Graduate thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Eirik Gjerde Buset

Cryptographic Evidence in Norwegian Courts

Graduate thesis in Cyber Security and Data Communication
Supervisor: Tjerand Silde
Co-supervisor: Katrien De Moor
June 2026

NTNU
Norwegian University of Science and Technology

Eirik Gjerde Buset

Cryptographic Evidence in Norwegian Courts

Graduate thesis in Cyber Security and Data Communication
Supervisor: Tjerand Silde
Co-supervisor: Katrien De Moor
June 2026

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Problem description

In recent years, encrypted communication has become central to the investigation and prosecution of serious crime. Large-scale international operations targeting platforms such as Sky ECC and EncroChat have provided law enforcement authorities with access to extensive communication data, which has subsequently been used as evidence in numerous criminal proceedings in Norway and many other countries. Norwegian courts have accepted the admissibility of such material when it was lawfully collected in the country of origin, even in situations where comparable investigative methods would not have been lawful for Norwegian authorities.

At the same time, this type of evidence raises concerns regarding transparency, verifiability, and fair trial guarantees. The material originates from complex technical intrusions into closed communication systems, and there is limited insight into the methods of collection, the processes of selection and filtering, and the overall completeness of the datasets. In practice, the defence gains access only to excerpts of communication, rather than the full underlying material. This creates a structural tension between effective law enforcement and principles of due process, evidential verifiability, and the right to a fair trial.

Although such evidence has become increasingly important in Norwegian criminal proceedings, there is little empirical research on how Norwegian courts and other institutional actors manage these challenges in practice. Issues relating to the chain of custody in the context of international cooperation, the presentation and filtering of large-scale datasets in court, and the emergence of informal standards in situations of technical uncertainty remain insufficiently examined.

In this master's thesis, we examine how encrypted and decrypted communication is handled as evidence in Norwegian criminal proceedings. Through qualitative interviews with different experts involved in the handling of such material, e.g. judges, defence lawyers, investigators, and academic experts, combined with an analysis of selected judgments, we analyse:

- The legal and procedural challenges that arise when encrypted communication is presented as evidence
- How reliability, credibility, and fairness are evaluated
- Which mechanisms aim to ensure transparency and maintain the chain of custody, particularly in the context of international cooperation
- What safeguards exist to prevent misuse or selective presentation of large-scale data sets
- Which standard or professional practises that guide forensic experts in decrypting and authenticating communication

– The extent to which courts rely on expert testimony to understand the technical dimensions of the evidence

We adopt a practice-oriented and descriptive approach. Rather than offering a normative evaluation of current law, we seek to shed light on how institutional actors manage technical uncertainty within the framework of Norwegian criminal procedure.

Approved: 2026-02-20 – Associate Professor Tjerand Silde, NTNU (Main supervisor)

Abstract

Evidentiary material from encrypted communication services such as Sky ECC and EncroChat has become more common in criminal proceedings in recent years. The many steps this evidence has undergone, from collection to use in court, raise questions about transparency, reliability, fairness, and technical uncertainty.

As we are unable to identify any prior research on how Norwegian legal actors address these questions, we find it important to study them in more detail. We therefore examine how collected communication material from encrypted platforms is handled, evaluated, and challenged as evidence in Norwegian criminal proceedings. Our study is qualitative and practice-oriented, based on 11 semi-structured interviews with judges, defence lawyers, police investigators, academic experts and a recently graduated lawyer. The interviews are supplemented by two selected Norwegian judgments to connect the participants' descriptions to concrete recent court decisions.

Our findings show that collected communication material is very strong evidence, but it is not self-explanatory. The many steps the evidentiary material has undergone make it more manageable for use in court, while limiting what the court and defence can see, understand, control, and challenge. There are multiple layers to evaluating this material, including technical reliability, completeness, fairness, interpretation of messages and metadata, and the connection between the digital user and the physical person. These control mechanisms include documentation, mirror tests, checksums, contradiction, new searches and an overall assessment. However, most of these control mechanisms only work after the material has been filtered and selected. We also see that legal actors are dependent on technical explanations and expert witnesses to understand the material. While this bridges the gap between law and technology, questions arise about the quality, independence, and control of experts.

Our study contributes empirical insight to a field of Norwegian criminal law practice that has not been examined before. The findings point to the need for clearer documentation, better access routines, greater visibility of uncertainty, greater technical understanding, and practical guidance for actors handling collected communication material as evidence.

Sammendrag

Bevismateriale fra krypterte kommunikasjonstjenester som Sky ECC og EncroChat har blitt vanligere i straffesaker de siste årene. Bevismaterialet har gjennomgått mange steg fra det ble innsamlet til det ble brukt i retten, og alle disse stegene gjør at det oppstår spørsmål om åpenhet, innsyn, pålitelighet, rettferdighet og teknisk usikkerhet.

Vi har ikke funnet noe tidligere forskning på hvordan norske rettslige aktører håndterer disse spørsmålene, noe som gjør det viktig å undersøke dem. Vi ser derfor på hvordan kommunikasjonsmateriale fra krypterte plattformer blir håndtert, evaluert og utfordret som bevis i norske straffesaker. Studien vår er kvalitativ og praksisnær og basert på 11 semistrukturerte intervjuer med dommere, forsvarere, etterforskere, akademiske eksperter, samt en nyutdannet jurist. Intervjuene er supplert med to utvalgte dommer, slik at deltakernes beskrivelser kan ses i sammenheng med konkrete rettsavgjørelser.

Funnene våre viser at kommunikasjonsmateriale fra krypterte plattformer er svært sterkt bevismateriale, men at det ikke er selvforklarende. Alle stegene materialet har vært gjennom gjør det mer håndterbart, men det begrenser hva retten og forsvaret får se, forstå, kontrollere og utfordre. Det er mange lag i vurderingen av dette materialet, blant annet teknisk pålitelighet, fullstendighet, om materialet kan utfordres på en rettferdig måte, tolkning av meldinger og metadata, og koblingen mellom en digital bruker og en faktisk person. Det finnes noen kontrollmekanismer, slik som dokumentasjon, speiltester, sjekksummer, kontradiksjon, nye søk, og en samlet bevisvurdering. Men de fleste kontrollmekanismene fungerer først etter at filtrering og utvelgelse er gjennomført. Vi ser også at rettslige aktører er avhengige av tekniske forklaringer og ekspertvitner for å forstå materialet. Dette bygger en bro mellom juss og teknologi, men det oppstår samtidig spørsmål om ekspertkvalitet, uavhengighet og kontroll.

Studien vår bidrar med empirisk innsikt i et felt av norsk strafferettslig praksis som ikke har blitt undersøkt tidligere. Vi peker på behovet for tydeligere dokumentasjon, bedre tilgangsrutiner, mer synlig usikkerhet, større teknisk forståelse og praktisk veiledning for aktører som håndterer kommunikasjonsmateriale fra krypterte plattformer som bevis.

Preface

This thesis is my final submission for the Master of Science in Cyber Security and Data Communication at the Norwegian University of Science and Technology. I wrote the thesis in the spring of 2026 as part of the Cryptology and Social Life project. The thesis was supervised by Associate Professor Tjerand Silde and Associate Professor Katrien De Moor from the Department of Information Security and Communication Technology (IIK) at NTNU.

Acknowledgements

I am very thankful to my supervisors, Tjerand and Katrien, for their excellent support, guidance, and engagement throughout the project. I am grateful to both of you for the opportunity to work on this interesting topic and for including me in the Cryptology and Social Life workshop. Our discussions and your highly valuable feedback have helped me shape the thesis and made the work more interesting along the way.

The participants in the study deserve a sincere thank you for taking the time to contribute and for sharing their experiences and professional perspectives. Without you, the study would not have been possible to conduct.

I also really want to thank Ragnhilde for your wonderful help at home and your support every day of the week. You have made everyday life amazing, and I am thankful for your emotional support and help with switching off and finding calm at home. You have also been an inspiration, kept me motivated, and pushed me further than I thought I could go on my own.

Without doubt, I also want to thank my family. They have given me a safe and supportive upbringing. My mother may have sparked my interest in cryptography when she taught me *røverspråk* as a child, and my father deserves thanks for encouraging me to study in Trondheim. I am also very thankful to have had my siblings, Vegard and Marte, in Trondheim throughout my time as a student.

Finally, I want to thank my friends and fellow students for good conversations, needed breaks, and for making my time as a student much better.

Contents

List of Figures

List of Tables

Chapter 1
Introduction

Digital communication has become a central part of many people's social lives. Popular messaging services such as Signal [Sig26], Facebook Messenger [Met26], WhatsApp [Wha26] and iMessage [App24] provide end-to-end encryption, illustrating that encryption has become common in widely used communication services. Encryption ensures confidentiality [Aum18, p. 1], which is an important mechanism for securing digital communication. Some services and devices are designed specifically to provide secure, closed communication, often referred to as *cryptophones*. The possession of these devices is not illegal [BĆ25, Sec. 4.1], but they are widely used by criminals and criminal organisations [OR23]. This has made such services relevant targets for law enforcement investigations, and large-scale international operations against encrypted communication platforms, such as EncroChat [Eur25] and Sky ECC [Eur26], have given law enforcement access to extensive communication material that was later used as evidence in serious criminal proceedings. In this thesis, we study the challenges that arise when communication material from these large-scale operations is used in Norwegian criminal proceedings.

1.1 Motivation

The use of material from encrypted communication platforms is visible in Norwegian case law. EncroChat and Sky ECC have been mentioned in multiple Norwegian judgments over the last couple of years, as shown in Figure 1.1.[1] This figure shows court decisions where EncroChat, Sky ECC, or both are mentioned, including

[1] The numbers are based on searches in Lovdata Pro [Lov26b] conducted on 22 May 2026, using the search terms `"encrochat"` and `"sky ecc"`, filtered to the legal source category *rettsavgjørelser*. All courts were included. English duplicates were removed by filtering out entries marked as *HRENG* and by manually checking titles. The EncroChat and Sky ECC lines show court decisions that mention each platform, while the third line shows decisions that mention both platforms. The categories are therefore not mutually exclusive. The numbers indicate court decisions that mention the relevant platform, not unique case complexes or cases in which the material was necessarily the main evidence. The 2026 numbers are incomplete and reflect results available at the time of the search.

decisions where platform material was central evidence and decisions where it was mentioned more peripherally. A similar development can be seen in the Netherlands, where Westers [WBJ+25, Table 6.1] provides an overview of Dutch judgments involving several types of encrypted communication, such as EncroChat and Sky ECC.

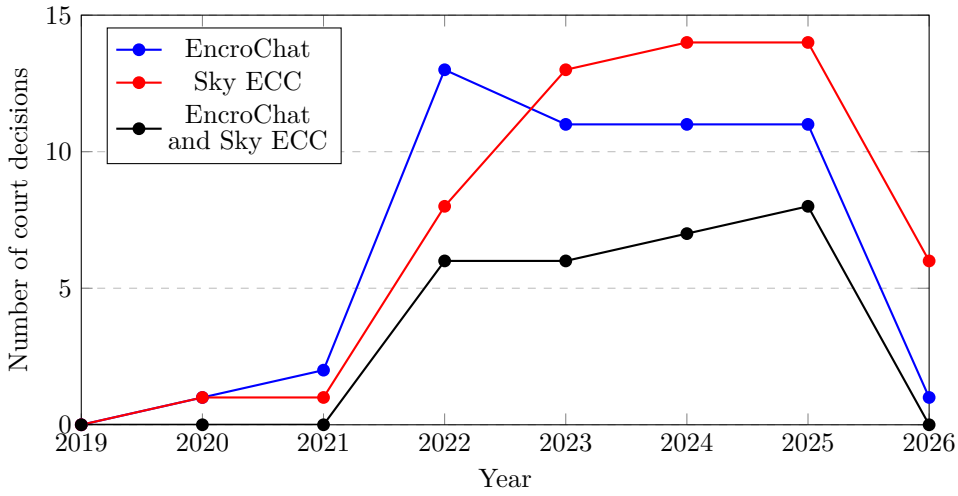


Figure 1.1: Norwegian court decisions mentioning EncroChat and Sky ECC in Lovdata Pro search results.

The repeated appearance of these platforms in Norwegian case law makes it relevant to examine how evidence from encrypted communication services is handled in Norway. This is important because the material reaches the court as data that has been collected, decrypted, processed, and selected through several technical and institutional steps. These steps make the material usable as evidence but raise questions about transparency, reliability, fairness, and the practicality of challenging it.

1.2 Problem Area

When evidentiary material comes from encrypted communication services, it may have undergone several technical and investigative processes before the court sees it. For both EncroChat [OvT22] and Sky ECC [Sag23], the material has been collected abroad and processed through international cooperation. Such material has later been used in several Norwegian cases, as shown in Figure 1.1. As shown later in Section 4.1.3, the court and the defence encounter the material in the form of excerpts, tables, timelines, or presentations, rather than the entire underlying dataset. This makes the material

more manageable for evidentiary presentation, but it does not remove the practical and technical difficulty of handling large filtered datasets, and questions arise about how the excerpts have been selected, documented, understood, and controlled. The material must also be assessed in terms of completeness, interpretation of messages and metadata, the link between digital identifiers and physical persons, and whether uncertainty and alternative explanations are sufficiently visible to be considered. These questions concern the reliability, credibility and fairness of the material as evidence.

Questions about control arise because the material is technically complex and often travels through international evidence chains, with limited opportunities to trace the full chain of custody. The actors need to understand what is documented, what can be verified, and which parts of the process are not directly visible. When direct insight is missing, the evaluation becomes more dependent on documentation, technical control points, and institutional trust. The technical complexity makes legal actors dependent on experts or technical explanations, raising questions about the quality and independence of those experts and whether the court has sufficient knowledge to evaluate their explanations. The problem area of this thesis is therefore how such material can be evaluated, controlled, challenged, and understood in practice.

1.3 Existing Research and Knowledge Gap

Existing research provides insight into the technical platforms and components of the international operations behind EncroChat [OvT22] and Sky ECC [OR23]. This research addresses legal and human rights issues which arise when material from such platforms is used in criminal proceedings [OvT22; OR23]. The literature discusses how encryption and material from encrypted platforms are included in criminal cases in other countries, especially in the Netherlands, where it points to issues concerning evidentiary value, legality, technological complexity, and competence [WBJ+25]. More broadly, literature on digital evidence raises issues of fair trial, reliability, transparency, and defence rights when technologically complex material is used in criminal cases [Sto24b].

At the same time, we were unable to identify empirical research which directly examines how Norwegian courts, defence lawyers, investigators and experts handle this type of evidence in practice. In other words, the existing literature provides insight into the platforms, operations, and several judicial and human rights issues that arise, but offers much less insight into how institutional actors actually evaluate and work with the material. This includes how reliability, credibility, and fairness are assessed in practice; how the chain of custody and international cooperation are handled in concrete cases; how excerpts of the material are presented in court;

and what informal standards and forms of competence shape the handling of this technically complex material.

This knowledge gap motivates this study. When material from encrypted platforms has come to play a central role in serious criminal cases, and research provides very limited insight into how such evidence is handled in practice in Norway, there is a need for an empirical, practice-oriented examination of this issue. We therefore examine how different actors understand, evaluate, and handle this type of evidence, which forms the basis for the objective and research questions presented in the next section.

