one’: analyzing the EncroChat operation in light of article 8(2) ECHR and existing surveillance frameworks.

Master Thesis TILT 2023

L.L.M. Law and Technology

Thesis Supervisor: Lorenzo Dalla Corte

Second reader: Suzanne Nusselder

Author: Clementine Bosland

Date: June 2023

Table of contents

Abstract

This thesis focuses on the implications and difficulties created by the law enforcement operation regarding EncroChat. During this operation the communication and metadata of EncroChat users were intercepted on a large scale by French and Dutch authorities which resulted in a debate surrounding the right to privacy as laid down in article 8 European Convention of Human Rights (ECHR). Primarily, the discussion in this thesis focuses on the question whether the breach of article 8 could be justified based on paragraph 2 of article 8 ECHR. This paragraph lays down the criteria which must be met for the breach to be justified. To add to this debate, this thesis discusses different surveillance frameworks which have been developed through jurisprudence of the European Court of Human Rights (the ECtHR) and the Court of Justice of the European Union (the CJEU). It argues for and against the applicability of the different frameworks also exhibiting the flaws that exist within the current frameworks. This is not meant as a pedantic attitude to the Dutch or European courts discussed but rather a manner to point out that technology might have developed past these frameworks which leaves technology and techniques such as the interception of encrypted data under regulated. Therefore, it is interesting to approach the subject of this thesis while keeping the *zeitgeist* in mind. As the criminal circuit in the Netherlands hardens it is expected for authorities to utilize increased investigatory powers. Still, before these investigatory powers are applied, a satisfactory framework must be present.

Chapter 1: Introduction

Recently, the hacking of encrypted communication companies led to breakthroughs in criminal prosecution, one example being the hack of the company EncroChat.[1] This hack, which involved the compromise of an encrypted communication network used by criminal organizations,[2] caused the interception of a vast amount of data. This resulted in the arrest of roughly 800 people worldwide,[3] and in the prosecution of (major) criminals in the Netherlands, the United Kingdom and France.[4] Government use of digital investigatory powers to collect large amounts of data on seemingly random groups of people to identify individuals who might be of interest to the investigatory authorities may sound like an Orwellian 'Big brother' situation to some,[5] to others they are justifiable police investigations.[6] This thesis explores if recent intercepting operations, such as the EncroChat operation,[7] were in fact 'Big Brother'-like actions, or if they can be justified based on article 8(2) ECHR.[8] Article 8 ECHR entails the right to respect for private and family life, home and correspondence.[9] Paragraph 2 of this article describes under what circumstances a public authority can interfere with this right, namely if the interference is "in accordance with the law, necessary in a democratic society, proportional and for a legitimate

[1] Thomas Lapierre, Heloïse Vigouroux and Julie Zorilla, 'Collection of Evidence by Judicial Authorities within the EU EncroChat Example', (*American Bar Association,* 1st of April 2021*)*, <https://www.americanbar.org/groups/international_law/publications/international_law_news/2021/spring/collection-of-evidence-by-judicial-authorities-within-the-eu-encrochat-example/?q=&wt=json&start=0>, accessed on 4 December 2022.

[2] Europol, 'Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe', 2 July 2020, <https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe>, accessed on 28 September 2022.

[3] Suzanne Flynn, 'The Case of EncroChat and the Presumption of Innocence in EU Law' *(Renforce Blog,* 26th of May 2020*),* <http://blog.renforce.eu/index.php/en/2022/05/26/the-case-of-encrochat-and-the-presumption-of-innocence-in-eu-law-2/> accessed on 10 October 2022.

[4] Bruce Zagaris & Michael Plachta, 'Transnational Organized Crime' (2020), vol. 36 International Enforcement Law Reporter 248,p. 249.

[5] George Orwell, *1984*, (1st ed. Secker & Warburg 1949).

[6] Maša Galič, 'Bulkbevoegdheden en strafrechtelijk onderzoek: wat de jurisprudentie van het EHRM ons kan leren over de normering van grootschalige data-analyse', (2022), vol. 8, Tijdschrift voor Bijzonder Strafrecht en Handhaving 130, p.130.

[7] Vanja Bajovic, 'Evidence from Encrochat and Sky ECC Encrypted Phones' (2022), vol.3, CRIMEN 154, p.179.

[8] Article 8 reads as follows: (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with 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.

[9] Council of Europe, 'Guide on Article 8 of the European Convention on Human Rights', [2022], <https://www.echr.coe.int/documents/guide_art_8_eng.pdf>, accessed on 11 October 2022, p.7.

aim."[10] To address the question of justification based on article 8(2) a legal framework must be utilized. As the test laid down in article 8(2) is in principle a broad proportionality test,[11] the answer to whether the breach is justified depends on the answer to the question if the EncroChat operation is seen as mass surveillance (the automated collection and processing of people's data irrespective of whether those people are liable for surveillance),[12] targeted surveillance ("the surveillance of a specific individual (or individuals) on a case-by-case basis, based on reasonable suspicion (or probable cause")[13] or strategic surveillance (a form of surveillance residing between individual and mass surveillance in regard to the amount of people targeted and the reasonable suspicion present). When the intensity of the surveillance increases, it becomes harder to justify based on article 8(2) ECHR. This is reflected in the balancing test distilled from the CJEU's case law 'Ministerio Fiscal'. Here the CJEU stated that when an interference with the right to data protection is not serious, it can be justified by the objective of investigating 'criminal offenses'[14] When an interference is serious, it can only be justified by "serious criminal offenses."[15] So if the EncroChat operation is considered a serious interference, it should have occurred to combat serious crime. If it's considered a minor interference it can be justified by the aim of combating 'criminal offenses'.

The prompt for the hack was that EncroChat phones were found by French and Dutch police during different criminal investigations.[16] Consequently, the French and Dutch police formed a Joint Investigation Team (JIT).[17] In the first stage of the hack the French police hacked the EncroChat server located in Roubaix.[18] Through this server the French police managed to place interception software, which in literature is used to describe various investigatory powers,[19]

[10] Article 8 (n 8).
[11] Lorenzo Dalla Corte, 'On proportionality in the data protection jurisprudence of the CJEU', (2022), vol. 12, International Data Privacy Law 259, p.262.
[12] Kevin Macnish, 'Mass Surveillance: A Private Affair?' (2020), vol.7, Moral Philosophy and Politics 9, p.10.
[13] Marie-Helen Maras , 'The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'?' (2012), Vol. 40, International Journal of Law, Crime and Justice 65, p.65.
[14] Judgment of 2 October 2018, *Ministerio Fiscal*, (C-207/16), ECLI:EU:C:2018:788, para. 57.
[15] Ibid, para. 56.
[16] Bart Schermer and Jan Jaap Oerlemans, 'De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?'(2022), vol.2, Tijdschrift voor Bijzonder Strafrecht & Handhaving 82, p. 82.
[17] Gerechtshof 's-Hertogenbosch, 27 June 2022, ECLI:NL:GHSHE:2022:2208, under 'De individuele onderzoekswensen'.
[18] Rechtbank Noord-Holland, 21 April 2022,ECLI:NL:RBNHO:2022:3650, para. 3.1.
[19] Carlos Liguori, 'Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate' (2020), vol. 26, Michigan Technology Law Review 317, p.341.

on all EncroChat devices.[20] Then, in the second stage, French investigators gathered incoming data from the first of April until the middle of June 2020.[21] In light of the JIT, the French investigators shared the data with Dutch authorities.[22] The Dutch police copied all the incoming data, via a secure connection, with the smallest delay possible.[23] Mid June 2020, EncroChat became aware of the hack and the interception of data and instructed its users to rid themselves of their phones.[24]

When assessing the EncroChat operation it must be noted that the data that was intercepted contained encrypted data. Encryption transforms ordinary information, or plaintext, into unintelligible ciphertext.[25] The plaintext can only be recovered by persons who are familiar with the algorithm which transformed the plaintext in the first place and an additional piece of information, 'the encryption key'.[26] This might be understood to mean that encryption used by EncroChat was decoded by the authorities.[27] This could be true, however, information regarding how the authorities gained access to the EncroChat data remains undisclosed to the public.[28]

1.1. Problem statement

One of the problems with investigatory operations such as EncroChat is that not only people who are the concern of a criminal investigation get hacked, but also people simply using the communication provider.[29] Additionally, the interception of data from the users of encrypted communication providers happened for extended periods of time and for some subjects without a foreseeable reason.[30] Law enforcement authorities have stated that after finding EncroChat phones in various criminal investigations they were "under the impression that *many, possibly all* EncroChat users were active in the criminal circuit."[31] Still, whether the EncroChat users were

[20] Schermer and Oerlemans,(n 16) 83.
[21] Cerian Griffiths and Adam Jackson, 'Intercepted Communications as Evidence: The Admissibility of Material Obtained from the Encrypted Messaging Service EncroChat', (2022), vol.86, The Journal of Criminal Law 271, p.271.
[22] Schermer and Oerlemans,(n 16) 83.
[23] Rechtbank Rotterdam, 25 June 2021, ECLI:NL:RBROT:2021:6113, para. 3.2.3.
[24] Griffiths and Jackson, (n 21).
[25] Abdelilah Sedeeg, Mohand Mahgoub and Muneer Saeed, 'An Application of the New Integral "Aboodh Transform" in Cryptography', (2016), vol.5, Pure and Applied Mathematics Journal 151, p.151.
[26] Schermer and Oerlemans,(n 16) 82.
[27] Milana Pisarić, 'Encrypted Mobile Phones', (2021) vol.11, Archibald Reiss Days 185, p.188.
[28] Ibid.
[29] Galič, (n 6).
[30] Schermer and Oerlemans, (n 16), 82.
[31] Rechtbank Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1279, para. 3.7. (unofficial translation).

criminal or not, the use of law enforcement powers should occur within the parameters as provided in article 8(2) ECHR. To establish if the operation happened within these parameters, this thesis focuses on whether the operation, and similar operations, can be assessed in current legal and jurisprudential frameworks and if these current frameworks permit the operation considering article 8 ECHR. The described problem is analyzed based on judgments from Dutch courts in light of landmark cases regarding bulk interception such as Big Brother Watch and Centrum för Rättvisa.[32] This analysis is not without limitations; due to the principle of mutual trust, information concerning the *modus operandi* of the authorities remains outside of the scope of Dutch judges, limiting the information available to base the thesis on. Mutual trust entails the high level of trust between member states, which provides the basis to recognize the judicial decisions of other member states as legally valid.[33]

For example, the district court of Midden-Nederland decided that the interception of data could not be reviewed based on the concept of mutual trust.[34] Along with the district court of Midden-Nederland, the district court in Limburg stated that the hack by French police should be perceived as valid due to the principle of mutual trust.[35] In regard to the obtainment by Dutch law enforcement the district court of Limburg stated that the examining magistrate had reviewed the principles of article 8 ECHR in regard to the obtaining of data by Dutch police and found that this would not cause a breach of article 8 ECHR.[36] Just as the courts of Midden-Nederland and Limburg, various courts have not tested the legality of the hack in light of article 8 ECHR because of the principle of mutual trust.[37] In these cases the courts note that in accordance with earlier jurisprudence from the Dutch supreme court,[38] Dutch courts are not at liberty to examine whether the French authorities gathered the evidence in accordance with the law.[39] Dutch courts have to trust that the French authorities have acted lawfully.[40]

---

[32] Big Brother Watch and Others v. The United Kingdom, ECHR 25 May 2021, (*Case 58170/13),* para 521 Centrum för Rättvisa v. Sweden, ECHR, 25 May 2021, (*Case 35252/08*).
[33]Auke Willems, 'Mutual Trust as a Term of Art in EU Criminal Law: Revealing Its Hybrid Character', (2016), vol. 9 European Journal of Legal Studies 211, p.213.
[34] Rechtbank Midden-Nederland, 16 September 2021, ECLI:NL:RBMNE:2021:4480, para.4.1.3.
[35] Rechtbank Limburg, 26 January 2022, ECLI:NL:RBLIM:2022:558, para.3.1.
[36] Ibid, para.3.3.2.3.
[37] For instance: Rechtbank Den Haag,11 March 2021, ECLI:NL:RBDHA:2021:2242; Rechtbank Limburg 26 January 2022 ECLI:NL:RBLIM:2022:571; Rechtbank Amsterdam, 8 July 2021 ECLI:NL:RBAMS:2021:3524
[38] Hoge Raad, 5 October 2010 , ECLI:NL:HR:2010:BL5629.
[39] Rechtbank Amsterdam, 8 July 2021 ECLI:NL:RBAMS:2021:3524, para 1.
[40] Ibid.

1.2. Literature review

This thesis provides the view that recent manners of evidence gathering used by law enforcement authorities might not be justified based on article 8(2) ECHR. To discuss this, the thesis includes an analysis regarding if and why Dutch courts have found the EncroChat operation justified based on article 8(2) ECHR. This analysis consists of case law and academic literature. Both are limited due to the recentness of the EncroChat operation. Still there are noteworthy academic papers present, as well as personal statements of value. For example, senior lawyer and former independent reviewer of terrorism legislation of the UK Lord David Anderson,[41] warned the Crown Prosecutor of England and Wales that there was a substantial risk that phone hacking warrants regarding EncroChat phones would be found unlawful.[42] He stated that the National Crime Agency (NCA) was "seeking to set aside the statutory requirement of an identified and circumscribed criminal enterprise in favor of a wholly general attempt to uncover serious criminality of all kinds."[43] These statements are relevant, as the evidence used in UK courts has been provided by the French and Dutch hack. Therefore, the unlawfulness Lord Anderson talks about is also applicable to the *modus operandi* of Dutch law enforcement authorities.[44] His criticism has not, yet, been repeated by Dutch courts. However, Dutch lawyers have expressed similar concerns. Recently, 133 Dutch lawyers published an open letter directed at the Dutch government in which they stated that the right to privacy is violated by the manner in which EncroChat data have been collected.[45] Some of these lawyers represent suspects in ongoing EncroChat investigations, so it could be argued that these lawyers might be biased towards the methods used by law enforcement authorities. However, some of the undersigned are not involved with the defense of an 'EncroChat suspect' and are still critical towards the methods used by Dutch law enforcement authorities. The letter emphasizes that this method of drawing attention to a problem in criminal law is highly unlikely but necessary because of the high

[41] MPs and Lords; Lord Anderson of Ipswich, <https://members.parliament.uk/member/4705/career> accessed on 28 September 2022.
[42] Bill Goodwin, 'EncroChat: Top lawyer warned CPS of risk that phone hacking warrants could be unlawful' (*ComputerWeekly*, 30th April 2021*)*, <https://www.computerweekly.com/news/252500061/EncroChat-Top-lawyer-warned-CPS-of-risk-that-phone-hacking-warrants-could-be-unlawful>, accessed on 28 September 2022.
[43] Ibid
[44] Europol, (n 2).
[45] Van Boom Advocaten, 'Brandbrief Strafrechtadvocatuur', (*vanboomadvocaten,* 22 October 2022), <https://vanboomadvocaten.nu/brandbrief-strafrechtadvocatuur/>, accessed on 4 December 2022.

likelihood of a breach of, among others, article 8 ECHR that comes with investigatory operations such as EncroChat.[46] So, various legal experts from different professions and nationalities have expressed their concerns regarding the operation.

