Encrochat

Stoykova, Radina

Published in:
Forensic Science International: Digital Investigation

DOI:
10.1016/j.fsidi.2023.301602

Forensic Science International: Digital Investigation 46 (2023) 301602

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

Encrochat: The hacker with a warrant and fair trials?

Radina Stoykova (Adi)

University of Groningen, the Netherlands

A R T I C L E I N F O

Keywords:
Digital forensics
Digital evidence
Fair trial
Reliability
Criminal procedure
Mutual trust
Police hacking
Presumption of innocence

A B S T R A C T

This paper introduces the *Encrochat* operation as an example of the technological, cross-border, and cross-disciplinary complexity of one contemporary digital investigation. The use of encryption for large-scale criminal activity and organized crime requires law enforcement to act pro-actively to secure evidence, to rely on cross-border evidence exchange, and to use more efficient digital forensic techniques for decryption, data acquisition, and analysis of volumized evidence.

The *Encrochat* investigation also poses the question whether the traditional fair trial principle can still ensure minimum state intrusion and upholding of legitimacy in the new ubiquitous investigation process, where digital forensics methods and tools for hacking and data acquisition are used to identify and arrest thousands of suspects and collect evidence in real-time during criminal activity. The operation is examined through the lens of the right to a fair trial, as codified in Art. 6 ECHR, in order to exemplify three challenging aspects. Firstly, in cross-border investigations there are no binding digital forensics standards in criminal proceedings or forensic reports exchange policy which demands reliability and compliance with Art. 6 ECHR-based evidence rules. Secondly, the defense's stand is not sufficiently addressed in current digital evidence legislation or mutual trust-based instruments at the EU level. Finally, the judicial process lacks scalable procedures to scrutinize digital evidence processing and reliability and is exposed to technology dependences. The identified gaps and their practical impact require a novel approach to digital evidence governance.

1. Introduction

The right to a fair trial, as codified in Art.6 ECHR (Council of Europe, 1950),encompasses fundamental principles of criminal procedure. Those principles are universally recognised and must be uphold to by all jurisdictions irrespective of the complexity and cross-border elements of contemporary investigations. This exposé provides a short description of the Encrochat operation followed by a delineation of the scope of the analysis of the fair trial principle in the context of such digital investigation.

1.1. Short description of the hack

The digital investigation of the encrypted criminal communication network *Encrochat* is one of the first in Europe on such a scale and demonstrates the coordinated cooperation between a French-Dutch joint investigation team (JIT),[1] Europol, and Eurojust (Eurojust-Europol, 2020). Europol suspected that *Encrochat* services were being used for the purpose of serious organized crime since 2017. Encrochat phones were equiped with anti-forensics technology to destroy evidence and to make law enforcement investigative measures difficult. All communication between *Encro*-devices was end-to-end encrypted (O'Rourke, 2020) making decryption warrants or server access warrants useless. They support dual operating systems – one for standard use and one modified. *Encrochat* installed their own encryption programmes, routing communication to their own servers and physically removed the GPS, camera, and microphone, GPS and USB port functionality from the phone (Zagaris and Plachta, 2020). Data port, recovery mode and debugging facilities were removed which prevent law enforcement forensic methods from accessing the phones (Gardiner and Sommer, 2021). The phones had other security features such as: Panic pin (instant handset wipe – wipes full phone contacts and messages with no back up memory); password wipe and wiping of the phone on request to the *Encrochat* dispatcher; messages seven days burn time to deletion on both sender

E-mail address: r.stoykova@rug.nl.

[1] A Joint investigation team (JIT) is a legal agreement between competent authorities of two or more States for the purpose of carrying out criminal investigations. See also Council Framework Decision 2002/465/JHA on joint investigation teams <http://data.europa.eu/eli/dec_framw/2002/465/oj > accessed 12.12.2021.

https://doi.org/10.1016/j.fsidi.2023.301602
Received 7 March 2023; Received in revised form 14 July 2023; Accepted 14 July 2023
Available online 22 July 2023

and receiver phones (Gardiner and Sommer, 2021). The communication was end-to-end encrypted using an OTR-based messaging app[2] which routed conversations through a central OVH-server based in France, EncroTalk, a ZRTP-based voice call service.[3] It also contained Encro-Notes, which allowed users to write encrypted private notes. A unique session key was generated for each communication. The session key was renewed for each message. The phones supported instant messaging, VoIP, IP calls. Encro-phones had an IMEI number, which can uniquely identify the device and a SIM card from the Dutch telecommunications provider KPN, but not necessarily the owner. Since encryption and decryption of messages was only possible on the phone, the only option to expose *Encrochat* as a network facilitating criminal communications was trough police hacking.

Eurojust hosted several meetings between French, Dutch, and UK law enforcement agents (LEA) and digital forensic specialists in order to prepare the infiltration of the network. Allegedly the French-Dutch JIT acquired a copy of the *Encrochat* server and some phones in order to understand how the encryption services worked (Gardiner and Sommer, 2021). Reportedly, the French digital crime unit (C3N) prepared a computer interception device to be deployed to the server and all terminal devices, which can record and redirect all DNS data streams to their servers. The technical device could also disable the wiping function on the devices and record or change the lock screen passwords (Cox, 2020). After seizure the data was further processed to the Europol server. The interception software was sent to all *Encrochat* phones as part of an update. According to an expert opinion of the digital forensics examiner *Campbell*,[4] who was not part of the operation, the implant was most likely designed to take snapshots of the messages in memory (during encryption/decryption while still in plain text) and to periodically send the data to the French C3N server. The service had around 60, 000 users (Mansfield-Devine, 2020) and it is unclear how many users were affected by the data interception measures. The JIT continued the data collection for a two-month period resulting in an "unprecedented amount of data" for evidence (Eurojust-Europol, 2020). The LEAs recorded the IMEI device number of the phones, the e-mail addresses, and the location of the respective radio cells. Europol actively supported the information exchange in the operation and further evidence exchange with other countries. Pursuant to European investigation orders (EIO),[5] parts of the data set were sent to the United Kingdom, Netherlands, Germany, Sweden, and Norway via the Europol's system. The *Encrochat* evidence collection resulted in a broad array of incidental, pending investigative proceedings in France (Zagaris and Plachta, 2020), an unprecedented number of arrests in the Netherlands and the UK, the seizure of illicit substances and weapons (Mansfield-Devine, 2020) and thousands of prosecutions and trials across Europe.

1.2. Scope of the analysis

This paper analyses the Encrochat investigation through the lens of the two fundamental principles enshrined in the right to a fair trial - equality of arms and presumption of innocence. Equality between the opposing parties means equal opportunity to present arguments and challenge the evidence and equal participation of the defence and prosecution in examining evidence. The presumption of innocence requires that *(i)* the members of a court should not start with the preconceived idea that the accused has committed the offence charged; *(ii)* the burden of proof is on the prosecution, and *(iii)* any doubt should benefit the accused.

The European Court of human rights (ECtHR) has a rich case law which interprets those principles and further delineates minimum requirements for criminal procedure and evidence handling. More comprehensive analysis is done elsewhere (Stoykova, 2022) but in extreme summary the derived requirements from the equality of arms principle are:

- *Fair procedure to evaluate the lawfulness and lawful use of evidence*
- *Possibility to challenge evidence: fair disclosure and information about evidence*
- *Sufficient time and facilities to prepare the defence evidence*
- *Possibility to maintain equality of arms against expert evidence*
- *Legal assistance in crucial stages of the evidence handling*

The presumption of innocence protection against wrongful conviction can be translated into three further requirements for:

- *Accurate Fact-Finding*
- *Protection against prejudicial effects in the evidence procedure*
- *Protection against reverse burden of proof*

The Encrochat case study demonstrates the real and imminent challenges with those legal requirements in digital evidence and digital forensics context. The analysis does not provide a comprehensive examination of all digital evidence challenges and their relation to fair trial, and neither will it be able to shed light on all legal questions arising from the *Encrochat* case, not least due to scarce availability of reliable facts. Rather, the *Encrochat* case has been selected as a case example for the complexity of cross-border, large-scale, digital investigations and where they can come into conflict with the fair trial safeguards. The *Encrochat* operation raises many questions in relation to the deadlock situation with criminal use of encryption and the lack of a consistent legislative approach. It also raises serious concerns in relation to data protection and telecommunication secrecy legislation. However, these separate issues are examined here only to a very limited extent, where they are related to digital evidence reliability and fair investigative procedures. It is rather an exemplary study on the *Encrochat* evidence reliability and quality of procedure in relation to the selected fair trial requirements. The aim is to identify incentives for a principle approach for further regulation and improvements in digital evidence procedures.

The fair trial principle provides that what is essential for procedural justice is the legitimacy of the investigative process and all stages thereof. In this sense, *Encrochat* evidence is only a result of a process with several stages and stakeholders, but the legitimacy and quality of this process, and not the results of it, are decisive for achieving a fair trial.

2. Lawfulness and fair use of the *Encrochat* evidence

The procedural and material scope of Art. 6 ECHR includes preliminary investigations[6] and cross-border cooperation for evidence

[2] Off-the-Record Messaging (OTR) is a cryptographic protocol that provides encryption for instant messaging conversations.

[3] ZRTP is a cryptographic key-agreement protocol to negotiate the keys for encryption between two end points in a Voice over IP (VoIP) phone telephony.

[4] Regina v A and Others [2021] EWCA Crim 128 [2021] QB.

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

[6] See Salduz v. Turkey ECHR 2008-V 59, paras 52–54; Dvorski v. Croatia [GC], App no 25703/11, (ECtHR 20 October 2015), para 77; Campbell and Fell v. the United Kingdom, App no 7819/77; 7878/77 (ECtHR 28 June 1984) paras 95–99; Imbrioscia v. Switzerland, App no 13972/88 (ECtHR 24 November 1993), para 36.

collection[7] such as the *Encrochat* operation. However, the nature of the Encrochat operation and its full scope are not entirely clear. At the EU level criminal investigation is defined as measures by a competent law enforcement authority for "establishing and identifying facts, suspects, and circumstances regarding one or several identified concrete criminal acts".[8] It is unclear if the police had identified criminal acts before the *Encrochat* evidence gathering, but considering the large amount of suspects and data collection, it is more likely that the operation can be classified as a criminal *intelligence* operation "to collect, process and analyse information about crime or criminal activities with a view to establishing whether concrete criminal acts have been committed or may be committed in the future".[9] The authorities in *Encrochat* acted at least with respect to some users proactively, they targeted the *Encrochat* organization, and prosecution cannot be the only objective of the operation since Europol commented that one of the objectives was to analyse the extent and operations of organized crime networks (Eurojust-Europol, 2020). The operation, therefore, has an element of targeted intelligence surveillance and a coordinated cooperation for preliminary investigation and digital evidence collection, which requires an examination whether and to what extent such operations fall within the scope of Art. 6 ECHR and when fair trial safeguards are invoked.