1.4 Objective, Research Questions and Scope

The objective of the project is to examine how communication material from encrypted platforms is handled as evidence in Norwegian criminal proceedings. We examine how different legal actors describe, evaluate, and handle this technically complex evidentiary material, which has moved from large encrypted datasets abroad and undergone several processing stages before being presented as excerpts in Norwegian courts. This leads to our research questions, which guide our study:

RQ1: *What legal and procedural challenges emerge when decrypted communication is presented as evidence during judicial proceedings?*

RQ2: *How do judges, defence lawyers, and investigators evaluate the reliability, credibility, and fairness of decrypted communication as evidence?*

RQ3: *What mechanisms ensure transparency and maintain the chain of custody when decrypted material is obtained through cooperation with foreign authorities?*

RQ4: *What safeguards exist to prevent misuse or selective presentation of decrypted evidence?*

RQ5: *What standards or best practices guide forensic experts in decrypting and authenticating communication?*

RQ6: *To what extent do judges and lawyers rely on expert testimony to understand technical aspects of decrypted evidence?*

Our study is limited to a Norwegian context and to how this type of evidence is handled in Norwegian criminal proceedings. Empirically, our study is based on 11 qualitative interviews with various institutional actors and two selected judgments.

Our main context is Sky ECC, with EncroChat serving as background and for comparison where relevant. EncroChat is included because it raises many of the same

evidentiary issues as Sky ECC: international collection, large-scale datasets, technical secrecy, partial insight into processing, and the use of selected communication material in court. The goal is to use EncroChat as a comparable example showing that the challenges studied here are not unique to Sky ECC. Since both EncroChat and Sky ECC have already been targeted and used as evidence in criminal proceedings, similar questions are likely to arise in future cases involving other platforms.

We conduct a practice-oriented, descriptive study, not a normative assessment of whether current law should be changed or a technical verification of the underlying Sky ECC material. We examine how legal actors describe, evaluate, challenge and work with this type of evidence in practice, including how they handle technical uncertainty, insight, control and expert dependence.

1.5 Contribution

Our study provides empirical insight into Norwegian practice and sheds light on a field of practice that has not been researched before. It shows how different actors describe the practical handling of communication material from encrypted platforms. We identify the practical questions legal actors face when technically complex evidence is used in court, especially questions concerning selection, documentation, interpretation, access, control, and expert dependence. By bringing together perspectives from judges, defence lawyers, investigators and experts, the study shows how these questions appear across different roles in the evidence process. We therefore provide a basis for further discussion of routines, competence, access, documentation, and expertise in cases where complex digital evidence plays a central role.

1.6 Thesis Structure

The remainder of the thesis is structured as follows. Chapter 2 provides the technical and evidentiary background needed to understand encrypted communication platforms, international data collection, processing, and presentation, as well as the limits of technical visibility. Chapter 3 explains the research design, data collection, interview process, judgment selection, data analysis, and ethical considerations. Chapter 4 presents the empirical findings from the interviews and selected judgments. Chapter 5 discusses the findings in relation to the research questions and considers their broader implications, limitations, and relevance to sustainability. Finally, Chapter 6 summarises the main findings, outlines the study's contribution, and points to future research directions.

Chapter 2
Technical and Evidentiary Background

This chapter provides the technical and evidentiary background needed to understand how communications from encrypted platforms are collected, processed, and presented as evidence in criminal proceedings. We focus primarily on Sky ECC, as this is the platform most central to the empirical material in this thesis. EncroChat is included because it raises many of the same evidentiary issues as Sky ECC, including international collection, large datasets, method secrecy, limited insight into processing, and the use of selected communication material in court. It is not analysed as a separate empirical case, but used as a comparable platform to show that the challenges discussed in this thesis are not unique to Sky ECC.

Unlike more widely used platforms such as WhatsApp and Signal, Sky ECC and EncroChat were tied to modified devices and closed communication ecosystems. This distinguishes them from more ordinary messaging services, both in how communication was technically organised and in how authorities later gained access to the data. We therefore outline the key technical characteristics of the platforms, how access to communication was achieved, how the material was processed and presented, and the limitations related to technical visibility.

2.1 Encrypted Communication Platforms

We begin by outlining the main characteristics of Sky ECC and EncroChat as communication platforms. We focus on technical features relevant for understanding how communication on these platforms was structured and later used as evidentiary material.

2.1.1 Technical Characteristics of Sky ECC and EncroChat

Sky ECC [OR23] was an encrypted communication service. Sky ECC phones supported encrypted messages, email, group chats, voicemail, and images. The service was operated from the United States and Canada, using computer servers based in

France. Sky ECC included messages that were automatically destroyed after a set period, a distress password, and a kill switch that allowed users to wipe data from the device.

EncroChat [OvT22] was a comparable encrypted communication service which offered modified smartphones with pre-installed apps for encrypted messaging, voice calls, emails and note-taking. Like Sky ECC phones, EncroChat devices can be understood as *cryptophones*, which are modified devices designed to enable anonymous, secure communication. For EncroChat, the camera, microphone, GPS, and USB port were removed or deactivated [Eur21, Para. 7.2]. All network traffic was routed through servers in France [OvT22]. The devices included functionality to delete all data stored on them.

Both services, therefore, combined encrypted communication with modified devices, closed communication environments, and deletion functionality. These characteristics are relevant because they shaped both how users communicated and how the resulting material later appeared as evidence.

2.1.2 User Identifiers, Metadata, and Messaging Features

The Borgarting Court of Appeal [LB-2024-142625] in Oslo, Norway, states that Sky ECC users were identified by a unique Sky ECC ID consisting of six letters and digits. Users could choose profile names, and different users could have the same profile name. The identification in the system was therefore connected to an internal Sky ECC ID, not to profile names.

The same judgment [LB-2024-142625] shows that the data provided access to the device's IMEI number, making it possible to link the Sky ECC ID, device, and SIM card. All traffic on the Sky ECC phones passed through data SIM cards owned by Sky Global, allowing the collection of telecommunications data related to their use. In the Sky ECC service, a user had to be added as a contact to send messages or add them to a group. The system, therefore, had a structure in which communication was tied to internal user identifiers, specific devices, and saved contacts. This relationship between platform users, identifiers, devices, and communication data is illustrated in Figure 2.1.

Communication within the Sky ECC system consisted of message exchanges between user profiles. For Sky ECC, the Borgarting Court of Appeal [LB-2024-142625] notes that the service supported one-to-one and group chats and that text, picture, and voice messages could be sent. Received messages were deleted from the phone after a user-defined period. The judgment states that the Joint Investigation Team (JIT) countries, France, Belgium, and the Netherlands, collected about a billion

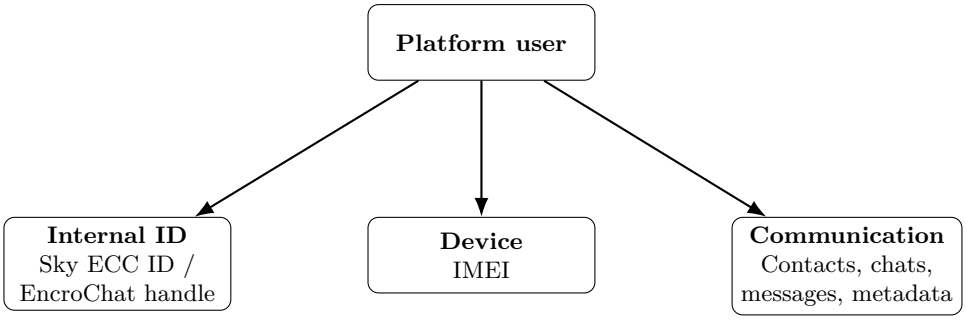


Figure 2.1: Simplified overview of how a platform user can be linked to identifiers, devices, and communication data.

messages distributed across 170,000 Sky ECC IDs, of which approximately 60% were decrypted at the time of the judgment.

In the EncroChat system, users were identified by platform-specific pseudonyms, as the Court of Appeal in England and Wales [Cou21, Para. 11] held that, to communicate with someone, a user needed to know that person's handle. Further, the Investigatory Powers Tribunal [Inv23, Para. 125] indicates that registered users were *"provided a randomly generated 'username' which does not identify them"*. The identification in EncroChat was therefore based on internal, platform-generated usernames.

In addition to platform-specific identifiers, the system included device-specific identifiers. In the German Federal Court of Justice 5 StR 457/21 [Bun22, Para. 12], it is stated that the collection included, among other things, the IMEI numbers, pseudonyms of EncroChat users, and the address books and contacts stored on the device.

For EncroChat, more than 120 million messages from approximately 60,000 users were collected [OvT22]. In both systems, the material consisted of large collections of messages connected to user IDs and metadata.

2.2 Interception and Technical Access

We now outline how available sources describe access to communication from Sky ECC and EncroChat. The section focuses on the international framework for data sharing and the technical interventions that appear to have enabled collection and decryption.

2.2.1 Interception Operations and International Data Sharing

The Sky ECC and EncroChat operations involved French authorities gaining technical access to the platforms' server infrastructure. In the Sky ECC operation [Sag23], a JIT was established among France, Belgium, and the Netherlands, and a French judge authorised the infiltration of the servers before the service was shut down. In the EncroChat case [OvT22], both servers and devices were hacked as part of a JIT among France, the Netherlands, and Europol.

After access was established, the collected material was made available within the JIT framework. In the Sky ECC operation, the three JIT countries developed a tool to decrypt the data [Sag23]. In Norway's case, Kripos received data multiple times since March 2021 [LB-2024-142625]. In the EncroChat case, data was transferred to Dutch authorities and Europol, and then shared with other European partners [OvT22].

2.2.2 Technical Access and Decryption

For Sky ECC, after the JIT was established, Dutch technicians developed a technique to copy the random access memory (RAM) of a Sky ECC server without the server going offline [OR23]. A man-in-the-middle technique was developed, enabling decryption of the messages. This approach aimed at obtaining encryption keys and/or passwords from the system.

Oerlemans and van Toor [OvT22] describe how the French authorities accessed EncroChat by hacking the servers and devices, and collecting the communication data within a JIT framework. Authorities took copies of virtual machines from EncroChat servers hosted by OVH in Roubaix, and installed a technical solution for data collection [APSS24]. Plaintext messages were also collected directly from the devices via distributed software, with end-to-end encryption left unchanged.

Together, the available sources describe both operations as interventions at the level of system architecture and key management, rather than as cryptanalytic breaks in the underlying encryption algorithms. The relevant weakness was therefore not the encryption algorithm itself, but the surrounding systems through which communication was accessed.

2.3 Data Processing and Representation

We now examine how available sources describe the processing of communication data from Sky ECC and EncroChat after collection. The section focuses on how the material was structured, analysed, and later presented as evidence in criminal proceedings.

2.3.1 From Raw Data to Structured Datasets

The collection of communications from Sky ECC and EncroChat resulted in large datasets comprising messages and associated metadata from the compromised platforms. The available sources provide only partial insight into how this raw data was stored, structured, and made accessible for further investigation.

For Sky ECC, the collected material was stored in PCAP files and later stored in a database [LB-2024-142625]. Norwegian police then received *data packages* for selected Sky ECC IDs and a *country package* in April 2024. The *data packages* contained one folder per Sky ECC ID, and each folder had subfolders for every user the ID had communicated with. The messages were provided in tabular CSV and XLSX formats. Media files were stored in another subfolder. The content of these data packages was exported from *Chat X*. *Chat X* is an artificial intelligence software [Goo24] developed by the Dutch police, which Europol has been using to read and analyse the decrypted messages. The *country package* was in JSON format, and these excerpts were directly from the JIT countries' database, not from Chat X [LB-2024-142625]. Kripos, the National Criminal Investigation Service in Norway, imported these JSON files into a database and then exported selected fields to CSV. The defence lawyers have received data from both the *data packages* and the *country package*, but not all of the available material. This shows that raw network traffic in PCAP format was collected, decrypted, and organised in a database by the JIT countries, then exported in structured formats (CSV/XLSX/JSON) before being sent to Norway, where it was again structured in a national database before being used in the investigation.

For EncroChat, national authorities gained access to the data through a web interface developed by the French authorities [LB-2021-164345]. This indicates that the data was collected in a structured, centralised database, enabling search and selection. Kripos received real-time data from April 2 [LB-2021-164345], showing that the material included a running data stream rather than only stored information. The Borgarting Court of Appeal judgment *LB-2022-147596* [LB-2022-147596] indicates that the evidentiary presentation relied on chat logs from Sky ECC and EncroChat, which the court considered highly credible. These logs are used together with other data sources, such as toll road passage records and cell site data. The use of the material, together with toll road and cell site data, presupposes the presence of timestamps and identifiers. At the same time, the Norwegian judgments offer limited insight into the concrete details of the steps from interception and decryption to the production of structured evidentiary material. The court describes which data types are involved and how the material was used as evidence, but not specifically which file format, parsing process, database architecture, or documentation were used in the transformation stage.

2.3.2 Investigative Software and Filtering

After the communication data had been collected and structured into datasets, the material had to be analysed to identify relevant information within the large volumes of messages and metadata.

There is limited publicly available information on how the Sky ECC operation was analysed after collection. The available sources mainly describe national analysis rather than a centralised analytical system. Oerlemans and Royer [OR23] state that in the Netherlands, the analysis was performed using the forensic platform *Hansken*, developed by the Dutch National Forensic Institute (NFI). This system is widely used in the Netherlands, where analysts can use *topic lists* to search for specific, relevant keywords. The Dutch NFI has been using artificial intelligence to analyse the large volume of intercepted data. For Belgium, Oerlemans and Royer [OR23] state that there is no case law addressing how data from the Sky ECC operation is analysed. From Norway, two police officers were sent to Europol in The Hague, where Kripos participated in an analysis project from April 2021 [LB-2023-104594]. They were able to search the decrypted material for content related to Norway. After a brief processing procedure, the relevant findings were sent to Kripos in Norway. From the Borgarting Court of Appeal judgment *LB-2024-142625* [LB-2024-142625], it appears that the *data packages* were exported from the analytical software *Chat X*, which was used by Europol to read and analyse messages. The judgment shows that the received data was imported into databases and structured by the Norwegian Police.

For EncroChat, available sources indicate that the analysis was conducted in cooperation with Europol [Eur21, Para. 7.2], and a large, dedicated team at Europol investigated messages received from the JIT partners [OvT22]. However, the sources say little about the specific technical tools and filtering procedures used. In *SF and Others v National Crime Agency* [Inv23, Para. 37-9] in England, Emma Sweeting, an Intelligence Operations Manager at the National Crime Agency, notes that keyword searches may be conducted by Europol. The same source states that all data would be sent to Europol, where triage would take place [Inv23, Para. 37-10], and that it is unknown if there is a filter at Europol.

Overall, the available sources provide limited insight into the specific analysis tools and filtering processes used in the Sky ECC and EncroChat investigations. Even where national practices are described, the detailed analytical processes used by the investigators remain undisclosed in publicly available sources.

2.3.3 Evidentiary Representations of Communication Data

When communication data from Sky ECC and EncroChat is used in criminal proceedings, the material is presented as selected message excerpts and chat logs, rather

than the full dataset. Norwegian case law illustrates this, with courts referring to specific conversations rather than the full datasets. For example, in the Borgarting Court of Appeal judgment *LB-2024-142625* [LB-2024-142625], part of the evidence is excerpts from Sky ECC communication between selected Sky ECC IDs. These chat logs are presented together with other evidence to reconstruct events relevant to the criminal investigation. A similar pattern appears in EncroChat cases. For example, in Agder Court of Appeal judgment *LA-2023-74900-3* [LA-2023-74900-3], concrete chat messages tied to specific users were presented in court, rather than the entire dataset. However, publicly available sources provide little information about how these messages are selected and transformed from the underlying datasets into the evidentiary material presented in court.

