BRILL
NIJHOFF

EUROPEAN JOURNAL OF CRIME, CRIMINAL LAW AND
CRIMINAL JUSTICE 30 (2022) 309–328

European Journal of
Crime, Criminal Law
and Criminal Justice
brill.com/eccl

Legal Aspects of the EncroChat Operation: A Human Rights Perspective

J.J. Oerlemans
Endowed professor of Intelligence and Law, Willem Pompe Institute for Criminal Law and Criminology, Utrecht University, The Netherlands
j.j.oerlemans@uu.nl

D.A.G. van Toor
Assistant professor, Willem Pompe Institute for Criminal Law and Criminology, Utrecht University, The Netherlands
d.a.g.vantoor@uu.nl

Abstract

In the EncroChat operation, French law enforcement authorities collected over 120 million messages from 60.000 EncroChat users. They cooperated with Dutch law enforcement authorities and Europol in a Joint Investigation Team. In the Netherlands, EncroChat data has already been used in over 200 criminal cases.

This article examines what lessons can be learned from the Dutch experience with the EncroChat operation from a human rights perspective, in particular the right to a fair trial.

Keywords

EncroChat – fair trial – cryptophone – joint investigation team – hacking – transparency – access to data

1 Introduction

From 1 April 2020 to 20 June 2020, the French *Gendarmerie* collected over 120 million EncroChat messages sent from approximately 60.000 mobile

telephones.[1] EncroChat was a communications service provider located in France. The company offered modified smartphones (also called 'crypto-phones' or 'PGP phones') running EncroChat software. This software and the modified hardware provided users with a high level of security and enabled users to automatically encrypt their calls and messages. All network traffic was routed through servers located in France. In order to collect the information, the servers and EncroChat phones were hacked by French law enforcement authorities, operating in a Joint Investigation Team (JIT) with the Dutch law enforcement authorities and Europol. The collected data was then transferred to Dutch law enforcement authorities and Europol. Europol also sent data to law enforcement authorities in other countries, based on corresponding geographic data ('geo IP data') of EncroChat users. According to the French authorities, the data can be traced back to users of over 100 countries. In many of these countries, the data is being used as evidence in criminal proceedings. It will supposedly take years to analyse all data.[2]

In the Netherlands, the EncroChat operation has already led to more than 200 judgments by criminal courts in the first two years after the operation.[3] In contrast, outside the Netherlands, there are only a handful of published and accessible cases.[4] In Dutch case law, more details became known about the operation, for example about the way the data was collected and further processed by law enforcement authorities.[5] Dutch case law also makes it clear how

1 Le Bureau des affaires criminelles, 'Retour sur l'affaire EncroChat', *Gendinfo.fr*, 31 July 2020.

2 Ibid.

3 The first case that can be found about the EncroChat operation is of the Court of Amsterdam 10 September 2020, ECLI:NL:RBAMS:2020:4495. The number of judgments is estimated, based on the search term "EncroChat" in the register of published judgments on the website 'rechtspraak.nl'. The search results are filtered to first instance judgments of criminal courts until 1 December 2022. See also for an analysis of Dutch case law following the EncroChat operation: B.W. Schermer & J.J. Oerlemans, 'De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie', 2 *TBS&H* (2022), 82–89.

4 See most notably, in Great Britain: Duncan Campbell, 'Two convicted in first murder plot case involving EncroChat messaging system', *The Guardian*, 14 March 2022. In Germany: LG Berlin, Beschl. v. 1.7.2021 (525 KLS) 254 Js 592/20 (10/21) and KG, Beschl. v. 30.08.2021 – 2 Ws 79/21. See about this cases T. Wahl, 'Verwertung von im Ausland überwachter Chatnachrichten im Strafverfahren', 7–8 *ZIS* (2021), 453 and D.A.G. van Toor, 'Het gebruik van resultaten uit de Encrochat-hack in de Duitse strafrechtspleging', 2 *TBS&H* (2022), 89–105.

5 Schermer & Oerlemans 2022, *loc. cit*.

suspects can exercise their right to a fair trial when they are confronted with EncroChat data.[6]

This article examines what lessons can be learned from the EncroChat operation and the Dutch criminal cases from a human rights perspective, more particularly the right to a fair trial as specified in the European Convention on Human Rights (ECHR). As the Netherlands does not have a Constitutional Court, the case law of the European Court of Human Rights (ECtHR) is omnipresent in Dutch national case law as focal point of human rights protection. The question whether the EncroChat operation and use of the collected data as evidence is in accordance with the right to a fair trial in Article 6 of the Convention is the most prominent in Dutch case law. This is due to the fact that a violation of the right to a fair trial can lead to the exclusion of evidence, whereas a violation of the right to respect of privacy in principle cannot lead to the exclusion of evidence.[7] Therefore, we focus on Article 6 to explain its important role in criminal proceedings in which evidence is used from the EncroChat operation.

In section 2, we present the details of the French EncroChat operation in chronological order. It covers Phase 1 of the operation, which entails the collection of EncroChat data. We will make clear why the right to a fair trial has been important to uncover the details of the operation. Section 3 is about Phase 2 of the operation, which entails the (further) processing of EncroChat data for criminal investigations. It includes an analysis of the sharing of data with other States in a JIT. In this section, we also explain how the Dutch judiciary approached the legality of a 'foreign investigation' and use of evidence in Dutch criminal investigations. In section 4, we discuss to which extent the defence has a right to access EncroChat data, as part of the principle of the equality of arms. We explain how the Dutch approach may meet this principle and what defence attorneys and public prosecutors can learn from this approach.