In some countries the mere collection of data is not considered enough to trigger Art. 6 ECHR safeguards. *Sunde* reports that the Norwegian Supreme court held that the mere copying of the data is not search and seizure, and only when the police are able to pick relevant files as evidence do suspect rights apply (Årnes, 2018, p.55). In the context of data protection, the Court of Justice in EU stated, to the contrary, that the mere access, retention, and communication of personal data to a third party, such as a public authority, constitutes an interference with the right to a private life, irrespective of the subsequent use of the information.[10] In the same vein, the ECtHR seems to be in favour of the view that the procedural guarantees of Art. 6 ECHR are invoked in the early stages of an investigation, when the investigative measures are directed to concrete suspects, which arguably includes targeted data collection for evidence. This interpretation means, that in the *Encrochat* case Art. 6 ECHR safeguards are triggered when the technical implant is distributed to suspects phones and the data is accessed by law enforcement, irrespective of its subsequent use.

For legal purposes, in most documented sources the *Encrochat* operation is classified as phone interception, however its technical characteristics relate it more closely to computer surveillance. As will be examined further, the authorities acquired Encro-phone data by the use of a technical implant which captures data in a volatile memory. In technical terms, volatile memory is a combination of data that is part of the transmission, and additional temporary processed data that is not intended for storage or transmission such as passwords and encryption keys. Both types of data can be obtained only with computer surveillance technology because phone interception does not capture data that is not yet stored, in between transmission, or that is never intended to be stored or transmitted.

Computer surveillance is a very intrusive investigation measure because it interferes with the right to privacy, data protection, and telecommunication secrecy and in addition may interrupt the security of the computer systems. While the first two interferences are well documented in ECtHR case law, the impact of law enforcement actions on the security of computer systems is rarely discussed. Given the secrecy of surveillance operations, the ECtHR held that applicants have a claim, even without factual proof,[11] as long as the Court is satisfied that "there is a reasonable likelihood that some such measures have been applied".[12] Arguably, computer surveillance encompasses very specific and intrusive investigative methods which require specific regulation with scope and safeguards distinct from interception given the reasons stated above. However, legislation is still underdeveloped or non-specific, which results in discrepancies between the legal categorization of the act and its technical features. This analysis advances the argument that the operation was in fact computer surveillance, but for the sake of aligning it with its official legal categorization as computer (phone) interception, those terms are used interchangeably.

The lawfulness and fair use of the Encro-phone evidence is evaluated first with respect to the requirements for quality of law and procedure in Art. 6 ECHR in conjunction with Art. 8 (2) ECHR and the procedural safeguards in Art. 6 ECHR for intrusive investigative measures. Further, the fair trial requirements are examined in the context of cross-border cooperation and in respect to the European mutual-trust-based investigative instruments. The analysis takes into consideration legislative evaluation and ECtHR case law in regard to both computer surveillance and interception.

2.1. Fair procedure to evaluate the lawfulness of Encrochat evidence

In evaluating whether the French interception of the *Encrochat* phones amounts to a violation of Art.8 ECHR, applying the established ECtHR's methodology will require to take into consideration whether there was an interference with individual rights, whether the measure was in accordance with the law, whether it pursued a legitimate aim, and if it was "necessary in a democratic society".

Allegedly, the *Encrochat* data collection from the encrypted devices was conducted according to the French criminal code (CCP-F). In France judicial interception measures are an "*extrema ratio* where other investigative methods would be unsuccessful or unavailable (under the principle of subsidiarity)." (Galli, 2016) The investigating judge, after obtaining the opinion of the public prosecutor, can issue a warrant to authorize the investigators to place an interception device in order to access data in all places and to record, store and transfer these data without the consent of the individuals concerned (Article 706-102-1 of the Code of Criminal Procedure). (EJN, 2022) Law 204/2004 extended the possibility to use judicial interceptions to preliminary and *in flagrante* police investigations (i.e., to cases where no *instruction* had yet been instituted) for a limited number of serious offences listed in article 706(73) of the CPP-F. They are authorized (and supervised) by the *juge des libertés et de la detention* on the application of the district prosecutor and cannot last longer than 15 days, renewable once under the same conditions of form and duration (Galli, 2016).

However, it is unclear which of those provision of the CCP-F were the legal bases for the computer surveillance. France also has a detailed law on domestic and foreign intelligence collection for law enforcement purposes which, however, requires a different authorization and supervision regime than judicial warrants (FRA, 2017). The law in France on international surveillance states that only "the prime minister can authorize the exploitation of targeted content data and metadata […] The French oversight body only performs ex post controls over the implemented measures." (FRA, 2017) There is no information on the authorization of this type having been granted or not. The legal bases and the procedure followed for the operation as well as to what extent the LEAs had reasonable suspicion about concrete suspects remains protected as military secret.

[7] Stojkovic v France and Belgium, App no 25303/08, (ECtHR 27 October 2011), para 41; Soering v UK, App no 14038/88 (ECtHR 7 July 1989), paras 85–88; Pellegrini v. Italy, App no 30882/96 (ECtHR 10 July 2001), para 40.

[8] ibid., Framework Decision 2006/960/JHA, Art. 2(b).

[9] ibid., Art. 2 (c).

[10] Opinion 1/15 on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, Opinion of the Court (Grand Chamber), 26 July 2017, §§ 124–125.

[11] Klass and Other v. Germany, App no 5029/71 (ECtHR 6 September 1978).

[12] Halford v. the United Kingdom ECHR 1997-III 1016, paras 47 and 48, and 53–60 and Ilya Stefanov v. Bulgaria, App no 65755/01 (ECtHR 22 May 2008).

In relation to the "quality of the law" requirements of the ECtHR, it could be considered that the French authorities allegedly ensured several safeguards. The seriousness of organized crime offences and the fact that the *Encrochat* network was end-to-end encrypted could justify the interception as a last resort measure. Official court documentation states that the French authorities obtained a judicial order to copy the server, judicial approvals for the use of a computer data interception device both on the server and on the terminal devices connected to this server and further judicial approval for redirection of all the data streams (DNS redirection) of the server in Roubaix. (OLG Hamburg, 2021, para 75) The reported time limit for the data collection was two months (Eurojust-Europol, 2020).

However, the lack of information on the quality of the investigative procedure does not exclude possible irregularities and violation of Art.8 (2) ECHR. In particular, it remains unclear whether the French judicial interception on such a broad scale is in accordance with the law in the meaning of Art. 8 (2). The ECtHR in the *Khan* case stated that the principle of legal certainty requires matters of intrusive surveillance measures to be regulated by law, which idicates clearly the scope of the discretion of the competent authorities and the manner of its exercise, especially when the technology available for use is continually becoming more sophisticated. This means that military guidelines and procedures are not appropriate basis for an operation like Encrochat. It is unknown what was the legal basis and time limit of the judicial warrants authorising the operation. Since the investigation was conducted by military proceedings and protected under the national security exemption, it can be assumed that the judge had limited opportunity to scrutinize the operation. If the French judges were not informed, for example, about the risks of the hacking operation, why a specific method was preferred over others, or what its accuracy was, the obtained warrants may serve a purely administrative compliance. At some point, the French NCA reported that 90% of the *Encrochat* users were using the service for criminal activity(Cox, 2020), and the NCA did not find any evidence of innocent suspects using it (Wright, 2020). Nevertheless, the *Hamburg* court reports that "32,477 users in 121 countries were affected by the data interception measure. Of these, 380 users were wholly or partially on French territory, of whom, according to the French authorities, at least 242 people - more than 60% - used the encrypted communication system for criminal purposes." (OLG Hamburg, 2021) This means that up to 40% of the people affected may have used the service for legal purposes, such as to protect their privacy. It is not stated how much of the *Encrochat*-data obtained in other jurisdictions was related to innocent individuals. There are no reports of whether and how the JIT authorities filtered out innocent people's messages after the initial data seizure. Such information is essential to evaluate how the investigative measure scope was limited, if it was in compliance with the presumption of innocence, and if effective remedies were taken to limit the impact of the PI and privacy infringements considering the broad scope of the interception. Moreover, given the *Encrochat* software architecture it was technically impossible to craft the interception implant to be deployed only to specific phones for which reasonable suspicion existed and for which the LEA had information that they were involved in criminal activity, and not in bulk.

Further, it cannot be assumed that the surveillance of such a large number of potential suspects *was based on facts* in each individual case. It is unclear if the French authorities complied with the ECtHR requirement of judicial oversight and notification throughout the entire surveillance operation – not only when it was first ordered, but also while it was being carried out or after it had been terminated. There is no information as to whether the surveillance was carried out by competent experts as required by Article 706-102-1 CCP and if there was an authorization for exploitation of the dataset.

Allegedly, the French authorities refused to disclose information on the interception technology or to provide a prosecution witness to be questioned in regard to this matter (Gardiner and Sommer, 2021). It was reported that the information exchange of the JIT seized data sets was facilitated by Europol's system Siena. However, there is no information on how the integrity of the initially seized, raw data from the interception device was preserved. There is no audit trial of the procedure observed to further examine, use, and store the *Encrochat*-data. It was also unclear if the data set was modified or filtered before it was exchanged with Europol and other countries. Considering, that some of the Encro-users were using the service for legitimate purposes and to protect their privacy, the JIT would be supposed to have employed a procedure for erasure and destruction of such data, as the ECtHR requires a data destruction procedure where an accused has been discharged by an investigating judge or acquitted by a court.

It becomes apparent that contemporary investigations like *Encrochat* have the methods and technology to identify suspects *ab initio* and collect digital evidence in real-time, which does not fit well with traditional lawfulness requirements for reasonable suspicion and identification of concrete crime. Considering the lack of documentation of the procedure, it cannot, at least in theory, be excluded that the bulk computer surveillance of the *Encrochat* network could be in violation of Art. 8 (2) ECHR. However, even if the *Encrochat* evidence was potentially unlawfully obtained, this does not automatically yield a violation of Art. 6 ECHR. Therefore, further considerations must evaluate if the use of such evidence could affect the overall fairness of the criminal proceedings.

2.2. Fair use of Encrochat evidence

ECtHR requires LEAs to uphold higher scrutiny for the use of special digital investigation methods and technology and account for irregularities in the way evidence is obtained for the prosecution. NFI forensics specialists stated that "attribution, evaluation, interpretation and reconstruction of digital traces and their origin often requires additional digital forensic science expertise, methodology, and technology beyond the competence of investigators" (van Baar et al., 2014). This means that the digital forensics work on the case had to be documented and produced in digital forensics reports and comply with forensic science standards.

Further, ECtHR identified three criteria for a fair use of the *Encrochat* evidence:

1. Quality of the evidence (whether the circumstances in which it was obtained cast doubt on its reliability or accuracy)
2. Contestability (opportunity of challenging the authenticity of the evidence and of opposing its use)

if those two criteria are in question, then the third one requires:

3. Supporting evidence (questionable evidence must be evaluated in the light of supporting evidence[13]

Each of these criteria is examined further to evaluate the *Encrochat* evidence and its fair use in criminal proceedings.

2.3. Accuracy and reliability of the Encrochat evidence

There are several factors in the Encrochat operation that might have impact on the reliability of the evidence. *Encro*-phones were designed to prevent mobile forensics and to limit law enforcement's ability to investigate digital data related to criminal activities. The digital forensic examiners had to developed *ad hoc* methods to infiltrate the network and collect the data, but this aspect has been largely overlooked by the press and the legal examination of the case so far. The Netherlands Forensic Institute (*NFI*) acknowledged that they cooperated with the French RCGN –the Cyberunit of the French gendarmerie – in the project

[13] Prade v. Germany, App no 7215/10 (ECtHR 3 March 2016), paras 34–35.