2.4 Limits of Technical Visibility

We now address the limits of what can be known about the material's technical handling from publicly available sources. The focus is on incomplete technical documentation and limitations in data completeness.

2.4.1 Incomplete Technical Documentation

Structural limits arise when the technical processes underlying the material are only partially visible in public sources. For Sky ECC and EncroChat, the exact methods used to obtain the data are not fully publicly known. For example, Sagittae [Sag23] states that the defence did not get insight into the *"exact manner of the French interception as the French authorities seek to keep that manner secret with a view to potential future operations"*.

Norwegian cases describe which data are received and how they are structured, rather than the entire technical process from collection to evidentiary material. For example, *LB-2023-104594* [LB-2023-104594] shows that the Norwegian police searched the analysis platform *Chat X* and sent excerpts to Kripos as Excel and media files. The judgments provide insight into how the material has been handled, but do not offer a detailed technical explanation of the process.

As a result, the technical chain linking interception to evidentiary material can be reconstructed only partially from publicly available sources.

2.4.2 Partial Capture

Even though the material from Sky ECC and EncroChat consists of large volumes of data, the datasets are not necessarily complete. This is shown in the Sky ECC material, where approximately a billion messages were captured, but only 60% were decrypted [LB-2024-142625]. This means that approximately 400 million messages

were still not readable in plaintext. Borgarting Court of Appeal [LB-2023-104594] states that this might have an impact on the assessment of the evidence. There are also situations where only incoming messages are available, not outgoing.

The material is limited in terms of time. For Sky ECC, the live data capture began in February 2021 and ended in March of the same year, when the servers were taken down [Sag23]. For EncroChat, live data capture began in April 2020 and continued until June 2020 [Sag23]. The collection phase, therefore, took place within specific time frames.

The datasets can therefore be large without necessarily providing a complete picture of the communication that took place. The limitations concern both what is publicly known about the process and the completeness of the material itself.

Chapter 3
Methodology

This chapter describes how we designed and conducted the study. First, we explain the exploratory qualitative research design and the use of interviews and selected judgments as complementary data sources. We then describe the literature review, participant recruitment, interview procedure, judgment selection, and data analysis, before discussing ethical considerations and main limitations.

3.1 Research Design

This study is an exploratory qualitative study of how communication data from encrypted platforms is handled as evidence in Norwegian criminal proceedings. We chose this design because we examined how different actors understand, evaluate, and handle this type of evidence in practice, rather than measuring prevalence or testing hypotheses. The research questions focus on experiences, evaluations, working practices, and institutional challenges and therefore require a design that can capture nuances, interpretations, and variation across actors' different perspectives.

3.1.1 Qualitative and Exploratory Approach

We chose a qualitative approach to explore and understand how the different actors make sense of this complex evidentiary material. Creswell [Cre09, p. 4] describes qualitative research as appropriate when the goal is to explore and understand the meaning individuals or groups ascribe to a social or human problem. This fits our study because we examined how police, academic experts, judges, and other legal actors understand and evaluate communication data from encrypted platforms as evidence. This is supported by Robson and McCartan [CM16, p. 25], who describe qualitative methods as suitable for capturing multiple perspectives.

The approach is exploratory. Creswell [Cre09, p. 18] recommends a qualitative approach when little research has been conducted on a subject, as it is exploratory. This is suitable for our study. To the best of our knowledge, there is no empirical

research on how Norwegian courts handle this type of evidence, and an exploratory design therefore gives space to examine a field where central assessments, practices, and standards are not fully mapped in advance.

Further, the study is descriptive and practice-oriented. The purpose was not to evaluate what the court should be or do, but to examine how the actors worked with, described and handled this technically complex evidence. This supports the choice of a qualitative, exploratory approach.

3.1.2 Data Sources and Complementary Perspectives

We focused primarily on qualitative interviews with actors across different parts of the chain of evidence. In addition, we used two selected judgments as supplementary document material. The judgments do not constitute an equivalent dataset, but selected parts considered relevant to the project were coded to situate the interview material within a concrete legal context and to illuminate how certain issues are reflected in the court's own description. The design, therefore, gives insight into the actors' practices and into how this type of evidence appears in formal legal proceedings. The interviews and judgments therefore illuminate the material from different angles, and together they provide complementary perspectives. This combination provides a limited form of triangulation, which helps counteract threats to validity [CM16, p. 171]. Figure 3.1 provides an overview of the data sources and their relationships within the analysis.

3.2 Data Collection

We now describe how the study material was collected. We first present the literature review, then describe the interview data collection and the selection of the judgments used as supplementary material.

3.2.1 Literature Review

We conducted the literature review early in the project to map existing research, identify knowledge gaps, and narrow the project's objectives. As Creswell [Cre09, p. 23] describes, a literature review helps the researcher to limit the scope to a precise area. We used the literature review to build the project's background and examine whether empirical research existed on the handling of communication data from encrypted platforms.

We designed the review as a targeted literature search and thematic review adapted to the project's purpose. Creswell [Cre09, p. 29] states that a literature review is to find and summarise studies on a topic, which we used as a starting point. The main focus was to find research on digital evidence, communication

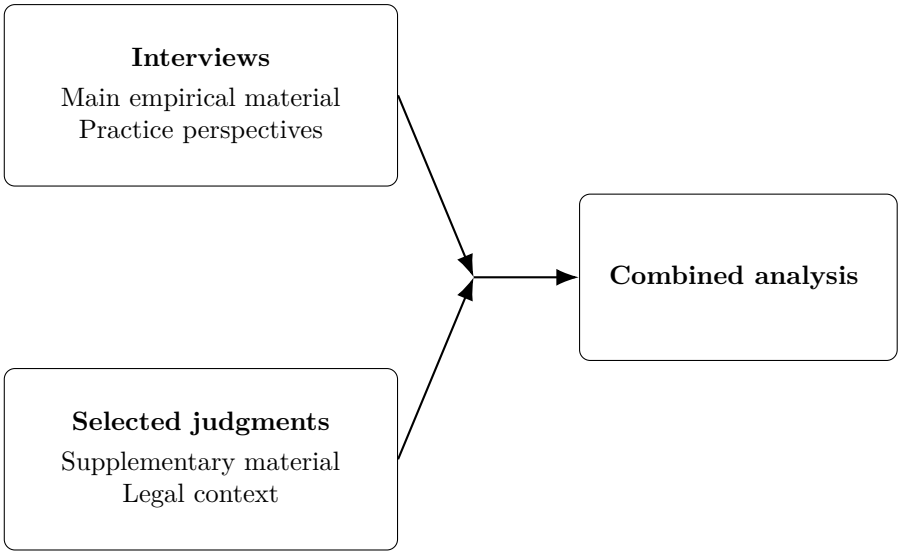


Figure 3.1: Overview of the study's data sources and how they are brought together in the analysis.

material from encrypted platforms, evidentiary assessment, technical uncertainty, transparency, selection and filtering, and international evidentiary cooperation in criminal cases.

We used Google Scholar [Goo26] as the main search tool. We also used Lovdata [Lov26a] and Lovdata Pro [Lov26b] to identify relevant Norwegian judgments, and regular Google searches to supplement, especially to find news reports, legal commentaries, and other material not available via Google Scholar. When we used grey literature such as media articles and legal commentaries, we considered the source's relevance, the author or publisher, and whether the material was used as contextual information rather than as the main basis for analytical claims. We based the search process on Norwegian and English search terms and their combinations. Some example search strings include:

- `"selected excerpts" digital evidence court`
- `digitalt bevis AND bevisrett`
- `"chain of custody" "cross-border" digital evidence`

In line with Creswell's recommendation [Cre09, p. 29] to identify key terms early and use them in searches after relevant literature, we organised the searches around central terms in the project and refined them as the research problem became clearer. We conducted forward and backward searches to identify additional relevant literature.[2]

[2]Parts of this paragraph are rewritten from the Specialisation Project [Bus25].

We documented the search process in a search log that recorded dates, search strings, databases, and brief comments on results for parts of the process. We consider the documentation insufficient to fully reproduce the review, but it has supported the project's development and helped identify central themes and knowledge gaps along the way. The literature review showed that there is relevant research on digital evidence more broadly, as well as related work on surveillance powers, human rights, and fair trial concerns. There were some studies on Sky ECC and EncroChat, particularly from the Netherlands and the UK. However, we found no empirical research that directly examined how Norwegian courts and other institutional actors handle communication data from encrypted platforms as evidence in practice, thus underlining the novelty of the current study.

3.2.2 Interview Data Collection

Interview Design

The interviews were semi-structured and open-ended. This aligned well with our study, and Creswell [Cre09, p. 181] states that qualitative interviews involve few unstructured, open-ended questions intended to elicit participants' views and opinions. Semi-structured interviews fit our study as they provide a shared thematic structure across participants while retaining flexibility to follow up on participants' own experiences, terms, and examples, and to allow different actors to illuminate different parts of the evidence chain.

The interview design was shaped in several steps. The participant identifiers used below refer to the overview in Table 3.2. The first two interviews had more open guides and were conducted with international academic experts to gain a broader overview before the remaining interviews focused more specifically on Norwegian practice and cases. The interview with A1 served as an early, open-ended background interview to identify central challenges, relevant perspectives, and questions for further exploration. The second interview, with A2, had a more technical, expert-oriented focus, addressing calibration and what experts can and cannot know under conditions of technical uncertainty. This interview was used to understand the limitations, assumptions, and blind spots in technical analysis.

After the first two interviews, a shared interview guide was developed for the other participants. First, overall themes were developed based on the research questions, identified knowledge gaps, and the need to understand workflow and practice. The shared interview guide contained open-ended main questions, follow-up questions, notes for the interviewer, reminders about consent and voluntariness, reflections on what each question addresses, and a mapping of questions to relevant research questions. It was structured to start with warm-up questions, then present the main

Table 3.1: Role-based emphasis in the interviews

Participant category	**Main emphasis in the interview**
Judges	Evidential assessment, the court's understanding of technical material, control questions, and courtroom safeguards.
Defence lawyers	Access to material, contradiction, equality of arms, and how the evidence can be challenged.
Police/investigators	Collection, analysis, selection, filtering, and preparation of the material for investigation and court.
Academic experts	Technical uncertainty, expert knowledge, methodological limits, and interpretation of technically complex evidence.
Recently graduated lawyer	Legal education and how questions concerning digital evidence and communication material from encrypted platforms are addressed in legal training.

questions with a deeper focus, and then proceed to round-off questions, as advised by Tjora [Tjo19, p. 114]. The interview guide is provided in Appendix A.

The guide served as a flexible interview protocol, allowing the same overall themes to be covered across participants while enabling adjustments to the interviews based on the participant's role. Examples of this role-based adjustment are shown in Table 3.1.

The guide included instructions for the interviewer, such as avoiding bias, asking open, non-leading questions, seeking concretisation when answers are too abstract, and using follow-up questions to clarify ambiguities. These instructions helped elicit the participants' own descriptions. They also helped to keep the interviews focused on how participants describe practice, uncertainty, control mechanisms, and challenges, rather than steering them toward confirming predefined assumptions.

Participant Categories

The interview sample included participants from different parts of the evidentiary chain and from different institutional perspectives, all of which are relevant to our study. Judges were included because they are responsible for evaluating evidence in court. We also interviewed defence lawyers to include the defence perspective on access, contradiction, and how the evidence can be challenged. The police participants were included to provide insight into the investigative handling, analysis, selection, and preparation of the material. Academic experts were included to give a broader perspective on digital evidence, criminal procedure and institutional practice. A

Table 3.2: Overview of interview participants, participant categories, and gender

ID	Participant category	Gender
J1	Judge	M
J2	Judge	M
D1	Defence lawyer	M
D2	Defence lawyer	M
P1	Police/investigator	M
P2	Police/investigator	M
P3	Police/investigator	F
A1	Academic expert	M
A2	Academic expert	M
A3	Academic expert	M
L1	Recently graduated lawyer	M

recent law graduate was included to gain insight into how questions related to digital evidence and materials from encrypted platforms are addressed in legal education. To ensure anonymity, while the differences in roles are visible in the analysis, participants are referred to using role-based pseudonyms, such as J1 and J2 for the judges, D1 and D2 for the defence lawyers, P1 to P3 for the police participants, A1 to A3 for the academic experts, and L1 for the recently graduated lawyer. This is shown in Table 3.2, which also includes each participant's gender. The table shows that the interview sample was strongly male-dominated, comprising 10 men and 1 woman. This imbalance is worth noting, as it may have influenced which experiences and perspectives are most visible in the material.

Recruitment and Sampling

The recruitment process started during the specialisation project in autumn 2025. The selection was purposive, aimed at recruiting participants who could illuminate different parts of the evidence chain. The actor groups were chosen because they represent different institutional positions in the handling of communication material from encrypted platforms as evidence. This follows Creswell's description of qualitative sampling [Cre09, p. 178], in which participants are purposively selected because they can help the researcher understand the problem and the research question. The recruitment process was iterative, with potential actor groups and individuals first broadly mapped. Then, the selection was narrowed based on who had relevant experience, who could provide specific perspectives, and which roles were missing.

We used several recruitment channels. Some participants were recommended by supervisors; some were identified through personal networks or acquaintances of

acquaintances; some were recruited through direct contact with institutions; and some were identified as relevant through online searches. For courts and Kripos, recruitment was conducted through institutional contact points via email before the request was sent internally to the relevant people. The recruitment process was influenced by practical access. Some potential participants did not respond, some lacked the capacity, and others assessed that they lacked sufficient competence in the area. For example, the Gulating Court of Appeal did not have the capacity to participate. The defence lawyers were the most challenging actors, and for a long time, we had only one defence lawyer before D2 was recruited late after reaching out to several relevant candidates. Overall, the recruitment strategy yielded a selection that covers central parts of the evidence chain and is also influenced by practical access, networks, and participant availability.

Interview Procedure

The interviews were conducted from December 2025 to April 2026, with most taking place at the end of February and the beginning of March. A timeline of this is shown in Figure 3.2. In total, 11 interviews were conducted, with one interview per participant. The interviews lasted for approximately 30-60 minutes. Nine were held digitally on Microsoft Teams, and two were held in person.

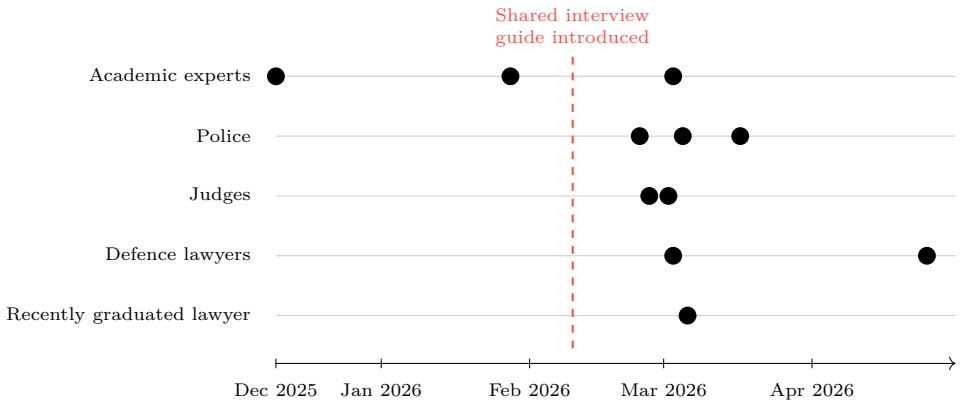


Figure 3.2: Timeline of the interviews by participant category. The dashed line marks the transition from the two initial background interviews to the interviews conducted with the shared interview guide.