6 See M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', 2 *BSb* (2021), 41–49; H. Henseler, 'Het inzagerecht en de groeiende omvang van digitaal bewijs', *EeR* 2020, 215–217; D.N. de Jonge & S.L.J. Janssen, 'Eindelijk toegang tot datasets. (Erg) langzaam maar zeker naar een nieuw normaal', 34 *NJB* (2021), 2793–2799; J. van der Pijl, 'De dataset langs de meetlat van art. 6 EVRM', 5 *NJB* (2022), 346–351; and M.M. Egberts, 'De reikwijdte van het inzagerecht en 'equality of arms' in het licht van grote datasets, Hansken en toekomstige ontwikkelingen', 2 *TBS&H* (2022), 119–129.

7 See M.J. Borgers & L. Stevens, 'The use of illegally gathered evidence in the Dutch criminal trial', *IACL 2010 report on Criminal Procedure* for an overview in English.

2 The EncroChat Operation – Collecting Data: Phase 1

Since 2017, the French Gendarmerie and Dutch law enforcement authorities discovered that suspects involved in organised crime regularly used EncroChat phones. Given the widespread use of the encrypted telephone solution by EncroChat in organised crime, the French authorities decided to open a case at Eurojust with the Netherlands in 2019. In 2020, France and the Netherlands decided to take action and started a JIT.[8] According to Europol's definition, 'a joint investigation team is an international cooperation tool based on an agreement between competent authorities – both judicial (judges, prosecutors, investigative judges, et cetera) and law enforcement authorities – of two or more States, established for a limited duration and for a specific purpose, to carry out criminal investigations in one or more of the involved States.'[9]

In Phase 1 of the EncroChat operation, the data was collected by French law enforcement authorities. By accessing servers and hacking the EncroChat cryptophones, the contents of these phones and other data were collected by French law enforcement authorities and shared with Dutch law enforcement authorities. This section presents the details of the French EncroChat operation in chronological order. We also make clear why the right to a fair trial ultimately provided more transparency about the operation in the Netherlands.

2.1 *EncroChat Phones*

EncroChat phones are mobile phone modified in order to communicate as anonymously and securely as possible. They contained the following pre-installed apps:

– 'EncroChat' for encrypted messaging;
– 'EncroTalk' for encrypted internet-based voice calls;
– 'EncroMail' for sending encrypted e-mail messages; and
– 'EncroNotes' for taking notes.[10]

The camera, microphone, GPS and USB port were removed or made unusable. Furthermore, a specific function was available to immediately delete all data stored on the device using a specific code (a 'wiper' functionality).[11]

8 Court of Rotterdam 25 June 2021, ECLI:NL:RBROT:2021:6113, para. 3.2.3.
9 See 'Joint Investigations Teams', *europol.eu*, 26 November 2021.
10 Gilbert Kallenborn, 'Comment les gendarmes ont siphonné EncroChat, la messagerie chiffrée des criminels', *01Net*, 3 July 2020. See also, Court of Noord-Nederland, 27 January 2022, ECLI:NL:RBNNE:2022:164.
11 See Annual report of Eurojust, 2020, para. 7.2.

EncroChat sold these so-called 'cryptophones' at a cost of about EUR 1.000 each. It offered subscriptions with worldwide coverage, for EUR 1.500 for six months with 24/7 support. The French authorities identified the company behind the cryptophone and discovered that servers were used from the internet service provider 'OVH', located in Roubaix, France. These servers facilitate the communications between these phones. By early 2020, EncroChat was one of the largest providers of encrypted digital communication, with a (very) high share of users presumably engaged in criminal activity.[12]

The focus of law enforcement authorities on companies such as EncroChat, can perfectly be explained in what Europol calls the criminal phenomena of "grey infrastructure".[13] In its 'Internet Organised Crime Threat Report 2021' Europol notes that EncroChat is an example of a service that offers a grey infrastructure, i.e.: a service that optimally shields criminals from the grasp of law enforcement authorities. It also states that:

> *although not all users of such services are necessarily criminals, the level of criminality associated with such services is often so high that national law enforcement agencies, after finding enough evidence of criminal abuse, could consider them to be criminal enterprise*.[14]

2.2 *Collecting Data From EncroChat Phones*

In Phase 1 of the operation, all incoming and outcoming communication was intercepted from approximately 60.000 mobile phones.[15] From 1 April 2020, at 17:15 hours, until the 20 June 2020, 17:20 hours, the French Gendarmerie collected the data from the IT infrastructure at an internet service provider in France. With more than 60 officers, the Gendarmerie led the investigation targeting the EncroChat encrypted telephone solution under the supervision of the magistrates of the *juridiction interrégionale spécialisée* (JIRS) of Lille.[16] Additionally, a copy (an 'image') was made of the servers and shared with

12 Ibid.

13 In criminological research, the use of a device such as a cryptophone is called a 'deviant security measure'. See E.H.A. van de Sandt, *The Technical Computer Security Practices of Cyber Criminals*, (Bristol: University of Bristol, 2019), p. 76, 99.

14 Europol, iOCTA report, 2021, p. 18.

15 In the Netherlands, the many details became available after publication of the case by the Court of Rotterdam 25 June 2021, ECLI:NL:RBROT:2021:6113, at para. 3.2.3. See J.J. Oerlemans, 'Meer duidelijkheid over EncroChat', 195 *Computerrecht* (2021) and J.J. Oerlemans, 'Meer duidelijkheid over EncroChat', *jjoerlemans.com* (blog).