When analyzing academic literature, the article that closest encapsulates the discussion formed in this thesis is an article written by Georgios Sattigae.[47] He argues that the EncroChat operation must not be considered mass surveillance but rather targeted interception.[48] The idea that EncroChat cannot be considered mass surveillance but rather targeted interception is supported by Dutch case law.[49] Still, the district court of Amsterdam, who finds EncroChat targeted surveillance,[50] bases this conclusion after stating that it is not clear what "bulk data" entails.[51] The court emphasizes that a differentiation must be made between "the more or less defined storage and analysis of particular data, and the indiscriminate storage, retrieval or search of large amounts of data."[52] Still, the court does not provide concrete criteria on which this differentiation can be made.

This is the point where literature can develop as EncroChat cases are approaching the ECtHR and the CJEU.[53] There is no clear consensus on where EncroChat belongs in the surveillance landscape which leaves the classification of the operation to the courts discretion. Consequently, judgments of Dutch courts caused legal experts to question whether fundamental rights can be protected with this method of evidence gathering.[54]

Another limitation regarding the development of literature relevant to this thesis is that the EncroChat operation raises *many* questions beside the question posed in this thesis, for example regarding the right to a fair trial (article 6 ECHR).[55] This means that not all literature regarding EncroChat is truly relevant for this thesis. Moreover, not all literature regarding the right to privacy is perfectly applicable as the operations discussed within this literature differ

[46] Ibid.
[47] Georgios Sagittae , 'On the Lawfulness of the EncroChat and Sky ECC-Operations' (2023), New Journal of European Criminal Law 1, published online ahead of print, available at: <https://journals.sagepub.com/doi/full/10.1177/20322844231159576>, accessed on 22 April 2023.
[48] Ibid, p.5.
[49] Rechtbank Amsterdam, 17 March 2023, ECLI:NL:RBAMS:2022:1243, para. 3.6.
[50] Ibid.
[51] Rechtbank Amsterdam, (n 49).
[52] Rechtbank Amsterdam, (n 49).
[53] Referrals have been made see: Referral of 24 October 2022, (*C-670/22*).
[54] Schermer and Oerlemans,(n 16), p.89.
[55] See: Radina Stoykova, 'Encrochat: The Hacker with a Warrant and Fair Trials?' [2023], Forensic Science International: Digital Investigation 1, p.1.

from the EncroChat operation. A comparison between past operations and the EncroChat operation resulting in an answer on how this line of literature applies to EncroChat has not been made.

Besides a doctrinal discussion, past case law regarding bulk interception reveals that the investigatory power is a controversial one.[56] For instance, in Big Brother Watch the grand chamber of the ECtHR stated that an unjustified violation of article 8 ECHR was present after bulk interception occurred in the UK.[57] Additionally, it is not only bulk interception which is controversial; a review of the history of encryption exhibits an ongoing debate regarding the regulation of encryption and the challenges policy makers face in deciding the optimal timing to impose regulations on encryption.[58] By including a short history of (the absence of) regulation regarding encryption this thesis provides the perspective that the EncroChat operation (and similar operations) are not unique in the difficult position they place judges in. Still, familiarity does not equal desirability; the probable absence of legislation urges for very detailed case law to provide legal certainty which could elongate the already existing queues Dutch judges battle with.[59]

The legislation with which this thesis is concerned is article 8 ECHR, more specifically article 8(2) ECHR and its corresponding jurisprudence by the ECtHR. Additionally, even though the legal framework of this thesis is based on article 8 ECHR, judgments from the CJEU are included, as the CJEU has provided interesting insights on accessing data, for example in La Quadrature du Net, [60] or Digital Rights Ireland.[61]

[56] India Trummer, 'Liberty v. SSHD & SSFCA: You Have the Right to Remain Silent; Anything You Say Will Be Gathered and Retained by the Government' (2020), vol. 28, Tulane Journal of International & Comparative Law 383, p.396.
[57] Big Brother Watch v. UK, ECHR, 25 May 2021, *(58170/13),* para. 427
[58] Bert Jaap Koops and Eleni Kosta, 'Looking for Some Light Through the Lens of 'Cryptowar' History: Policy Options for Law Enforcement Authorities Against 'Going Dark', (2018) vol. 34, Computer Law and Security Review 1, p.3.
[59] Floor Ligtvoet, 'Rechters gaan lange wachttijden rigoureus aanpakken door 'agressieve' werving', (*NOS,* 27 November 2019),
<https://nos.nl/nieuwsuur/artikel/2312320-rechters-gaan-lange-wachttijden-rigoureus-aanpakken-door-agressieve-werving>, accessed on 29 May 2023.
[60] Judgment of 6 October 2020, *La Quadrature du Net and Others*, (C-511/18), ECLI:EU:C:2020:791
[61] Judgment of 8 April 2015, *Digital Rights Ireland*, (C‑293/12 and C‑594/12), ECLI:EU:C:2014:238

1.3. Gap in literature

Through jurisprudential research it became apparent that Dutch district courts are unanimous regarding one aspect of the EncroChat cases; the suspects that have been unveiled through the hack and interception have to be convicted and punished, the right to privacy does not stand in the way of any convictions.[62] For example, the district court Midden-Nederland decided that no breach of article 8 ECHR had occurred when it came to the actions of the Dutch law enforcement authorities.[63] The court argued that a legitimate aim (legitimacy principle derived from article 8(2) ECHR) and a legal basis (legality principle derived from article 8(2) ECHR) were both present and that the manner of obtaining the messages was proportional (proportionality principle).[64] The court affirmed that the interception was necessary based on the suspicion regarding the *suspect's* involvement with organized crime.[65] This is a quite blunt manner of reasoning as the court in essence declares that the entire law enforcement operation was necessary based on the suspicion against *one* individual. No reference was made to the argument provided by the prosecution that the suspicion regarding *EncroChat* justified the interference with the right to privacy.[66]

Along with the district court Midden-Nederland, the district court in Limburg stated that the hack by French police should be perceived as valid due to the principle of mutual trust.[67] Outside of the courts however many legal experts,[68] as well as journalists,[69] state that with the manner of interception conducted during the EncroChat operation, fundamental rights, such as the right to privacy, will not be sufficiently protected. This new point of friction between courts and experts provides an interesting gap in existing research prompting the question if current

[62] For example: Rechtbank Gelderland, 8 December 2021, ECLI:NL:RBGEL:2021:6584;
Rechtbank Midden-Nederland, 17 June 2021, ECLI:NL:RBMNE:2021:2570;
Rechtbank Amsterdam, 8 July 2021, ECLI:NL:RBAMS:2021:3524
[63] Rechtbank Midden-Nederland, (n 34).
[64] Ibid
[65] Rechtbank Midden-Nederland, (n 34).
[66] Rechtbank Midden-Nederland, (n 34).
[67] Rechtbank Limburg, (n 35)
[68] See: Schermer and Oerlemans,(n 16) 82.
[69] Camil Driessen and Jan Meeus 'Unieke hack van EncroChat leidt tot veel lastige juridische vraagstukken', (*NRC* 9 juni 2021),
<https://www.nrc.nl/nieuws/2021/06/09/unieke-hack-van-encrochat-leidt-tot-veel-lastige-juridische-vraagstukken-a4046752?t=1663235372> accessed on 15 September 2022.

legal and jurisprudential frameworks are even appropriate to address recent investigatory operations. These uncertainties resulted in the main research question.

1.4. Research question and outline

For this thesis the main research question is: *have Dutch courts wrongly deviated from earlier mass surveillance frameworks based on article 8(2) ECHR by permitting bulk interception as occurred in the EncroChat operation?*

The sub-questions that can be derived from the main question are the following: How did the EncroChat hack and the interception of EncroChat messages occur from a factual and legal perspective? Which surveillance framework, if any, is fit to assess EncroChat and similar operations? What are the criticisms and implications of the Dutch courts' judgments regarding the EncroChat operation?

The thesis is structured as follows: after the first chapter, which introduced the main problem and the legal background, the second chapter addresses the factual perspective. This chapter describes how the messages got intercepted by the French and Dutch authorities, what legal basis they provided for the hack and the interceptions, and what the initial responses were from legal scholars and lawyers. Hence, the second chapter addresses the question: how did the EncroChat hack and the interception of EncroChat messages occur from a factual and legal perspective? A separate substantial chapter is needed for this analysis of the hack and interception of the messages because it is important to understand the nuances between the different stages of the interception to adequately answer the main research question.

Then, the third chapter includes an analysis of ECtHR and CJEU case law regarding bulk interception and surveillance, and provides arguments for and against the applicability of said case law to the EncroChat operation. This chapter addresses the question: Which surveillance framework, if any, is fit to assess EncroChat and similar operations?

The fourth chapter discusses arguments provided by legal scholars and lawyers. Additionally, this chapter provides notable case law from other European countries. This chapter addresses the question: What are the criticisms and implications of the Dutch courts' judgments regarding the EncroChat operation? A look forward is provided as the EncroChat operation does not exist in a vacuum. The body of case law surrounding the operation is constantly developing

rendering earlier judgments meaningless or meaningful. The fifth and last chapter summarizes and concludes the thesis.

1.5. Methodology and method

To reach a substantial answer to the question and sub-questions posed in this thesis, doctrinal legal research is done. As the thesis aims to assess whether judgments made by Dutch courts are valid and agreeable considering article 8(2) ECHR and earlier European jurisprudence, thorough knowledge of article 8(2) ECHR and the jurisprudential framework is important. This knowledge is gathered through case law by the ECtHR and the CJEU. To review how article 8 ECHR has been interpreted in light of bulk interception through bulk hacking, Dutch case law is mainly utilized as it is the Dutch-French Joint Investigation Team's (JIT) operation this thesis focuses on. Still, as the subject of bulk interception of encrypted telecommunication providers and their users is fairly new, case law of jurisdictions facing the same legal questions is included to add perspective. Furthermore, Dutch newspapers are used to describe the debate occurring in society. Lastly, to review the validity of the judgments made by Dutch courts, blog posts and journal articles written by legal experts are analyzed and utilized to provide arguments for and against the judgments.

Even though a thorough analysis is made, this thesis has various limitations. Firstly, there are still uncertainties regarding the manner of hacking and intercepting.[70] Secondly, while this thesis concerns European law as its framework, it is not feasible to include cases regarding EncroChat from all European countries involved, which is why the scope of this thesis is mostly limited to the Netherlands. Even though the Netherlands is one of the important players in the EncroChat hack, including other European countries would create more holistic research. In this respect there are also limitations to the academic research that can be done on this subject. As EncroChat cases are submitted to courts in various countries, articles are being written by academics of different nationalities in regards to the judgments made in their country. This results in academic literature in languages beyond Dutch and English, which have not been included.

[70] Radina Stoykova, 'Digital Evidence: Unaddressed threats to fairness and the presumption of innocence', (2021), vol. 42 Computer Law and Digital Review 1, p.6.

Chapter 2: What happened?

"*My head's still baffled how they got on all my guys*" one EncroChat user wrote another in an intercepted message.[71] His bewilderment and incomprehension is understandable as the EncroChat hack was the grandest government hack thus far.[72] To provide more clarity on this matter, this chapter answers the first sub-question: *How did the EncroChat hack and the interception of EncroChat messages occur from a factual and legal perspective?*

The aim of this chapter is to demonstrate that the Encrochat hack can be divided into three different stages, namely; the interception software being placed on the server and existing data located on the server and EncroChat devices being copied, incoming and outcoming data being intercepted and lastly the transmission of the data to the Dutch authorities. The difference between the stages is important as the different stages also provide different implications for article 8 ECHR. To provide context for the problems discussed in regard to each stage, a short overview of the discussion surrounding encryption is provided. Furthermore, this chapter aims to explain the reasoning behind the *modus operandi* of the hack. By explaining the reasoning, this chapter lays the foundation for the analysis conducted in chapter three. The difficulty with finding an answer to the first sub-question is that the governments involved in the EncroChat hack refuse to disclose how the hack happened.[73] Luckily, via judgments more information became apparent. This chapter attempts to unite these scattered pieces of information to form a clear and detailed timeline.