All participants received an information letter by email before the interviews. The letter explained the purpose of the project, what participation entailed, that the interview would be recorded, that participation was voluntary, how personal data would be treated, that participants would be anonymised, and that there would be

no negative consequences for not participating or for later requesting deletion of data. Consent was collected in different ways. Some signed the consent form and returned it, whereas most confirmed by email that they had received the information letter and consented to participate. Everyone also gave their oral consent at the beginning of the interview. The participants were also reminded at the beginning that the interview would be recorded; that they could choose not to answer any question; that we were interested in their own experiences and assessments; that they could take back anything they said; and that more information was available in the information letter.

All interviews were recorded using the Nettskjema Diktafon mobile application [Uni26b] and stored in Nettskjema [Uni26a], where they were automatically transcribed. For English interviews, we used OpenAI Whisper V3; for Norwegian interviews, we used NB Whisper. After the automatic transcription, we reviewed the transcripts while listening to the recordings and manually corrected mistakes where necessary. The Norwegian interviews required more manual correction than the English ones. Since all interviews were audio-recorded, transcription was planned as part of the interview procedure, in line with Creswell's recommendation [Cre09, p. 183] that researchers plan transcription when audiotaping is used.

A1 and A2 were interviewed in English, and the remaining interviews were conducted in Norwegian. The transcriptions were not translated before analysis, and the English and Norwegian transcriptions were coded together in NVivo [Alf26]. Quotations were translated only when being used in the thesis text.

After each interview, we wrote short notes to record immediate reflections, impressions from the interview, possible themes to follow up on later, and points for analysis in NVivo.

3.2.3 Judgment Data Collection

Selection of Judgments

Two judgments were selected as supplementary document material: the Oslo District Court judgment TOSL-2022-185848 and the Borgarting Court of Appeal judgment LB-2024-142625. We found these judgments by searching Lovdata and Lovdata Pro using terms such as `Sky ECC` and `EncroChat`. The judgments were selected for their detail and ability to address the research questions. This aligns with Creswell [Cre09, p. 178], who notes that a key idea in qualitative research is to purposively select documents to help the researcher understand the research questions.

The Oslo District Court judgment was chosen because it is the first-instance judgment in the same case complex and shows how the case was treated and presented

in the District Court. The Borgarting Court of Appeal judgment was chosen because it is the appeal judgment in the same case complex and provides further detail about the Sky ECC material. These cases are particularly relevant, as the Oslo District Court [TOSL-2022-185848] writes that the main part of the indictments against the seven defendants is tied to material which Kripos received from Europol from Sky ECC. The case was extensive, as the District Court [TOSL-2022-185848] held the main hearing from 19 September to 12 December 2023 and heard evidence from 26 witnesses. The appeal hearing spanned 26 court days and involved 18 witnesses [LB-2024-142625]. The case has been featured in the media, and was described as one of the largest drug cases in Norwegian history [Sto24a; SE24].

Role of Judgments in the Study

The interviews are the primary material in the study, and the judgments serve as supplementary material. They should not be treated as the same kind of data as the interviews, and they are used mainly to provide context. They give a concrete legal framework around what the participants describe in the interviews. This allows comparison of the interview findings with an actual Sky ECC case in the Norwegian courts. Creswell [Cre09, p. 178] mentions that qualitative researchers often gather several forms of data, rather than relying on a single data source. The interviews offer the actors' experiences and evaluations, whereas the judgments provide the court's own descriptions of how the evidence has been understood, presented, and evaluated; together, they offer complementary perspectives. The judgments are compared with the interviews to determine whether themes from the interviews appear in the court's reasoning. For example, participants discussed fragmentation, and the Borgarting judgment describes fragmentation in the form of one-sided dialogue and missing messages. The judgments, therefore, tie the actors' experiences to court practice. They show how the challenges participants describe in practice are reflected in concrete court decisions.

3.3 Data Analysis

The data analysis focused primarily on the interview material, with the selected judgments serving as supplementary documents. We analysed the interviews thematically to identify patterns in how participants described the handling of communication material from encrypted platforms as evidence, technical uncertainty, access, insight and control, and the use of experts. The interview analysis was mainly inductive, meaning that the codes grew largely from the material rather than from a predefined codebook. At the same time, the analysis was informed by the research questions and the interview guide. This aligns with Creswell's description of qualitative analysis [Cre09, pp. 184-185], in which they build their patterns, categories, and themes from the bottom up.

Before coding, we familiarised ourselves with NVivo by watching two tutorial videos by Jaroslaw Kriukow [Kri25; Kri26]. We began the coding with the L1 transcript because it was less technical and provided a practical entry point into NVivo and the material. At first, we coded more openly, selecting text excerpts that seemed relevant to the research questions. We started with short quotations, but later included longer excerpts and paragraphs when context was important. The coding remained flexible, and new codes were created as new themes or perspectives emerged. This follows Creswell's description of coding [Cre09, p. 186], as he describes it as *"the process of organising the material into chunks or segments of text before bringing meaning to information"*.

We used NVivo to organise and code all the interview transcripts and the selected parts of the judgments. The codes served as a folder system, allowing text excerpts from different interviews to be grouped under a single theme. This enabled us to see which themes recurred across participant groups. We exported the codes from NVivo and printed them for easier reading on paper and to view connections outside the NVivo interface.

After one main coding round, we reviewed and reorganised the codes. We merged overlapping or similar codes into broader codes. Then, the codes were organised into four larger analytical themes, corresponding to the structure in the results chapter:

- From Communication Material to Evidentiary Excerpts
- Transparency, Traceability and the Limits of Visibility
- Interpretation, Uncertainty and Evidential Reliability
- Expertise, Dependence and Safeguards in Court

Table 3.3 gives an overview of the final coding structure at the subtheme level, including the number of files and references coded under each subtheme.

We analysed the judgments selectively, and we did not code the entire judgments, as only parts of them were relevant for our study and research questions. We focused on the parts of the court opinions where the court describes and treats the Sky ECC material as evidence, and the purpose was to examine how courts describe and handle the same kinds of issues mentioned in the interview material. The coding of the judgments was therefore more deductive than the coding of the interviews, as it relied on codes already in the coding tree. When a judgment excerpt matched an existing code, it was coded under that code; otherwise, a new code was created. The judgments were used as supplementary coded material.

We then read the material across participant groups and compared it with the selected judgment excerpts. This allowed us to see which themes multiple actors described, where tensions between perspectives arose, and which themes were tied to a specific role. This was important because the research questions concern different

Table 3.3: Overview of coding structure

Main theme	Subtheme	Files	References
From communication material to evidentiary excerpts	Access, search and filtering	7	12
	Selection and exclusion	11	31
	Transformation into courtroom material	7	25
Transparency, traceability and the limits of visibility	Documentation and chain of custody	8	23
	Limited insight	11	35
	Practical limits on verification	10	22
Interpretation, uncertainty and evidential reliability	Incomplete and fragmented material	6	12
	Interpretation and meaning	7	24
	Sources of error and overconfidence	6	17
Expertise, dependence and safeguards in court	Technical competence of legal actors	7	18
	Experts and expert dependence	10	37
	Courtroom safeguards	9	49

actors in the evidentiary process, and the analysis is not only about what is said but also about which actor said it. While writing the results chapter, coded excerpts were used to identify relevant examples and quotations. We used quotations selectively where they expressed a central point. Multiple findings were therefore presented as summaries of the participants' descriptions, with some direct quotations where the formulation was especially precise or analytically useful. The results chapter was written thematically rather than interview-by-interview, so the findings are presented after the analytical themes, including views from different actors along the way.

3.4 Ethical Considerations

The project was reported to Sikt [Sik26], the Norwegian Agency for Shared Services in Education and Research. Sikt assessed the processing of personal data before the main data collection. This assessment supported the planning of data handling in accordance with Norwegian privacy requirements. The legal basis for processing personal data was consent, and an information letter was sent to all participants before the interview. The information letter explained the project's purpose, what participation entailed, that the interview would be recorded, how data would be

stored and used, that participation was voluntary, their right to withdraw consent, and their right to request the deletion of information. All participants either signed the consent form or confirmed via email that they received the information. We also reminded the participants of this at the beginning of the interview. The purpose of this reminder is to ensure informed participation in practice and to clarify that the participant has control over what participation entails.

Participants are referred to by role-based pseudonyms in the thesis, and unnecessary identifying details were removed during the review of the automatic transcription. We recorded the interviews using the Nettskjema Diktafon mobile application, while transcripts and NVivo files were stored on a password-protected laptop and in OneDrive. The automatic transcription was performed through the Nettskjema/Autotekst solution. UiO [Uni26c] describes Autotekst as a service that uses models from OpenAI and the National Library of Norway and states that it runs on secure servers at the University of Oslo in Norway. The recordings were not uploaded manually to external transcription services. Raw data will be deleted by the end of the project period. Even though the participants are professional actors, the material was handled with care because of sensitive topics such as criminal proceedings, evidentiary practices, and institutional work.

Limitations of the study are discussed in Section 5.7.3.

Chapter 4
Results

This chapter presents the findings from the interviews, supplemented by observations from two selected judgments: the first-instance judgment from the Oslo District Court and the appeal judgment from the Borgarting Court of Appeal. The presentation follows how communication material from encrypted platforms moves from large volumes of data, through search, filtering, documentation, and interpretation, to the court's handling of it as evidence. We organise the chapter into four analytical parts that show how communication material from encrypted platforms becomes usable evidence, how access limits and documentation shape what actors can verify, how uncertainty affects the interpretation of messages and metadata, and how the court tries to understand and control the technically complex evidence. We use participant identifiers throughout the chapter to indicate the role perspective behind each finding. An overview of the participant categories and identifiers is provided in Table 3.2. Figure 4.1 provides an overview of how the four parts of the results chapter relate to the research questions.

4.1 From Communication Material to Evidentiary Excerpts

The first part follows how material from encrypted platforms is processed before it reaches the court. The findings show how large volumes of data are searched, filtered, selected, and transformed into evidentiary excerpts for presentation in court.

4.1.1 Access, Search, and Filtering

A first feature of the *life-cycle* of technically complex evidentiary material is that the process starts with very large datasets that must be made searchable and manageable before they can be used further. Several participants described this as a process of navigating extensive, unstructured material, where a full review is not possible in practice. P2, for example, explained that they naturally do not have the time to sit and read about 170,000 users. Similarly, P3 described that in such cases, it is a matter of *"finding the needle in the haystack"*, and also explained that search-based

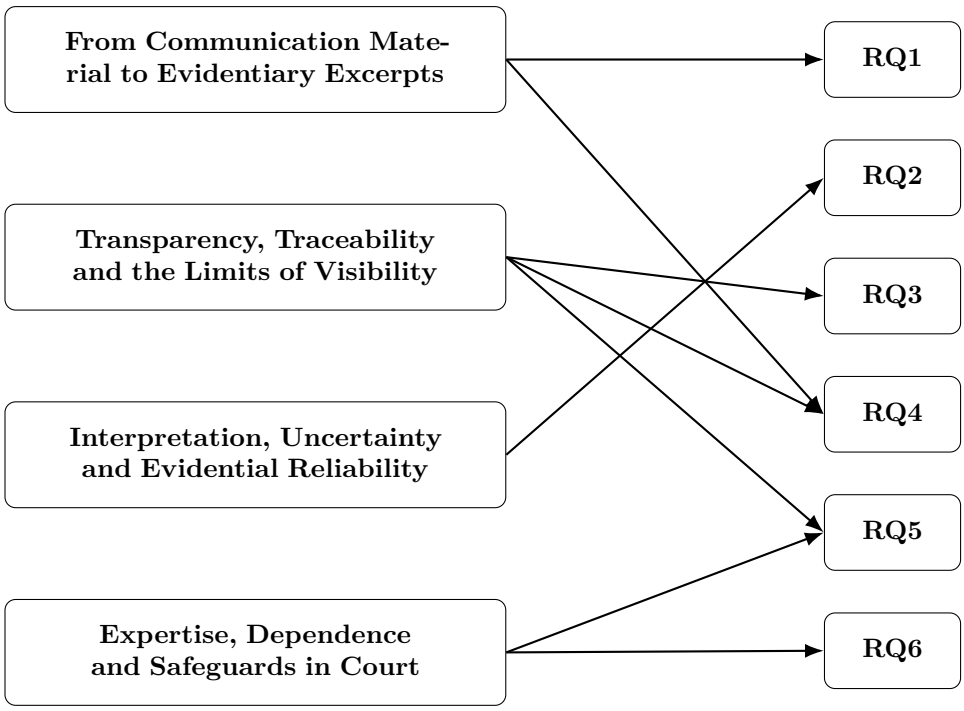


Figure 4.1: Overview of how the four results sections relate to the research questions. The arrows indicate the main connections, although several findings are relevant across more than one research question.

approaches are essential when the information volume is very large. J1 referred to material that had been converted to PDFs totalling several thousand pages, while D1 pointed out that a full presentation of all relevant material could involve millions of lines of content. The participants' descriptions could therefore point to the process, to a large extent, starting with large amounts of material that had to be searched, sorted, and filtered before it could be used further. This process from large datasets to more manageable evidentiary material is illustrated in Figure 4.2.

The **filtering** of the material seems to be guided by some clear operational criteria. P2 described two central evaluations: First, was it possible to identify the user behind the Sky ECC ID, and, if so, were the criminal acts sufficiently concrete to be investigated further? Material that fulfilled this criterion was sent to the relevant police district, either as a basis for a new case or to help an ongoing investigation.

The work on limiting the material started with a search for conditions that could be tied to Norway. P2 explained that in the large dataset, the police searched for Norwegian names of places, such as *"Oslo"*, *"Bergen"*, *"Porsgrunn"*, and *"Skien"*,

as well as specific Norwegian words, such as *"kjøre"* and *"høre"*, to find users with a higher likelihood of Norwegian relevance. Searches were therefore a necessary approach to the material, because the datasets were too large to read. At the same time, this is not described as a limitation of the material alone. P2 mentioned that once a specific user's material was first sent to Norway and the chats were read by the police here, the material could be expanded through connections in the read communications. If that user was communicating with others who appeared relevant to Norway, those users could be requested and disclosed later.

The participants described how search and filtering were supported by concrete tools and by combining the material with other digital data sources. The Court of Appeal judgment [LB-2024-142625] describes the same process, where the court described that the material was received through selected data packages and a later country package, and that Kripos imported JSON files into a database before exporting selected data to CSV. P2 explained that Excel was used for the selection work because it has a low entry barrier and is available to anyone working with the material. P2 described how the material was connected to other investigative leads, such as combining the Sky ECC data with telecommunications data from the Norwegian mobile network. J1 mentioned that communication material could be evaluated together with other traffic data. Figure 4.2 therefore summarises how access, search and filtering interact in making the material usable.

4.1.2 Selection and Exclusion

Multiple participants remarked that material that has already been selected and filtered through earlier stages of the process is presented in court. The fact that **selection** happens before the evidence reaches the court is central. J2 pointed out that *"in an extensive body of material, some degree of selection will inevitably have to take place"*, and it is the prosecuting authority that makes that selection. J1 similarly stated that selection largely occurs before the material reaches the judge and noted that this makes questions of representativeness, completeness, and context relevant. Selection therefore appears as an early and integrated part of how the material is transformed into an evidence basis.