16 Joint press release Europol/Eurojust, 'Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe', 2 July 2020.

Dutch law enforcement authorities in January 2019, October 2019, February 2020 and June 2020. This information consisted of metadata, back-ups of certain apps installed on EncroChat phones, administration data, IP addresses, client data and databases with passwords.[17]

To collect the data from EncroChat phones, a 'hacking tool' (also called 'malicious software' or malware, when it is used by criminals) was uploaded as an update from a French server on connected EncroChat phones. The hacking tool was reportedly developed by the *Service Technique National de Captation Judiciaire* (STNCJ) in France.[18] The tool made it possible to register the following data from all mobile phones that were active in that time-frame of two months:

- IMEI-data (an identifying number of mobile phones);
- subscriber names;
- passwords;
- saved chat messages;
- images;
- location data (also called 'geodata'); and
- notes.[19]

After the operation, EncroChat sent a message to its users stating:

> *Today we had our domains seized by government entities.* (...) *With control of our domain they managed to launch a malware campaign against the carbon*[20] *to weaken its security.* (...) *You are advised to power off, and physically dispose of your device immediately.*[21]

Of course, by then, French law enforcement authorities had already secured the data.

2.3 *Lesson Learned: the Right to a Fair Trial is a Transparency Enabler*

In the Dutch EncroChat cases, it proved difficult for the defence to obtain information about the way the evidence was collected and which investigatory powers were used. After unrelenting questions from criminal defence lawyers, more details finally became available through Dutch court decisions. These

17 Court of Amsterdam 17 March 2022, ECLI:NL:RBAMS:2022:1273.

18 See Court of Midden-Nederland 12 April 2022, ECLI:NL:RBMNE:2022:1389.

19 Court of Rotterdam 25 June 2021, ECLI:NL:RBROT:2021:6113, at para. 3.2.3.

20 The word 'Carbon' is used as slang for 'EncroChat phones'.

21 See, e.g., Tom Duffy, 'The single text that sent shockwaves through UK crime underworld after police hack', *mirror.co.uk*, 3 July 2020.

details, coupled with the official press releases about the operation, made it possible to reconstruct the EncroChat operation in section 2.1 and 2.2 above.

Keeping the operation secret challenges the right to a fair trial under article 6 ECHR, more specifically the principle of equality of arms. Part of the principle of equality of arms is transparency about the manner in which the evidence is gathered. At the same time, law enforcement authorities and the public prosecutor can have a legitimate interest in keeping information about the operation secret. For example, for national security reasons, to keep certain police methods secret, or to protect the privacy of others. However, as the ECtHR explained in case law, keeping this information secret is allowed only insofar as it is strictly necessary. In order to ensure that the accused receives a fair trial, any difficulties caused to the defence by a limitation on its rights must be sufficiently counterbalanced by the procedures followed by the judicial authorities.[22]

We believe that – to a certain extent – information about how evidence was collected and which investigatory powers were applied should be available to the defence. This enables the defence to challenge the legality of the operation and thereby challenge possible abuse of power by law enforcement authorities. In addition, judges should be able to decide on the method of acquisition and reliability of the evidence.[23] This is especially important in the context of EncroChat, in which (complex) software is used to collect the data. The use of software challenges the confidentiality, integrity and availability (CIA-triad) of data and can have a major influence on the reliability of evidence.[24] So far, there are no details available about the software that was used in the EncroChat investigation.

Dutch defence lawyers frequently question the integrity of EncroChat data that is used as evidence in criminal proceedings.[25] The main argument is that the data shared by French law enforcement authorities is processed and

22 See, e.g., ECtHR 31 March 2009, ECLI:CE:ECHR:2009:0331JUD002102204 (*Natunen/Finland*), para. 40–43, ECtHR 4 September 2019, ECLI:CE:ECHR:2019:0604JUD003975715 (*Sigurður Einarsson and Others/Iceland*), para. 85–86. See further section 4.1.

23 See A. Stoykova, 'Standards for Digital Evidence: an inquiry into the opportunities for fair trial safeguards through digital forensics standards in criminal investigations', *Computer Law & Security Review* 2021, 42, 1–20.

24 See P. Sommer, 'Evidence from hacking: A few tiresome problems', *Forensic Science International: Digital Investigation* 2022, 40, 301–333.

25 See, e.g., Court of Rotterdam 11 October 2022, ECLI:NL:RBROT:2021:9906, para. 6.5.10; Court of Rotterdam 11 April 2022 (ECLI:NL:RBROT:2022:2809, para. 5.3.3; Court of Midden-Nederland 12 April 2022, ECLI:NL:RBMNE:2022:1389; High Court of 's-Hertogenbosch 25 April 2022, ECLI:NL:GHSHE:2022:1387; Court of Oost-Brabant 14 July 2022, ECLI:NL:RBOBR:2022:2871.

different from the original data stored on EncroChat phones. In Dutch case law, it is reported that the Netherlands Forensic Institute conducted an investigation and found that the messages obtained from French law enforcement authorities were not different from the messages later found and decrypted on five seized EncroChat phones. However, they did find that the hacking and interception software did not operate continuously, not *all* messages on EncroChat phones were intercepted during the operation, and there had been instances of a mix-up in outgoing and incoming calls from EncroChat phones.[26] Each time, the defence failed to establish in which respect the data that is used as evidence is unreliable or why it tainted all EncroChat data used as evidence. Moreover, often times, there were multiple sources of evidence (besides EncroChat data) available in these criminal proceedings. Therefore, it has never been successfully argued by Dutch lawyers that the data from the EncroChat operation used as evidence is not reliable. As a result, no data from the EncroChat operation used as evidence has ever been excluded in Dutch criminal cases.

In sum, the defence can argue that the defence and judiciary must have sufficient details of the evidence gathering activities and the (further) processing of EncroChat data in order to have a fair trial in accordance Article 6 ECHR. In Dutch case law, this ultimately provided more details about the EncroChat operation and presented the opportunity to test the reliability of the evidence derived from collected EncroChat data.