Cerberus, which developed the "advanced methods and techniques to crack encrypted information of criminals" used to infiltrate the *Encrochat* network. France denies any Dutch participation in the operation itself. Nevertheless, the *NFI* was responsible for a sub-project which developed "methods specifically for anti-GPU algorithms, a security that is increasingly used today, including in mobile phones". Interestingly, with such methods a vulnerability in the Direct Memory Access (DMA) capabilities of a mobile GPU can be exploited for a privilege escalation in order to circumvent the encryption(Danisevskis et al., 2014), which corroborates with the UK expert witness testimony on how the *Encrochat* phones were accessed.[14] In any case the quality of the *Encrochat* investigation process cannot be accessed without evaluation of the scientific validity of the digital forensics work. As the digital forensic methods and tools are *ad hoc* developed the only possibility to assess their reliability is to get access to forensic reports and chain of custody documentation which can demonstrate data integrity preservation and reliability validation. (Sommer, 2022), (Antwi-Boasiako et al., 2017)

Digital evidence is volatile and could be, intentionally or not, tampered with or modified – it also depends on technical environment (information availability and forensic acquisition standards) and legal procedure (access and collection procedural rules). The legal evaluation of the reliability of digital evidence depends also on the justification and appropriateness of selected digital forensic process, methods, and tools for each step of data acquisition, examination, and analysis.

However, accuracy and reliability assessment of Encro-evidence is burdensome due to the complexity of the operation. In each of those steps, different tools, methods, and examiner expertise were used. They need to be sufficiently documented to be cross-examined according to digital forensics standards by all parties in the criminal proceedings. As digital forensics standards might vary according to jurisdiction, the starting point for evaluation is compliance with the tree fundamental principles in all forensic sciences: *integrity* (maintain and safeguard the integrity and original condition of digital artefacts); *reliability* (documentation that demonstrates that a forensic tool, technique, or procedure functions correctly and as intended); and *chain of custody* (the record identifying the chronology of the movement and handling of digital artefacts). They are elaborated in international digital evidence and digital forensics standards (ISO/IEC 27037:2012;ENFSI, 2015; Interpol, 2019). Further, EU and CoE have jointly adopted a guide for law enforcement, prosecutors, and judges, for quality assurance in work with electronic evidence which also contains minimum requirements for search and seizure, live forensics, and chain of custody (Jones et al., 2014). ECtHR also requires procedures to be followed for examining, using, and storing the data for evidence and summary reports to communicate the recordings intact and in their entirety with the defence and the judge.[15]

2.3.1. Data integrity

In terms of data acquisition and its integrity in the *Encrochat* case, the examiners could only predict potential alterations and errors since they did not have access to the device itself. The technical implant on the phone had taken snapshots of the volatile data and redirected it to the LEA server. A forensic examiner can explain which measures were taken to ensure secure transmission and data preservation. Hashing a master copy or a zip file for each acquisition ensures that no changes were introduced into the data after its initial acquisition during further digital forensic activities performed on the working copies. Further, the ISO recommends the data to be acquired in static binaries with the use of expert competence and validated tools. If inconsistencies in the acquired data exist, this should also be documented in the forensic report (ISO/IEC 27037:2012).

As previously discussed, in several jurisdictions access to the *Encrochat* raw data was requested. Raw data is defined as "data that has been extracted or acquired in a form that is unmodified by the analytical process." (ENFSI, 2015) Since law enforcement did not have access to the data on the phone (the original data source), they had to perform remote data acquisition which is a forensic methodology for processing of volatile data[16] to preserve its integrity and accuracy. If the examiners followed digital forensic standards the data acquired from the technical acquisition device is the raw data. The technical implant data is the forensic copy and therefore the only "original" forensic evidence. It is an original because it is created under controlled forensic procedures, which allows to determine its authenticity and integrity. A standard procedure is that a forensic copy is stored first as back up on a storage server, and another copy is sent to an examination and analysis platform. On this platform the forensic copy is pre-processed to filter out redundant or irrelevant data, to classify and authenticate meta data, and to attribute the relevant content data to concrete suspects. The forensic copy preserves integrity information in relation to the device (phone IMEI, suspect (owner) and country) and to the messages (time stamps and data formats) and potentially information for the digital forensics process. It is unclear if Europol's Siena system was used for exchange of the "original" forensic copies, only to store and exchange the reports after the pre-processing steps, or also as an examination and analysis platform. Each of the digital forensic techniques require several processing stages and secure storage locations (see Fig. 1).

The acquired data set quality's may not be very good considering all the obfuscation techniques built into the phones to destroy meta and content data, and geo location tagging. It is peculiar that some sources report that the *Encrochat* company removed GPS, camera, and microphones on all phones, while the authorities reported that criminals were openly messaging and sending pictures of their criminal conduct. It remains an open question if the integrity of the data set in each individual case can be validated by forensic examiners, to what extent the obfuscation methods used affected the data presented as evidence, and if the metadata related to chats is sufficient in order to establish the connection between the conduct, the phone, the suspect and the data. In any case these questions can be answered by digital forensics examiners in expert reports, otherwise the data itself has limited probative value and raises questions about its integrity and admissibility.

2.3.2. Reliability of forensic methods and tools

The European Network of Forensic Science Institute (ENFSI) has published a best practice manual for the forensic examination of digital technology (ENFSI, 2015). The institute stresses the lack of "any [internationally] recognized quality standards" for digital forensic processes and systems, resulting from the lack of transparency (Council of the European Union, 2011). The manual emphasizes the importance of procedures to verify and validate the evidence processing at the process level, as the processes include multiple human-based and instrument-based functions. Since in digital forensics it is never possible to validate tools exhaustively, or to guarantee data accuracy, ENFSI recommends routine inspections of the generated output for issues and full documentation of the digital forensics process.

Crafting a technical implant, placing it as an update on the *Encrochat* server, and harvesting a phone's volatile memory requires an understanding of the security architecture of *Encrochat* network, extensive testing of the technical implant, and a secure storage server for data and backups. The operation required live network forensics, mobile forensics, and presumably several techniques for data pre-processing, examination, and analysis. Live network forensics refers to collection of

[14] Regina v A and Others [2021] EWCA Crim 128 [2021] QB 791 – Witness statement by officer Campbell of the National Crime Agency cybercrime unit <https://madden-finucane.com/files/2021/02/2021-02-05_r-v-a-b-c-d.pdf> accessed 12.12.2021.

[15] See Huvid. v. France, para 34.

[16] Defined in ISO/IEC 27037 as data that is especially prone to change and can be easily modified.

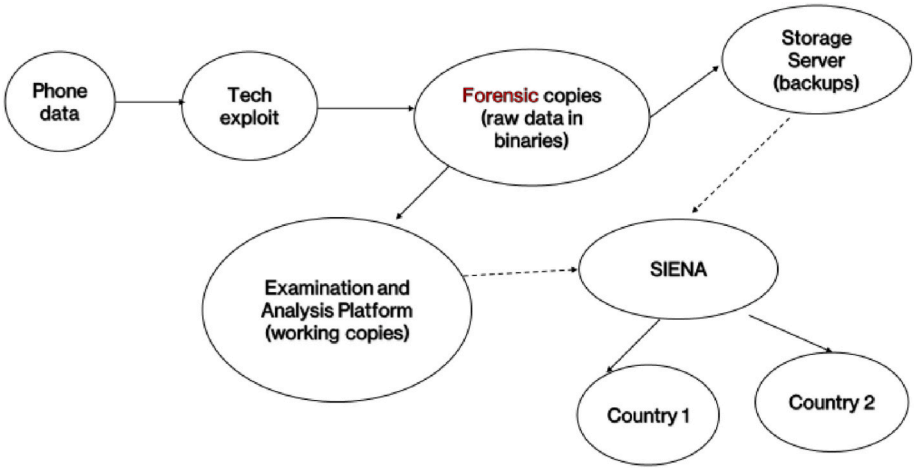

Fig. 1. Potential data processing operations in Encrochat

digital evidence from running systems (Adelstein, 2006). Potentially, this was necessary to examine the *Encrochat* server, to place the interception device as an update to the system, and to perform remote acquisition of volatile data from the handsets. The *Encrochat* remote live acquisition of volatile data is not a straightforward forensic process since it always results in some minimal alterations on the device, creates only a logical copy of the data, and evidence dynamics can occur at every stage of the transmission. In such case a standard practice is that the forensic examiner must be able to "explain the recovery process involved and assure the court that any data loss would not adversely affect the remaining evidence presented." (Boddington et al., 2008) Moreover, live recovery does not create a bit-for-bit image of the target drive. It takes a snapshot of the targeted part of the system, which is not always reproducible later. Mobile forensics standards define the vulnerability exploitation of a system as a decryption method to access the phones. Decryption methods for mobile forensics are still a research area and there is no agreed standard for methods, disclosure, or validation (Fukami et al., 2021).

In such cases, *Edmond* proposed reliability as an obligatory legal requirement in order to foster legal evaluation of forensic findings in addition to a system for resolving preliminary questions on evidence reliability (Edmond, 2012a), (Edmond, 2012b) He further argues, that "reliability must be determined independently of other evidence and should not be adjusted because of the anticipated value of other evidence, the strength of the overall case, or through the classification of some evidence as 'additional'." Arguably, an independent digital forensic examination should be facilitated considering the large scale of the operation and the need to minimize errors and bias. Under a non-disclosure agreement, the validity of the technical operation can be scrutinized at least in the JIT work (as not all of the forensic processing is protected as a military secret). Even in respect to secret investigative measures there are validation methods which do not require full disclosure, e.g., black-box testing. *Sommer* provided a detailed analysis of the operation in the view of several digital forensic standards and concluded that covert investigations result in complex questions about the reliability of the tools, methods, and preservation techniques used as well as lack of audit trails to enable its cross-examination by other parties in the criminal proceedings (Sommer, 2022).

Even if we agree that the police hacking method should be kept secret, the complete refusal of forensic reports on the Encro-operation is arguably disproportionate and limits the possibility for scrutinizing digital forensics methodology. However, the international digital forensic standards, guidelines, and best practices are not binding, while the cross-border investigation and cooperation regime in Europe has no binding rules of procedure for the use of digital forensic science for criminal proceedings. The lack of digital evidence regulation in cross-border cases impacts not only the forensic reliability evaluation of such evidence, but also is to the disadvantage of the defence and limits the judicial process to scrutinize such evidence on valid grounds. Questions can be raised as to the appropriate procedural protection for suspects and defendants against arbitrary interference or exaggerated or misleading expert evidence specially in cross-border scenarios. It also imposes challenges to the presumption of innocence in relation to accurate fact-finding, evidence prejudicial effects, and reverse burden of proof. For example, it must be examined if prejudicial effects are not accidently embedded into the way technology is used e.g. by deliberately using the tool to collect and examine only incriminating data. Not only the large scale of the evidence collection and the fact that it was performed periodically need to be taken into consideration, but also that *Encrochat* information can be coupled with big data analytics to examine and analyse it for further attribution, which renders the potential further use of Encro-data for prosecution very broad. This might have much more severe consequences for the presumption of innocence as it may create a state of constant suspicion for a large number of individuals.