Another point in the material is that selection is also formed by priorities during the investigation. The participants said that it is not always possible or necessary to follow everything further, even when the material contains more information than is used in the case. P1 said that in some cases, a case could be cut short if the case is sufficiently clarified, mentioning that it often becomes a question of resources. J1 stated that it is *"always a balancing of thoroughness and efficiency"*. This was described as a practical prioritisation challenge in cases where the material is larger than can realistically be followed up on. At the same time, the participants noted

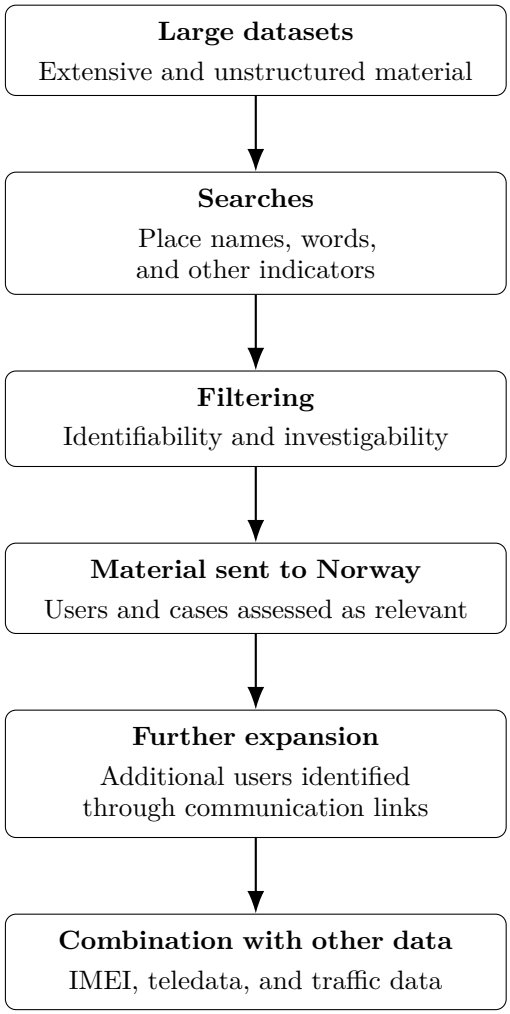


Figure 4.2: Analytical overview of how large communication datasets were described as being searched, filtered, expanded, and combined with other data sources in practice.

that such priorities are connected to the type of case and the investigative value. P1 noted that organised crime tends to justify more extensive use of resources, while P2 mentioned that when the police cannot identify the person behind a Sky ECC profile, they may close the case. Selection, therefore, depends on the content of the material, as well as on which parts investigators can realistically and usefully pursue further.

Selection can affect which context becomes visible when the evidence is later presented in the case. J1 pointed out that the selected material may later raise questions about its representativeness and completeness, and whether messages have been taken out of context, indicating that the court is aware that selection can become problematic when it affects context. From the defence perspective, D1 explained that a single message can convey a one-sided meaning when presented without the corresponding communication. D1 pointed to examples in which messages supporting one hypothesis were included, while other messages in the same conversation were omitted. D2 mentioned that this material also contains information supporting the defence's case and cited a case in which a client was acquitted because the defence found messages in the material that the police did not present. A3 pointed out that the meaning of some messages could change upon seeing the whole conversation, and P3 noted that some defence lawyers have described themselves as *"being at the mercy of the police selection process"*. P2 mentioned that limited access to materials outside one's own case is not unique to Sky ECC but applies more generally in criminal cases. Selection, therefore, serves as a practical necessity while also shaping how the material is later understood and evaluated.

4.1.3 Transformation into Courtroom Material

When the material is first made available to the court, it is presented through the parties' submissions of evidence, often in written form as part of the case documents. J1 stated that evidentiary material is often submitted to the court via written submissions. Material from encrypted platforms is therefore within the ordinary procedural framework in which evidence is brought to the court, and J1 stated that the material is not presented in any other way than other evidentiary material.

The material is often processed and made more readily available to the judge. J1 described the material as already processed and presented in a conventional evidentiary format. J2 pointed in the same direction and says that they see very little of the pre-processing and analysis of the material before it reaches the court. J1 pointed out that the way the material is presented in court does not appear to be encrypted, so what the court sees is not the encrypted communication but a decrypted, already processed version.

In court, the material is further presented in formats that make it readable and manageable. Multiple participants described the communication being presented as

excerpts, tables, timelines or PowerPoint presentations, and that messages are read as part of the evidentiary presentation. P2 explained that timelines and excerpts were prepared, while J1 and D1 referred to slide presentations that displayed selected excerpts of the material on screen. P2 mentioned that the technical parts of the material could be explained in simplified terms without going into detail on the encryption methods. P1 pointed out that in other cases where decryption is done, *"there will be a technical report on what is done to decrypt"*. The transformation into **courtroom material**, therefore, involves both selection from a larger dataset and adaptation into formats that can be presented and handled in the practical courtroom setting.

The selected Oslo District Court judgment [TOSL-2022-185848] illustrates this transformation. The court describes that the prosecution had simplified the case by splitting the indictment into 54 events and that the presentation relied on different excerpts and presentation documents.

4.2 Transparency, Traceability and the Limits of Visibility

This section presents documentation and the limits of what actors can see and verify. The findings show which conditions are necessary to trust the material, and where the actors encounter limitations in what they can actually see, follow, and verify.

4.2.1 Documentation, Provenance and Chain of Custody

Half of the participants described three elements as essential for trusting this type of material: **documentation**, **provenance**, and **chain of custody**. P3 mentioned that transparency is *"the core of reliability"* and emphasised the need for clear documentation of who handled the material, what they did, and when. They distinguished between protecting specific decryption methods and documenting the handling chain, arguing that while some methods may need protection, the handling chain is not protected in the same way. A1 described provenance as the history of a document's origin and distinguished it from the chain of custody, which concerns whether proper methods were followed at each step of transfer or handling. L1 suggested that verifiability may be sufficient if the evidence can be checked. D1 noted that without full insight into how the material from encrypted platforms was collected and processed, it is dangerous for the courts to place undue weight on the evidence. Documentation and traceability, therefore, form part of the basis for trusting the material.

This basis for trust was in practice tied to concrete forms of documentation. P2 mentioned that Kripos, for example, performed mirror tests, meaning they compared data from seized phones with data received from abroad, and the comparisons

matched. An illustration of this can be seen in Figure 4.3. Mirror tests also appear in the Borgarting Court of Appeal judgment [LB-2024-142625], where the court referred to mirror tests conducted by both the Netherlands Forensic Institute and Kripos. The judgment noted that the checksums were identical, which supports the conclusion that the reading, decryption, and storage process had not changed the data. P3 pointed out that there are other forms of integrity control, for example, using hash sums, which enable later demonstration that seized material has remained unchanged. An example of this was explained in the District Court judgment [TOSL-2022-185848], which stated that media files from seized phones were compared with received data using checksums, and no discrepancies were found in sender, recipient, or time information where such information existed in both datasets. In another case concerning decryption attempts, P1 explained that these attempts, including failures, are logged and that the logs would normally be found in the case reports. Together, these points indicate that documentation and chain of custody derive their meaning from how digital material is tested, stored, and documented throughout the process.

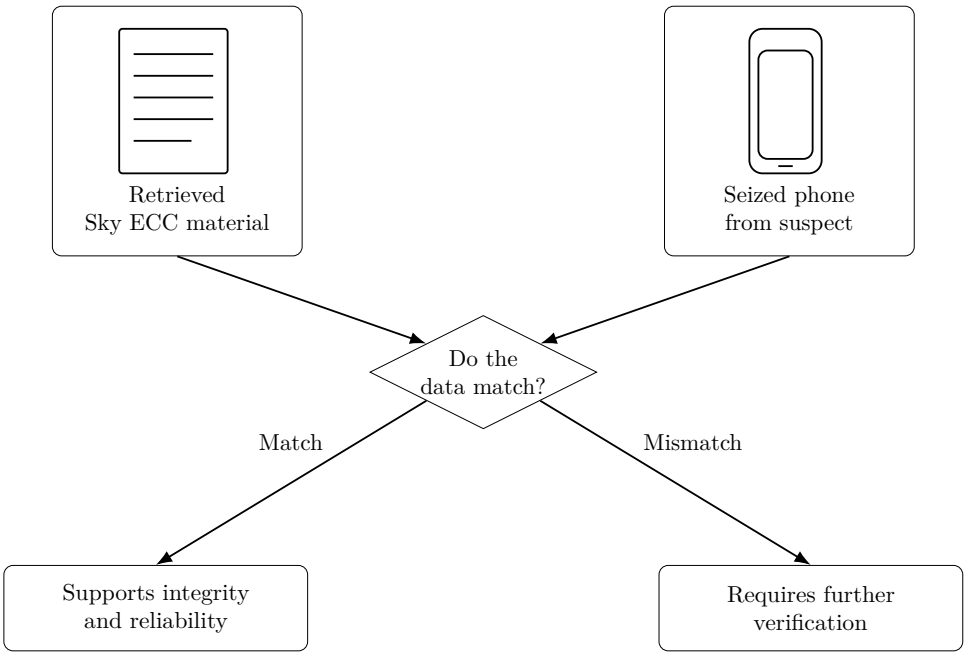


Figure 4.3: Simplified illustration of a mirror test. Received Sky ECC material is compared with data retrieved from a seized phone. A match supports the integrity and reliability of the material, while a mismatch may indicate a need for further verification.

Multiple participants described reliability as tied to the handling chain around

the material. P3 emphasised the importance of traceability, chain of custody, and documentation of who did what, and when. A1 expressed this explicitly by saying that *"reliability is a chain"*. A1 further said that every step had to demonstrate that procedures were properly followed and also highlighted the importance of trained personnel, storage, routines, and certification. Trusting the material is therefore tied to whether the entire handling can be tracked and reasoned through multiple stages, rather than to a single technical assessment.

4.2.2 Limited Insight into Collection, Processing and Selection

Another recurring theme throughout the interviews is that several actors mentioned they have to use evidentiary material without **full insight** into the process or the full evidentiary basis. P2 confirmed that there are parts of the process or material where they lack full insight, but still have to work with the material. From the defence perspective, D1 described this as a central challenge in the Sky ECC cases. J1 nuanced this by mentioning that full insight is generally rare, not only in this type of case. Together, these accounts suggest that limited insight is not an exceptional feature of these cases, but a condition which shapes how the different actors need to work with material as evidence. This gradual narrowing of what different actors can see and verify is illustrated in Figure 4.4.

Insight also seems to be distributed differently among the actors, as it appears deliberately limited by the way information is shared. P1 stated that in other cases where evidence material is received from Kripos, they usually receive only *"what they need to know"*, and added that one should not have more information than is needed for the work. P2 explained that defence lawyers have access only to material from their own case, which emphasises that insight is not equally distributed among the actors in the process. From the defence perspective, D1 connected this to a question of *"equality of arms"*, which is whether both parties have a sufficiently fair opportunity to access and challenge the material. D2 described a more concrete limitation, saying that the defence may receive extracted material by requesting new searches with the police present, but does not receive the complete security file. The Borgarting Court of Appeal judgment [LB-2024-142625] illustrates a similar limitation, noting that the defence had not received all Sky ECC material, and stated that the right of access had to be limited to what could be considered the documents of the case, and that this did not give the defence a right to access messages from all the approximately 950 Sky ECC IDs that Norwegian Police had received and could be used in Norwegian criminal cases. Limited insight, therefore, concerns both what information exists and how access to the material is shared and restricted among the actors.

Another aspect of the limited insight is that central parts of the collection and

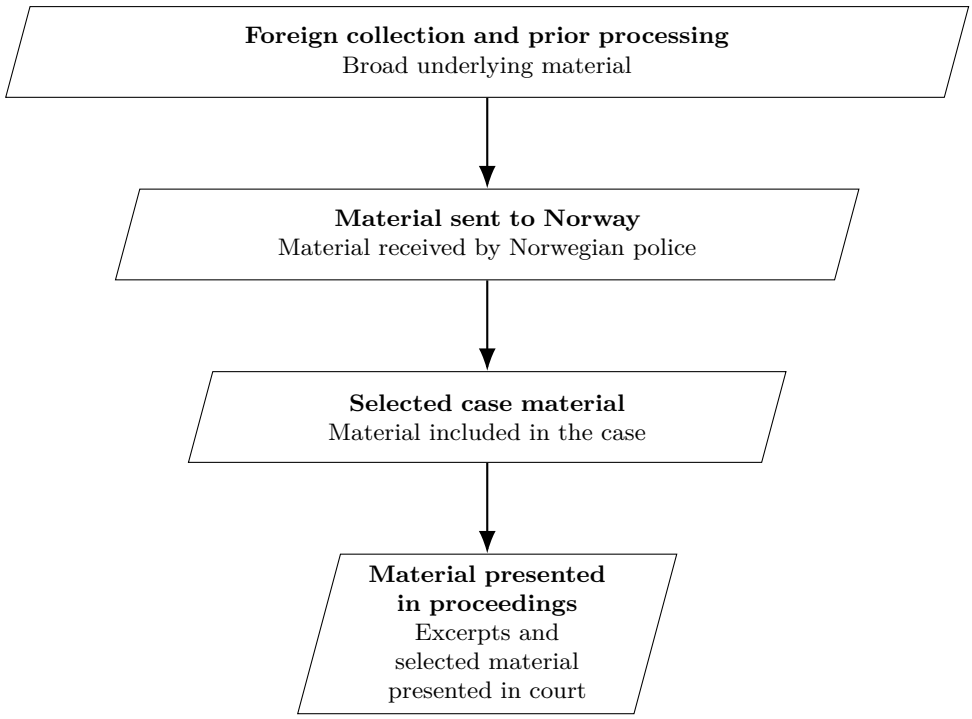


Figure 4.4: Illustrative overview of how visible material narrows through the evidentiary chain, from broad underlying material to the more limited case material and excerpts later presented in court.

processing are outside of what the Norwegian actors actually see. P2 described this as a result of a covert investigation and stated that, in such cases, the entire chain is unavailable because method protection limits actors' insight into it. L1 added that this type of cooperation may also rely on institutional trust and suggested that cooperation within Europe may be easier to trust because the countries share legal frameworks, including the European Convention on Human Rights, whereas evidence from countries with less shared legal or institutional grounding might be evaluated differently. D1 pointed out that the material could have been through multiple stages of processing in different countries, and said that *"we have no insight into what happens before the material reaches the Norwegian police"*. At the same time, J1 pointed out that this is not necessarily visible in court, because the material could be presented in the same way as it was collected by Norwegian police. The District Court judgment [TOSL-2022-185848] mentions the same limitation, which states that the defence had access to the same evidence as the prosecution but lacked the background material from Europol. Limited insight also reflects that important

parts of the evidence chain lie outside what is visible to the actors.

4.2.3 Practical Limits to Verification

One practical limitation, raised especially by P3 and supported by P1, is that the police's handling of digital material is poorly regulated and varies across practices. P1 described the regulation of such examinations as very open. P3 pointed out that disclosure of evidence is often governed by legislation and cooperation agreements, whereas the handling of the material itself is much less regulated. P3 also described digital forensics as a field that is less regulated than other forensic disciplines, but noted that there are variations both between countries and within specific countries. They also stated that some laboratory settings outside Norway are more closely aligned with standardisation requirements, including ISO standards, and cited England as an example. However, P3 emphasised that much of the handling of digital traces takes place outside laboratory settings. Laboratory standardisation, therefore, may support parts of the process, but it does not cover the whole evidentiary chain.