3 The EncroChat Operation – Processing Data: Phase 2

In Phase 2 of the operation, the French Gendarmerie shared the collected data with the Dutch Police and Europol. The data was then distributed to other European partners, including the United Kingdom, Sweden and Norway. A large, dedicated team at Europol investigated – in real time – millions of messages and data received from JIT partners during the investigation. The team cross-checked and analysed the data and provided and coordinated with the JIT partners the information exchange to concerned countries.[27]

Eurojust intensively facilitated judicial cooperation, during the extensive use of European judicial cooperation instruments such as European Investigation

26 Court of Midden-Nederland 12 April 2022, ECLI:NL:RBMNE:2022:1389; Court of Oost-Brabant 14 July 2022, ECLI:NL:RBOBR:2022:2871.

27 Annual report of Eurojust, 2020, par 7.2.

Orders.[28] Throughout the investigation, the JIT members organised nine coordination meeting at Eurojust to bring all involved parties together in a secure environment, identify parallel or linked investigations, decide on the most suitable framework for cooperation and solve potential conflicts of jurisdiction.[29]

As a result of the operation, new investigations were initiated, thousands of people were arrested and large amounts of drugs were confiscated. For example, in the Netherlands, more than 100 persons were arrested as a result of the EncroChat operations and analysis of the data. In April 2021, there were 200 ongoing criminal investigations arising from EncroChat.[30] In Sweden, more than 200 suspects were identified in 2021.[31] In the United Kingdom, the National Crime Agency reported that 2.631 people had been arrested in the United Kingdom following the analysis of EncroChat messages and 1.384 had been charged.[32]

In what follows, we will briefly explain the data sharing possibilities in a JIT, how Dutch law enforcement authorities provided extra safeguards, and what lessons can be learned from the Dutch approach to processing EncroChat data for (future) criminal investigations.

3.1 *Processing and Sharing EncroChat Data in a JIT*

With the technical complexities and transnational character of the use of EncroChat cryptophones in mind, the decision to start a JIT appears to be a good choice.[33] Apparently, French law enforcement authorities took the

28 See, e.g., 'EncroChat-Data may be used for the Investigation of Serous Offences', *bundesgerichtshof.de*, 25 March 2022 (Decision of 2 March 2022 – 5 StR 457/21). The European Investigation Order (EIO) is a judicial decision issued in or validated by the judicial authority in one EU country to have investigative measures to gather or use evidence in criminal matters carried out in another EU country. It is valid throughout the EU, but does not apply in Denmark and Ireland. The EIO was established by Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *Official Journal of the European Union* L 130/1, 1 May 2014.

29 Annual report of Eurojust, 2020, para. 7.2.

30 Dutch annual report National Police 2020, p. 31.

31 Annual report of Eurojust, 2020, para. 7.2.

32 Duncan Campbell, 'Two convicted in first murder plot case involving EncroChat-messaging system', *The Guardian*, 14 March 2022.

33 See Article 13(1) of the EU Convention on Mutual Assistance, 12 July 2000: (...) *A joint investigation team may, in particular, be set up where:* (*a*) *a Member State's investigations into criminal offences require difficult and demanding investigations having links with other Member States* (*b*) *a number of Member States are conducting investigations into criminal offences in which the circumstances of the case necessitate coordinated, concerted action in the Member States involved.* See also L.W. Verbeek & T. Beekhuis, 'Executieve jurisdictie: het

lead in the investigation. As a result, based on the EU Convention on Mutual Assistance, the activities took place under French criminal procedure law.[34]

Dutch law enforcement officials could have been allowed to be present when the investigative measures took place and even take certain investigate measures if they were approved by the competent authorities in France.[35] Article 30(2)(a) of the EU Convention on Mutual Assistance and Article 5 of the Europol Regulation state that joint teams can also include representatives of Europol in a supporting capacity.[36]

French law enforcement authorities are authorised to share data with another member of the JIT (i.e., Dutch law enforcement authorities and Europol) under the following conditions: (a) only for the purposes for which the team has been set up, (b) subject to the prior consent of the Member State where the information became available, for the purposes of detecting, investigation and prosecuting other criminal offences, (c) for preventing an immediate and serious threat to public security, or (d) for other purposes to the extent that this is agreed between Member States setting up a JIT.[37]

When the number of participating States in the JIT is increased in the course of its duties, the providing State's approval must again be requested for sharing information with new States. In this operation, the data was apparently also shared with Germany, Norway, Sweden and the United Kingdom. As stated in 3.2, a Europol team cross-checked and analysed the data and provided and coordinated with the JIT partners the information exchange to the concerned countries.[38]

In short, the EU Convention on Mutual Assistance allows for a French investigation and sharing of data with Europol and Dutch law enforcement authorities as its JIT partners.

(grote) obstakel in grensoverschrijdende opsporingsonderzoeken naar (gebruikers van) cryptoaanbieders?', 2 *TBS&H* (2022), 106–118.

34 See Article 13(a)(b) EU Convention on Mutual Assistance.

35 Art. 13(5) and 13(6) EU Convention on Mutual Assistance.

36 See also article 4(1)(h) Europol Regulation (Regulation 2016/794, *Official Journal of the European Union* L 135/53). On 9 December 2020, the Commission published a proposal for a Regulation amending Regulation 2016/794 (COM(2020) 796 final), which would allow for broader powers for data-analysis. See for a critical discussion of the proposal: S. Eskens, 'New and extensive data processing powers proposed for Europol, *European Law Blog*, 30 July 2021. See further about possibilities to gather evidence and share data in a JIT: C. Rijken, 'Joint Investigation Teams: principles, practice, and problems. Lessons learned from the first efforts to establish a JIT', 2 *Utrecht Law Review* (2006), 99–118.

37 Art. 13(10) EU Convention on Mutual Assistance.

38 Annual report of Eurojust 2020, para. 7.2.

3.2 *Dutch Approach to Foreign Evidence Gathering and Sharing Data*

In the Netherlands, Dutch defence lawyers (extensively) debated a theory that the evidence was illegally obtained under Dutch law and should therefore be excluded.[39] Dutch courts disagreed.