After the technical device initially seized data from Encro-phones, it became clear that a significant number of individuals, potentially up to 40% in France, were using the service for legitimate purposes – to protect their privacy, confidential information, intellectual property etc. Moreover, some of the correspondence might have been related to privileged (e.g., lawyer, physician, priest), or otherwise confidential or sensitive personal data. The authorities must provide information on how data of innocent suspects was protected, erased, or destroyed, and to notify the respective jurisdictions. The lack of such information once again testifies about the limited accountability in cross-border investigations.

2.3.3. *Chain of custody*

The chain of custody documents chronologically the history of the digital evidence from the time it was identified, collected or acquired by the investigating team up to its present status and location (ISO/IEC 27037:2012, para 6.1)

The physical and logical chain of custody must be documented with respect to all stages of the processing in order to verify the integrity preservation of the data and the reliability of the methods and tools used. The physical chain of custody provides the information for the proportionality assessment of the technique, to establish who had access to the data, and to identify potential errors in processing. The logical chain of custody assists in assessing the quality and probative value of the processing from the technical point of view, while legally it ensures that evidence can be challenged on valid grounds, and bias and parallel construction of evidence are exposed. The fact that no chain of custody can be established, at least with respect to the cross-border cooperation

in *Encrochat*, means that parallel construction of evidence or loss of exculpatory evidence are not excluded.

Sommer reported that the UK authorities preserved the data obtained from Europol and the chain of custody of its further processing, but they had no information on the processing before that (Gardiner and Sommer, 2021). It is notable that no information on digital forensic reports or compliance with forensic science standards has been provided so far in the *Encrochat* operation. However, it is desirable that expert evidence is presented and evaluated as such, even in large-scale investigations, instead of portraying it as a technology-assisted investigative operation obfuscating the methodological shortcomings.

2.4. Contesting Encrochat digital forensics expertise

The ECtHR requires the defence to have the opportunity to confront the forensic expert and her findings. The prosecution has an obligation to "disclose to the defence all material evidence in their possession for or against the accused."

In theory, in order to challenge the *Encrochat* evidence on valid grounds the defence must have access to the original forensic copy to cross-examine it against the information attributed to the defendant and to search for exculpatory data. Currently, there is no information about the accuracy and integrity preservation of the "original" forensic copy and backups generated. Judges most probably will have to rely on the data provided by Europol in each country, which as shown consists of only a part of the acquired forensic copies. Such data is a result of several pre-processing operations. Nevertheless, the appointed digital forensic experts in each respective jurisdiction can perform a digital forensic examination of the derivative dataset as long as France provides access to the raw data for comparison.

Even if reports on the French operation are kept secret, after Europol distributed the data sets to other jurisdictions, individualized investigations were brought up against suspects. In principle, The ECtHR identified the need to know how relevant data was selected[17] while all relevant material or evidence must be made available to both parties.[18] It was made clear that France will not appoint a digital forensic expert for any of the subsequent trials in other jurisdictions (Gardiner and Sommer, 2021). It is unclear also if the defence in each subsequent trial will be presented at least with an individualized digital forensic report to cross-examine the findings of the forensic examiner who has worked to identify the relevant data in the concrete investigation. It is understandable that law enforcement must protect sensitive forensic methodology, know-how, and tools. This is a relevant ground for non-disclosure of the technical device, the infiltration of the network, and the decryption methods. However, this is just a small part of the forensic acquisition, and it is unclear why other processing steps for examination and analysis of the data have not been presented. In each individual case a forensic report can examine the derivative dataset and provide information on the forensic paths, time stamps, MD5 hash verifications, reporting on missing or corrupted data, or exculpatory observations by the forensic examiner, probabilistic findings, and confidence level in respect to the forensic authentication and identification of the relevant data sets. These are all standard digital forensics requirements, performed with known tools and methodology which can be presented for validation if *Encrochat* evidence is to be used as forensic evidence in criminal trials. The defence and judges must at least have information on the mandate of the forensic examination and analysis of meta and content data, how the data was preserved, and the temporal, link and functional analysis performed to attribute it to suspects/defendants (Pollitt et al., 2018). Excerpts of chat communication without the necessary digital forensic metadata and interpretation cannot be considered authentic or trustful.

The lack of a procedure obliging law enforcement to produce evidence accountability information is conveniently disguised under layers of computer-facilitated operations and human-machine interactions. Each of these operations might be inaccurate, biased, or erroneous and preclude the opportunity of the defence to fair examination at a very early stage of the investigation. And this possibility exists with respect to thousands of criminal cases relying on *Encrochat* data. If attribution and individualization of *Encrochat* evidence regarding a concrete crime and suspect cannot be procedurally examined, there is no guarantee that the authorities did not plant/construct evidence, targeted suspects to obtain higher convictions, cherry-picked suspects, or used it as leverage to obtain confessions. The lack of forensic reports or information on the data presented as evidence in subsequent investigations might result in treating the suspect as convicted and put her/him in a position to prove his/her innocence. If context or content data is erroneously, partly, unintentionally omitted this could hamper the evaluation of the degree to which the defendant was involved in the criminal activity and therefore the severity of her/his conviction. Allegedly, a large number of chat messages were missing or appeared as duplicate entries (Gardiner and Sommer, 2021) and it is unclear if the messages were corrupted, intentionally deleted, or tampered with in any way during processing.

Encrochat evidence was challenged on many reliability grounds in Dutch courts. This includes claims that the *Encrochat* evidence is of unknown origin, unreliable, and untestable[19] the ownership and use of Encro-phones, accounts and chats cannot be clearly attributed to concrete suspects or crimes[20]; one phone might have been used by several users; the *Encrochat* conversations presented are incorrect, edited, incomplete, and out of context which aims at drawing an unjustifiably incriminating picture.[21] Respectively some magistrates provided the opportunity for the defence to present an overview of conversations recorded in the Dutch surveillance file that they wish to investigate further. Another judge authorized an additional official report with regard to the (degree of) reliability of each of the measurements included in the file that led to the attribution between the phone, data, and suspect, further analysis of the "running parallel" of a normal telephone set and an *Encrochat* set, and an official report on the operation and the processing by the reporting officers of source material transferred from the Dutch investigation (operation *Lemont*) to the conversations shown in the case file with the possibility for the defence to question police officers and their official report. It appears that forensic science reports and objective measurements for reliability validation of data integrity, methods and tools, and of the attribution of data to individuals, are not yet produced by the prosecution, but the courts seem to be satisfied with police officers' testimony and their hearsay reports based on a confidential report.

The missing, corrupted, or duplicated *Encrochat* entries can be compared to a similar situation in the *Mirilashvili* case examined by ECtHR. The court stated that if the defence could not support claims of intentional destruction or manipulation of the recordings and the case file does not reveal any reason to believe that the authorities acted in bad faith, the government cannot be held responsible for not disclosing information they did not have or that might have been lost.[22] This reasoning of the court is problematic, especially with respect to the requirement that novel approaches to crime investigation must ensure "adequate procedural safeguards", including most notably clear and foreseeable standards of proof. The burden of proof should be on the prosecution also with regards to processing the data according to data integrity preservation principles and to account for existing

[17] Rook v. Germany no 1586/15, 25 July 2019.
[18] Ruiz-Mateos v. Spain no. 12952/87, 23 June 1993.
[19] Court of The Hague, ECLI:NL:RBDHA:2020:13315.
[20] Court of The Hague, ECLI:NL:RBDHA:2021:284; Zeeland-West Brabant Court, ECLI:NL:RBZWB:2021:732; Court of The Hague, ECLI:NL:RBDHA:2021:2242.
[21] Court of Rotterdam, ECLI:NL:RBROT:2021:396.
[22] Mirilashvili v. Russia, § 212 and Jasper v. UK § 57 – cited above.

inconsistencies and possible errors. Moreover, it is unclear how the defence can support claims about data inconsistencies, when not allowed to examine the "original" forensic copy against the data adduced in the case file. As stated in *Bendenoun* case[23] the defendant might be in a possession of her/his own files and records to support claims of inconsistencies or missing documentation. However, the *Encrochat* cases are different since the Encro-phones were equipped with automatic deletion or destruction of messages, which means that by the time of indictment the defence might no longer be in possession of the information which might be exculpatory or reduce a sentence. In this case, the only *Encrochat* evidence that could be examined is in the possession of the prosecution.

Considering that the lawfulness of the evidence collection is questionable and that there is insufficient information on the reliability of the process, methods, and tools for data processing, *the significance of the Encrochat evidence is expected to be limited.* The origin and integrity of the derivative data cannot be evaluated and, therefore, there is no possibility to evaluate the authenticity and reliability of the *Encrochat* evidence. The data sent from Europol's Siena system to the respective jurisdictions must be evaluated in each individual case by competent digital forensic examiners. Under a non-disclosure agreement, the examiner could potentially verify the data obtained for concrete suspects against the hashed master copy and to comment on the quality of the data. However, such a process will require thousands of forensic examinations in each subsequent investigation and access to the French master copy which most likely will not be granted. This demonstrates that even the Europol systems do not support digital forensics standards for evidence reliability validation and reporting. There are no documentation and validation procedures implementable or enforceable for the methods and tools used in the *Encrochat* operation. If the courts accept the Encro-evidence, its reliability and probative value must be scrutinized in the trial proceedings, and it is questionable if this can be done efficiently.

In summary, irrespective of the impressive digital forensics methods and tools which enabled the *Encrochat* operation and despite the significant improvement in coordinated cross-border cooperation by law enforcement, what matters for a fair trial is the accuracy, reliability, and lawfulness of the digital forensics process. The identified inconsistencies show that the defence and the trial process as a whole are put in a disadvantageous position to scrutinize evidence in respect to the sophisticated and scientific methods of investigation. It can be argued that if digital forensic standards were not met and processes documentation was not kept from the first handling of the data for evidence purposes, any further procedures for disclosure and orality are quite limited in their ability to evaluate evidence reliability. It can be concluded that large-scale, digital investigations must be complemented with legislation establishing minimum process-level digital forensics standards which will provide documentation on evidence reliability, and its lawful and fair processing.

3. Possibility to challenge *Encrochat* evidence

Arguably, the evidence rule to be informed and so to have the possibility to challenge the evidence means that not only the *Encrochat* evidence can be potentially challenged, but also the defence has a legitimate interest in understanding the processing operations for data examination and analysis as additional information to evaluate the evidence trustfulness and completeness.

Consequently, the *Encrochat* evidence may result in thousands of disclosure requests, exculpatory evidence collection, and expert evidence requests to examine its reliability. This could potentially overburden the judicial and disclosure process considering the volume of data collected. For each individual case, Art. 6 ECHR will require a procedure whereby it could be established whether the evidence in the possession of the prosecution that had been excluded from the file might have reduced the sentence or put into doubt the scope of the alleged criminal activity.[24] The ECtHR even required the defence to be involved in the definition of the criteria for determining what may be relevant and to conduct further searches for exculpatory evidence.[25] Moreover, the judge must be in a position to "monitor the relevance to the defence of the withheld information both before and during the trial".[26] That kind of scrutiny might never be achieved in each individual case resulting from the *Encrochat* operation. Moreover, the defence might need assistance with forensic aid, access to datasets and forensic software which in the spirit of *Rook* should be granted. Considering the secrecy and unclear nature of the cross-border cooperation it is most likely that the evidence rules on the possibility to challenge and disclose evidence will be exercised only in respect to the received information in each jurisdiction but excluding the origin and prior-processing.