Another practical limit is that in some cases, **verifiability** depends on information that cannot be readily recreated. P2 described this with an example from telecommunications data, in which information had to be secured early to avoid loss. P1 mentioned that documentation about data collection and handling varies from case to case, and J1 similarly described varying degrees of traceability and verifiability of the contents of the underlying case file before the material reaches the court. It seems that practical verifiability largely depends on what is retained, documented, and available in each case.

A third source of difficulty for verifiability is that knowledge of how the material is handled is not always presented clearly or consistently. For example, D1 mentioned that, in some cases, there was different and partly contradictory information about which tools had been used to handle the material. In this context, J1 pointed out that it may be taken for granted that the material has undergone more quality control than it actually has. Further, A2 mentioned that much of what is known about such processes has only become visible through legal disputes, in which technical details had to be examined more closely. L1 mentioned that confidence in how foreign authorities have handled evidence may, in some cases, be largely based on trust and vary by jurisdiction. The chosen Court of Appeal judgment [LB-2024-142625] also illustrates how such limitations on verifiability can manifest in practice. The defence argued that the chain of evidence was unknown and sought to question foreign personnel involved in the collection, processing, and transmission of the material. French authorities rejected the request, partly because the technical solutions are classified, but also because the personnel involved in the data collection could not testify before foreign courts. The District Court judgment [TOSL-2022-185848]

noted that this affected evidential weight: when Norwegian investigators relayed answers they had received from unnamed Europol colleagues, those responses had less evidentiary weight because no one could contradict or question those persons directly. Conditions like these may make it more difficult to obtain a stable and verifiable picture of how material has actually been handled.

4.3 Interpretation, Uncertainty and Evidential Reliability

The previous section showed that actors face limits in what they can see, follow, and verify. This section zooms in on how these limits affect the interpretation and evidentiary meaning of the material. We will look into incomplete and fragmented communication, the need to interpret language, metadata and technical traces, and the risk that digital evidence may appear more certain or objective than the underlying material supports.

4.3.1 Incomplete and Fragmented Material

In this type of material, **completeness** seems to be the exception rather than the norm. Several participants described the evidentiary picture as comprising both known and unknown gaps, and therefore, it must be interpreted with awareness of what may be missing. P2 described this gap between *"known unknown"*, and *"unknown unknown"*, and explained *"known unknown"* as messages they could see that existed, without seeing the messages in cleartext, and *"unknown unknown"* was referred to as messages or communication that they did not know that they were missing. Figure 4.5 illustrates this distinction. J2 pointed in the same direction, noting that the court was accustomed to a fragmented picture of the evidence, where some pieces might be invisible. J1 emphasised that completeness is rarely present. Taken together, this shows that evaluating communication material from encrypted platforms as evidence involves incompleteness, in which the absence of information is part of the uncertainty.

A concrete form of **fragmentation** mentioned by several participants was that, in some cases, communication is only one-way. D1 pointed out that when the evidence is based on messages from a single sender without replies from the recipient, one has only one side of the picture. Similarly, P2 reported that in some cases, they received messages from device A to device B, but the replies were missing, leaving the material incomplete and fragmented. J2 said that this is something the court has to take into account, and that they have to consider whether there may be messages that do not appear in the material, were not delivered, were not read, or were withdrawn. The selected Court of Appeal judgment [LB-2024-142625] addresses the same concern, stating that Sky ECC material must be used with caution when only one side of the dialogue is visible, and that the court must take into account messages that may not

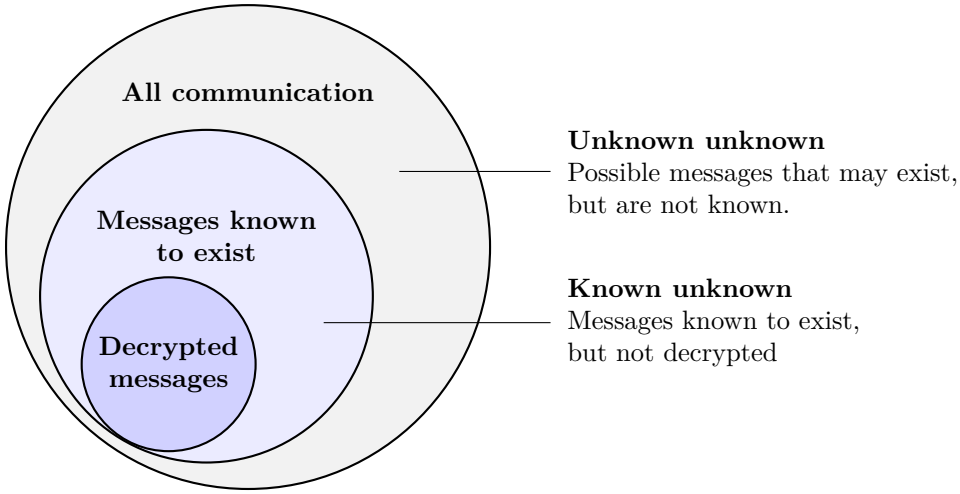


Figure 4.5: Illustration of decrypted messages, known unknowns, and unknown unknowns in the evidentiary material. The proportions of the circles are illustrative and do not reflect the actual proportions of the underlying material.

have arrived, been read, or been recalled. This suggests that fragmentation concerns both the amount of available material and the integrity of the dialogue structure itself.

It is worth noting that what is missing is not necessarily random or insignificant to understanding the case. D1 noted that the police themselves have stated that only parts of the material are known and decrypted, and that, therefore, there are millions of messages whose content one does not know. D1 mentioned that this matters because there might be a lack of later corrections or follow-up messages, which could change how previous messages were understood. They also gave an example in which information provided to the court about the completeness of the material later proved incorrect after new datasets were received from abroad. This suggests that the material might *appear* more complete and comprehensive than it might actually be.

4.3.2 Interpretation and Meaning

One thing mentioned multiple times by the participants is that **user identification** is not straightforward, as it is not easy to say with certainty that a data carrier, an account, or a cryptographic key belongs to a specific person. J1 described this as a classic fallacy, and A1 noted that a digital signature does not, in itself, indicate that the specific person performed the signing, only that this person's key was used.

From the defence perspective, D2 described this as the central identification issue in many cases, namely, whether the police have sufficient information to establish that the particular person used the mobile device or user account in question. D2 further explained that when the messages themselves are highly incriminating, the dispute often shifts toward the identification issue, namely, whether the prosecution can connect the user behind the communication to the defendant. D2 stated that they look at both what confirms the link between the user and the client and what constitutes exclusionary evidence that may weaken or contradict that link. D1 pointed out that in some environments it is common to exchange phones, so the same person may not use the same phone over time. The Borgarting Court of Appeal [LB-2024-142625] evaluated whether specific persons actually used specific Sky ECC-IDs, and built this on a pattern such as message content, travel routes, telecommunication data, pictures, addresses, meeting and continuity over time. This suggests that the connection between the digital carrier and the human actor must be established through a separate assessment and cannot be inferred solely from technical traces.

Another recurring feature of the material is that the meaning of the communication must be established through **interpretation**, language, slang, and context. P2 described this as a practical challenge with the material and explained that it may take time to understand what it actually covers. P2 emphasised that words and expressions cannot be given a specific meaning without explanation. For example, if the police say that *"10 yay"* means 10 kg of cocaine, it has to be explained and substantiated why this is a reasonable interpretation. D2 mentioned that in many events, the material is often so incriminating from the outset that it is difficult to explain away, whereas in situations with less material, there may be more room to work with context and interpretation. P3 pointed out that understanding a text in communication depends on human perception and that such messages can be interpreted in several ways. This means the material's meaning is shaped by the context and interpretations that the actors involved rely on.

Technical traces and metadata require interpretation, even when they seem straightforward. J1 explained that timestamps are a recurring example of this and said it is a classic mistake to assume they are automatically in local time. They also pointed out that system-generated data is sometimes mistaken for user-generated actions, and that there might be alternative explanations, such as an account being hacked and used by someone other than the person initially associated with it. In the same vein, A3 pointed out that technically correct statements can create a misleading impression if they are given a broader meaning than they actually support. For example, the statement *"BankID is approved by Norwegian authorities at the highest security level"* is correct, but it does not necessarily support every broader conclusion that can be drawn from it about security in a concrete evidentiary context.

Together, these examples show that both metadata and system information, as well as technically correct statements, must be interpreted.

The interpretive issues described in this subsection took different forms, but several recurring types can be distinguished. These are summarised in Table 4.1.

Table 4.1: Interpretive issues in communication material from encrypted platforms and their potential evidential risks

Type of interpretive issue	**Example from the material**	**Potential evidential risk**
User identification	A device, account, or cryptographic key cannot automatically be linked to one person	Wrong attribution of actions
Language and slang	Expressions such as *"10 yay"* require contextual interpretation	Misinterpretation of content
Metadata	Timestamps may not reflect local time	Incorrect reconstruction of sequence or timing
System-generated vs. user-generated data	System activity may be mistaken for deliberate user action	False inference about conduct
Fragmented communication	One-way communication or missing replies	Incomplete understanding of meaning
Technically correct but misleading statements	A true statement may still support an overly broad conclusion	Overstated evidential value

4.3.3 Sources of Error and Overconfidence

Even though digital evidence and communication need to be interpreted, several participants noted that this type of evidence might readily be met with a particular form of trust. P3 mentioned that judges are educated in law, not technology, and described how digital evidence might appear as a *"gold mine"* compared to witnesses who might remember badly, disagree with others, or lie. P3 pointed out that because digital evidence appears precise, stable, and machine-generated, it might be perceived as more objective than it is. Similarly, J1 mentioned that technical data is sometimes initially considered entirely objective. A1 described a related point by referring to the notion that mathematical proof can almost automatically be translated into legal proof, but they emphasised that this is not the case. This points to a source

of **overconfidence**, where the technical form of the evidence might lend it greater authority than the underlying basis of assessment necessarily justifies.

Another feature of the material is that **sources of error** may arise in the interpretive work surrounding the evidence. J1 emphasised that investigators, even when they are acting in good faith and doing their best, may still make mistakes and be influenced by bias. This was described more concretely from the defence perspective: D1 pointed out that it is primarily the police's interpretation that shapes how the material is understood during the investigation, and provided an example in which the police later changed their reports and reached opposite conclusions about who controlled a device at different times. D1 tied this to the danger of interpreting messages without grounding them in other evidence, adding that when investigators become *"blind to one's own hypothesis"*, serious mistakes might happen. This suggests that overconfidence concerns both how the evidence appears and how actors may interpret it in light of existing expectations and hypotheses.

Sources of error may lie in the tools, concepts and technical systems surrounding the evidence. P3 mentioned that the way information is presented through the analysis tools might affect how it is evaluated, for example, due to sequencing or a visual emphasis that might direct attention and therefore also the interpretation. A1 pointed out that technical terminology may create misleading associations, for example, when the word *signing* makes the digital process appear equivalent to an ordinary signature, even though it is not. J1 cited the Danish telecommunications scandal as an example in which software errors led to more than 10,000 court cases having to be reviewed afterwards. D1 noted that when artificial intelligence is used for material selection, an additional uncertainty arises about the correctness of the output. Taken together, this shows that sources of error may appear in the ways information is processed, presented, and conceptualised.

4.4 Expertise, Dependence and Safeguards in Court

This final section presents findings on how the court understands and controls technically complex material. We look into limited technical competence among legal actors, dependence on experts and technical explanations, and the courtroom safeguards used to challenge, control, and evaluate the material.

4.4.1 Technical Competence of Legal Actors

Multiple participants described judges and other legal actors as people with **limited technical understanding**. P2 mentioned that many court actors are not technically skilled personnel, and A3 said that most legal professionals do not have technical expertise whatsoever, but emphasised that it is not their job to have it either.

P1 mentioned that it is common for both defence lawyers and judges to lack an understanding of digital traces. At the same time, J1 nuanced this by mentioning that his technical competence may not be that high. Together, these points indicate that limited technical competence is common among legal actors, even when technically complex material is used as evidence.

A practical consequence of knowledge limitations is that technological questions often need to be translated and framed at a level that is comprehensible to non-technical actors. A3 described this as a pedagogical challenge and said that the underlying technology must be understood so that the court actually can understand what the issue is about. P1 mentioned the risk this might create by pointing out a hypothetical scenario where a malicious person with high technical competence in principle could explain himself very one-sidedly without the judges or defence lawyers being able to challenge it, and described situations where actors in court simply trust the explanation. A2 mentioned that it is quite difficult to communicate this, even to journalists who specialise in such cases. A1 mentioned that in many countries, courts are not the most technically advanced places. This suggests that complex technical material can be difficult to make understandable in a legal setting.

A1 and L1 noted that this is a structural issue, with few people competent in both law and technology. A1 stated directly that interdisciplinarity is difficult and noted that there might be few experts in both fields. They pointed out that the legal world is a *"a bit of its own little bubble"*. L1 pointed out that this kind of evidentiary understanding is largely outside legal education and that one has to learn it largely in practice. This suggests that the distance between law and technology might be high.

4.4.2 Experts and Expert Dependence

A recurring point in the interview material is that the court often depends on **expert witnesses** to understand the technical aspects of this type of evidence. P2 said that there were expert witnesses who could explain matters P2 could not explain themselves, and that this helped clarify the case and made difficult material understandable to the court. Similarly, J2 mentioned that one would be dependent on expert testimony to understand and clarify technical aspects, such as the reliability of decrypting the case material. L1 said that an understandable summary of what is relevant for the case from a neutral expert would give good coverage. It is also worth noting that technical experts were called in by both the District Court [TOSL-2022-185848] and the Court of Appeal [LB-2024-142625]. Together, this suggests that, to a large extent, technically complex material needs to be conveyed by people who can translate it into something the court can actually work with.

Even though many actors mentioned a dependence on experts, it seems that

independent cryptographic/data technical experts are less often in court than experts in other fields, and that the technical material is presented by the police's own people. J1 specifically pointed out that the court very rarely brings in independent experts on technical data questions, and that there are few cases in which independent technical data experts explain anything. From the defence perspective, D1 said that decrypted material is rarely handed over to an independent agency but is analysed and processed by Kripos, and that the prosecution has not called expert witnesses, whereas the defence has. P3 said that in the Norwegian context, it is usually the internal data investigators who present the evidence, and A3 mentioned that when one side has technical information and the other does not, it creates a very uneven landscape in court. So it seems like the technical frame for the evidence, more often than not, is presented by actors close to the material, and that the balance, therefore, might become uneven.

The reliance on experts raises questions about who is actually being used as an expert in court and how well the court is prepared to evaluate them. P2 said that some expert witnesses appear to be people with a CV, saying whatever they are paid to say, rather than being clear and independent. P1 pointed out that many actors in court have too little competence with digital traces to be able to evaluate how strong an alleged expert is, and pushed it to the limit by saying that some might think that a person who knows how to change the ink in a printer is a data expert and could therefore be an expert witness in these cases. P3 added that the threshold for appearing as an expert in Norwegian courts is quite low, which might create space for both self-declared experts and pseudoscience. A3 mentioned that, in the end, it is up to the court to decide whether to believe the expert. This makes the expert role important and vulnerable, because the evaluation of the expert's quality is placed in the hands of actors who might have limited prerequisites to control it.