As a principle of mutual trust, the Dutch judiciary does not investigate the legitimacy of the evidence that has been gathered by foreign law enforcement authorities on foreign territory any further, unless it interferes with the right to a fair trial.[40] For example, the Court of Rotterdam considered, in response to such a defence, that

> *the judicial authorities in France authorised the use of interception tool and obtained the necessary permissions. The Dutch public prosecution service repeatedly emphasised the criminal investigation was directed to a company on French territory.* (…) *For that reason, and with reference to the principle of trust in these matters, the Court will not test the legitimacy of the warrant of a French judge*.[41]

3.3 *A Good Practice: Extra Safeguards to Process Shared (Bulk) Data*

In the Netherlands, an "extra" warrant – thus after the interception of the EncroChat data by French authorities in the case against EncroChat – was requested by the public prosecution service in order to use the data in other investigations. At first, not much was known about the extra warrant. After approximately one year and three months since the first case law following the

39 B.W. Schermer & J.J. Oerlemans, *loc. cit.*

40 T. Kraniotis, 'Het vertrouwensbeginsel bij de interstatelijke samenwerking in strafzaken', dissertation Radboud University 2016, Deventer: Wolters Kluwer, p. 450. See in the context of EncroChat: of EncroChat: S.G.A.M. Adams, 'Vertrouwen is goed, maar controle is beter. De interpretatie van het interstatelijke vertrouwensbeginsel door Nederlandse feitenrechter bij samenwerking tussen EVRM-lidstaten in het kader van internationale digitale rechtshulp in strafzaken en het beginsel van equality of arms', 74 *DD*, 959–981 and the following case law: Court of Amsterdam 16 July 2021, ECLI:NL:RBAMS:2021:3707; Court of Rotterdam 11 October 2021, ECLI:NL:RBROT:2021:9906, para. 6.5.17; Court of Midden-Nederland 17 June 2021, ECLI:NL:RBMNE:2021:2570; Court of Oost-Brabant 1 June 2021, ECLI:NL:RBOBR:2021:2557. Only the court of Court of Noord Holland 4 May 2022, ECLI:NL:RBNHO:2022:3844, para. 3.5 took a different approach, but did not sanction with the exclusion of evidence. See regarding the approach to foreign evidence gathering activities and EncroChat in Germany: 'EncroChat-Data may be used for the Investigation of Serous Offences', *bundesgerichtshof.de*, 25 March 2022 (Decision of 2 March 2022 – 5 StR 457/21).

41 Court of Rotterdam 25 June 2021, ECLI:NL:RBROT:2021:6113, at para. 3.2.4 (translated from Dutch by the authors).

EncroChat operation, more details about the warrant became known and were tested in court.[42]

In the extra warrant, the Dutch public prosecution office requested authorisation for hacking as an investigatory power and wiretapping.[43] The request for a warrant argued that there was a reasonable suspicion EncroChat users were guilty of crimes such as money laundering, leading a criminal enterprise, drug trafficking, weapon trafficking, (attempted) murder, hostage taking and extortion. The aim of the EncroChat operation was threefold: (1) to identify EncroChat users, (2) to investigate the criminal organisations they were part of, and (3) to collect evidence about crimes committed or yet to be committed by these criminal organisations.

In its warrant, the investigative judge ordered certain limitations on the analysis of the data transferred by French authorities in order to avoid a 'fishing expedition'. The data was available to Dutch law enforcement authorities, but essentially only in an investigation against EncroChat and its role in organised crime (and other criminal offences committed by the company).[44] Initially, the data was not gathered in any ongoing investigation into individuals committing offences. But after analysis of the EncroChat data, hundreds of individuals who committed crimes (as part of organised criminal structures) were exposed. Therefore, additional warrants were requested and granted to further analyse the EncroChat data in order to gather evidence in criminal investigations.

An important limitation of the warrant was that the EncroChat data was only eligible for analysis with the use of keywords related to the investigated crimes or suspects. In addition, the data analysis had to be reproducible. The investigative judge also demanded a technical description in the warrant about how the computers were hacked, with what kind of software and how the integrity of the data would be secured. Note that the text of the warrant partly remains classified to avoid mentioning personal data of judges and public prosecutors involved, as well as naming or providing the technical description of what kind of software is used in the operation.[45] Finally, measures had to be taken to avoid reading privileged communications and the investigation

42 As previously stated, the first case that can be found about the EncroChat operation is of the Court of Amsterdam 10 September 2020, ECLI:NL:RBAMS:2020:4495. The details of warrant became known in a judgment of the Court of Gelderland 8 December 2021, ECLI:NL:RBGEL:2021:6584, para. 2.1.

43 Specified in article 126uab and article 126t of the Dutch Code of Criminal Procedure.

44 Court of Rotterdam 20 October 2020, ECLI:NL:RBROT:2020:9899, para. 4.2.

45 Court of Rotterdam 11 October 2021, ECLI:NL:RBROT:2021:10412.

was authorised for an initial duration of four weeks (with the possible extension upon request).

It is now standard practice in the Netherlands to request a warrant in order to create a subset of the collected EncroChat data and use that data as potential evidence in criminal proceedings.[46] We view this as a 'good practice', because another judge will test the principles of proportionality and subsidiarity, while taking into account the reproducibility of evidence and protecting privileged communications. The extra warrant therefore further protects the fundamental rights of the individuals involved.

4 Accessing EncroChat Data by the Defence

In many Dutch cases, the defence argued *all* the collected EncroChat data should be disclosed to the defence as part of the principle of the equality of arms (article 6 ECHR). Suspects were confronted with EncroChat data, which incriminated them for serious crimes such as murder, participating in a criminal enterprise and drug trafficking. In order to challenge evidence derived from the EncroChat operation, the defence argued the data should be accessible in order (a) to review its integrity, (b) to review the reliability (because all EncroChat messages are sent under pseudonyms) and (c) whether exculpatory evidence could be found in the dataset.