Even if a judge would want to establish how the authorities identified information relevant to the particular case, this will most likely require digital forensics expertise and access to the original forensic copies. However, information on selecting relevant evidence is either protected as a military secret or may have never been documented. Even in cases where a judge decides not to disclose *Encrochat* evidence, the judge must be provided with the full forensic reports and the content of the surveillance materials in order to issue a reasoned and substantiated non-disclosure decision.

Some Dutch courts reasoned that the JIT investigation proceedings were directed at the company *Encrochat*, and therefore the suspects in subsequent investigations are not suspects in the Dutch *Encrochat* operation *Lemont*.[27] They concluded that only the evidence further collected in subsequent concrete investigations is relevant to the case and cannot be excluded. However, firstly, the *Encrochat* operation investigated and intercepted not only the company, but all its users alike. Secondly, the Netherlands are in favour of the use of unlawfully obtained, but *reliable* evidence, impose restrictions on exclusionary rules and rather compensate the use of unlawfully obtained evidence with a reduction of the final sentence (Borgers and Stevens, 2010). On the other hand, the Dutch judges acknowledged that the *Encrochat* evidence served as a legal basis for authorization of further investigative measures and further evidence collection in multiple investigations. In other words, the legality of the further authorized investigative measures would depend on the reliability of the *Encrochat* evidence, and not on its lawful acquisition. And even more so the defence has a legitimate interest in having access to and cross-examine it. Anything to the contrary would expose the suspect to parallel construction of evidence and reverse burden of proof which contradict the presumption of innocence.

It can be concluded that a refusal to share the documents regarding the interception of *Encrochat* conversations and the procedural documents is in principle incompatible with the right to a fair trial within the meaning of Art. 6 ECHR. It is likely that the defence has a legitimate interest in accessing this information in preparation of the defence or during the trial. If judges do not examine the matter with sufficient scrutiny, the defence might be placed at a serious disadvantage *vis-à-vis* the prosecution.

In such a large-scale investigation as *Encrochat*, the forensic reports on the multiple steps of data processing must be prepared for judicial oversight continuously throughout the duration of the investigation. It becomes apparent that existing judicial systems lack concretely codified requirements and processes to efficiently scrutinize the lawfulness, reliability, and the chain of custody at each step of digital evidence

[23] Bendenoun v. France, App no 12547/86 (ECtHR 24 February 1994).

[24] Matanović v. Croatia, cited above, para 183–186.

[25] Rook v. Germany and Sigurður Einarsson and Others v. Iceland, cited above.

[26] Jasper v. the UK, cited above, para 56.

[27] Court of Rotterdam, ECLI:NL:RBROT:2020:9899; Court of Amsterdam, ECLI:NL:RBAMS:2020:4923.

processing in cross-border and large-scale cases like *Encrochat*.

The previous sections argued that it is doubtful if the *Encrochat* evidence was obtained lawfully and that there is limited information to evaluate its origin, reliability, and accuracy. Each court must evaluate the reliability of the evidence against concrete defendants, but if digital forensic reports are not produced in the proceedings at least with respect to the datasets provided by Europol or this forensic examination cannot be cross-examined the only effective remedy to protect a fair trial will be to exclude *Encrochat* evidence from the case. However, if the judge authorizes an independent digital forensic examination on a case-by-case basis, the reliability of the evidence might be evaluated. Considering that some countries have more than a thousand cases related to *Encrochat* data, it is questionable if the judicial system will be able to facilitate forensic examinations and their contestation with respect to limited resources and procedural efficiency. For those reasons, it is likely that the *Encrochat* evidence cannot be the sole and decisive evidence on which a conviction can be based, should the principles inherent to Art. 6 ECHR be upheld in national court proceedings. In view of the ECtHR case law, the Art. 6 ECHR guarantees will require at a minimum *Encrochat* evidence to be corroborated with other supporting evidence of which the reliability and lawful acquisition can be cross-examined. It is a different question if the supporting evidence doctrine is an appropriate way to endorse digital evidence which is not contestable.

4. Digital evidence rules under the EIO and JIT regime?

Germany and the UK reported that they used EIOs as a legal basis to acquire *Encrochat* evidence. The EIO regime relies on national evidence rules in the executing and requesting state. Such rules, especially in respect to illegally obtained evidence abroad and its admissibility vary strongly between states (Vermeulen et al., 2010). At the beginning of the *Encrochat* investigation, ensuring that the protection afforded by Art. 6 ECHR and the inherent evidence rules were under French responsibility, while French authorities acted under national jurisdiction. The moment when the JIT was formed and EIOs were issued, the mutual trust regime was activated – and all actions on evidence processing and human rights protection were according to EU rules on cooperation and mutual trust. However, at the end of the operation after the execution of the EIOs, the rules on the use of the evidence and fair trial protection are under national jurisdiction again. If the executing state (France) does not provide sufficient information to evaluate the lawfulness, reliability and authenticity of the evidence, the requesting states (The Netherlands, The UK, Germany, Sweden and Norway) will not have sufficient information to evaluate if the use of such evidence at trial will be in compliance with Art. 6 ECHR.

Further, JITs allow parallel investigative proceedings and unlimited information and evidence exchange between states. Some formal requirements must be adhered to e.g., when the JIT was formed, what was its legal basis, mandate, who were the supervision leaders and what was the operation action plan,[28] since all actions from that date on must comply with European Union law. Arguably, they must be complemented with substantive obligations for law enforcement accountability like the mandate, evidence processing conditions, proportionality and justification of methods and tools used, disclosure agreements etc. Further, there is no information whether the French authorities have asked for continued permission to intercept Swedish or Norwegian citizens according to the EIO notification schema and if such notification was evaluated by a judge for its compliance with fair trial requirements. Consequently, the EIO and JIT regime does not contain any evidence rules or obligations for forensic reporting which introduces a specific problematic and a level of complexity to Art. 6 ECHR broadly debated in national courts.

3.1. National courts evaluation of the EIO regime

In the UK, the EIO was challenged on the basis of Art.7 (3) EIO-Directive (Grange, 2020) – as it cannot be issued for an offence that is unknown to the investigating authority or that has not been committed. The High Court ruled to the contrary: EIO covered investigations into criminal offences, and there could be an investigation into an offence even if it turns out that no offence has in fact been committed. The court held that there was no need to establish that an offence is already known to the investigating authority at the time an EIO is issued and that the EIO does not need to identify any particular person who is suspected of having committed an offence. Other UK lawyers argued that the EIO is invalid because the operation is out of the EIO personal and material scope (The Upsidedown Times, 2021). Firstly, since France was part of a JIT and they are exempt from the EIO scope, the UK had to request information from Europol. Secondly, cross-border surveillance is also beyond the scope of EIO and even pursuant to Article 40 *Convention Implementing the Schengen Acquis* a bilateral agreement is necessary in order to perform forward surveillance on the scale of the French operation. It is possible that such a bilateral agreement was signed in the JIT formation but the legal basis for the surveillance in the remaining countries is unclear.

The EIO regime was not only challenged on formal, but also on substantive grounds. In *Bremen*, an accused objected that the EIO requirements had not been met and that therefore the *Encrochat* evidence is inadmissible and unlawfully obtained. The defence reasoned that proceedings against unknown persons cannot satisfy the proportionality evaluation required in Art. 6 (1) (a) and (b) in conjunction with Art.11 (f) EIO-Directive. In addition, the requirement of Art. 6 (1) (b) EIO is not met since there is no similar investigation measure in Germany which allows interception of communications on such a large scale and without cause. A High court in *Bremen* reasoned that under the mutual recognition regime the legality of the French operation can be scrutinized only on very limited grounds and as long as the formal requirements for EIO and cross-border exchange are met, the evidence will be admissible. The judgment states that the German authorities acquired intelligence about *Encrochat* on the bases of Art. 7 of the framework decision 2006/960/JHA of the Council of 18 December 2006 on the simplification of the exchange of information and knowledge between the law enforcement authorities of the member states of the European Union. A judicial revision by the German criminal court responsible for the investigative proceedings was conducted on the bases of the *Convention on Mutual Assistance in Criminal Matters.*[29] Further *Encrochat* evidence was obtained lawfully and in accordance with Art. 31 (1) and (2) of the EIO Directive and had been facilitated by the Europol information-exchange system. In respect to the allegations of disproportionate interception of German citizens by French LEA, the court concluded that "usability of illegally collected or obtained information is therefore to be measured solely by the right to a fair trial outside of legal prohibitions (see BVerfG, decision of 07.12.2011–2 BvR 2500/09 et al., Juris Rn. 115 ff., BVerfGE 130, 1)".

In another case, the *Hamburg* court acknowledged that prohibition of the exploitation of evidence can in principle arise from the unlawfulness of the measure taken abroad as well as the unlawfulness of the cross-border data transfer itself -(OLG Hamburg, 2021, para 75) The court referred to the French measure of deploying the interception device to all phones as only possible "due to the lack of other investigation options". The court considered that in the particular case, the interception of the accused's device was proportionate in respect of the large amount of narcotics, and that similar measures can be authorized pursuant to

[28] Europol/Eurojust, Joint Investigation Teams Manual, 13598/09 COPEN 178 ENFOPOL 218 EUROJUST 55 EJN 35, Brussels, 4 November 2011.

[29] Convention of 29 May 2000 established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union - Council Declaration on Article 10(9) - Declaration by the United Kingdom on Article 20.

Section 100b (3) of the German Code of Criminal Procedure. The court concluded that the cross-border transfer is also lawful and noted that "when examining foreign decisions, it would be particularly wrong to derive the requirements for rule of law action from simple German criminal procedural law. This does not apply to foreign matters and cannot claim any validity. The assessment criteria are fundamental rights such as the core of German fundamental rights or the rights guaranteed by the ECHR" (OLG Hamburg, 2021) Most Dutch and German courts reasoned that they have limited jurisdiction to scrutinize the French investigation measures and, based on the principle of mutual trust, they must assume that the member states respected human rights.

3.2. Lack of digital forensics and evidence requirements in EIOs

The leaked UK EIO, shows significant inconsistencies (The Upside-down Times, 2021), such as: it is not stated that the requested investigation measure is interception and what is the UK law provision authorizing similar measures; and there is no assessment of the proportionality of the measure or any considerations on protection for suspects and accused. This is an indication that the Art. 6 EIO requirements are not met. It is unclear also how the UK as an issuing state could assess the proportionality of an investigative measure such as real-time evidence collection and its impact on such a large number of suspects' and defendants' rights. Arguably, such an evaluation will require specific guarantees on evidence handling and evidence rules, which will ensure that the use of such evidence in further proceedings in the issuing state will not be contrary to the right to a fair trial. No such requirements are stated in the leaked document.