2.1. The role of encryption

Before discussing the phases, it is important to note that the EncroChat hack is not the first scenario in which the discussion surrounding government interception in combination with encryption is held.[74] The problem with digitally encrypted communication used by civilians dates back to the 1960s.[75] However not until the 1990s does the discussion surrounding encryption become truly relevant for this thesis. During these years the discussion gravitated towards the

[71] Joseph Cox, 'How Police Secretly Took Over a Global Phone Network for Organized Crime', (*Vice,* 2 July 2020) <https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked>, accessed on 7 February 2023.
[72] Peter Sommer, 'Evidence from hacking: A few tiresome problems', (2022), vol. 40, Forensic Science International: Digital Investigation 1, p.1.
[73] Ibid.
[74] Craig Jarvis, 'Crypto Wars: The Fight for Privacy in the Digital Age', (first ed., CRC Press, 2021).
[75] Ibid, p.63.

problem with legally gaining access to and intercepting encrypted communications.[76] The first public key encryption had just been developed and various governments took legal action to prevent having to find manners to enter the encrypted communication, by illegalizing them.[77] For example the Dutch government drafted a law in 1994 to ban crypto completely except for people who received an official license.[78] While the US government wanted to outlaw encryption that did not allow government access.[79] Another example from the US is the Clipper Chip, developed around 1990. This cryptographic chip would make it possible for law enforcement authorities to decrypt encrypted messages for surveillance measures.[80] These ideas were eventually abandoned.[81]

The problem was, and still is, that it is not clear to manufacturers and governments alike how to design encryption that provides a secure communications system, while still allowing the government access when it is needed.[82] This has resulted in a manifestation of the Collingridge dilemma. The Collingridge dilemma entails that influencing technological developments is possible when the consequences of the technology are not clear yet, yet once these consequences are clear it is difficult or near impossible to change them.[83] The Collingridge dilemma manifests itself with regard to encryption exactly as it is described before. When encryption embarked it was plausible legislation limiting the use of encryption would be created, although it seems that the 1990s were already too late for this kind of legislation.[84] However now, when most companies are using end-to-end encryption,[85] it appears unimaginable to implement legislation, or other forms of regulation, to restrict the use of encryption even if governments are aware of

[76] Koops and Kosta, (n 58) 896.
[77] Koops and Kosta, (n 58) 896.
[78] Koops and Kosta, (n 58) 896.
[79] Koops and Kosta, (n 58) 896.
[80] Sushovan Sircar, The Crypto Wars: Interpreting the Privacy versus National Security Debate from a standards perspective, (M.A. thesis, Georgetown University 2017)
[81] Koops and Kosta, (n 58) 897.
[82] Koops and Kosta, (n 58) 898.
[83] Olya Kurdina and Peter-Paul Verbeek, 'Ethics from Within: Google Glass, the Collingridge Dilemma, and the Mediated Value of Privacy', (2019), vol. 44, Science, Technology, & Human Values 291, p.291
[84] The Dutch legislation which would ban encryption for most people caused public outcry: Koops and Kosta, (n 58) 896.
[85] Nabeel Ahmed, 'What is end-to-end encryption and why are tech companies focusing on it?', (*The Hindu,* 12 December 2022),
<https://www.thehindu.com/sci-tech/technology/what-is-end-to-end-encryption-and-why-are-tech-companies-focusing-on-it/article66251153.ece#:~:text=End%2Dto%2Dend%20encryption%20is%20used%20to%20secure%20communications.,end%2Dto%2Dend%20encryption.> accessed on 8 March 2023.

the (negative) implications encryption has. The technology is too far ingrained in society and therefore impervious to restrictions.

The fact that legislation has not managed to keep pace with developments in encryption, whether that is due to the pace of the creation of legislation or because of the disempowerment governments experience regarding encryption, fuels the idea that the answer to the question posed in this thesis will be formed in jurisprudence. As jurisprudence regarding EncroChat is still developing, legal uncertainty for governments, and users of encrypted communication providers alike, is present.

2.2. EncroChat Timeline

EncroChat devices were modified mobile phones, the camera and GPS were removed, which enabled secret and encrypted messaging and voice calls.[86] EncroChat promised its users full anonymity and provided its own encrypted operating system.[87] In 2017 the French Gendarmerie noticed that EncroChat devices were regularly found during investigations on criminal organizations.[88] During the same period, the Dutch police started an investigation called 26Lemont.[89] The concern of this investigation was to investigate EncroChat's complicity to money laundering, participating in a criminal organization and complicity to the crimes committed by its users.[90] So, before joining forces, both the French police and the Dutch police already conducted criminal investigations regarding EncroChat.[91] In April 2020, the Dutch and French authorities decided to work together in the form of a Joint Investigation Team (JIT) with the participation of Europol.[92] On the first of April the French Gendarmerie started intercepting and retaining the messages sent by Encrochat users.[93] The vagueness surrounding this operation is reflected in the variation in dates provided as the end date of the operation. In one judgment of the district court of Oost-Brabant the 20th of June is stated to be the end date,[94] while in another

[86] European Parliament, 'EncroChat's path to Europe's highest courts' EP(2022), 739.268, <https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)739268> accessed on 7 March 2023
[87] Pisarić, (n 27), p.188.
[88] Paul Reedy, 'Interpol review of digital evidence for 2019–2022', (2023), vol.6, Forensic Science International: Digital Investigation 1, p.2.
[89] Rechtbank Oost-Brabant, 2 February 2022, ECLI:NL:RBOBR:2022:312, para. 1.1.
[90] Ibid
[91] Rechtbank Oost-Brabant, (n 89).
[92] Europol (n 2).
[93] Rechtbank Oost-Brabant, (n 89).
[94] Rechtbank Oost-Brabant, (n 89).

judgment by the district court of Amsterdam the 14th of June is said to be the end date,[95] on the other hand Europol stated that the end date was the 13th of June.[96] The district court of Noord-Holland stated 26th of June as the end date, adding almost two weeks to the operation in regard to other Dutch courts.[97] All in all it can be concluded that the operation lasted from the beginning of April to somewhere mid-June.

During this period the French authorities collected messages, information on contacts, notes written on the EncroChat phones and metadata from the users.[98] Metadata are 'data about data'.[99] This means that data should not be seen as raw data without context, for example, if someone sends a message, the time at which the message was sent also provides information. The time is not the 'content' data but still provides information; the person who sent the message was awake and online at that time. So if data should be seen as potential information, [100] metadata will be potential information describing potential information.[101] In the case of EncroChat this means for instance IP addresses. An IP address tells the observer of the data from where the message was sent, therefore the IP address is potential information about other potential information. The defense argued on multiple occasions that by also collecting metadata, such as location data,[102] law enforcement authorities created a fairly complete picture of EncroChat users' lives.[103]

Besides the *live* interception, the French authorities made four copies of the EncroChat infrastructure collecting even more metadata.[104] So two types of data can be differentiated: data copied from the EncroChat server; server data, and data directly intercepted from the EncroChat telephones; telephone data.[105] Both contained content data, such as messages, as well as metadata. This thesis focuses on both telephone data and server data, however, as discourse regarding EncroChat focusses mainly on 'telephone data' this thesis naturally gravitates towards 'telephone data' as well.

---

[95] Rechtbank Amsterdam, 21 November 2022, ECLI:NL:RBAMS:2022:6875, para. 5.1.2.
[96] Europol, (n 2).
[97] Rechtbank Noord-Holland, 23 July 2021, ECLI:NL:RBNHO:2021:6213, para. 1.5.
[98] Rechtbank Oost-Brabant, (n 89).
[99] Jeffrey Pommerantz, *Metadata* (MIT Press, 2015), p.19.
[100] Ibid, p.22.
[101] Pommerantz, (n 99), p.22
[102] Rechtbank Amsterdam, (n 31) 3.2.
[103] See for instance: Rechtbank Den-Haag 19 July 2022, ECLI:NL:RBDHA:2022:7423, para.4.2.2.
[104] Rechtbank Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1280, para.3.6.
[105] Ibid, para.3.2.

2.2.1. Interception software

As mentioned before, the precise way the French authorities collected the data remains unclear as it is treated as a French state secret.[106] However, a general description of the operation can be provided. Supposedly, the JIT obtained a copy of the EncroChat server and a few EncroChat devices, this way they were able to understand the encryption of the devices.[107] Then, the French authorities developed a 'computer interception device' that was to be placed on all telephones via an update sent from the server.[108] This device was able to redirect all the outgoing and incoming data from EncroChat devices to the French server and to change the passwords and disable other security measures available on the devices.[109] The interception software was placed on the devices as part of an update.[110] This software initially only made copies of the data that was saved on the devices.[111] The data saved on the devices included messages, IMEI numbers (unique serial numbers used to identify devices),[112] usernames, passwords, saved messages, saved images, location data and saved notes to the French authorities.[113] This is defined as phase 1 of the operation.[114]

Then in phase 2 the software intercepted outgoing and incoming messages.[115] These messages were intercepted while they were readable, thus not yet encrypted.[116] This means that the messages were intercepted before they were sent and thus encrypted, or after they had been decrypted on the device of the receiver.[117] Lastly, phase 3 of the operation consists of Dutch authorities processing the received data.[118] So in short, the *interception* consists of two stages. In the first stage historic data was collected from the device.[119] Then, during the second stage, messages were gathered from the devices on an ongoing basis.[120] The third, and last, phase of the

[106] Rechtbank Amsterdam, (n 95).
[107] Stoykova, (n 50).
[108] Stoykova, (n 50).
[109] Stoykova, (n 50).
[110] Stoykova, (n 50).
[111] A & Ors, R. v Regina, The Royal Court of Justice London, 5 February 2021, para.12.
[112] Mayank Sahni, 'Detecting and Automated reporting of change in IMEI number', (2014), vol.3, International Journal of Advancements in Research & Technology 186, p.186.
[113] Rechtbank Amsterdam, (n 104) 3.2.
[114] Rechtbank Limburg, 26 January 2022, ECLI:NL:RBLIM:2022:571, para.3.3.2.4.
[115] Rechtbank Amsterdam, (n 39) 'Wat houdt de Encrochat-hack in?'
[116] The Royal Court of Justice London, (n 111) para.14.
[117] Ibid.
[118] Rechtbank Limburg, (n 35) 3.3.2.4.
[119] The Royal Court of Justice London, (n 111) para.14.
[120] Ibid.

operation does not relate to the interception but only to the processing by the Dutch authorities. It's important to note the difference between the various phases of this operation as the different phases have attracted different implications for article 8 ECHR.[121] This is reflected in the ECtHR's judgment in Big Brother Watch.[122] Here, the ECtHR describes bulk interception as "a gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses."[123]

2.2.2. Phase 1 and its problems

In EncroChat procedures defense attorneys have stated that the interception of EncroChat messages caused an unjustified interference of article 8 ECHR.[124] To prove this point a multitude of requests was posed to various courts, requests such as access to all intercepted server data including the underlying authorizations.[125] In regard to this first stage it seems that these requests are made to gather the evidence to prove the absence of a valid legal basis in French law for the operation as well as a disproportionate manner of approaching the operation. As mentioned previously, phase 1 consists of obtaining the *saved* data, so the server data. This was done, according to the authorities, by the French investigatory authorities.[126] So there must be a valid basis in French law. The response to these requests from Dutch courts in regard to this phase is that the principle of mutual trust prevents them from judging the legality of the operation and therefore the defense does not have a right to the requested documents.[127] The general rebuttal from the defense is that the principle of mutual trust should not apply as Dutch authorities provided a large technical input, therefore the operation cannot be seen as a solely French operation but also a Dutch operation.[128] This would mean that the principle of mutual trust is not applicable.[129] This statement was refuted by, among others, the district court of Gelderland,[130] and the district court of Amsterdam,[131] by stating that even though Dutch authorities developed

[121] Rechtbank Limburg, (n 35) 3.3.2.4.
[122] Big Brother Watch (n 57).
[123] Big Brother Watch (n 57) 324.
[124] Rechtbank Limburg, 20 June 2023, ECLI:NL:RBLIM:2023:3624, para. 3.3.
[125] Rechtbank Amsterdam, 18 December 2020, ECLI:NL:RBAMS:2020:6443, para. 2.
[126] Rechtbank Limburg, (n 35) 3.3.2.1.
[127] Rechtbank Limburg, (n 35) 3.3.2.1.
[128] Rechtbank Amsterdam, 21 November 2022, ECLI:NL:RBAMS:2022:6814, para. 5.1.4.
[129] Rechtbank Gelderland, 20 December 2022, ECLI:NL:RBGEL:2022:7425, para. 2a.2
[130] Ibid
[131] Rechtbank Amsterdam, (n 128)

the technique that made it possible to decrypt the messages and the technique that allowed them to copy the server without the server shutting down, this does not make the operation a Dutch operation.[132] The principle of mutual trust remains applicable.

2.2.3. Phase 2 and its problems

Phase 2 entails the interception of *live* messages, so the telephone data, from the French authorities and the transmission of those messages to the Dutch authorities.[133] This was done with the assistance of Europol.[134] For phase 2 Dutch courts have also stated that due to the principle of mutual trust they are not able to judge the legality of this transmission.[135] In one case the defense stated that in line with Big Brother Watch v. the UK the acts of a member state who receives data from another member state must be reviewed under European Union Law.[136] The district court in Limburg did not follow this line of reasoning as it stated that Big Brother Watch v. the UK was only applicable to the sharing of data between a member state and a non-member state.[137] In this case the sharing and receiving took place between two member states. As France is already obliged to adhere to the duties and obligations stemming from the ECHR there is no need to check if the rights of the suspect have been protected sufficiently.[138] The court does not clarify on what part of the Big Brother v. UK case law this argument is based.