In this section we will analyse if the argument that *all* data should be disclosed under article 6 ECHR is valid. We first analyse ECtHR case law with regard to the equality of arms when suspects are confronted with this kind of 'large datasets'. Second, we will discuss Dutch current practices with regard to providing suspects access to EncroChat data. Third, we will examine what lessons can be learned from both case law and Dutch practice.

4.1 *Equality of Arms*

As part of a fair trial, the ECtHR has consistently considered that the procedure should be adversarial and that there should be 'equality of arms' between the prosecution and defence.[47] This means the prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party. In addition, Article

46 Egberts 2022, *op. cit.*, p. 123. See also Court of Gelderland 8 December 2021, ECLI:NL:RBGEL:2021:6584.

47 See, e.g., ECtHR 22 July 2004, nos. 39647/98 and 40461/98, ECLI:CE:ECHR:2004:1027JUD003964798 (*Edwards and Lewis/The United Kingdom*), para. 46.

6(1) ECHR requires that the prosecution authorities disclose to the defence all material evidence in their possession for or against the accused.[48]

However, the disclosure of all relevant evidence is not an absolute right.[49] In any criminal proceedings there may be competing interests against disclosure.[50] In some cases, it may be necessary to withhold certain evidence from the defence in order to preserve the fundamental rights of other individuals or to safeguard an important public interest, such as national security or the need to protect witnesses at risk of reprisals or keep secret police methods of investigation of crime.[51] Only such measures restricting the rights of the defence which are strictly necessary, are permissible under the right to a fair trial in Article 6(1).[52] Moreover, in order to ensure that the accused receives a fair trial, any difficulties caused to the defence by a limitation on its rights, must be sufficiently counterbalanced by the procedures that are followed by the judicial authorities.[53]

The disclosure of data in a case where large datasets are seized, is fundamentally different from "normal" criminal cases with, for example, witnesses and CCTV footage as evidence.[54] Bulk datasets contain a lot of information about other individuals as well. In large datasets collected from cryptocommunication providers, with most clients being involved with organised crime, information about rivals could be found or information that one associate is communicating with law enforcement authorities. Due to the danger of implicating those involved, a *carte blanche* disclosure of the complete dataset could mean a violation of the positive obligations to protect the fundamental rights of respect for life (Article 2 ECHR) and respect for bodily integrity (Article 3 ECHR).

48 See, e.g., 4 July 2017, no. 2742/12, ECLI:CE:ECHR:2017:0404JUD000274212 (*Matanović/Croatia*), para. 151–152.

49 ECtHR 26 March 1996, no. 20524/92, ECLI:CE:ECHR:1996:0326JUD002052492 (*Doorson/The Netherlands*), para. 70.

50 ECtHR (GC) 16 February 2000, no. 28901/95, ECLI:CE:ECHR:2000:0216JUD002890195 (*Rowe and Davis/the United Kingdom*), para. 61.

51 Ibid. See also ECtHR (GC) 16 February 2000, no. 27052/95, ECLI:CE:ECHR:2000:0216 JUD002705295 (*Jasper/the United Kingdom*), para. 52.

52 See, e.g., ECtHR 12 April 1997, nos. 21363/93, 21364/93, 21427/93 and 22056/93, ECLI:CE:ECHR:1997:0423JUD002136393 (*Van Mechelen and Others/the Netherlands*), para. 58 and ECtHR 22 July 2004, nos. 39647/98 and 40461/98, ECLI:CE:ECHR:2004:1027JUD003964798 (*Edwards and Lewis/The United Kingdom*), para. 46.

53 See, e.g, ECtHR 31 March 2009, no. 21022/04, ECLI:CE:ECHR:2009:0331JUD002102204 (*Natunen/Finland*), para. 40.

54 See, e.g., S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, (Springer 2020), p. 90 and further.

The ECtHR developed the following procedure for large datasets. In order to analyse the data, law enforcement authorities filter the raw dataset (also known as a 'primary dataset') into a 'secondary dataset'. Where the raw dataset is unstructured and contains *all seized data*, the secondary dataset "only" contains *all data relevant* for criminal investigations. Still, this dataset is a large volume of information on all kinds of suspects and crimes. The next step is to compile the 'tertiary dataset' with all the relevant information for *a specific investigation*. The question of whether and which dataset should be disclosed, must be reviewed with regard to the three different datasets.[55]

As for the raw dataset, there is no obligation to disclose all information, especially not when law enforcement authorities did not review the relevance of the data themselves.[56]

When the raw dataset is searched and thereafter filtered using specific search terms to create a secondary dataset, it could be necessary to include the defence in this process.[57] The ECtHR does not consider it necessary that the defence can use the search engine or any analytical software programs themselves: they can also provide law enforcement authorities with search terms. In that sense, a specific request to filter the raw dataset using specific search terms is also a safeguard against fishing expeditions.[58] In *Sigurðður Einarsson and others*, the Court was critical that tagged files in the secondary dataset were only reviewed by law enforcement authorities to assess their relevance for the case. The Court recalls that:

> *a procedure, whereby the prosecution itself attempts to assess the importance of concealed information to the defence and weigh this against the public interest in keeping the information secret, cannot comply with the above-mentioned requirements of Article 6 § 1* (*Rowe and Davis, § 63*).[59]

The tertiary dataset contains information that is relevant to a single case. For this type of dataset, the general rule is clear: it contains information that is

55 See Attorney-General Harteveld's opinion on the Ennetcom dataset, 8 March 2022, ECLI:NL:PHR:2022:219, para. 6 and further. See, similarly, ECtHR 4 June 2019, no. 39757/15, ECLI:CE:ECHR:2019:0604JUD003975715, (*Sigurður Einarsson and Others/Iceland*).