Following the formal structure of the EIO template, at least in theory, the requesting state can specify procedures for the execution of the EIO under section I. From the leaked UK EIO it is visible that the law enforcement authorities requested all documentation and items related to the EIO execution to be send to the UK police authorities (The Upsidedown Times, 2021). However, the document does not specify formal requirements for chain of custody, proof of origin, data integrity and preservation, and digital forensic examination reports on the *Encrochat* forensic copies. Instead, what is requested is witness statements regarding the data, which is in contradiction to digital forensic standards. Allegedly, it was reported that France refused expert witness testimony in any subsequent proceedings on the grounds of Art. 11 (1) (b) EIO. Even if France agrees to dedicate forensic experts to clarify reliability contestation of *Encrochat* evidence, it is unclear if France will have sufficient experts to participate in the cross-examination of such a large amount of data in so many subsequent investigations and trials across Europe. Moreover, no EIO legislation addresses how forensic expert reports can be exchanged and cross-examined in a way that: (i) the exchange does not compromise the scientific validity of the evidence; and (ii) all forensic actions before and after the EIO can be traced back and validated. Moreover, the digital forensic standards describe digital data processing for evidence purposes as a continuous procedure where the acquisition, although crucial, is only an initial stage and is followed by an examination which is the process of identifying relevant data for each individual investigation and analysis which verifies the origin and reliability of the relevant data. Pursuant to the EIO the acquisition of data can be performed in one jurisdiction while further examination and analysis will be carried out in another. This means that if the mutual trust regime is not guided by minimum harmonized evidence law standards and digital forensic standards, the integrity and reliability of the evidence cannot be preserved or evaluated. In the light of the need for accountability of evidence processing and traceability of its origin and its reliability, an effective EIO regime must be supported by evidence systems and technology-assisted processes for data integrity preservation and examination. In the *Encrochat* case, the data processing was facilitated by Europol. Reportedly, Europol investigated in real time the millions of messages and data it received from the JIT partners (Zagaris and Plachta, 2020). However, the responsibility of such a supra-national organization with respect to evidence handling and protection of defence rights is not clear. It appears desirable that large-scale evidence collection operations like *Encrochat* be facilitated by evidence systems designed to incorporate digital forensics standards.

The negative effect of the identified inconsistencies with respect to the *forum regit actum* principle is enhanced in operations which involve more than two countries. In the *Encrochat* case, the principle will require the executing state to comply with formal requirements of evidence handling from five different states. Further, it is quite likely that the requesting state does not specify any formalities in the EIO form, as was apparent from the UK EIO form. Moreover, with respect to digital evidence the proportionality assessment of the investigation measure will depend also on the stages of the digital forensic processing. The proportionality of the acquisition does not necessarily mean that further examination and analysis were also conducted in a proportionate manner.

The provisions empowering the executing state to control the investigative measure requested – (i) refusal on fundamental rights grounds Art.11(1) (f); (ii) right to select less intrusive measure Art.10 (3); and (iii) the exception from the *forum regit actum* in Art. 28 (4) – are unclear in their practical application. They require the executing state to evaluate potential fundamental rights risks but what could trigger such an evaluation and on what grounds is not elaborated in the text. It is also unclear what are the requirements for an intrusiveness assessment. Arguably, this requires not only legal evaluation but also depends on the digital forensic evaluation. Many novel methods and tools for digital evidence gathering are not evaluated with respect to their intrusiveness and no criteria has been developed considering the dynamic scientific and technological advancements in the field. Best practice, in digital forensics, is the forensic examiner being able to justify the selected method and tool. Such a justification will require the comparison of different methods and selecting the most suitable according to the forensic task. Again, several methods can be selected for the same task, and different methods are necessary for different stages of the processing. Therefore, the intrusiveness of the measure must be continuously evaluated and is not just selected once. The same applies to the fundamental rights infringement evaluation. Each stage of the evidence processing can potentially infringe different rights, therefore at the moment of the reception of the investigation request the executing state can only vaguely assess it. However, the EIO does not require any impact assessment or any documentation of the investigation measures which can demonstrate that infringements to human rights are limited to the minimum. The leaked UK EIO shows that the evidence requested was already in the possession of the French authorities, which will exclude the application of Art. 28 (4) to the case.

The *Encrochat* operation raises suspicions also in terms of so-called *evidence forum-shopping*. For example, if German investigative authorities cannot obtain a warrant for a particular measure resulting in an encroachment of a fundamental right, instead of having to abandon that measure they could turn to a friendly authority abroad that has the necessary powers. For example, in "the United Kingdom and France, compared to domestic surveillance, there is no safeguard banning the collection and access to communications content" (FRA, 2017), while in Germany this is subject to specific authorization. Moreover, a bulk acquisition warrant in the UK can authorize only communication data acquisition (IPA, s158 (6)) and not that acquired in France *Encrochat* content data.

The *Encrochat* operation can also be challenged in respect of the CJEU jurisprudence on privacy and data protection. CJEU ruled that bulk surveillance operation must be limited to what is strictly necessary and proportional. The court stated "that the directive on privacy and electronic communications, interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of such criminal proceedings, where those persons suspected of having

committed criminal offences are not in a position to comment effectively on that information and evidence."[30] The case was argued as out of scope for EU law on grounds of the national security exception but the CJEU disagreed stating that: the directive on privacy and electronic communication did not permit Member States to adopt, for the purposes of national security, domestic legislation intended to restrict the scope of the rights and obligations in the directive, in particular the obligation to ensure the confidentiality of communication and traffic data. Even if the national security exemption applies to the French methods and tools for data acquisition, the further processing, analysis and exchange of the data with other jurisdictions must be in compliance with EU law. Considering that the CJEU claims supremacy on mutual recognition matters and privacy of telecommunications (Directive 2002/58/EC) applies even to national security measures if the *Encrochat* operation is challenged before the CJEU, the necessity and proportionality evaluation might require the French authorities to disclose how data was collected and analysed.

It appears that mutual trust instruments like the EIO create a formal procedure for cooperation in evidence gathering, which is focused on cooperation between law enforcement authorities, without much consideration of the defence's stand or enforcement of digital forensic science standards. This results in individualized trials where the defence and the judges are ill positioned to scrutinize on valid grounds the validity and integrity of the investigation and the reliability of the digital evidence.

3.3. Admissibility debate

The *Encrochat* evidence has sparked a debate about its admissibility and lawfulness between judges and defence lawyers in Europe. Inadmissibility claims based on the questionable lawfulness of the *Encrochat* evidence acquisition refer to the JIT operation as "skimming off massive amounts of data without any cause" and "mass surveillance that seems to lack specific purposes" (Stukenberg, 2021). Defence lawyers in the Netherlands,[31] Germany (Stukenberg, 2021), and Sweden (Jönsson, 2021) expressed the doubt if comparable investigative powers exist in their jurisdictions (as required by the EIO regime) and refer to the French interception as "fishing expeditions" which may result in *evidence forum-shopping* if such evidence is further used. The *Berlin* Judge Rothbart reported that the use of the *Encrochat* evidence will jeopardize the fairness of the court proceedings since there was insufficient information on the legal basis and access to *Encro-data*.[32] The Regional court in Berlin decided against the use of the chat data as the French surveillance measure encroaches seriously on the right to protection of the confidentiality and integrity of information technology systems and on telecommunications secrecy[33]; while German authorities were not informed to evaluate its proportionality according to Art. 31 EIO and no reasonable suspicion can be derived from the sole use of encrypted phone.[34] In Sweden, inadmissibility was also discussed in respect to the reliability and trustfulness of the *Encrochat* evidence. Allegedly, the interception of the encrypted network was approved by the French Internal Security Service (DGSI) and authorized by a judge but remains confidential since it falls under the "military state secrets" (nl Crimesite, 2021). Judges cannot form an opinion on the reliability of the decryption technique, the quality of the "forensic" copy of the data produced by the interception device, or how it was further processed and analysed before being handed to other countries.

Encrochat evidence was considered admissible by some courts in the UK, Germany, and the Netherlands, although on very different and controversial grounds. English law prohibits the use of interception evidence, however the court of Appeal in London decided that messages in volatile memory are not part of the transmission, and for legal purposes are considered stored,[35] which made *Encrochat* evidence lawfully obtained and admissible. The Investigatory Powers Act 2016 (IPA)[36] in the UK differentiates between interception of data in transit (Section 4 (4) (a) IPA) and interception of stored data (section 4(4) (b) IPA). A lawful interception of data in transit requires either a targeted or bulk interception warrant (Section 6 (1) (a) (i) and (ii) IPA). A lawful interception of stored data is pursued under a targeted or bulk equipment interference warrant (Section 6 (1) (c) (i) and (ii) IPA. However, interception of data in transit is inadmissible as evidence in court proceedings (Section 56 and Schedule 3 para 2 IPA). In fact, only the UK court came out with the conclusion that data in volatile memory is stored, which is peculiar from both a legal and technical point of view. In other court decisions the French interception of telecommunications was undoubtedly in fact computer surveillance of data in transfer.[37] It might be that the UK court decision was directed against the archaic exclusionary rule in English law against interception evidence. Nevertheless, the decision was criticized for its long-term negative effects on privacy and telecommunication secrecy, as well as for failing to recognize foreign, unlawfully, and improperly obtained evidence which also raises serious questions as to its reliability (Goodwin, 2021), (Madden, 2021) Defence experts argued that on a case-by-case basis the defendants must request access to the data sets available in the UK and cross-examine relevant information regarding their case for its reliability, accuracy, and correct attribution to the suspect (Gardiner and Sommer, 2021). However, as a general argument, *Encrochat* evidence can be excluded as unfair and obtained in breach of human rights provisions (section 78 PACE), or because it constituted bulk interception, not targeted – and therefore lacked a legal basis (Gardiner and Sommer, 2021).

In the Netherlands, several courts did not examine the legality of the French operation and its compliance with Art.8 ECHR based on the principle of legitimate expectations.[38] They referred to a decision of the Dutch supreme court stating that "investigative acts that are carried out under the responsibility of the foreign authorities of another state that has acceded to the ECHR, the task of the Dutch criminal court is limited to ensuring that the manner in which the results of this investigation are used in the criminal proceedings against the accused, does not infringe his right to a fair trial, as referred to in Art. 6 (1) ECHR. It is not the task of the Dutch criminal court to assess whether the manner in which this investigation was conducted is in accordance with the relevant rules of law applicable in the relevant foreign country."[39] The defense lawyer in one of the Flamenco cases expressed doubts about the court's impartiality since allegedly "judges had given their opinion about the acquisition and use of the material, while the file was not yet complete and questions had not been answered." (nl Crimesite, 2021) In Bremen, the evidence was considered admissible as long as the formal requirements

[30] Judgments in Case C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [2020] ECLI:EU:C:2020:790 and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others [2020] ECLI:EU:C:2020:791. See CJEU press release No 123/20, Luxembourg, 6 October 2020, available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf.

[31] Court of Amsterdam, ECLI:NL:RBAMS:2020:4923.

[32] ibid.

[33] In Germany, the IT fundamental right to confidentiality and integrity of information technology systems is derived from Art, 10 GG (see fundamentally BVerfG v February 27, 2008 - 1 BvR 370/07and 595/07 juris §. 187ff.).

[34] LG Berlin, decision of 1.7.2021 (525 KLs) 254 Js 592/20 (10/21).

[35] Regina v A and Others [2021] EWCA Crim 128 [2021] QB 791.

[36] Investigatory Powers Act 2016.

[37] OLG Bremen, decision of December 18, 2020 - 1 Ws 166/20: https://www.burhoff.de/asp_weitere_beschluesse/inhalte/6074.htm and (OLG Hamburg, 2021).

[38] Zeeland-West Brabant Court, ECLI:NL:RBZWB:2021:732 and Court of The Hague, ECLI:NL:RBDHA:2021:2242.