2.2.4. Phase 3 and its problems

In phase 3 of the operation the messages were processed by Dutch authorities in light of operation 26Lemont.[139] For this phase Dutch courts were unable to dismiss the arguments made by the defense based on the mutual trust principle, as this part of the operation was done solely by Dutch authorities.[140]

[132] Rechtbank Gelderland, (n 129).
[133] Rechtbank Amsterdam, (n 104) 3.2.
[134] Open letter of concern, from Fair Trials Organisation and others to the European Commission and the European Parliament (*Fair Trials,* 18 February 2022), <https://www.fairtrials.org/app/uploads/2022/02/EnroChat_LetterofConcern.pdf> accessed on 20 February 2023.
[135] Rechtbank Limburg, (n 35) 3.3.2.1.
[136] Ibid, para. 3.3.2.4.
[137] Ibid
[138] Ibid
[139] Ibid
[140] Ibid

In light of this phase the case Big Brother Watch v. the UK was, once again, mentioned by the defense.[141] The defense stated that the obtaining of the messages was in breach of article 8 ECHR and did not meet the safeguards created in the Big Brother Watch v. the UK case.[142] The court dismissed this argument by explaining that the EncroChat case and the operation discussed in Big Brother v the UK were not each other's equivalent. It stated that bulk interception entails untargeted interception of data of large undefined groups,[143] which, according to the court, did happen in Big Brother Watch but not in the EncroChat operation.[144] This is a very succinct description of bulk interception when compared to the definition provided by the ECtHR which describes bulk interception as a "gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses"[145]

Based on the definition of bulk interception provided by the district court of Gelderland, it can be argued that bulk interception did not occur in regard to the EncroChat case as precise targets were present. Namely the EncroChat server and its users. At the time of the operation, the company EncroChat was suspected of partaking in criminal offenses. EncroChat users were suspected of using the EncroChat phones for criminal purposes because of the features the phones had.[146] It may appear strange to utilize having a certain phone as a reason to suspect somebody of a crime, even if the phones are often found on crime sites. However, it appears that technology has developed too quickly, without regulation following at the same pace. Therefore, existing legislation has to be "stretched out" to become applicable to new technologies. In light of the idea that technology develops at a higher pace than legislation, adhering to "broad" interpretation of legislation to be able to regulate new technologies is practical. Still, too broad of an interpretation can cause problems regarding the legal certainty.[147]

2.3. Interim conclusion

This chapter forms the foundation for the next two chapters in which, among others, the jurisprudence referenced by the defense, prosecution and courts will be analyzed. What this

[141] Rechtbank Gelderland, (n 129) 'Toepasselijkheid EU-recht en EVRM'.
[142] Rechtbank Gelderland, (n 129) 'Toepasselijkheid EU-recht en EVRM'. referenced safeguards found in: Big Brother Watch (n 57) 36.
[143] Rechtbank Gelderland, (n 129) 2a.6.
[144] Ibid.
[145] Big Brother Watch, (n 57) 325.
[146] Rechtbank Gelderland, (n 129) 'Toepasselijkheid EU-recht en EVRM'.
[147] Anna Butenko and Pierre Larouche, 'Regulation for Innovativeness or Regulation of Innovation?' (2015), vol. 7 Law, Innovation and Technology 52, pp.66-67.

chapter aims to demonstrate is the uncertainty regarding the way the operation took place, the timeline of the operation and the involved parties of the operation. Besides highlighting the uncertainty, this chapter provides an insight into the EncroChat operation and its phases. The importance of the distinction between these phases cannot be stressed enough. The phases that have been differentiated will be discussed separately in following chapters to enhance the clarity of the thesis.

Furthermore, this chapter reveals the presence of the Collingridge Dilemma.[148] What this dilemma suggests is that legislation is unable to keep pace with technological developments. Therefore, it seems desirable that a framework is developed in an alternative to legislation, such as through jurisprudence. Whether such a framework is currently present is discussed in the following chapters. Still, the unclarity regarding the applicability of existing legislation urges courts, both domestic and European, to provide critical and detailed judgments to enhance legal certainty.

To conclude, as the operation is a fairly recent one, the discourse surrounding it is still developing. This means that new information regarding the interception tool, the legal implications, or the entire operation could become public. This uncertainty regarding the disclosure of new information and its legal implications steers this thesis away from an analysis of possible outcomes and towards the analysis of existing frameworks.

[148] First described in: David Collingridge, The Social Control of Technology, Pinter, London (1980).

Chapter 3: Worrying precedent or logical interpretation?

"In the EU legal framework, it is recognised that the fundamental rights of all people, including suspects and accused persons, must be upheld and protected. We are very concerned that the current handling of the EncroChat issue threatens the Rule of Law and fundamental rights protected by EU law. That, if it is allowed to pass unchecked, sets a worrying precedent."[149] These words are derived from an open letter which is undersigned by lawyers from the Netherlands, Norway, Belgium, France, Germany, Sweden, and the United Kingdom.[150] In this letter the lawyers express their concern in regard to the current handling of EncroChat cases. A similar open letter was published and signed by 133 Dutch lawyers.[151] This chapter explores whether the mentioned concern is justified or if the current state of Dutch case law is in line with earlier CJEU and ECHR jurisprudence regarding bulk interception. Therefore, it answers sub-question two: Which surveillance framework, if any, is fit to assess EncroChat and similar operations?

This chapter presents the legal framework in which bulk interception has been assessed in the past and draws parallels between past cases and EncroChat cases. Based on this analysis a conclusion is drawn whether Dutch courts should adhere to the precedent provided by the ECtHR and CJEU case law or are justified in deviating from the verdicts of the ECtHR and the CJEU.

3.2. Surveillance case law

To determine if the EncroChat operation causes an unjustified interference of article 8 ECHR, it is necessary to review within which judicial framework this operation must be assessed. Therefore, this section includes jurisprudence regarding mass surveillance, strategic surveillance, and targeted surveillance. Through analyzing jurisprudence regarding the different methods of surveillance it can be concluded which framework is applicable to EncroChat, if any.

One form of surveillance is mass surveillance. Mass surveillance can be defined as "the automated collection and processing of people's data irrespective of whether those people are liable for surveillance."[152] In the past the ECtHR has stated that for mass surveillance to be legal

[149] Fair Trials Organisation, (n 134).
[150] Ibid.
[151] Van Boom Advocaten, (n 45).
[152] Macnish, (n 12).

it must be accompanied by legal safeguards, providing respect for citizens' Convention rights, which includes article 8 ECHR.[153] Especially, since collected data contain an increasing number of metadata.[154] Increased metadata collection, means law enforcement authorities know more than just the content of a message, the location and time of sending the message are also known. This provides a more complete image of someone's life. So, mass surveillance has the potential to cause an unjustified breach of article 8 ECHR but this can be rectified by adequate legal standards.[155]

One prominent case on mass surveillance is *Centrum för Rättvisa* .[156] In this case the ECtHR came to the conclusion that Sweden's law regarding the bulk interception of electronic signals for foreign intelligence purposes violated the right to privacy under Article 8 of the ECHR.[157] An unjustified breach of article 8 ECHR was present due to three shortcomings, namely: "the absence of a clear rule on destroying intercepted material which does not contain personal data; the absence of a requirement in the Signals Intelligence Act or other relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration is given to the privacy interests of individuals; and the absence of an effective *ex post facto* review."[158] In this judgment the ECtHR focuses on the adequacy of the Swedish legal system as a whole instead of a breach of article 8 ECHR regarding identified individuals. The ECtHR found that "clear and detailed rules"[159] on the interception of telecommunications and internet communications are essential, especially given the continually evolving sophistication of relevant technology.[160]

When reviewing other judgments regarding mass surveillance it appears that the ECtHR handles mass surveillance cases by addressing the capability of the legal system providing sufficient safeguards rather than addressing the individual breach in light of article 8(2) ECHR.

---

[153] Szabo and Vissy v. Hungary, 12 January 2016, CJEU, *(37138/14)*, para. 68.
[154] Ibid.
[155] Repeated in Zakharov v. Russia, ECHR, 4 December 2015, *(47143/06)*, para.232
[156] Centrum för Rättvisa v. Sweden, ECHR, 25 May 2021, (*35252/08*)
[157] Statewatch, 'Insufficient safeguards in bulk signals-intelligence gathering risked arbitrariness and abuse', (*Statewatch* | 26 May 2021)
<https://www.statewatch.org/news/2021/may/echr-bulk-communications-data-interception-by-uk-and-swedish-spy-agencies-violated-right-to-privacy/>, accessed on 23 March 2023.
[158] Centrum för Rättvisa, (n 156) 369.
[159] Ibid, para. 247.
[160] Ibid.

For instance, in Big Brother Watch and Others v. The United Kingdom,[161] the ECtHR found that the UK's mass surveillance law was in breach of article 8 ECHR.[162] The Grand Chamber explained that legislation allowing bulk interception does not have to cause an unjustified breach of article 8 ECHR provided that the legislation is surrounded by end-to-end safeguards minimizing the risk of abuse of bulk interception and assessing the necessity and proportionality of the interception, which was not the case in the UK.[163]

Based on the Big Brother Watch judgment, Georgios Sagittae argues that the EncroChat operation is not a form of bulk interception and therefore not a form of mass surveillance.[164] Based on Big Brother Watch, Sagittae gathers that for bulk interception to be present communications of a large number of people who are not the target of authorities must be intercepted, the interception must be directed at international communications and the purpose must be to monitor the communications of persons outside the State's territorial jurisdiction.[165] This is a narrow interpretation of the considerations of the ECtHR. The ECtHR states that bulk interception is "*generally* directed at international communications", and that "while the communications of the surveilling State might not be excluded the purpose of bulk interception in *many cases* is to monitor the communications of persons outside the State's territorial jurisdiction."[166] The ECtHR more so reiterates what is the current state of bulk interception methods, it does not state that this is the only form in which bulk communication can appear, therefore naming the attributes mentioned before 'characteristics' not 'requirements'.[167]

This is also found in the consideration of the ECtHR where it states that bulk interception *typically* follows a certain process, namely: "the interception and initial retention of communications and [traffic data], the application of specific selectors to the retained communications and [traffic data], the examination of selected communications data and [traffic data] by analysts, the subsequent retention of data and use of the "final product", including the sharing of data with third parties."[168] This description of different stages aligns well with the stages distilled in the EncroChat operation set out in chapter two. Still, if discrepancies occur

[161] Big Brother Watch (n 57).
[162] Ibid para 427.
[163] Ibid paras. 350 and 427.
[164] Sagittae, (n 47), p.5.
[165] Ibid p.6.
[166] Big Brother Watch (n 57) 344.
[167] Ibid para. 354.
[168] Ibid para. 325

between the stages distilled in Big Brother Watch and the EncroChat operation this still does not have to mean that the operation cannot be considered bulk interception, as the ECtHR states that not all bulk interception operations necessarily follow the same order.[169] Consequently, the EncroChat operation can be interpreted as bulk interception and can therefore be assessed as mass surveillance. Legislation enabling mass surveillance can be deemed unlawful by the ECtHR, but this does not have to be the case if the process of mass surveillance is surrounded by "end-to-end safeguards.[170] These safeguards are explained later on in this chapter.

Another form of surveillance is targeted surveillance. Targeted surveillance can be defined as "the surveillance of a specific individual (or individuals) on a case-by-case basis, based on reasonable suspicion (or probable cause)."[171] The largest distinction between targeted and mass surveillance is the presence or absence of a *reasonable suspicion* regarding an *identified person*.[172] The ECtHR found that bulk interception is in its essence untargeted.[173] Therefore, the requirements of a reasonable suspicion regarding an individual, necessary for targeted interception, could not be upheld.[174]

Based on the conclusion that the EncroChat operation does constitute bulk interception, which follows from the requirements set out in Big Brother Watch, and bulk interception is in its essence untargeted, the EncroChat operation cannot be considered targeted interception regarding the *users.* In contrast, there was a reasonable suspicion present regarding the leaders and the company itself, the data intercepted regarding them can be considered targeted.

Sagittae partially argues the same in his recent article.[175] He argues that because suspicions towards the company EncroChat and its leading "figures" were present, this indicates a targeted interception.[176] Additionally, he states that earlier interceptions of smaller crypto communication providers prove that crypto phones were popular among criminals committing

[169] Ibid.
[170] Ibid, para. 350.
[171] Maras, (n 13).
[172] Big Brother Watch (n 57) 317.
[173] Ibid.
[174] Claudia Aradau and Emma Mc Cluskey, 'Making Digital Surveillance Unacceptable? Security, Democracy, and the Political Sociology of Disputes', (2022), vol.16, International Political Sociology 1, p.12.
[175] Sagittae (n 47), p.6.
[176] Ibid.

serious crimes which presents a suspicion against individuals and companies providing crypto communication.[177]

Based on these findings he considers the requirement of reasonable suspicion to be fulfilled. This is an understandable conclusion in regard to the providers and its leading figures as the question whether a reasonable suspicion is present is answered by analyzing if there are factual indications for suspecting *that person* of planning, committing or having committed criminal acts.[178] Still, as it is not only the company EncroChat and its leading figures who have been prosecuted based on the intercepted data, stating that the EncroChat operation was a targeted one does not seem to be a satisfactory answer.

Lastly, there is a third form of surveillance that might be applicable namely, strategic surveillance. Strategic surveillance which, confusingly, is sometimes used to describe mass surveillance,[179] can also be understood as a form of surveillance residing between individual and mass surveillance in regard to the amount of people targeted. Strategic surveillance is discussed by the ECtHR in Liberty v UK.[180] Here the ECtHR distills 5 stages in which the interception took place, most importantly the ECtHR notes that *"a warrant would be issued, specifying an external communications link or links to be physically intercepted. Such warrants covered very broad classes of communications, for example, "all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe". All communications falling within the specified category would be physically intercepted."*[181] So strategic surveillance entails the interception of data from groups of people who have been targeted based on a common denominator, the stance taken in this thesis is that it is not desirable for EncroChat to be considered strategic surveillance. If the appearance that a lot of criminals use a provider is appreciated as a fulfilling denominator to intercept all communication and metadata of this server this could pave the way for interception of communication from popular apps such as SnapChat and Instagram as they are used frequently to deal drugs.[182] This comparison is not without flaws, EncroChat is not comparable to SnapChat and Instagram regarding size or

[177] Sagittae (n 47), p.6.
[178] Zakharov (n 156) 260.
[179] Jonida Milaj and Jeanne Bonnici, 'Unwitting subjects of surveillance and the presumption of innocence', (2014), vol.30, Computer Law and Security Review 419, p.423.
[180] Liberty v. UK, ECHR, 1 July 2008, (*58243/00)*
[181] Ibid, para. 43
[182] Leah Moyle et. al., '#Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs', (2019), vol.63, International Journal of Drug Policy 101, p.105.

popularity.[183] Still, encrypted communications providers are legal, and can be used for other aims than criminal endeavors.[184] For online surveillance mass surveillance, and strategic surveillance are difficult to distinguish. This is due to the fact that strategic interception lends itself to physical situations rather than online. Strategic surveillance in physical situations could entail police observation of a beauty parlor which it suspects to be a front for money laundering. The people observed are not identified and could be random. However the significant difference between this physical surveillance and online surveillance is that when targeting civilians in the physical world, police only see a snapshot of their day; the moment they spend in the beauty salon. While, when using EncroChat as the common denominator police receive far more than a snapshot; intercepting millions of live messages[185] in addition to stored communications data,[186] and metadata.[187] Due to this difference it is particularly undesirable to subsume EncroChat under strategic surveillance.