56 ECtHR 4 June 2019, no. 39757/15, ECLI:CE:ECHR:2019:0604JUD003975715 (*Sigurður Einarsson and Others/Iceland*), para. 90.

57 Ibid.

58 Ibid.

59 Ibid, para. 91. In *Rowe and Davis*, the court refers to 'the requirements of adversarial proceedings and equality of arms and incorporated adequate safeguards to protect the interests of the accused' (para. 62).

considered relevant in a single case, this data can be used against the suspect, and should be disclosed.[60]

Lastly, the defence should have an 'effective opportunity' to access and analyse the data.[61] To make any discovery possible, it seems necessary to provide the defence with *readable* (not encrypted) data for review. Alternatively, the defence can be provided with access to the e-discovery program in which the data is made accessible on the premises of law enforcement authorities.[62]

The above analysis of ECtHR case law shows that it is not clear (yet) where exactly a line is drawn in accessing data from the EncroChat operation. Clearly, the defence is not required to be able to analyse *all* data that is gathered in the operation (i.e., the raw dataset of approximately 25 million messages),[63] especially when the first screening is done automatously.[64] However, it is not clear to which extent the defence should be able to access data in the secondary dataset which contains data from other criminal investigations relating to other individuals. There are competing interests at heart. On the one hand, it is possible that the secondary dataset contains exculpatory evidence, for example that the defendant's role in the organisation is smaller than suspected. On the other hand, disclosure of the complete secondary dataset raises potential issues under Article 2, Article 3 and Article 8 of the Convention, due to the fact that the secondary dataset contains information on other individuals. Either way, any difficulties caused to the defence by a limitation on its rights, must be sufficiently counterbalanced by the procedures that are followed by the judicial authorities.

We conclude as follows: all information that is deemed relevant in a particular case and can be used against the suspect in a criminal case (the tertiary dataset), should be disclosed to the suspect. In addition, they should have the sufficient facilities (an 'effective opportunity') to access and analyse the data. The defence should be able to explain why they require further access to EncroChat data (on top of the data that is actually being used in his particular case), including data that is not part of the dataset created by the public

60 See ECtHR 25 July 2019, no. 1586/15, ECLI:CE:ECHR:2019:0725JUD000158615 (*Rook/Germany*), para. 58.

61 See ECtHR 25 July 2019, no. 1586/15, ECLI:CE:ECHR:2019:0725JUD000158615 (*Rook/Germany*), para. 63, 67 and 70 and ECtHR 4 June 2019, no. 39757/15, ECLI:CE:ECHR:2019:0604 JUD003975715 (*Sigurður Einarsson and Others/Iceland*), para. 91.

62 Attorney-General Harteveld's opinion on the Ennetcom dataset, 8 March 2022, ECLI:NL:PHR:2022:219, para. 6.15.

63 Cf. S.G.A.M. Adams, *loc. cit*.

64 ECtHR 4 June 2019, no. 39757/15, ECLI:CE:ECHR:2019:0604JUD003975715 (*Sigurður Einarsson and Others/Iceland*), para. 90.

prosecution with certain key words. These possibilities can be viewed as counterbalance measures as meant by the ECtHR when access to certain data is restricted.

4.2 *Access to EncroChat Data in the Netherlands*

From Dutch case law and literature on the topic, the following Dutch approach to the access to EncroChat data by the defence emerges.[65] The Dutch public prosecutor's office enables the defence to search through the tertiary dataset that contains information that deemed relevant by the prosecution for the case against the defendant. And, upon a reasoned request, they can search through the secondary dataset. The analysis can take place in a 'data room' on the premises of the Netherlands Forensic Institute.

The defence is able to access all relevant and not-relevant data regarding a suspect in a particular criminal case, but not data that is used in a different criminal investigation. This is deemed necessary in order not to endanger future investigations, but also to avoid dangers for other individuals in the dataset.[66] Notably, in a case concerning data from a different cryptophone provider ('Ennetcom'), the Dutch Supreme Court found this approach to accessing information by the defence lawful.[67]

As for practical matters, the defence can make use of the same analysis software which the Dutch law enforcement authorities use.[68] In addition, upon request, defence attorneys generally seem to be able to obtain a copy of the EncroChat data that is deemed relevant to the investigation of their client in an Excel format.[69] This appears to be an 'effective opportunity' to access and analyse the data. One step further would be to enable the defence to use a virtual private network in order to conduct a remote search of the data from a location of their preference.[70] This is not made possible at the time of writing and experts warn adequate expertise to use the software is required, which can be provided with training.[71]

65 See, e.g., D.N. de Jonge & S.L.J. Janssen, *loc. cit.*; S.G.A.M. Adams, *loc. cit.*; M. Galič, *loc. cit.*; M.M. Egberts, *loc. cit.*

66 Cf. Court of Amsterdam 1 April 2021, ECLI:NL:RBAMS:2021:1507, para. 58 and Court of Amsterdam 21 May 2021, ECLI:NL:RBAMS:2021:2585, para. 70.

67 Supreme Court 28 June 2022, ECLI:NL:HR:2022:900.

68 The software is called Hansken. See also H.M.A. van Beek et al., 'Digital forensics as a service: Game on', *Digital Investigation* 2015, p. 20–38.

69 See also D.N. de Jonge & S.L.J. Janssen, *loc. cit.*

70 This option was considered in the case of the Court of Amsterdam 21 May 2021, ECLI:NL:RBAMS:2021:2585, para. 34–38. See also M.M. Egberts, *loc. cit.*

71 See H. Henseler, *loc. cit.*

Overall, with the case law in section 4.1 in mind, the Dutch approach seems to meet the criteria set by the ECtHR with regard to the equality of arms principle.