4.4.3 Courtroom Safeguards

Two things that are often mentioned in the material as central control mechanisms are **contradiction** and the **role of the defence**. P2 said that the encrypted evidence has been *"twisted and turned quite thoroughly"*, and that the defence lawyers have been well prepared and have fought hard to dispute the evidence. J2 pointed out that this is exactly as it should be: the prosecuting authority presents the evidence, and the defendant's task is to question it. Similarly, J1 said that many lawyers can probe efficiently to carry out checks and inspect the material. A3 mentioned how the opposing party can clarify, correct or contradict explanations that otherwise would have remained unchallenged. Together, this suggests that an important safeguard in cases like this is that the material is being met by actors who try to challenge, nuance and test what is presented.

Participants described the court as an actor that tries to control the technical material through questions, evaluation of control routines, and internal evaluation tools. J1 mentioned that they have become more aware of the need to examine which internal control mechanisms exist before such evidence is presented in court, for example, by reviewing reports, quality assurance measures, or other forms of internal control within the police. J2 mentioned that the court often asks control questions to get to the bottom of the material being presented. J2 said that some questions might prompt the presentation of more material. Further, J1 stated that judges can review the evidence presented at the office after the court is finished for the day. J1 referred to the development of a checklist intended to help judges ask the right control questions. Safeguards in court, therefore, also depend on the judge's active role in examining how the material was produced and how it should be assessed.

Another safeguard mentioned is an **overall assessment** of the evidence, in which the court considers the encrypted material alongside the rest of the case. J2 emphasised that expert witnesses and technical evidence are only parts of the total evidence, and that the court must always take into account the possibility of something creating reasonable doubt. Similarly, J1 mentioned that they always try to hold this type of evidence up against all other information in the case. J1 said that they always try to judge the whole rather than just one trace. D1 clearly stated that cryptographic material alone, without other points of reference in time and space, must be used with great caution. D2 mentioned a more pragmatic defence strategy, which was not about challenging the evidence in principle, but about examining the material's weaknesses and their significance in the specific case. The chosen District Court judgment [TOSL-2022-185848] adopts a similar approach, holding that limited control and potential errors must be taken into account when evaluating the evidence alongside other evidence in the case. The court emphasised that the defence had access to the same evidence as the prosecution in Norway, had the ability to question Norwegian investigators, present its own evidence, and include a privately appointed expert on the Sky ECC material. Courtroom safeguards, therefore, include a comprehensive and cautious assessment where uncertainty, gaps, and alternative explanations are tested against the full evidential picture.

Chapter 5
Discussion

In this chapter, we discuss our findings in relation to the six research questions. We first address each research question in a separate section, before synthesising the findings in an overall discussion. We move from the specific findings presented in Chapter 4 to a broader discussion of how communication material from encrypted platforms is transformed, assessed, challenged, and understood as evidence in Norwegian criminal proceedings.

5.1 Procedural Challenges in Presenting Communication Material from Encrypted Platforms

Our first research question asks which legal and procedural challenges arise when decrypted communication is presented as evidence in judicial proceedings. We treat this as a question about communication material from encrypted platforms more broadly, including message content, metadata, technical identifiers, and selected evidentiary excerpts. We find that the main challenge lies in making large and technically complex evidentiary material usable in court. As shown in Section 4.1, the material enters the courtroom already processed: it has been searched, filtered, exported, selected, and converted into a legal format. The court therefore sees a version of the underlying dataset, rather than the full dataset itself. These preparatory steps are necessary, but they shape the conditions for later testing and contradiction in court.

The underlying dataset is too extensive for direct review in court. Several participants described the material as large and difficult to handle in its entirety: P2 noted that reading material for 170,000 users is unrealistic, while D1 and J1 referred to long PDFs and millions of lines of content. This makes search and filtering necessary before the material can be used as evidence. In Section 4.1.1, we see that the Borgarting Court of Appeal judgment describes several stages of technical processing, and in Section 4.1.3, the Oslo Tingrett judgment splits the

case into several events and presents the evidence through excerpts and presentation documents.

The volume of data means that the court cannot review the material directly. Instead, the court needs a reduced and organised version of the material. The evaluation, therefore, begins after other actors have already decided which material is sufficiently relevant to bring forward. Selection and processing are not unique to cases involving communication material from encrypted platforms, as criminal proceedings generally involve some degree of evidentiary selection. However, the scale of the material, the technical processing involved, and the number of steps between the underlying dataset and the material presented in court make this condition especially important. Since selection occurs across unusually large, technical, and partly opaque datasets, it becomes difficult to treat it as a purely neutral or practical step. We summarise this procedural tension in Table 5.1 by examining what each makes possible and the risk it introduces.

Table 5.1: Procedural tension in transforming communication material from encrypted platforms into courtroom evidence

Step	**Necessary function**	**Procedural risk**
Search and filtering	Makes large datasets manageable and searchable	Relevant material may fall outside the search or filtering criteria
Selection	Focuses the case on material considered relevant	Context, representativeness, and alternative interpretations may be reduced
Formatting and presentation	Makes the material readable through excerpts, tables, timelines, or slides	The material may appear cleaner, more coherent, and more complete than the underlying dataset
Courtroom assessment	Allows the court to evaluate the material within ordinary evidentiary procedures	The assessment begins after prior processing has already shaped what is visible and challengeable

Selection and presentation, therefore, become central procedural issues. As we saw in Section 4.1.2, some degree of selection is inevitable, and it occurs before the material reaches the judge. The court only meets excerpts of the communication, and this is important because the selection influences what the court actually gets to read, understand and evaluate. Both defence lawyers illustrated in Section 4.1.2 that omitted material may matter for the interpretation of the evidence, and A3 described that the meaning of a single message can change when the entire conversation or more context is visible. This shows that material not presented may be important for understanding what is actually presented. The forms of presentation reinforce this, as

the material is often presented as excerpts, tables, timelines, chat logs, or PowerPoint slides, as we saw in Section 4.1.3. These formats do make the material more readable and more manageable in court, but they may give it a cleaner, more coherent form than the underlying material would otherwise have. Therefore, the presentation form influences what appears relevant, central, and understandable to the court, and a procedural challenge is to make the material understandable without obscuring potential uncertainty or context. At this point, the procedural issue intersects with fairness. When the material is reduced to a manageable size, questions arise about whether the defence can still examine what is left out and how the excerpts were selected. This concern is highlighted by Stoykova [Sto24b, Sec. 3.4], who argues that digital evidence poses challenges to fair trial because effective contestation may require access to the chain of evidence, explanations of processing decisions, and even forensic assistance.

As shown in Section 4.4.3, control mechanisms include the parties' presentation of evidence, questions in court, contradiction, evaluation of weaknesses, and an overall assessment of the evidence. The court, therefore, treats the material through standard control mechanisms, even though it has undergone several stages of selection and processing. However, as shown in Section 4.2.3, the court does not get direct insight into the entire technical and international process behind the material, which means the court does not have direct control over it. Section 4.2.3 also showed that parts of the control become more indirect when information about technical or international steps is presented through other actors. The Oslo District Court judgment [TOSL-2022-185848] handled this by emphasising that the limited control options and potential errors had to be taken into account when evaluating the material. This illustrates practical judicial handling, in which the material is treated within a regular framework, while recognising that the control mechanisms may be limited. The central point is therefore that the court's control occurs within material that is already delimited, processed, and presented by other actors. The court's handling, therefore, concerns material that has already been shaped by prior searches, filtering, selection, and technical preparation, shaping what the court can see.

The focus on analysis, filtering, selection, and presentation aligns with research on data-driven investigation. Oerlemans and Royer [OR23] point out that attention often focuses on data collection, whereas data analysis has received less attention in case law and research. Our findings in this study suggest that this later phase is central to the procedural challenge, because it is in this phase that large technical datasets become usable courtroom evidence. This transformation involves searching, filtering, selecting, formatting, and presenting. Within these steps, there are multiple central challenges, such as the volume of data, the need for filtering and selection before the material reaches the court, a simplified presentation format, possible loss of context, limited direct control over prior processing, and the need to view the

material alongside other evidence. These steps are necessary for the material to be usable in court, but they also determine what the court can see, understand, and evaluate. The main procedural challenge is closely tied to the many steps between the underlying communication data and the material ultimately presented in court.

5.2 Assessing Reliability, Credibility and Fairness

Our second research question concerns how judges, defence lawyers and investigators evaluate the reliability, credibility and fairness of decrypted communication as evidence. The findings suggest that actors evaluate the material through several layers, starting with technical reliability. This means determining whether the material has been decrypted, handled, and documented in a way that makes it usable. The evaluation then assesses whether the material is sufficiently complete, whether the content can be interpreted correctly, and whether the messages and metadata are coherent. Further, it concerns the connection between digital traces and an actual person, before turning to fairness: whether uncertainty and alternative explanations are visible enough to be included in the court's overall assessment. This layered understanding, moving from technical usability and completeness to interpretation, user identification, and fairness, is summarised in Table 5.2, which also includes the main risk associated with each layer. The main point is therefore that communication material from encrypted platforms is evaluated as technical traces that must be interpreted, controlled, and understood within a broader evidentiary context.

Technically correct decryption is only one layer in evaluating reliability. Even if the messages are correctly decrypted, the material may still be incomplete and fragmented. This is explained in Section 4.3.1, where P2 explained the difference between *"known unknown"* and *"unknown unknown"*, where *"known unknown"* is the messages the actors know exist, but cannot read in plaintext, and *"unknown unknown"* is the messages which actors do not know are missing. P2's distinction suggests that, from the police perspective, reliability is about what the available material can actually show and, at the same time, what is known to be missing and what may be missing without being known. Incompleteness becomes especially evident in one-way communication, where only one side of the dialogue is available, and answers or follow-up messages may be missing. D1's point in Section 4.3.1 about the lack of answers and subsequent corrections shows how such gaps can influence understanding of the messages actually visible. From the defence perspective, reliability depends on whether the material provides sufficient context for proper understanding. J2 mentioned in Section 4.3.1 that the court is used to fragmented evidential pictures, which shows that incompleteness does not necessarily make the material useless, so from the judge's perspective, incompleteness is something that needs to be taken into consideration in the overall assessment of the evidence. In the same subsection, Section 4.3.1, we also see that in the Borgarting Court of Appeal judgment, it

Table 5.2: Layers in the evaluation of communication material from encrypted platforms as evidence

Evaluation layer	**Main question**	**Central risk**
Reliability	Is the material technically usable, documented, and sufficiently complete?	Technically correct decryption may still leave gaps, fragmentation, or unknown missing material
Credibility	Can the meaning of the messages, metadata, and technical traces be anchored in context?	Messages or metadata may be interpreted too narrowly, too broadly, or as more objective than they are
User identification	Can the digital user, account, device, or Sky ECC-ID be connected to a physical person?	A digital trace may be wrongly attributed to a person
Fairness	Are uncertainty, weaknesses, and alternative explanations visible enough to be challenged and assessed?	The defence may challenge the material only within a frame already selected and structured by others

is stated that the Sky ECC material must be used with caution where only one part of the dialogue is visible, and they had to take into account that there are messages which never got to the recipient, were not read, or were recalled. The different actors address the issue from different roles within the evidence process. The police perspective in the material emphasises what the available dataset can show and the known gaps. The defence perspective emphasises how those gaps can affect context, alternative explanations, and interpretations. The judicial perspective views incompleteness as a limitation that must be taken into account in the overall assessment. Therefore, reliability is evaluated by examining the relationship among the visible material, the missing material, and the meaning these gaps might have for understanding the case.

Credibility concerns how the content of the messages is interpreted and anchored in the evidential context. We show in Section 4.3.2 that messages need to be interpreted through language, slang and context. P2's examples with *"10 yay"* showed that expressions must be explained and supported before they acquire a specific evidentiary meaning. In the same paragraph, we saw P3's point that text interpretation requires human understanding and that messages can often be interpreted differently. D2 nuanced this by explaining that some material is so incriminating that it cannot be explained away, whereas less material may allow more space for context and

interpretation. Further in Section 4.3.3, J1 pointed out that technical data is sometimes initially thought of as entirely objective, and in Section 4.3.2, J1 noted that timestamp and system data also require interpretation, which affects credibility in avoiding technical fallacies. P2 indicated that, from the police perspective, credibility requires that the interpretation is explained and substantiated, and D2 shows that, from the defence perspective, the evidential interpretation of a message may be more or less convincing depending on how strongly it points in one direction, and on how much context is available. J1 showed that, from the judge's perspective, credibility requires awareness of potential technical fallacies, such as time stamps, system data, and assumptions of objectivity. P3's point that digital evidence appears more precise, stable and machine-generated adds to this. Westers [WBJ+25] supports this, stating that once data is decrypted, it is considered trustworthy because it is unlikely to have been altered. This suggests that communication material from encrypted platforms may be perceived as more objective than a witness statement, even though it is still selected, processed and interpreted before it becomes evidence in court. Credibility, therefore, lies in whether the meaning of the communication can be anchored in language, context, technical understanding and the broader evidentiary picture, including awareness of the apparent objectivity created by the digital format.

User identification can be treated as a separate evaluation layer in RQ2 because those messages must be tied to an actual person before they have full evidentiary meaning. As we show in Section 4.3.2, one cannot automatically equate a data carrier, an account, a cryptographic key, or a Sky ECC-ID with a specific person. This is one of the classic fallacies J1 described, and A1 raised a similar point about digital signatures: a signature shows that a key was used, not that a specific person performed the signing. D2 said that this is one of the most central questions in many cases: whether the police have enough information to know that the person using the mobile or account is actually this specific person. D1's point that mobile phones are often switched or borrowed in certain environments shows that digital identity cannot be directly equated with a physical person. From the police perspective, we see that user identification is a practical threshold for the investigation, as mentioned in Section 4.1.1: it must be possible to identify the person behind the Sky ECC ID. The Borgarting Court of Appeal judgment shows that the court evaluated user identifiers using several indicators over time, described in Section 4.3.2, and that the court based its evaluation on patterns in message content, travel routes, telecommunication data, pictures, addresses, meetings, and continuity in the dialogue. The judgment shows that user identification is based on several indicators pointing in the same direction.

However, there is still tension in the identification. From the police perspective, identification is done quite early, so the material can be sent for further processing and investigation. From the defence perspective, the same point seems more critical:

a possible connection between a Sky ECC-ID and a person may not be enough. D1's critique shows that identification can become vulnerable if the police interpret messages in a specific narrative. D1's example in Section 4.3.3, in which the police changed their assessment of who had used the same device, shows that the coupling between user and person can be insecure. D2 provided a more pragmatic defence perspective. We see in Section 4.3.2 that when the messages are very incriminating, the contest often shifts to the issue of identification, where the defence work is about examining the weaknesses in the coupling between the client and the user. The tension, therefore, lies in the fact that the same identification moments can be used to build up and to challenge the coupling between a digital user and a physical person. The Borgarting judgment [LB-2024-142625] illustrates how the court handled this by evaluating whether several indicators pointed in the same direction. User identification, therefore, becomes a credibility question because the evidentiary interpretation of the messages depends on who the communication can be attributed to. A message can be correctly decrypted and fairly interpreted, but if the coupling is weak, its evidentiary meaning becomes less clear. This shows that the actors evaluate the same coupling from different roles. The police need to establish a user to take the material further; the defence tests and challenges the coupling; and the court evaluates whether the identification is sufficiently anchored in the overall evidentiary picture.