In this chapter the stance is taken that the legal frameworks of targeted and mass surveillance should be combined to provide a legal framework in which operations such as EncroChat can be reviewed. A reflection of this combination can be found in Big Brother Watch,[188] the ECtHR states that bulk interception is not necessarily used to target individuals however it *can* be used for this purpose.[189] However not in the sense that a specified individual is present but more so that individuals are selected based on a common feature,[190] for EncroChat this could be the type of phone used. As explained before: EncroChat as a common denominator is too broad to render it strategic surveillance.

What this would entail is that when interception takes place due to a reasonable suspicion against an identified individual, the presence or absence of end-to-end safeguards would not need to be analyzed by courts as this entails targeted surveillance. When data of large groups of not-yet identified individuals is intercepted and used in prosecution the presence of end-to-end

[183] Apps like Instagram and Snapchat are considered a necessity in everyday life: Tae Rang Choi and Yongjung Sun 'Instagram versus Snapchat: Self-expression and privacy concern on social media', (2018), vol.35, Telematics and Informatics 2289, p.2289.
[184] Griffiths and Jackson, (n 21).
[185] Furkan Gözükara, 'Challenges and possible severe legal consequences of application users identification from CNG-Logs', (2021), vol.39, Forensic Science International: Digital Investigation 1, p.16.
[186] Rechtbank Amsterdam, (n 104) 3.2.
[187] Rechtbank Oost-Brabant, (n 89) 1.1.
[188] Big Brother Watch (n 57) 346.
[189] Ibid.
[190] Ibid.

safeguards should be analyzed by courts. This model could also be applicable to other situations such as online child abuse and cyber-attacks.[191]

3.3. The ECtHR's case law on surveillance

In practice this would mean that the ECtHRs would first have to assess whether a reasonable suspicion against EncroChat and its leading figures was present. Then, for the plethora of data that was also intercepted the ECtHR could adhere to its current framework regarding bulk interception. Currently, the process of bulk interception must be surrounded by "end-to-end safeguards."[192]

For member states to ensure that their legislation provides "end-to-end safeguards", the requirements developed in Weber and Saravia v. Germany should be included in national legislation.[193] These requirements are: "the nature of the offenses which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; 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 the tapes destroyed."[194]

In Big Brother Watch the ECtHR added two extra requirements, namely: "the procedures and modalities for supervision by an independent authority of compliance with the above safeguards, and its powers to address non-compliance; the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance."[195]

These criteria should not be interpreted as replacements of the criteria of article 8(2) ECHR, they should be used to ensure the compliance with article 8(2) ECHR, more precisely the 'in accordance with the law' requirement.[196] These requirements leave a margin of appreciation for member states to develop an interception regime.[197] This is in line with earlier jurisprudence

[191] Aradau and Mc Cluskey, (n 174), p.13.
[192] Centrum för Rättvisa (n 156) 264.
[193] Weber and Saravia v. Germany, ECHR, 29 June 2006, (*Case 54934/00*), para. 95.
[194] Ibid.
[195] Big Brother Watch, (n 57) 361.
[196] Bart van der Sloot, 'Big Brother Watch and Others v. the United Kingdom & Centrum för Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?' (2021), vol. 7, European Data Protection Law Review 319, p.323.
[197] Ibid.

of the ECtHR where it does not focus on the fact that data about large numbers of people are gathered in the absence of the suspicion of a crime and even underlines the need for secrecy regarding the manner of interception.[198]

In case of EncroChat the criterium which has in particular not been, adequately, fulfilled is one of the two criteria added in Big Brother Watch; the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

3.3.1. Ex post facto review

In Big Brother Watch the ECtHR stated that the two new requirements, including the *ex post facto review*, would be "fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime"[199] The ECtHR does not provide a description of what this review exactly entails. However, it finds that due to the presence of the Investigatory Powers Tribunal in the UK, the requirement had been fulfilled. This tribunal provided the opportunity for anyone to make a complaint, whether specific or in general, regarding the regime. After which the tribunal was able to "examine both the "above the waterline" and "below the waterline" arrangements, in order to assess the Convention compliance of the regime."[200] With "below the waterline" the ECtHR means the "internal arrangements regulating the conduct and practice of the intelligence services."[201] So documents that are treated as confidential would be made known to the tribunal. At this time, a similar procedure is not present in the Netherlands. Of course, courts are independent authorities, however Dutch courts do not have access to French 'below the waterline' documents.

Based on the stance taken that EncroChat should be assessed within the mass surveillance framework, in conjunction with Big Brother Watch , the absence of an *ex post facto* review means end-to-end safeguards were not present. Therefore, based on ECtHR case law, the 'in accordance with the law' requirement has not been fulfilled which renders an unjustified breach of article 8 ECHR.

[198] Van der Sloot, (n 196).
[199] Big Brother Watch, (n 57) 350.
[200] Ibid, para. 512.
[201] Ibid, para. 33.

3.4. The CJEU's case law on surveillance

Still, the ECtHR's case law is not the only relevant body of case law. The interpretation of the ECtHR is partially based on the analysis that is done by the CJEU in its jurisprudence. For instance, in Digital Rights Ireland,[202] which is concerned with the legitimacy of the EU Data Retention Directive,[203] which mandated EU-wide data retention requirements.[204] Data retention entails the "general and indiscriminate retention of communications metadata from all users regardless of prior suspicion."[205] The CJEU examined the directive on a similar assessment as previously conducted by the ECtHR. Namely, the CJEU does not state any 'victim requirements' that must be met,[206] but rather assesses the directive as a whole. This means that for the case to be admissible, the applicant does not need to have been inconvenienced personally.[207] In its assessment of the legislation the CJEU considers, among other things, whose data is retained and their possible threat to public security, if objective criteria are present which determine the limits of access and offenses that may justify an interference with the right to privacy and data protection.[208]

What must be noted when analyzing a complex investigatory process such as EncroChat in context of jurisprudence such as Digital Rights Ireland, is that Digital Rights Ireland (and other similar cases such as Tele2 and Watson)[209] were concerned with "classic retention of data" on a general and indiscriminate basis for law enforcement and national security purposes.[210] Whereas the EncroChat operation consisted of the interception, transmission *and* retention of data. Therefore, it is also worth discussing cases where a range of investigatory activities occurred, such as La Quadrature du Net,[211] and Privacy International.[212] These cases were

[202] *Digital Rights Ireland*, (n 61).
[203] Paul de Hert and Gianclaudio Malgieri, 'Article 8 ECHR Compliant and Foreseeable Surveillance: The ECTHR's Expanded Legality Requirement Copied by the CJEU. A Discussion of European Surveillance Case Law', (2020), Vol. 6, Brussels Privacy Hub 1, p.27.
[204] Alena Birrer, Danya He, Natascha Just, 'The state is watching you—A cross-national comparison of data retention in Europe', (2023), vol. 47, Telecommunications Policy 1, p.2.
[205] Ibid.
[206] de Hert and Malgieri, (n 23) 30.
[207] Ibid
[208] *Digital Rights Ireland*, (n 61). 54.
[209] Judgment of 21 December 2016, *Tele2 Sverige and Watson*, (C‑203/15 and C‑698/15), ECLI:EU:C:2016:970.
[210] Sarah Eskens, 'The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature du Net and others and Privacy International', (2022), Vol. 8, European Data Protection Law Review 143, p.143.
[211] *La Quadrature du Net and Others*, (n 60).
[212] Judgment of 6 October 2020, *Privacy International*, (C-623/17), ECLI:EU:C:2020:790.

involved with a range of investigative activities, namely, data retention and transmission and automated data analysis both on general and indiscriminate basis (mass surveillance) and of a targeted nature.[213] As argued before, EncroChat could also be considered a combination of investigatory powers namely mass and targeted surveillance.

When considering combating serious crime as a basis for data retention the CJEU states that the retention of traffic and location data is permissible in light of *targeted* retention.[214] Provided that it is limited to "[certain] categories of data, the persons concerned, the means of communication affected and the retention period adopted."[215] In regard to non-targeted (mass) retention, the CJEU states that criminal offenses cannot have the effect of justifying interference that is as serious as that the retention of data of large groups of people,[216] without there being "at least an indirect link between the data of the persons concerned and the objective pursued."[217] Such a link entails that any relationship must be present between the data which must be retained and a threat to public security.[218] The retention must be limited to "(i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute through their data being retained, to fighting crime."[219] So, based on Tele2 and La Quadrature du Net, fighting serious crime can be a basis for the general retention of *traffic and location* data but only if there is an (indirect) link. For this indirect link to be present the idea that retaining someone's data could help fight serious crime is enough.

In regards to *communication* data the CJEU provides a similar test to the test of the ECtHR. The CJEU states that "legislation that establishes a general body of rules for the retention of communications data is in breach of the rights guaranteed in article 7 (...) of the Charter,[220] unless that legislation is complemented by a body of rules for access to the data, defined by national law, which provides sufficient safeguards to protect those rights."[221] With

[213] Eskens, (n 210) 143.
[214] *La Quadrature du Net and Others,* (n 60) para. 147.
[215] Ibid.
[216] Ibid, para 145.
[217] Ibid.
[218] *Tele2 Sverige and Watson*, (n 209) 106.
[219] Ibid.
[220] Article 7 of the Charter is the equivalent of article 8 of the Convention: Judgment of 5 October 2010, *J. McB v. L. E.*, (C-400/10), ECLI:EU:C:2010:582, para. 53.
[221] *Tele2 Sverige and Watson*, (n 209) 53.

safeguards the CJEU suggests "clear and precise rules providing for access to and use of retained data and in so far as access to that data is not made dependent on prior review by a court or an administrative body."[222] These safeguards are similar to the ECtHR safeguards, however no *ex post facto* review is ordered.

Most recent in the line of jurisprudence of the CJEU regarding data retention, the ECtHR adjudicated the Prokuratuur case.[223] Prokuratuur is concerned with investigating authorities obtaining pre-trial personal data on the charged individual from a provider of electronic communications.[224] In this case the CJEU stated that article 15(1) of the ePrivacy Directive,[225] precludes national legislation that allows public authorities to access traffic or location data on a general and indiscriminate basis in light of combating criminal activities.[226] Furthermore, the CJEU stated that general access to all retained data, regardless of whether there is any link with intended purpose, cannot be regarded as being limited to what is strictly necessary.[227] The national legislation concerned with access must be based on *objective* criteria in order to define the circumstances and conditions under which the competent national authorities can be granted access to the data in question.[228] Based on this, the rule can be distilled that in regard to the goal 'fighting crime' only the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime can be accessed by the competent authorities, unless national security is in danger.[229]

Based on La Quadrature du Net and Privacy International it can be concluded that EU law does not contain a legal basis for the general and indiscriminate retention of traffic and location data to combat crime, unless there is at least an indirect link.[230] This criterion is

[222] Ibid.
[223] Judgment of 2 March 2021, *Prokuratuur*, (C-746/18*)*, ECLI:EU:C:2021:152.
[224] Ibid, paras. 16-17.
[225] Article 15 of the ePrivacy directive reads as follows: "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system."
[226] *Prokuratuur*, (n 223) 30.
[227] Ibid, para. 50.
[228] Ibid.
[229] Ibid.
[230] Eskens, (n 210) 149.

intensified in Prokuratuur where the CJEU stresses that only the data of "suspects" may be accessed and only based on *objective* criteria.[231]

The Prokuratuur judgment was adjudicated after the first EncroChat judgments and stipulates that the CJEU does not find indications of criminal behavior sufficient for access to the retained data. Objective criteria must be present in *legislation* so not based on case law. At this time these criteria are not present in Dutch legislation.[232]

3.1. The Dutch Supreme Court

On the 13th of June the Supreme Court of the Netherlands provided its first judgment regarding EncroChat.[233] The Supreme Court judged in line with lower Dutch courts in the sense that it stated that due to the principle of mutual trust the Dutch judge is not at liberty to assess whether an unjustified breach of article 8 ECHR occurred.[234] This judgment was not surprising as, in June 2022,[235] the Dutch Supreme Court stated that evidence gathered via a similar hack, that of the company Ennetcom, is permissible.[236] Furthermore, the Supreme Court stated that Big Brother Watch and Centrum för Rättvisa do not have the effect that the public prosecutor is always obligated to seek a warrant from the magistrate judge when conducting bulk interception.[237] As Big Brother Watch and Centrum för Rättvisa do not concern a criminal investigation regarding encrypted communication providers.[238] However, in light of the Supreme Court judgment regarding EncroChat,[239] Attorney General Paridaens wrote a conclusion in which she stated that the fact that the Big Brother Watch and Centrum för Rättvisa judgments pertain to interception of communications by secret services does not interfere with the applicability of the framework set out in these judgments to criminal law cases.[240]

Besides Attorney General Paridaens', non binding, opinion, the general consensus among Dutch courts has been that because of the principle of mutual trust, it is not up to them to

[231] *Prokuratuur*, (n 223) 50.
[232] Gerechtshof Den Haag, 12 May 2023, ECLI:NL:GHDHA:2023:903, para. 4.
[233] Hoge Raad, 13 June 2023, ECLI:NL:HR:2023:913.
[234] Ibid, paras. 6.5.2.-6.5.3.
[235] More precisely, 28 June 2022.
[236] Hoge Raad, 28 June 2022, ECLI:NL:HR:2022:900.
[237] Hoge Raad, (n 233) 6.24.2 and 6.24.4.
[238] Ibid., 6.24.4.
[239] Hoge Raad, (n 233).
[240] Attorney-General for the Dutch Supreme Court, 9 May 2023, ECLI:NL:PHR:2023:477, para. 5.7.3.

judge whether article 8 ECHR was unjustifiably breached during the EncroChat hack.[241] This means that Dutch courts will not order the public prosecutors to disclose the manner of hacking and intercepting the data.[242]

3.5. Interim conclusion

Based on this chapter the following analysis could be made by Dutch courts. For the targeted surveillance directed at the company EncroChat and its leading figures, the courts should assess whether a reasonable suspicion regarding an identified individual is present. Then, for phase 1 and 2, the obtaining of the *saved and live data* by French investigatory powers,[243] and the transmission of that data to and access of that data by Dutch authorities, the courts assess whether the French legislative framework contains enough safeguards as set out in Weber and Big Brother Watch to offer adequate and effective protection from abuse of surveillance. Currently, an examination of the French framework is still absent because of the previously mentioned principle of mutual trust. The two requirements developed in Big Brother Watch[244] attempt to create *ex post* clarity in situations where legal certainty is not an option. Therefore, these requirements offer an alternative to the existing line of jurisprudence in which much is left unanswered based on the principle of mutual trust. Especially the *ex post facto* review offers options for both the right to privacy to be protected while simultaneously combating serious crime.