4.3 *Lesson Learned: Using the Right to a Fair Trial to Access to Data*

The case law of the ECtHR with regard to the access of data obtained by law enforcement authorities teaches us that the defence should have access to the data that is used in a criminal case against a suspect. The defence can reason why they require further access to data and should be able to have a role in creating a new dataset by using keywords. In addition, they should have an effective opportunity to analyse the data.

Practitioners can learn from Dutch practical experience in providing access to EncroChat data (section 4.2). These requests to access EncroChat data will undoubtedly arise in criminal proceedings in other States as well. The public prosecution office and judiciary should prepare for this and invest in an infrastructure to facilitate these data access requests.

5 Conclusion

As EncroChat messages are admitted as evidence in several other Council of Europe Member States as well – for example in Germany, France, Norway, Sweden and the United Kingdom – those criminal justice systems can profit from the already extensive judgments of Dutch criminal courts. These criminal justice systems must also meet the minimum standards of the right to a fair trial as set by the ECtHR. In this article we examined what lessons could be learned from the Dutch experience with the EncroChat operation from a human rights perspective, in particular the right to a fair trial.

We first set out the details of the EncroChat operation. Based on an analysis of Dutch case law, in combination with press releases of the French and Dutch law enforcement authorities, it became clear how French law enforcement authorities gathered 120 million messages and other data from an estimate of 60.000 EncroChat users. The operation was made possible by taking over servers at an internet service provider and hacking cryptophones with a hacking tool. The operation has already led to over 200 judgments of criminal courts in the Netherlands.

Dutch case law shows that the right to a fair trial in Article 6 ECHR proved important in three ways:

1 Providing transparency about the operation;
2 Providing a legal basis to test the reliability of the evidence obtained; and

3 Providing access to data used as evidence against suspects in a criminal case.

First, this article shows article 6 ECHR can be a transparency enabler. Keeping the operation secret challenges the right to a fair trial under article 6 ECHR, more specifically the principle of equality of arms. Part of the principle of equality of arms is transparency about the manner in which the evidence is gathered. Law enforcement authorities and the public prosecutor can have a legitimate interest to keep information about the operation secret. However, keeping this information secret is allowed only insofar as it is strictly necessary and must be counterbalanced by the procedures followed by the judicial authorities.

The analysis of Dutch case law showed how questions of the defence attorneys, with an (often implicit) basis in article 6 ECHR, led to discovery of details about the EncroChat operation in France (Phase 1) and how the data was shared by French authorities and further processed by Dutch authorities (Phase 2). It enabled the defence to challenge the legality of the operation and challenge possible abuse of power by law enforcement authorities. In contrast with most defence attorneys, Dutch courts found the EncroChat operation in France lawful and that evidence could be used in criminal cases. We also explained how a JIT allows participating States to share data with each other in a lawful manner. For the transferred data from the initial investigation (targeted EncroChat) to other investigations (targeting EncroChat users), an extra requirement, in the form of a judicial warrant, was used in the Netherlands. This way another (Dutch) judge will test the principles of proportionality and subsidiarity with regard to the processing of the EncroChat data, while taking into account the reproducibility of evidence and the protection of privileged communication. This should be viewed as a good practice in our opinion, because it provides additional protection to the fundamental rights of the individuals involved. Public prosecution services of other States may consider adopting this good practice of requesting 'an extra warrant' to create a subset of EncroChat data for criminal proceedings.

Second, the right to a fair trial also provides a legal basis to test the reliability of the evidence and the method of acquisition. Especially when (complex) software is used in the collection of data, this can have a major influence on the reliability of evidence because it challenges the confidentiality, integrity and availability (CIA-triad) of data. The Netherlands Forensic Institute reported that the hacking and interception software did not operate continuously, not all messages on EncroChat phones were intercepted during the entire operation and there had been instances of a mix-up in outgoing and incoming calls from EncroChat phones. However, these shortcomings did not lead to the

conclusion that *all* evidence from the EncroChat operation is unreliable. So far, Dutch defence attorneys failed to establish that the EncroChat data used as evidence was unreliable and no data has been excluded from evidence. We expect that defence attorneys in other States will also argue that EncroChat data used as evidence is not reliable. The public prosecution office and law enforcement authorities can prepare for this argument and explain why the particular EncroChat data that is used is reliable. In addition, we recommend that other sources of evidence are used besides EncroChat data. Multiple sources of evidence may validate each other and strengthen the case.

Third, the right to a fair trial enables the defence – to a certain extent – to access EncroChat data that may be relevant. Suspects need to be able to access the data in order (a) to review its integrity, (b) to review its reliability (because all EncroChat messages are sent under pseudonyms) and (c) to determine whether exculpatory evidence can be found in the dataset. The analysis showed that, while suspects cannot access *all* information collected in the EncroChat operation, they have a right to access data that is deemed relevant in their case. In addition, the defence should be able to reason why they require further access to EncroChat data, including data that is not part of the dataset created by the public prosecution service. They should also have the sufficient facilities (an 'effective opportunity') to access and analyse the data.

In the Netherlands, the defence can argue why they should be able to access both types of data based on key words and the use of filters. Sometimes access is refused because of ongoing (other) criminal investigations or for privacy reasons of individuals involved. The defence is facilitated in accessing the data at the Netherlands Forensic Institute and can use the same software as law enforcement authorities use to search and analyse the EncroChat data themselves. They can also request the data, which could then be provided to the defence in a readable format. Practitioners can learn from Dutch practical experience in providing access to EncroChat data. In our view, the public prosecution office and judiciary should prepare for requests of defence attorneys to access EncroChat data and States should invest in an infrastructure to facilitate these requests.