[39] Supreme Court of the Netherlands, ECLI: NL: HR: 2010: BL5629.

for a European Investigation order (EIO) (Directive 2014/41/EU) and cross-border exchange are upheld. Another German court did not examine the *Encrochat* operation in its totality but decided that the single interception of the accused's phone was proportionate considering the large amount of narcotics involved and the encrypted network, which required such a measure.[40] The authenticity and integrity of *Encro-chats* was raised in OLG Brandenburg.[41] In its scattered preliminary argumentation, the court stated that data integrity is a factual matter to be examined on a case-by-case bases, but so far, the court find no indications "that the communication content and location data have been changed or falsified by transmission errors or manipulations".[42]

The OLG Berlin decision, was overruled by the Higher court which concluded that *Encrochat* data classifies as "accidental discoveries" from another procedure and can be used as evidence pursuant to Section 100e, Paragraph 6, No. 1 of the Code of Criminal Procedure.[43]

This brief overview shows very different interpretations of evidence admissibility and reliability, as well as a serious divergence, even between courts of the same jurisdiction, in the evaluation of the legality and the contestability of the digital evidence acquired in the *Encrochat* operation. It is likely that in some cases the admissibility and probative value of the evidence will be challenged further to higher courts on constitutional or human rights grounds (Sehl, 2021).

Finally, the *Encrochat* evidence was brought to the higher courts in Germany and Norway who concluded that it may be used for the purpose of investigating serious criminal offences. The German Federal Court reasoned, that *Enchrochat* evidence is beyond all doubt proof of criminal activities (German Federal Court, 2022). The court however, focused on the plain text and content rather than considerations about the authenticity of the data or the reliability of the forensics methods and tools. Further the court decided that there is no legal grounds to cross-examine the legality of the French investigation and, as long as the evidence is lawfully exchanged via EIO, German courts can make use of it while any further issues can be compensated at the time of utilization (in each individual proceedings). Indeed, during trial each defendant can bring up questions about inconsistencies in the evidence or challenge its reliability. However, such contestation can hardly be on informed basis due to the complexity of the data processing and the lack of information or disclosure of the forensics employed. Similarly, the Norwegian Supreme Court rules that the *Encro-evidence* can be used under three conditions: *(i)* the evidence is acquired in compliance with the French criminal procedure; *(ii)* the defendant must be provided with access to the whole data acquired as evidence; *(iii)* the use of the evidence must not contradict basic human rights and values (in each individual case) (Supreme Court of Norway, 2022). Challenging the *Encrochat* operation on human rights grounds remains the only opportunity to scrutinize the evidence from hacking, and it is still to be seen, if an individual case will reach the ECtHR. Nevertheless, there is no legislative framework or quality requirements for cross-border covert investigations and subsequent use of evidence from hacking. This means that the operation in its entirety and future large-scale investigations will receive limited scrutiny as to their lawfulness and fairness.

4. Human rights protection in cross-border investigations?

The *Encrochat* operation shows the importance of pre-emptive evidence gathering and international cooperation for effective prosecution where the investigative stage is outcome-determinative, data-driven, and complex. It is expected of modern prosecutions to increasingly show some or all of these characteristics. However, it seems that national legislators, international bodies, or the ECtHR itself have not yet developed a clear framework as to how human rights, and in particular, Art. 6 ECHR is to be uphold in international evidence exchange.

In respect to digital evidence, the digital forensic process can be considered a crucial stage of the investigation, where the equality of arms-based and the presumption of innocence-based evidence rules cannot be disregarded, and the judicial process might not sufficiently exonerate procedural deficits in the early stages of the investigation. In addition, cross-border evidence-gathering is becoming the predominant form of digital evidence collection, which amplifies its complexity, volumes, and significance for fair administration of evidence and protection of innocent suspects.

As the *Encrochat* example shows, effective measures to examine the evidence's origin, reliability, and chain of custody are of high importance for the defence and the judicial process as a whole. On the other hand, the individual responsibility of the state, advanced by the ECtHR, might be insufficient to cover new forms of cross-border evidence gathering and cooperation in investigations, while shared responsibility might be impractical and overburden the judicial process in several countries, if not complemented with minimum evidence rules, standards, and systems to facilitate evidence processing.

It should be taken into account that the ECtHR has a specific jurisdiction and in the interpretation of the court does not allow the examination of evidence procedures' reliability or cross-border cooperation mechanisms, which, as demonstrated, negatively impacts the defence's stand in such proceedings. In the light of the constant evolution of the ECHR and ECtHR role to develop further and innovate human rights principles according to societal needs, it can be argued that this approach should be modernized and improved with respect to the evolution of digital evidence practices. Developing of a principle approach and minimum standards for digital evidence based on Art. 6 ECHR, which can ensure that States' responsibility under Art. 6 ECHR can be effectively exercised and the cross-border element of evidence processing does not affect the evidence rules of contestability, lawfulness, and reliability in any way. In addition, such a universal fairness-based approach to evidence rules will improve effective prosecution since it will allow the development of digital evidence processes and systems which can support such standards on a large scale for multiple investigations in multiple jurisdictions such as in the *Encrochat* case. Such a common evidence law could be initially developed under European Union efforts to create cooperation in criminal matters (AFSJ). This requires the examination of the *Encrochat* investigation in the context of the mutual trust regime of EU law.

The *Encrochat* case shows that even when the mutual trust instruments provide exceptions on the basis of human rights protection, in practice such a "potential risk" evaluation is quite weak. The judge's authorization and oversight of investigation measures pursuant to JIT or EIO requests, is limited since methods of evidence processing are kept secret and access to the content of surveillance files is restricted. Consequently, judges presented with *Encrochat* evidence would be left to try and guess whether the trial will be fair based on political documents and opinions.

The *Encrochat* operation also demonstrates that cross-border cooperation in digital investigations includes exchanging of forensic reports, and this requires EU-level policy which currently does not exist. In one scenario, a forensic acquisition, examination, and analysis can be performed in one country and the results can be sent to another for further investigative or trial proceedings. This means that the forensic report should be based on certain universal evidence rules that can ensure its verification and validation of results in the receiving country. In a second scenario, different stages of the forensic examination can be performed in different countries. A hypothetical example could be that France performed acquisition of the digital data, while Europol and the Dutch authorities performed pre-processing, identification, and examination of relevant data, which consequently was transferred to the UK or

[40] Higher Regional Court (OLG) Schleswig, decision of 04/29/2021 - 2 Ws 47/21.
[41] Higher Regional Court (OLG) Brandenburg, decision of 08/03/2021 - 2 Ws 102/21.
[42] ibid., OLG Brandenburg.
[43] KG, decision of 08/30/2021 - 2 Ws 79/21.

Sweden for digital evidence analysis and attribution to concrete suspects. In the traditional singular criminal investigation, the forensic process was completed in one lab according to certain standards for the examiner, methodology and tools providing accountability of the process for its cross-examination by other parties to the criminal proceedings. In the new scenarios the forensic process is either performed in a foreign lab which, if not specified in the mutual recognition regime, has no obligations to provide accountable forensic reports to another jurisdiction – or the forensic process is split between different jurisdictions, while the validity of consequent stages will depend on the validity in any of the previous stages. Arguably, the mutual trust regime should provide for a forensic reports exchange policy which demands accountability information. *Encrochat* is only an example of the limitations of the mutual trust regime in relation to Art. 6 ECHR compliance. The overall problem is outlined by *de Hert* as a general critique of the whole CFR stating that "the Charter […] lacks a *sui generis* reflection about what rights are needed in a Union with divided competences that is supposed to concentrate first and foremost on the transnational aspects." (Paul de Hert et al., 2016)

From a legal point of view, such a *sui generis* positive human rights policy for evidence processing must ensure that every stage of the evidence handling in a mutual trust context is accountable against fair trial requirements. The goal of the EU legislator to achieve efficient mutual-trust instruments, digital investigations, and mutual admissibility of digital evidence is a motivation for harmonization of minimum evidence rules and standards including on expert reports exchange (Vermeulen et al., 2010) (Kusak, 2016), (Kusak, 2019) This will benefit concrete and practical evidence rules to be implemented in the design and use of evidence processing technology. From a technical perspective, the digital evidence domain is largely technology dependent and science driven. Digital forensic science standards cannot be replaced by formal requirements for information exchange. Large-scale evidence acquisition, examination and exchange can be complemented with formal validation procedures to ensure the reliability of the evidence.

5. Conclusion

The *Encrochat* evidence brings up many questions of procedural inaccuracies and fair trial challenges that are archetypical for the digital evidence problematic. There is a strong opposition between two effects. On the one hand there is the broad discretion of mutual-trust cooperation mechanisms in combination with the employed proactive digital forensics techniques for evidence collection in bulk. On the other, there is the lack of sufficient fair trial safeguards and evidence rules at several stages of the cross-border cooperation in combination with insufficient information on the reliability and accuracy of the data acquisition, examination, exchange and further use of evidence for investigative purposes in multiple jurisdictions.

The analysis of the *Encrochat* operation in relation to Art. 6 ECHR shows serious deficits of evidence rules and procedures that cannot be compensated at each individual trial. The opportunity for the judicial process to scrutinize the operation is very limited in particular with regards to:

- whether the *Encrochat* evidence was lawfully obtained in respect to Art. 8 (2) ECHR requirements;
- whether the requirements of mutual trust instruments at the EU level were upheld by the requesting and executing state and if such a mutual trust regime has the required safeguards to ensure fair trial in subsequent investigations and trials;
- whether the use of *Encrochat* evidence is in compliance with Art. 6 ECHR inherent evidence rules for contestability, disclosure, and reliability of (expert) evidence;
- whether the traditional digital forensics and quality of investigation standards for individual investigations are suitable and enforceable to regulate cross-border digital evidence collection;
- whether law enforcement agencies can demonstrate accountable and reliable processes for digital evidence handling; and
- whether the use of specialist digital forensic processes, methodologies, and tools can be independently validated and justified as proportionate and necessary.

The analysis makes apparent that the sophistication of technology-facilitated crimes demands broad investigative powers and international cooperation in order to achieve efficient prosecution. However, the law and procedure enabling such operations are not sufficiently scrutinized on the basis of fair trial and digital forensics standards. Fair trial safeguards are still interpreted as trial-based and individualized, while evidence rules in practice are still strongly bound to concrete jurisdictions. This contrasts with contemporary large-scope investigative mechanisms, ubiquitous digital evidence collection, and sophisticated digital forensics technologies with cross-jurisdictional effects. Consequently, the ability of the defence and the whole judicial process to scrutinize such operations is significantly diminished. Digital investigations and mutual trust mechanisms are not equipped with scalable procedures, evidence systems, and technology design which can provide an audit trial of the evidence processing and procedural steps essential for the consequent evaluation of their legality, reliability, fairness, necessity, and proportionality. The presumption of innocence-based evidence rules are challenged and even disregarded early in the investigation.

Therefore, the three main findings of this analysis, summarized below, are incentives to harmonize and develop further digital evidence procedural rules:

- there are no binding digital forensics standards in criminal proceedings or forensic reports exchange policy which demands reliability and compliance with Art. 6 ECHR-based evidence rules;
- the defense's stand is not sufficiently addressed in current digital evidence legislation or mutual trust-based instruments at the EU level; and
- the judicial process lacks scalable procedures to scrutinize digital evidence processing and reliability and are exposed to technology dependences.