In theory, an analysis of phase 3 should be less complex as it contains the processing of the data by Dutch authorities, so the principle of mutual trust does not apply. Therefore, courts could assess whether the Dutch legislative framework is in line with the safeguards developed just as done in, among others, Big Brother Watch. However. as mentioned in chapter 2, Dutch courts dismissed this argument by explaining that the EncroChat case and the operation discussed in Big Brother v the UK were not each other's equivalent.[245]

Besides the jurisprudence of the ECtHR, the retention of the data by the Dutch authorities could also be assessed in light of the CJEU legislation. While Dutch courts have in the past stated that the La Quadrature du Net case is not applicable to the EncroChat hack as this case

[241] See for instance; Rechtbank Rotterdam, 21 February 2023, ECLI:NL:RBROT:2023:1316, para.3.2.2.
[242] Ibid.
[243] Rechtbank Limburg, (n 35) 3.3.2.4.
[244] Big Brother Watch (n 57) 361.
[245] Hoge Raad, (n 233) 6.24.4.

concerned the processing of data by communication provider services, not law enforcement authorities,[246] the court of appeal Den Haag recently rendered both La Quadrature du Net and Prokuratuur applicable.[247] The court of appeal stated that the obligation to request written permission from a magistrate judge before retrieving traffic and location data follows from these two cases.[248] Still, the court of appeal did not tie consequences to the absence of the written permission due to the fact that these requirements were not widely known at the time of the EncroChat operation.[249]

To conclude, as EncroChat legislation develops it is important to critically evaluate existing guidelines provided through case law. As the right to privacy is a fundamental right, which must be harbored, it can be fruitful for courts to attempt to circumvent the principle of mutual trust by testing the requirements laid down in Weber and Big Brother Watch. Courts would not have to assess whether the French authorities acted lawfully in their EncroChat investigation but merely if the French law provides sufficient safeguards to facilitate such an operation. This is possible as countries are not obliged to consistently recognise the legislations of other member states if confidence in the effectiveness of the legal system of the respective Member State is lacking or absent.[250]

When conducting this assessment courts would have to come to the conclusion that the requirement of *ex post facto* review has not been fulfilled in Dutch or French law in regard to the EncroChat operation.

[246] Gerechtshof 's-Hertogenbosch, 25 April 2022, ECLI:NL:GHSHE:2022:1387, under 'Richtlijn 2002/58'
[247] Gerechtshof Den Haag, (n 232) 4.
[248] Ibid.
[249] Ibid.
[250] Nathan Cambien, 'Mutual Recognition and Mutual Trust in the Internal Market', (2017), vol.2, European Papers 1, p.9.

Chapter 4: Security trumps privacy?

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."[251] This quote from Edward Snowden, an employee of an American consultancy firm specializing in security employed by the Central Intelligence Agency (CIA), who proved that the American National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) conducted widespread covert mass surveillance of the public,[252] captures the importance of the question posed in this thesis. Additionally, this quote can be interpreted in different perspectives, providing the idea that the privacy versus security debate does not only occur in mass surveillance situations.

Therefore, this chapter discusses the criticism and different viewpoints provided through foreign case law. Additionally, it includes a legal analysis of the arguments provided by Dutch courts in chapter two in light of the framework set out in chapter three. By doing so this chapter addresses sub-question three: *What are the criticisms and implications of the Dutch courts' interpretation of the EncroChat operation?*

4.1. Interpretations throughout Europe

From the previous chapter it can be concluded that the ECtHR and the CJEU are attempting to find a balance between the right to privacy and harboring security. Repeatedly, the courts state that the methods of mass surveillance are not acceptable (protecting the right to privacy), but then provide some margin of appreciation by stating criteria that allow the use of mass surveillance techniques.[253] In comparison to foreign judges, Dutch courts have diminished the opportunity to analyze whether this margin of appreciation was properly interpreted by law enforcement authorities. This was also one of the points of criticism in the Fair Trials letter of concern, the letter states that there is a likelihood that fundamental rights were infringed during this procedure, and that an adequate review by an independent judicial authority is still absent

[251] Alan Rusbridger, Ewen MacAskill and Janine Gibson, 'Edward Snowden: a right to privacy is the same as freedom of speech – video interview',(*The Guardian,* 22 May 2015) <https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video>, accessed on 2 May 2023.
[252] Jens Branum and Jonathan Charteris-Black, 'The Edward Snowden affair: A corpus study of the British press', (2015), Vol 9(2), Discourse and Communication 199, pp.199-200
[253] See for instance: Judgment of 2 March 2021, *Prokuratuur*, (C‑746/18), ECLI:EU:C:2021:152, para 50.

regarding EncroChat.[254] As set out in chapter two, Dutch courts most often refer to the principle of mutual trust in regard to phase 1 and 2. When addressing this the court of Limburg simply states "based on the principle of legitimate expectations, the court must trust that the interception in France took place on an adequate legal basis and in accordance with Article 8 ECHR."[255] The court's task in the present case is limited to ensuring that the manner in which the results of this foreign investigation are used in the criminal case does not violate the right to a fair trial, as referred to in Article 6(1) of the ECHR."[256] The court does not refer to any of the options presented in European case law.

The same cannot be said for various foreign judges. In a recent judgment by the Italian Supreme Court in regard to the SkyEEC hack,[257] SkyEEC and EncroChat hack can be considered legally similar,[258] the Italian Court of Cassation found that the evidence gathered through the hack cannot be used if the involved authorities do not disclose their manner of obtaining the evidence.[259] The Italian Supreme Court does not disregard the principle of mutual trust however with this judgment it underlines the undesirability of convicting people based on incomplete information.

The verdict of the Italian Supreme Court is also relevant for the assessment of the justifiability of the breach of article 8 ECHR, as more information on the manner in which the authorities gathered the evidence could provide for more substantial arguments regarding whether or not the breach of article 8 ECHR was justified. In this manner Dutch courts could adhere to the balancing test distilled from the CJEU's case law 'Ministerio Fiscal'. Here the CJEU stated that when an interference with the right to data protection is not serious, it can be justified by the objective of investigating 'criminal offenses'[260] While serious interferences can only be justified in light of the investigation of serious crime.[261] A proportionality test in essence. This balancing test is difficult to do based on incomplete information.

---

[254] Fair Trials Organisation, (n 134).
[255] Rechtbank Limburg (n 124) (unofficial translation).
[256] Ibid.
[257] Corte di Cassazione, 15 July 2022, Cass, 32915/22, unofficial translation found at: <https://canestrinilex.com/en/readings/due-process-requires-transparency-of-evidence-gathering-in-sky-ecc-proceeding-cass-3291522/>, accessed on 6 March 2023.
[258] Rechtbank Gelderland, 20 December 2022, ECLI:NL:RBGEL:2022:7440, para.3a.1.
[259] Corte di Cassazione, (n 257).
[260] *Ministerio Fiscal*, (n 14) 57.
[261] Ibid, para.56.

Besides Italian courts, German courts have also provided notable case law. Unlike other German courts the Regional Court of Berlin has suspended a judgment in order to pose questions to the CJEU.[262] The Berlin court included questions regarding the proportionality and necessity of the legal basis used in Germany to receive the EncroChat data.[263] The Berlin court also stated that the lack of transparency regarding the *modus operandi* might result in a breach of European law which could render the evidence inadmissible.[264] This is not the first time that the Berlin court has judged contrary to the Higher Regional Court and the Federal Court of Justice in Germany, in a 2021 judgment the Berlin Regional Court ruled that evidence obtained from a hack must be deemed inadmissible because there was no suspicion of a crime before the hack.[265]

This outcome is what many lawyers throughout Europe have sought to achieve and was partially repeated in Dutch jurisprudence, still without consequences.[266] However, the chance of the ECHR, or the CJEU for that matter, to reject the admissibility of EncroChat evidence based on the rights of an *individual* being breached is slim, as the ECHR and the CJEU have in the past adressed bulk interception cases by assessing the entire legal system as opposed to focussing on the individual case present.[267]

4.2. Alternative case law

As mentioned before, phases 1 and 2 are largely left undiscussed in Dutch jurisprudence due to the principle of mutual trust. Additionally, it has also been explained that many (criminal) lawyers are of the opinion that the right to privacy has been breached due to the EncroChat operation.[268] Yet, criticism can also be based on case law which is not related to surveillance or EncroChat. Besides desirability it is worth thinking about how sustainable it is to obstruct an effective practice of the defense rights by adhering to the principle of mutual trust.[269]

---

[262] Referral of 24 October 2022, (*C-670/22*).
[263] Thomas Wahl, 'EncroChat Turns into a Case for the CJEU', (2022), vol.3 Eurcim 197*,* p.198.
[264] Ibid.
[265] Ibid.
[266] The court of Amsterdam stated that the interception was initially used in regard to the suspicion towards EncroChat and then later used for its users: Rechtbank Amsterdam, 16 July 2021, ECLI:NL:RBAMS:2021:3707, under '*bepalende invloed'*
[267] See for instance Big Brother Watch and Centrum för Rättvisa.
[268] See Dutch letter of concern: Van Boom Advocaten, (n 45) and EU letter of concern: Fair Trials Organisation, (n 134).
[269] Stijn Adams, 'Vertrouwen is goed maar controle is beter', (2021), vol.47, Delikt & Delinkwent 958, p.961.

In 2000 the ECtHR stated that the principle of mutual trust can be set aside when there are strong implications that the gathered evidence (in this case data) was obtained unlawfully.[270] An indication could be the idea that norms based on international conventions were abandoned.[271] The judge can decide this *ex officio* based on the court documents or because the defense provides concrete indications that justify further investigation.[272]

Just before the judgment of the ECtHR, the Dutch Supreme Court also passed a judgment discussing the principle of mutual trust.[273] In this case the pseudo-purchase of XTC in Germany which targeted Dutch individuals looking for XTC suppliers was discussed.[274] In this case the Dutch Supreme Court stated that, the idea that the principle of mutual trust entails that the decision making process and the actions of foreign authorities cannot be reviewed by the Dutch courts in light of for instance the proportionality and subsidiarity principles or the "Tallon-criterium"[275] *cannot* be seen as a factual statement.[276] The Tallon-criterium entails that a suspect may not be brought to commit acts other than those to which his intent was already previously directed.[277] The decision of the Supreme Court is in line with the reasoning of the court of appeal in this case which stated that the judge should be able to test the acceptability of the "tool" used and the diligence with which it was used.[278]

Besides this possibility of addressing the actions of foreign authorities in light of certain principles it is noteworthy that if EncroChat had been a purely national investigation there is a significant chance that an analysis of the lawfulness had occurred.[279] This creates a situation in which law enforcement authorities are able to circumvent obligations they would have to adhere to in a national procedure by framing operations as international operations. This concern is reflected in the *2018* judgment regarding Big Brother Watch "(...) states could use intelligence

[270] Echeverri Rodriguez vs. the Netherlands, ECHR, 27 June 2000, ECLI:NL:XX:2001:AE0193, point 4 of annotation by Schalken.
[271] Ibid, point 2 of annotation by Schalken.
[272] Echeverri Rodriguez (n 270).
[273] Hoge Raad, 8 February 2000, ECLI:NL:HR:2000:ZD1780.
[274] Jan Koers, 'Nederland als verzoekende staat bij de wederzijdse rechtshulp in strafzaken. Achtergronden, grenzen en mogelijkheden', (Final published in 2001, Wolf Legal Publishers), p.486.
[275] To provoke someone to commit a crime they were not planning on committing, see: Rob ter Haar and Gert Meijer, 'Tallon-criterium (uitlokking)', (2011), vol.3, Praktijkwijzer Strafrecht.
[276] Hoge Raad, (n 273) 3.3.
[277] Karel Harms, 'Positieve Uitlokking van Ethisch Hacken: Een Onderzoek naar Responsible-Disclosure Beleid' (2017), vol. 46, Netherlands Journal of Legal Philosophy 196, p.205.
[278] Koers, (n 274).
[279] Adams, (n 269) 967.

sharing to circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations, a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorized in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques."[280]

When assessing the current line of jurisprudence regarding EncroChat it can be concluded that Dutch courts adhere to a broad interpretation of the principle of mutual trust.[281] For instance, the court Zeeland-West-Brabant simply stated that it does not belong to the task of the Dutch judge to assess if the investigation was executed in line with foreign law.[282] Still, this is not the only option. As demonstrated before, the Dutch judge does have the power to assess if the investigation is in line with various (international) principles if there are strong implications that the gathered evidence was obtained illegally.[283] Additionally, the judge could adhere to the framework set out in chapter 3.

4.3. Shift in case law

As mentioned in chapter 1, the case law surrounding EncroChat is still developing. One point that illustrates this is that several Dutch courts have stated that the obtaining of data of unidentified users of EncroChat happened without authorization from the examining magistrate, although this was required in view of the Prokuratuur judgment.[284] Various courts consider that: "the Prokuratuur judgment applies here, and the requested mast data[285] should not, in retrospect, have been requested by a public prosecutor without prior independent review by a judicial authority or an independent administrative entity."[286] Consequently, the courts found a violation of Union Law to be present.[287] The district courts of Amsterdam and the Hague both address this problem but do not tie any consequences to the actions of the prosecution because the courts find

[280] Big Brother Watch, (n 57) 423.
[281] Adams, (n 269) 975.
[282] Rechtbank Zeeland-West-Brabant, 31 March 2021, ECLI:NL:RBZWB:2021:1556, r.o.3.3.3.
[283] Echeverri Rodriguez (n 270).
[284] Rechtbank Amsterdam, 21 November 2022, ECLI:NL:RBAMS:2022:6803, para. 5.2.3. In conjunction with *Prokuratuur*, (n 223) 52-54.
[285] Form of metadata.
[286] Rechtbank Den Haag, 21 October 2022, ECLI:NL:RBDHA:2022:11585 para.4.3. and Rechtbank Den Haag, 12 July 2022, ECLI:NL:RBDHA:2022:6757, para.8.3. (unofficial translation).
[287] Ibid.

that it is plausible that the magistrate judge, had he been approached with a request to review the claims beforehand, would have given permission for them to be made.[288] This seems to be strongly contradicting the requirements discussed before, especially the 'the procedure to be followed for examining the people liable to have their telephones tapped'[289] and 'the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance.'[290] It seems that in EncroChat cases these requirements have not been taken into consideration or at the least have been interpreted very broadly and judges are left to decide whether this is a desirable manner of operating.[291]As Prokuratuur was adjudicated in 2021, after the EncroChat operation, it is not strange that these requirements were not taken into account. However, what these considerations regarding the applicability of Prokuratuur do illustrate is the fact that the current state of jurisprudence is not cast in stone. A shift from a European court to a slightly more privacy protective system can influence Dutch courts to do the same.

Such change can also be distilled from the recent initiative of the Swedish Prime Minister at the 'informal meeting of justice and home affairs' in January 2023 where he proposed a High Level Expert Group to be formed.[292] This group would focus on the access to data by law enforcement authorities.[293] As a reaction the French authorities actually mention the EncroChat operation as an example of the crucial role access to data play in fighting organized crime.[294] Still, the French authorities agree that such a group should be formed to tackle the difficulties regarding " (...) the complexity of jurisdictional competences to deal with phenomena, or the need to have a clear legal framework for the conservation of connection data and to preserve the effectiveness of investigation tools."[295]

---

[288] Ibid.
[289] Weber and Saravia, (n 193) 95.
[290] Big Brother Watch, (n 57) 361.
[291] Stoykova, (n 70), p.7
[292] Council of the European Union, Proposal to establish a High-Level Expert Group on Access to Data, [2023], 5601/23, p.1, <https://www.statewatch.org/media/3854/eu-council-presidency-hleg-access-to-data-5601-23.pdf>, accessed on 27 June 2023.
[293] Ibid.
[294] Council of the European Union, 'Proposal to establish a High-Level Expert Group on Access to Data - Compilation of replies by delegations', [2023], 5601/23, p.14, <https://data.consilium.europa.eu/doc/document/ST-7184-2023-REV-1/en/pdf>, accessed on 27 June 2023.
[295] Ibid.

4.4. Interim conclusion

At this time Dutch courts have primarily used the principle of mutual trust as a reason not to address questions regarding EncroChat. What this chapter aims to do is provide a broader perspective on the manner in which courts can handle situations in which the difference in pace between the development of technology and law causes questions that due to a legal principle cannot be answered easily. At this time it seems that in the haste to cover all EncroChat cases, in a short period of time; EncroChat evidence has already been used in more than 200 cases,[296] courts have opted for the solution to base judgments on less information and therefore fail to fulfill the requirement that "clear procedures for independent *ex post facto* review of such compliance"[297] and the "powers vested in the competent body in addressing instances of non-compliance"[298] must be present.[299] This results in a line of jurisprudence which does not address a substantial part of the operation and the discussion surrounding it. This compares unfavorably to courts from other jurisdictions which attempt to provide detailed answers and to earlier Dutch case law in which the Dutch Supreme Court has attempted to provide solutions for situations in which the principle of mutual trust obstructs satisfactory adjudication.

Additionally, the straightforward line Dutch courts chose compares bleakly to the recent initiative of European leaders which are attempting to create an expert group that can provide "a comprehensive horizontal approach that considers the need to uphold all fundamental rights in digital environments as well as the need to guarantee information security and cybersecurity (...)."[300]

Still, in case of EncroChat an expert group might not be necessary to uphold fundamental rights as the ECtHR[301] and the CJEU[302] have yet to pass judgments on the matter.

---

[296] Jan Jaap Oerlemans and Dave van Toor, 'Legal Aspects of the EncroChat operation: A Human Rights Perspective', (2022), European Journal of Crime, Criminal Law and Criminal Justice 309, p.320.
[297] Big Brother Watch, (n 57) 361.
[298] Ibid.
[299] Ibid.
[300] Council of the European Union, (n 292)
[301] As of yet no Dutch courts have referred EncroChat to the ECHR, in two British cases questions have been posed to the ECHR see: Hendrik Mildebrath, 'EncroChat's path to Europe's highest courts', (16 December 2022), <https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)739268>, accessed on 30 May 2023.
[302] As of yet no Dutch courts have referred EncroChat to the CJEU, the court of Berlin has posed questions to the CJEU among others regarding breaches of rights under EU law, see: 'Thomas Wahl, EncroChat Turns into a Case for the CJEU, *Eurcim,* 18 November 2022, <https://eucrim.eu/news/encrochat-turns-into-a-case-for-the-cjeu/>, accessed on 30 May 2023. This preliminary ruling took place on 28 June 2023, ruling yet to become public (30 June 2023).

Chapter 5: Conclusions

This thesis focused on the EncroChat operation and the interpretation of Dutch courts regarding the question if the operation caused an unjustified interference with article 8 ECHR. Additionally, the main research question prompted other questions, such as if current frameworks are adequate to assess EncroChat, and similar operations, or if new legislative or jurisprudential frameworks must be developed. If no framework is entirely appropriate to assess EncroChat, which is the view that is taken in this thesis, this demonstrates that the Collingridge dilemma is still present in regard to encryption just as it was in the 1990s. To circumvent the dilemma regarding regulation, this thesis provides a sketch of a jurisprudential framework which would allow the EncroChat operation, and others, to be assessed by a national judge without having to breach the principle of mutual trust, attempting to reduce the gap between regulation and technology caused by the difference in pace. Likewise, this thesis attempts to reconcile the arguments made by defense attorneys and privacy advocates on the one hand, and national authorities on the other hand, by doing so creating a framework in which both privacy and security can be harbored.

5.1. Answer to main question

This thesis sought to answer the following question: *Have Dutch courts wrongly deviated from earlier mass surveillance frameworks based on article 8(2) ECHR by permitting bulk interception in the manner discussed in this thesis?*

In answering this question a few issues became apparent. One of these issues is the presence of the principle of mutual trust. On the one hand, the principle of mutual trust enforces the trust member states have in each other, it has a very practical aspect, two judges will not have to address the same operation. On the other hand, the reactions EncroChat caused not only with the accused but more so with scholars and lawyers prove that this principle might have to be rethought to provide detailed domestic case law. Simultaneously, the historic debate discussed in this thesis proves that encryption is, and has been, a difficult subject in the context of regulation. Most significantly, based on this thesis it can be concluded that there is a jurisprudential framework present to address the EncroChat operation. By combining the framework used for targeted surveillance, in this case used for leading figures, with the framework used for mass surveillance, in this case used for priorly unknown individuals who have been prosecuted based

on EncroChat data, courts can discuss the breach in a timely manner. Still, the idea of strategic monitoring as discussed in Liberty v UK, which has not (extensively) been discussed in Dutch jurisprudence yet, also provides a framework which could be useful. However, the precedence courts would create by allowing the mere indication that EncroChat phones are used by criminals to fulfill the requirement of a common denominator needed for strategic surveillance to be present paves the way for large amounts of data being intercepted under the guise of strategic surveillance.

5.2. Importance of thesis and implications for the future

The findings described in section 5.2. are of significance in multiple ways. Firstly, the thesis exhibits that courts might seem to be the most appropriate place to create frameworks for invasive technologies which develop at a quick pace, but this is not always the case. When unprecedented events, such as vastly undersigned letters of concern take place, it might be desirable to interfere with the direction in which jurisprudence is developing. One way in which to redirect the direction of development is by referring questions to the CJEU or the ECHR, which has happened.

Still, the method in assessing whether an unjustified breach has occurred cannot change drastically as judgments have already been made based on the assumption that no unjustified interference has taken place. Cases that are each other's equivalent should be treated equally.[303] Therefore, disregarding or circumventing the principle of mutual trust is not a 'fix-all' solution. However, as no judgments have been made by the ECHR or the CJEU, focusing on a potential breach of the idea of equal treatment for equal cases would be getting ahead of things. That breach can be discussed in another thesis.

[303] Andrei Marmor, 'Should like cases be treated alike?', (2005), vol.11, Legal Theory 27, p.27.

Bibliography

Primary sources

Legislation

- Article 15 Directive 2002/58/EC
- Article 126uba Dutch Code of Criminal Procedure
- Article 6 European Convention on Human Rights
- Article 8 European Convention on Human Rights

Case law

- A & Ors, R. v Regina, The Royal Court of Justice London, 5 February 2021
- Attorney-General for the Dutch Supreme Court, 9 May 2023, ECLI:NL:PHR:2023:477
- Big Brother Watch and Others v. The United Kingdom, Third Chamber of the ECHR, 13 September 2018, *(Case 58170/13)*
- Big Brother Watch and Others v. The United Kingdom, ECHR, 25 May 2021, (*Case 58170/13)*
- Centrum för Rättvisa v. Sweden, ECHR, 25 May 2021, (*Case 35252/08*)
- Corte di Cassazione, 15 July 2022, Cass, 32915/22
- Court de Cassation, 11 October 2022, ECLI:EN:CCASS:2022:CR01226
- Court of Justice of the European Union, 6 October 2020, ECLI:EU:C:2020:791
- Judgment of 8 April 2015, *Digital Rights Ireland,* (C‑293/12 and C‑594/12), ECLI:EU:C:2014:238
- Echeverri Rodriguez vs. the Netherlands, ECHR, 27 June 2000, ECLI:NL:XX:2001:AE0193
- Gerechtshof Arnhem-Leeuwarden, 16 November 2022, ECLI:NL:GHARL:2022:9878
- Gerechtshof 's-Hertogenbosch, 25 April 2022, ECLI:NL:GHSHE:2022:1387
- Gerechtshof ‘s-Hertogenbosch, 27 June 2022, ECLI:NL:GHSHE:2022:2208
- Gerechtshof Den Haag, 12 May 2023, ECLI:NL:GHDHA:2023:903
- Hoge Raad, 8 February 2000, ECLI:NL:HR:2000:ZD1780
- Hoge Raad, 5 October 2010 , ECLI:NL:HR:2010:BL5629
- Hoge Raad 22 April 2022, ECLI:NL:HR:2022:612
- Hoge Raad, 28 June 2022, ECLI:NL:HR:2022:900

- Hoge Raad, 13 June 2023, ECLI:NL:HR:2023:913
- J. McB v. L. E., CJEU, 5 October 2010, *(C-400/10)*
- Judgment of 21 December 2016, *Tele2 Sverige and Watson*, (C‑203/15 and C‑698/15), ECLI:EU:C:2016:970
- Judgment of 2 October 2018, *Ministerio Fiscal*, (C-207/16), ECLI:EU:C:2018:788
- Judgment of 6 October 2020, *La Quadrature du Net and Others*, (C-511/18), ECLI:EU:C:2020:791
- Judgment of 6 October 2020, *Privacy International*, (C-623/17), ECLI:EU:C:2020:790
- Liberty v. UK, ECHR, 1 July 2008, (*58243/00)*
- Prokuratuur, CJEU 2 March 2021, *(C‑746/18)*
- Rechtbank Amsterdam, 18 December 2020, ECLI:NL:RBAMS:2020:6443
- Rechtbank Amsterdam, 8 July 2021 ECLI:NL:RBAMS:2021:3524
- Rechtbank Amsterdam, 16 July 2021, ECLI:NL:RBAMS:2021:3707
- Rechtbank Amsterdam, 15 February 2022, ECLI:NL:RBAMS:2022:568
- Rechtbank Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1279
- Rechtbank Amsterdam, 17 March 2022, ECLI:NL:RBAMS:2022:1280
- Rechtbank Amsterdam, 21 November 2022, ECLI:NL:RBAMS:2022:6803
- Rechtbank Amsterdam, 21 November 2022, ECLI:NL:RBAMS:2022:6814
- Rechtbank Amsterdam, 21 November 2022, ECLI:NL:RBAMS:2022:6875
- Rechtbank Amsterdam, 20 December 2022, ECLI:NL:RBAMS:2022:8233
- Rechtbank Amsterdam, 17 March 2023, ECLI:NL:RBAMS:2022:1243
- Rechtbank Den Haag,11 March 2021, ECLI:NL:RBDHA:2021:2242
- Rechtbank Den Haag, 21 October 2022, ECLI:NL:RBDHA:2022:11585
- Rechtbank Den Haag, 12 July 2022, ECLI:NL:RBDHA:2022:6757
- Rechtbank Den-Haag 19 July 2022, ECLI:NL:RBDHA:2022:7423
- Rechtbank Gelderland, 8 December 2021,ECLI:NL:RBGEL:2021:6584
- Rechtbank Gelderland, 20 December 2022, ECLI:NL:RBGEL:2022:7425
- Rechtbank Gelderland, 20 December 2022, ECLI:NL:RBGEL:2022:7440
- Rechtbank Limburg 26 January 2022 ECLI:NL:RBLIM:2022:571
- Rechtbank Limburg 26 January 2022, ECLI:NL:RBLIM:2022:558

- Rechtbank Limburg, 20 June 2023, ECLI:NL:RBLIM:2023:3624
- Rechtbank Midden-Nederland, 17 June 2021, ECLI:NL:RBMNE:2021:2570
- Rechtbank Midden-Nederland, 16 September 2021, ECLI:NL:RBMNE:2021:4480
- Rechtbank Midden-Nederland, 12 April 2022, ECLI:NL:RBMNE:2022:1423
- Rechtbank Midden-Nederland, 23 January 2023, ECLI:NL:RBMNE:2023:169
- Rechtbank Noord-Holland, 23 July 2021, ECLI:NL:RBNHO:2021:6213
- Rechtbank Noord-Holland, 21 April 2022,ECLI:NL:RBNHO:2022:3650
- Rechtbank Oost-Brabant, 2 February 2022, ECLI:NL:RBOBR:2022:312
- Rechtbank Rotterdam, 25 June 2021, ECLI:NL:RBROT:2021:6113
- Rechtbank Rotterdam, 21 February 2023, ECLI:NL:RBROT:2023:1316
- Rechtbank Zeeland-West-Brabant, 31 March 2021, ECLI:NL:RBZWB:2021:1556
- Rechtbank Zeeland-West-Brabant, 26 April 2023, ECLI:NL:RBZWB:2023:2889
- Referral of 24 October 2022, (*C-670/22*)
- Roman Zakharov v. Russia, ECHR, 4 December 2015, (*47143/06*)
- Szabo and Vissy v. Hungary, 12 January 2016, CJEU, *(37138/14)*
- Weber and Saravia v. Germany, ECHR 29 June 2006, (*Case 54934/00*)