At the same time, the *Encrochat* case shows that all jurisdictions face some similar issues with respect to the reliability of the digital evidence and its evaluation, which can serve as grounds for further harmonization. Human rights protection, digital forensics methodology, responsible design and use of investigative technology are factors which do not depend on a concrete jurisdiction and provide the basis for development of minimum digital evidence standards and formal validation procedures in the investigative stage of criminal proceedings as well as in cross-border cooperation.

From the point of view of Art. 6 ECHR, the *Encrochat* operation brings to light urgent techno-legal questions of digital evidence reliability, enforcement of digital forensics standards in police operations, chain of custody and integrity of data processing, as well as defense representation in cross-border investigations.

Declaration of competing interest

The author declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Adelstein, F., 2006. Live forensics: diagnosing your system without killing it first. Commun. ACM 49 (2), 63–66. https://doi.org/10.1145/1113034.1113070. Feb.

Antwi-Boasiako, A., Venter, H., 2017. A model for digital evidence admissibility assessment. In: Peterson, G., Shenoi, S. (Eds.), Advances in Digital Forensics XIII, IFIP Advances in Information and Communication Technology. Springer International Publishing, Cham, pp. 23–38. https://doi.org/10.1007/978-3-319-67208-3_2.

Årnes, A. (Ed.), 2018. Digital Forensics: an Academic Introduction. John Wiley & Sons Inc, Hoboken, NJ.

Boddington, R., Hobbs, V., Mann, G.A., 2008. 'Validating Digital Evidence for Legal Argument', 6th Australian Digital Forensics Conference. Edith Cowan University, Perth Western Australia. https://doi.org/10.4225/75/57b269e240cb7.

Borgers, M.J., Stevens, L., 2010. The use of illegaly gathered evidence in the Dutch criminal trial. In: Netherlands Reports to the Eighteenth International Congress of Comparative Law. Intersentia, pp. 569–594 [Online]. https://research.vu.nl/en/publications/the-use-of-illegaly-gathered-evidence-in-the-dutch-criminal-trial. (Accessed 8 May 2021).

Council of Europe, 1950. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) (ECHR) as Amended by Protocols Nos. 11 and 14. *ETS 5*. 1950.

Council of the European Union, 2011. 'Council Conclusions on the Vision for European Forensic Science 2020 Including the Creation of a European Forensic Science Area and the Development of Forensic Science Infrastructure in Europe'. 3135th JUSTICE and HOME AFFAIRS Council Meeting [Online]. Available: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/126875.pdf.

Cox, J., 2020. 'How Police Secretly Took over a Global Phone Network for Organized Crime', *Vice*, Feb. 07. https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked. (Accessed 11 July 2021).

Danisevskis, J., Piekarska, M., Seifert, J.-P., 2014. Dark side of the shader: mobile GPU-aided malware delivery. In: Lee, H.-S., Han, D.-G. (Eds.), Information Security and Cryptology – ICISC 2013, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 483–495. https://doi.org/10.1007/978-3-319-12160-4_29.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 Regarding the European Investigation Order in Criminal Matters, 2014.

Edmond, G., 2012a. Is reliability sufficient? The law commission and expert evidence in international and interdisciplinary perspective (Part 1). Int. J. Evid. Proof 16, 30–65. https://doi.org/10.1350/ijep.2012.16.1.391.

Edmond, G., 2012b. Advice for the courts? Sufficiently reliable assistance with forensic science and medicine (Part 2). Int. J. Evid. Proof 16 (3), 263–297. https://doi.org/10.1350/ijep.2012.16.3.405. Jul.

Eurojust-Europol, 2020. Dismantling of an Encrypted Network Sends Shockwaves through Organised Crime Groups across Europe (Press Confernce) [Online]. https://www.eurojust.europa.eu/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe. (Accessed 20 October 2022).

European Network of Forensic Science Institutes (ENFSI), 2015. Best Practice Manual for Forensic Examination of Digital Technology [Online]. Available: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf [Online]. Available:

European Union Agency for Fundamental Rights, 2017. Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II, Field Perspectives and Legal Update. Publications Office, LU [Online]. https://data.europa.eu/doi/10.2811/792946. (Accessed 11 July 2021).

Fukami, A., Stoykova, R., Geradts, Z., 2021. A new model for forensic data extraction from encrypted mobile devices. Forensic Sci. Int.: Digit. Invest. 38, 301169 https://doi.org/10.1016/j.fsidi.2021.301169.

Galli, F., 2016. The interception of communication in France and Italy – what relevance for the development of English law? Int. J. Hum. Right. 20 (5), 666–683. https://doi.org/10.1080/13642987.2016.1162412. Jul.

Gardiner, S., Sommer, P., 2021. 'Ecrochat Webinar', Mar. 03. https://www.25bedfordrow.com/site/seminars/encrochat-webinar.

German Federal Court (BGH). decision of 2 March 2022 – 5 StR 457/21 EncroChat-Data may be used for the Investigation of serious criminal Offences. 2022. [Online]. Available: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/EN/2022/2022038.html.

Goodwin, B., 2021. 'Judges refuse EncroChat defendants' appeal to supreme court', *ComputerWeekly.com*. Mar 15. https://www.computerweekly.com/news/252497819/Judges-refuse-EncroChat-defendants-appeal-to-Supreme-Court. (Accessed 11 July 2021).

Grange, E., 2020. The first and last challenge to the EIO? blogpost: https://www.corkerbinning.com/first-last-challenge-the-eio/. (Accessed 20 October 2022).

International Criminal Police Organization (Interpol), 2019. Global Guidelines for Digital Forensics Laboratories [Online]. Available: https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf.

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2012. ISO/IEC 27037 eForensics Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. https://www.iso27001security.com/html/27037.html. (Accessed 3 September 2020).

Jones, Nigel, George, Esther, , Fredesvinda Insa Mérida, Rasmussen, Uwe, Völzow, Victor, 2014. Electronic Evidence Guide v.2. 0'. Council of Europe [Online]. Available: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf.

Jönsson, T., 2021. DEBATT: "Encrobevisning bör avvisas av svenska domstolar". Dagens Juridik. Mar. 22. https://www.dagensjuridik.se/debatt/debatt-encrobevisning-bor-avvisas-av-svenska-domstolar/. (Accessed 11 July 2021).

Kusak, M., 2016. Mutual admissibility of evidence in criminal matters in the EU: a study of telephone tapping and house search. IRCP - Institute for International Research on Criminal Policy 53. Antwerpen: Maklu.

Kusak, M., 2019. Mutual admissibility of evidence and the European investigation order: aspirations lost in reality. ERA Forum 19 (3), 391–400. https://doi.org/10.1007/s12027-018-0537-0.

Madden, P., 2021. Madden & Finucane express grave concerns over today's Encrochat judgment at the English Court of Appeal in London. Madden & Finucane Solicitors. Feb. 05. http://madden-finucane.com/2021/02/05/madden-finucane-express-grave-concerns-over-todays-encrochat-judgment-at-the-english-court-of-appeal-in-london/. (Accessed 11 July 2021).

7. In: Mansfield-Devine, S. (Ed.), 2020. Hundreds of Alleged Criminals Arrested after European Authorities Infiltrate Encrypted Chat Service. Computer Fraud & Security, pp. 1–3. https://doi.org/10.1016/S1361-3723(20)30067-1. Jul. 2020.

nl, Crimesite, 2021. EncroChat: de reconstructie van de hack (UPDATE). Crimesite. Feb. 10. https://www.crimesite.nl/encrochat-de-reconstructie-van-de-hack/. (Accessed 11 July 2021).

European Judicial Network (EJN). 'Electronic evidence: France'. https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/France_Fiches%20Belges-on-electronic-evidence.pdf.

Higher Regional court (OLG) Hamburg**, decision of 3/21/2021 -** 1 Ws 2/21, 1 Ws 2/21 - 7 OBL 3/21.2021. [Online]. Available: https://www.landesrecht-hamburg.de/bsha/document/JURE210003021.

O'Rourke, C., 2020. 'Is this the end for "encro" phones?'. Comput. Fraud Secur. 11, 8–10. https://doi.org/10.1016/S1361-3723(20)30118-4. Nov. 2020.

Paul de Hert, 2016. EU criminal law and fundamental rights. In: Mitsilegas, V., Bergstrom, M. (Eds.), Research Handbook on EU Criminal Law, Research Handbooks in European Law. Edward Elgar Publishing, Cheltenham, UK.

Pollitt, Mark, Casey, Eoghan, Jaquet-Chiffelle, David-Olivier, Gladyshev, Pavel, 2018. A framework for harmonizing forensic science practices and digital/multimedia evidence. NIST - OSAC Task Group on Digital/Multimedia Science. Jan. 11. https://www.nist.gov/news-events/news/2018/01/framework-harmonizing-forensic-science-practices-and-digitalmultimedia. (Accessed 2 July 2020).

Sehl, Dr M., 2021. '"Encrochats" vor deutschen Gerichten. Der verbotene Datenschatz aus Frankreich?', *LTO.de - Legal Tribune Online*, Nov. 08 [Online]. Available: https://www.lto.de/recht/justiz/j/encrochat-krypto-telefon-ueberwachung-daten-frankreich-deutschland-beweis-verwendung-verwertung-strafverfahren/?r=rss.

Sommer, P., 2022. Evidence from hacking: a few tiresome problems. Forensic Sci. Int.: Digit. Invest. 40, 301333 https://doi.org/10.1016/j.fsidi.2022.301333.

Stoykova, R., 2022. 'The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations'. Septentrion 28. https://doi.org/10.2139/ssrn.4232504. Rochester, NY.

Stukenberg, T., 2021. Vorwurf Befugnis-Shopping: Streit um Encrochat-Ermittlungen vor Gericht. https://netzpolitik.org/2021/streit-um-encrochat-ermittlungen-vor-gericht/.

Supreme Court of Norway, 2022. Computer Material Obtained by French Authorities Can Be Used as Evidence in Norwegian Criminal Proceedings [Online]. Available: https://www.domstol.no/no/hoyesterett/avgjorelser/2022/hoyesterett—staff/HR-2022-1314-A/.

The Upsidedown Times, 2021. Encroleaks 2: EIO, Money for Nothing and Kiddy Fiddlers Go Free. The Upsidedown Times. Jan. 18. https://upsidedowntimes.wordpress.com/2021/01/18/encroleaks-2-eio-money-for-nothing-and-kiddy-fiddlers-go-free/.

van Baar, R.B., van Beek, H.M.A., van Eijk, E.J., 2014. Digital forensics as a service: a game changer. Digit. Invest. 11, S54–S62. https://doi.org/10.1016/j.diin.2014.03.007.

Vermeulen, G., De Bondt, W., van Damme, Y., 2010. EU cross-border gathering and use of evidence in criminal matters: towards mutual recognition of investigative measures and free movement of evidence?. In: IRCP-Series, No. V. 37. Antwerpen, Portland: Maklu.

Wright, R., 2020. Hundreds Arrested across Europe as French Police Crack Encrypted Network. The Financial Times. Feb. 07. https://www.ft.com/content/7006913f-be3d-49b5-8ba7-7c5b78b551b2.

Zagaris, B., Plachta, M., 2020. Transnational organized crime section I EU and law enforcement dismantle encrypted network of transnational organized crime. IELR 36 (7), 248–255.