Secondary sources

Doctrine

Adams S, ‘Vertrouwen is goed maar controle is beter’, (2021), vol.47, Delikt & Delinkwent 958

Aradau C, McCluskey E, ‘Making Digital Surveillance Unacceptable? Security, Democracy, and the Political Sociology of Disputes’, (2022), vol.16, International Political Sociology 1

Bajovic V, 'Evidence from Encrochat and Sky ECC Encrypted Phones' (2022), vol.3, CRIMEN 154

Birrer A, He D, Just N, ‘The state is watching you—A cross-national comparison of data retention in Europe’, (2023), vol. 47, Telecommunications Policy 1

Branum J and Charteris-Black J, ‘The Edward Snowden affair: A corpus study of the British press’, (2015), Vol 9(2), Discourse and Communication 199

Butenko A, and Larouche P, 'Regulation for Innovativeness or Regulation of Innovation?' (2015), vol. 7 Law, Innovation and Technology 52

Cambien N, 'Mutual Recognition and Mutual Trust in the Internal Market', (2017), vol.2, European Papers 1

Collingridge D, The Social Control of Technology, Pinter, London (1980)

Dalla Corte L, 'On proportionality in the data protection jurisprudence of the CJEU', (2022), vol. 12, International Data Privacy Law 259

De Hert P. and Malgieri G., 'Article 8 ECHR Compliant and Foreseeable Surveillance: The ECTHR's Expanded Legality Requirement Copied by the CJEU. A Discussion of European Surveillance Case Law', (2020), Vol. 6, Brussels Privacy Hub 1

Eskens S., The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature du Net and others and Privacy International, (2022), Vol. 8, EDPL 143

Galič M, 'Bulkbevoegdheden en strafrechtelijk onderzoek: wat de jurisprudentie van het EHRM ons kan leren over de normering van grootschalige data-analyse', (2022), vol. 2, Tijdschrift voor Bijzonder Strafrecht en Handhaving, 130

Griffiths C and Jackson A, 'Intercepted Communications as Evidence: The Admissibility of Material Obtained from the Encrypted Messaging Service EncroChat', (2022), vol.86, The Journal of Criminal Law 271

Gözükara F, 'Challenges and possible severe legal consequences of application users identification from CNG-Logs', (2021), vol.39, Forensic Science International: Digital Investigation 1

Harms K, 'Positieve Uitlokking van Ethisch Hacken: Een Onderzoek naar Responsible-Disclosure Beleid' (2017), vol. 46, Netherlands Journal of Legal Philosophy 196

Jarvis C, 'Crypto Wars: The Fight for Privacy in the Digital Age', (first ed., CRC Press, 2021)

Koers J, 'Nederland als verzoekende staat bij de wederzijdse rechtshulp in strafzaken. Achtergronden, grenzen en mogelijkheden', (Final published in 2001, Wolf Legal Publishers)

Koops B. J. and Kosta E., 'Looking for Some Light Through the Lens of 'Cryptowar' History: Policy Options for Law Enforcement Authorities Against 'Going Dark',(2018) vol. 34, Computer Law and Security Review 1

Kurdina O and Verbeek P, 'Ethics from Within: Google Glass, the Collingridge Dilemma, and the Mediated Value of Privacy', (2019), vol. 44, Science, Technology, & Human Values 291

Liguori C, 'Exploring Lawful Hacking as a Possible Answer to the 'Going Dark' Debate' (2020), vol. 26, Michigan Technology Law Review 317

Lyon D, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique,' (2014), vol.2, Big Data & Society 1

Macnish K, 'Mass Surveillance: A Private Affair?' (2020), vol.7, Moral Philosophy and Politics 9

Maras M, 'The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the 'Others'?' (2012), Vol. 40, International Journal of Law, Crime and Justice 65

Marchant G., Addressing the Pacing Problem, In: Marchant, G., Allenby, B., Herkert, J. (eds) The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight. The International Library of Ethics, Law and Technology, vol 7. Springer, Dordrecht

Marmor A, 'Should like cases be treated alike?', (2005), vol.11, Legal Theory 27

Milaj J, Jeanne Bonnici, 'Unwitting subjects of surveillance and the presumption of innocence', (2014), vol.30, Computer Law and Security Review 419

Moyle L et. al., '#Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs', (2019), vol.63, International Journal of Drug Policy 101

Orwell G, *1984*, (1st ed. Secker & Warburg 1949)

Oerlemans J and van Toor D, ‘Legal Aspects of the EncroChat operation: A Human Rights Perspective’, (2022), European Journal of Crime, Criminal Law and Criminal Justice 309

Pisarić M, 'Encrypted Mobile Phones', (2021) vol.11, Archibald Reiss Days 185

Pommerantz J., *Metadata*, First edition, MIT Press, 2015

Rang Choi T and Sun Y ‘Instagram versus Snapchat: Self-expression and privacy concern on social media’, (2018), vol.35, Telematics and Informatics 2289

Reedy P, ‘Interpol review of digital evidence for 2019–2022’, (2023), vol.6, Forensic Science International: Digital Investigation 1

Sahni M, ‘Detecting and Automated reporting of change in IMEI number’, (2014), vol.3, International Journal of Advancements in Research & Technology 186

Schermer B and Oerlemans J.J, ‘De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?’(2022), vol.2, Tijdschrift voor Bijzonder Strafrecht & Handhaving 82

Sedeeg A, Mahgoub M and Saeed M, ‘An Application of the New Integral “Aboodh Transform” in Cryptography’, (2016), vol.5, Pure and Applied Mathematics Journal 151

Sircar S, ‘The Crypto Wars: Interpreting the Privacy versus National Security debate from a standards perspective’, (M.A. thesis, Georgetown University 2017)

Sommer P, ‘Evidence from hacking: A few tiresome problems’, (2022), vol. 40
Forensic Science International: Digital Investigation 1

Stoykova R, ‘Digital Evidence: Unaddressed threats to fairness and the presumption of innocence’, (2021), vol. 42 Computer Law and Digital Review 1

Stoykova R, ‘Encrochat: The Hacker with a Warrant and Fair Trials?’ [2023], Forensic Science International: Digital Investigation 1

Ter Haar R and Meijer G, ‘Tallon-criterium (uitlokking)’, (2011), vol.3, Praktijkwijzer Strafrecht

Trummer I, 'Liberty v. SSHD & SSFCA: You Have the Right to Remain Silent; Anything You Say Will Be Gathered and Retained by the Government' (2020), vol. 28, Tulane Journal of International & Comparative Law 383

Van der Sloot B, 'Big Brother Watch and Others v. the United Kingdom & Centrum för Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?' (2021), vol. 7, European Data Protection Law Review 319

Van Toor D, 'Het enkele gebruik van cryptophones als basis voor procesrechtelijke concepten', (2022), vol.2, Tijdschrift voor Bijzonder Strafrecht & Handhaving 77

Wahl T, 'EncroChat Turns into a Case for the CJEU', (2022), vol.3 Eurcim 197*,* p.198

Willems A, 'Mutual Trust as a Term of Art in EU Criminal Law: Revealing Its Hybrid Character', (2016), vol. 9 European Journal of Legal Studies 211

Zagaris B and Plachta M, 'Transnational Organized Crime' (2020), vol. 36 International Enforcement Law Reporter 248

Online sources

Advies AG aan Hoge Raad over prejudiciële vragen in EncroChat en SkyECC-zaken', (Hoge Raad | 9 May 2023), <https://www.hogeraad.nl/actueel/nieuwsoverzicht/2023/mei/advies-ag-hoge-raad-prejudiciele-vragen-encrochat-skyecc-zaken/#:~:text=De%20uitspraak%20van%20de%20Hoge,al%20dan%20niet%20te%20volgen.>, accessed on 30 May 2023

Ahmed N, 'What is end-to-end encryption and why are tech companies focusing on it?', (*The Hindu,* 12 December 2022), <https://www.thehindu.com/sci-tech/technology/what-is-end-to-end-encryption-and-why-are-tech-companies-focusing-on-it/article66251153.ece#:~:text=End%2Dto%2Dend%20encryption%20is%20used%20to%20secure%20communications.,end%2Dto%2Dend%20encryption.> accessed on 8 March 2023

Andriga R, 'Al tientallen strafzaken na EncroChat-hackandhet einde is nog niet in zicht', *NOS,* 18 December 2021, <https://nos.nl/artikel/2361112-al-tientallen-strafzaken-na-encrochat-hack-en-het-einde-is-nog-niet-in-zicht>, accessed on 9 October 2022

Council of Europe, Guide to the Case-Law of the of the European Court of Human Rights; Data protection, 31 August 2022, <https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf>, accessed on 23 March 2023

Council of Europe, 'Guide on Article 8 of the European Convention on Human Rights', [2022], <https://www.echr.coe.int/documents/guide_art_8_eng.pdf>, accessed on 11 October 2022

Council of the European Union. Proposal to establish a High-Level Expert Group on Access to Data, [2023], 5601/23, https://www.statewatch.org/media/3854/eu-council-presidency-hleg-access-to-data-5601-23.pdf> ,accessed on 27 June 2023

Council of the European Union, 'Proposal to establish a High-Level Expert Group on Access to Data - Compilation of replies by delegations', [2023], 5601/23, p.14, <https://data.consilium.europa.eu/doc/document/ST-7184-2023-REV-1/en/pdf>, accessed on 27 June 2023

Cox J, 'How Police Secretly Took Over a Global Phone Network for Organized Crime', *Vice,* 2 July 2020 <https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked>, accessed on 7 February 2023

Dickson H., The Latest EncroChat Ruling From the French Supreme Court, *Bedford Row,* <https://www.25bedfordrow.com/site/in-focus/the-latest-encrochat-ruling-from-the-french-supreme-court#_edn3>, accessed on 24 March 2023

Driessen C and Meeus J 'Unieke hack van EncroChat leidt tot veel lastige juridische vraagstukken', *NRC*, 9 juni 2021

<https://www.nrc.nl/nieuws/2021/06/09/unieke-hack-van-encrochat-leidt-tot-veel-lastige-juridische-vraagstukken-a4046752>, accessed on 19 October

European Commission, *Impact Assessment Report,* 25 May 2022, <https://www.echr.coe.int/documents/guide_art_8_eng.pdf>, accessed on 27 September 2022

European Commission, *What the European Commission does in law* <https://ec.europa.eu/info/about-european-commission/what-european-commission-does/law_en#proposing-laws>, Accessed on 10 October 2022

Europol, 'Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe', 2 July 2020, <https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe>, accessed on 28 September 2022

Fair Trials Organisation and others to the European Commission and the European Parliament, Open letter of concern, (18 February 2022), <https://www.fairtrials.org/app/uploads/2022/02/EnroChat_LetterofConcern.pdf> accessed on 20 February 2023

Flynn S, 'The Case of EncroChat and the Presumption of Innocence in EU Law' *(Renforce Blog 26th of May 2020)* <http://blog.renforce.eu/index.php/en/2022/05/26/the-case-of-encrochat-and-the-presumption-of-innocence-in-eu-law-2/> accessed on 10 October 2022

Goodwin B, EncroChat: Top lawyer warned CPS of risk that phone hacking warrants could be unlawful, 30 April 2021, https://www.computerweekly.com/news/252500061/EncroChat-Top-lawyer-warned-CPS-of-risk-that-phone-hacking-warrants-could-be-unlawful, accessed on 28 September 2022

Lapierre T, Vigouroux H. and Julie Zorilla, 'Collection of Evidence by Judicial Authorities within the EU EncroChat Example', (*American Bar Association,* 1st of April 2021*)*, <https://www.americanbar.org/groups/international_law/publications/international_law_news/20

21/spring/collection-of-evidence-by-judicial-authorities-within-the-eu-encrochat-example/?q=&wt=json&start=0>, accessed on 4 December 2022

Ligtvoet F, 'Rechters gaan lange wachttijden rigoureus aanpakken door 'agressieve' werving', (*NOS,* 27 November 2019), <https://nos.nl/nieuwsuur/artikel/2312320-rechters-gaan-lange-wachttijden-rigoureus-aanpakken-door-agressieve-werving>, accessed on 29 May 2023

Mildebrath H, 'EncroChat's path to Europe's highest courts', (16 December 2022), <https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)739268>, accessed on 30 May 2023

Ministry of Justice of the Netherlands, 'Influence of organised crime on society' <https://www.government.nl/topics/crime-that-undermines-society/influence-of-organised-crime-on-society> accessed on 7 September 2022

MPs and Lords; Lord Anderson of Ipswich, <https://members.parliament.uk/member/4705/career> accessed on 28 September 2022

Rusbridger A, MacAskill E and Gibson j, 'Edward Snowden: a right to privacy is the same as freedom of speech – video interview',(*The Guardian,* 22 May 2015) <https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video>, accessed on 2 May 2023

Sagittae G, 'On the Lawfulness of the EncroChat and Sky ECC-Operations' (2023), New Journal of European Criminal Law 1, p.5, published online ahead of print, available at: <https://journals.sagepub.com/doi/full/10.1177/20322844231159576>, accessed on 22 April 2023

Statewatch, 'Insufficient safeguards in bulk signals-intelligence gathering risked arbitrariness and abuse', (*Statewatch* | 26 May 2021) <https://www.statewatch.org/news/2021/may/echr-bulk-communications-data-interception-by-uk-and-swedish-spy-agencies-violated-right-to-privacy/>, accessed on 23 March 2023

Van Boom Advocaten, 'Brandbrief Strafrechtadvocatuur', (vanboomadvocaten.nu), <https://vanboomadvocaten.nu/brandbrief-strafrechtadvocatuur/>, accessed on 4 December 2022