The tension concerning fairness lies in whether the material is actively challenged while the challenge remains limited by earlier selection and structuring. As shown in Section 4.4.3, P2 pointed out that the evidence has been *"twisted and turned quite thoroughly"*, and that the defence has fought hard to dispute the evidence. This indicates that, from the police perspective, the material has not been simply accepted but actively challenged through the adversarial process. J2 pointed out that this is exactly how the process should work, reflecting the judge's perspective: the prosecution presents the evidence, and the defence questions it. At the same time, the defence perspective reveals a tension: it is possible to challenge the material, but the challenge occurs within a frame that the police have already selected and structured. D1's critical perspective in Section 4.2.2 pointed out that if selection, context and access are limited, it is hard to test the material on equal terms, whereas D2's more pragmatic perspective is that when the material is already being used, the defence work is about finding weaknesses in the material, rather than trying to get the material rejected. As shown in Section 4.4.3, the court addresses this by conducting an overall assessment and integrating the material with other evidence. The tension is that the court uses ordinary legal mechanisms, but these mechanisms operate on material that has already been technically processed and shaped by the investigation. Fairness, therefore, becomes a question of whether the uncertainty, selection and possible weaknesses are visible enough for the defence to challenge the evidence meaningfully and for the court to evaluate reliability and credibility in a

proper way.

Overall, this shows that the various legal actors evaluate communication material from encrypted platforms across several layers, such as reliability, credibility, user identification, and fairness. Reliability is about the relationship between the visible material and what might be missing; credibility is about how well the messages' evidentiary meaning can be explained and anchored in context. User identification is about how well the digital identification can be coupled to a physical person, and fairness is about how uncertainty, weaknesses and alternative explanations are visible enough in the evaluation. The actors see these layers from different roles: the police have to make the material manageable and usable, and couple it to persons; the defence tests weaknesses and possible alternative explanations; and the court evaluates the material from an overall perspective. The most central finding is that communication material from encrypted platforms can be very strong evidence, but its strength depends heavily on interpretation, context, identification, and the visibility of uncertainty. Communication material from encrypted platforms is therefore evaluated as technically produced traces that must be interpreted, controlled, and placed within a broader evidentiary picture.

5.3 Transparency, Chain of Custody and Foreign-Collected Material

We will now look at our third research question, which examines the mechanisms used to support transparency and maintain the chain of custody when decrypted material is obtained through cooperation with foreign authorities. Our findings show that the central challenge is primarily how far the actors can follow the material through an international chain of evidence, and that this chain is only partially visible to the Norwegian actors. We therefore examine how documentation, technical control points, and institutional trust are used to make the material verifiable in the absence of full visibility. We illustrate this relationship between partial visibility and different forms of control in Figure 5.1.

As shown in Section 4.2.1, P3 described transparency as the core of reliability and linked it to documenting who handled the material, when, and what they did. A1's point about that *"reliability is a chain"* aligns with that. Documentation and traceability could be understood as central mechanisms for transparency and chain-of-custody management. The evidentiary material must be traceable through the process by which it was collected, transferred, handled, and presented. If Norwegian actors lack insight into parts of this process, it becomes harder for them to assess the chain of custody. Trust then becomes more dependent on documentation, technical verification and institutional trust.

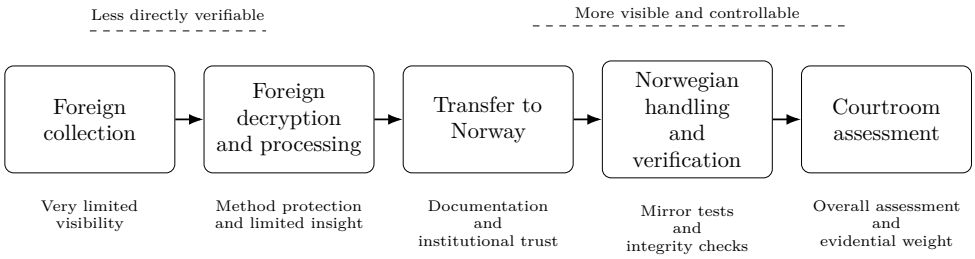


Figure 5.1: Partial visibility and different control mechanisms across the international evidence chain.

When full visibility is unavailable, technical verification mechanisms become important for making trust more concrete. As we see in Section 4.2.1, P2 mentioned that mirror tests enable the Norwegian Police to compare received data with data from seized mobile devices. The Borgarting Court of Appeal [LB-2024-142625] describes the same mechanism through mirror tests and identical checksums. The Oslo District Court [TOSL-2022-185848] also uses checksums. P3's point about hash sums follows the same logic as checksums: integrity can be documented by showing that seized material has remained unchanged over time. These mechanisms make the received material more verifiable by determining whether it aligns with other available sources and whether it has been altered. However, the entire chain remains partly hidden. A checksum shows that a file has not been changed, but it does not show how that file was created or selected. A mirror test shows consistency between the received data and seized devices, but it does not make the collection process fully visible. These mechanisms remain important, as they shift the assessment from pure institutional trust to concrete technical control. Still, they only offer point-based verification, not full transparency. This connects to Oerlemans and Royer [OR23], who discuss Sky ECC in relation to equality of arms and point to transparency, the reliability of evidence, and access to datasets as central elements. This fits our findings, as both mirror tests and checksums strengthen reliability at a specific point but do not provide the broader transparency and access needed to test the entire evidence chain.

Even though technical verification provides a partial answer to the chain-of-custody issue, the earlier foreign steps remain unclear. The main transparency challenge, therefore, arises before the material reaches the Norwegian police and courts. As shown in Section 4.2.2, central parts of collection and processing are outside the view of Norwegian actors. P2 described this as tied to covert investigation and protection of methods. This shows that visibility depends on how covert and border-crossing investigation structure what can be controlled. In Section 4.2.3, we

can see D1's point about partly contradictory information about tools, which shows limited visibility into how the material was handled before it reaches the Norwegian police. P1's *"need-to-know"* point in Section 4.2.2 shows that information could be limited within the police as well. Actors, therefore, appear to receive the information needed for their role, but not all possible background information.

At the same time, we have seen that full insight is generally rare, and limited insight is not unique to the Sky ECC cases or to foreign-collected material; the international link makes this restriction more visible and harder to control. The challenge is that Norwegian actors can only control parts of the material after it has been received, but cannot trace it back to its collection and processing abroad. The chain of custody is therefore only partially visible.

In Section 4.2.1, P3 separated the protection of decryption methods and documentation of the handling chain, and this separation is important because method protection could be legitimate, while the handling chain remains important for assessing the material's reliability. Method secrecy and chain of custody should therefore be kept analytically separate: one protects how the material was decrypted, while the other documents who handled the material, what was done, when it was done, and how its integrity was controlled. When insight into earlier parts of the evidence chain is lacking, institutional trust becomes more important. As shown in Section 4.2.2, L1 indicated that cooperation within Europe is easier to trust because the countries share legal frameworks, including the European Convention on Human Rights. This shows that trust in the material is also built upon legal and institutional frameworks around the cooperation. At the same time, the need for traceability remains. Method protection and international cooperation may explain why some information is not fully available, but they do not remove the need for verifiability. The less insight the actors have into the concrete handling chain, the more the evaluation needs to rely on documentation, technical control points, and institutional trust.

Taken together, we see that transparency and chain of custody are supported by several mechanisms operating at different levels. A central mechanism the actors mentioned is documentation and traceability, meaning the material should be able to be tied to who did what, when, and how integrity was controlled. At the same time, our findings show that the Norwegian actors do not have full access to the entire handling chain. Therefore, technical control mechanisms become very important. Mirror tests, checksums, hash sums and comparison with seized material therefore make the material more verifiable. These mechanisms support evaluations of integrity, consistency, and specific handling steps, but they do not provide full visibility across the entire international chain of evidence. The chain of custody is only partially visible to Norwegian actors, and when earlier foreign stages cannot be inspected, the evaluation must rely on a combination of documentation, technical verification, and

institutional trust.

5.4 Safeguards Against Misuse and Selective Presentation

In this section, we examine the safeguards in place to prevent misuse or selective presentation of decrypted evidence. Misuse means the risk that the material is selected, interpreted, or presented in a way that gives an incomplete or misleading evidentiary picture. The findings suggest that safeguards can make selected material contestable, supplementable and subject to assessment. The main tension is that selection happens early, while many safeguards operate after the material has already been filtered, selected and made available as case material, as illustrated in Figure 5.2. The safeguards are therefore mainly corrective rather than preventive.

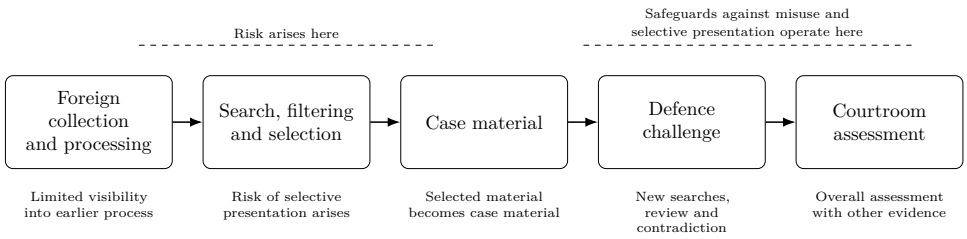


Figure 5.2: The temporal relationship between early selection and later safeguards against misuse and selective presentation.

As shown in Section 4.1.2, the material is too extensive to present in full. J2's point about selection being inevitable and J1's point that most of the selection occurs before the material reaches the judges show that the court is meeting a delimited material. This makes selective presentation a practical risk, even though no one is actively trying to misuse the material. Selection, however, is not unique to communication material from encrypted platforms. Police and prosecution select and present evidence in ordinary criminal cases as well. What makes this more challenging is the scale of the material, the technical processing before presentation, and the limited access to the underlying data. In Section 4.3.3, D1 described the risk of becoming blinded by one's hypothesis, and mentioned that messages supporting one hypothesis were shown, while other communications in the same conversation were left out. Section 4.1.2 showed that D2 had found material which supported the defence case, which the police had not presented. The presentation formats of tables, timelines, and PowerPoint make the material usable for the court, but they reinforce the risk of selective presentation, which can make a selected part of the material appear relevant, readable, and coherent. Selection cannot be avoided, and

the relevant safeguards are therefore those that make the selection visible, contestable, and supplementable.

Now, we will look at which safeguards actually exist. A very central one, as we see in Section 4.2.2, is that the defence gains access to the case's documents and can use the material made available in the case. At the same time, this access is restricted because not all underlying material automatically becomes part of the case's document. D2 explained that the defence can obtain new material by requesting new searches with the police present, but they cannot obtain the entire security file. The ability to request additional material, therefore, functions as a safeguard, but only within specific limits. This places more responsibility on the defence, as they need to know what to ask for or which searches to conduct, which can be challenging when they don't know the full data basis. This is an important limitation of the safeguard: the selection can be challenged, but it does not give the defence the same overview as the actors who first made the selection.

Another central safeguard is contradiction. P2's point in Section 4.4.3 that the material has been *"twisted and turned quite thoroughly"* shows that the evidence has not been accepted without resistance. We also saw that J2 mentioned that the prosecution presents the evidence and the defence questions it, and J1 pointed out that the defence probes and inspects the material efficiently. The court, therefore, functions as a safeguard in questioning and evaluating weaknesses. An overall assessment of the material serves as a safeguard because it is evaluated alongside other evidence. The safeguards can make the selection challengeable, supplementable, and subject to evaluation within the broader evidentiary picture.

The safeguards against misuse and selective presentation exist, and the most important ones are the possibility of new searches, the defence review, contradiction, and an overall assessment. These safeguards reduce the risk for misuse and selective presentation, but do not eliminate it, as they operate after the material has been filtered, selected, and presented.

5.5 Standards and Best Practices

This section addresses research question 5, which asks which standards or best practices guide forensic experts in decrypting and authenticating communication. Our main finding is that there are concrete practices and control mechanisms, but they do not identify a standard regime that covers the entire evidence chain.

Our findings identify some concrete practices which can guide decryption and authentication. For decryption, we see in Section 4.1.3 that P1 stated that, in other cases, a technical report will normally be produced detailing how the material is

decrypted. This points to a central practice: documenting the decryption process so it can be evaluated afterwards. In Section 4.2.1, we see some mechanisms for authentication are mirror tests, checksums, and comparisons with seized material. As discussed in Section 5.3, these mechanisms only control parts of the chain. There are control points in authentication, but they do not constitute a complete standard or best-practice framework for the entire process of extracting, decrypting, handling, and presenting the material. The role and limitations of these practices are summarised in Table 5.3.

Table 5.3: Practices and control mechanisms relevant to decryption and authentication

Practice or control mechanism	**What it supports**	**Limitation**
Technical reports	Document what has been done during decryption or technical processing, so that the process can be evaluated afterwards	Only covers the specific process described in the report, and depends on the level of detail and availability of the documentation
Documentation and traceability	Helps actors follow who handled the material, what was done, and when	Documentation varies between cases and may not cover the entire international evidence chain
Mirror tests	Compare received data with data from seized devices, supporting confidence that overlapping material matches	Only verifies material that can be compared with seized devices, and does not verify the entire collection or selection process
Checksums and hash sums	Support integrity control by showing whether specific files or data have changed	Show data integrity, but not whether the material is complete, correctly interpreted, or representative
Laboratory standards and accreditation	May support quality control in some forensic laboratory settings	Much digital evidence handling occurs outside such laboratory settings, and standards may not cover the whole process

We saw in Section 4.2.3 that P3 pointed out that digital forensics is less regulated than other forms of forensics. This is supported by Stoykova [Sto24b, Sec. 1], who points to the lack of standard legal procedures for digital forensics methods. However, P3 mentioned that there are variations both across borders and within countries. ISO standards and accreditation exist in some laboratory contexts outside Norway, but

much of the handling of digital evidence occurs outside the laboratory. We saw that P1 said documentation of collection and handling varies from case to case, and J1 said that traceability and verification of evidence upon reaching the court also vary. So standards and best practices can only guide the assessment of communication material from encrypted platforms to the extent that relevant parts of the process are visible and documented. When documentation and traceability vary so much from case to case, the question becomes whether the process surrounding them is sufficiently documented to allow others to assess how the material was handled. Our findings show that there are some standards that may guide the process, but we cannot identify a clear standard or best-practice regime that covers the whole evidence chain.

Overall, forensic work on communication material from encrypted platforms is guided by practical mechanisms, such as technical reports, documentation, mirror tests, and checksums. There are some best practices or standards being used in parts of the process. However, we are unable to find a central framework for the entire process, from collection to decryption, and further to authentication, handling, and presentation.

5.6 Expert Dependence and Technical Understanding

This section examines research question 6, which explores the extent to which judges and lawyers rely on expert testimony to understand the technical aspects of decrypted evidence. The short answer is that they rely heavily on technical explanations because many legal actors lack technical competence. We see this is Section 4.4.1, where both P2, A3, P1 and J1 all mentioned limited technical competence among legal actors. Therefore, technical material must be translated into a form that legal actors can understand and use in evidence evaluation. A2's point in Section 4.4.1 that technical uncertainty can be difficult to communicate even to specialised journalists further supports this. At the same time, it is understandable that they don't have technical expertise, as they have an education and practice in law, not technology. A3 explicitly stated that it is not the legal actor's job to possess technical expertise. Meeuwissen [MdRE+24] supports this and states that it is impossible for judges to keep up with the latest developments in all forensic areas of expertise and to close this knowledge gap themselves by attending educational courses or by acquiring expertise. Our point is that, as A1 and L1 mentioned, a few people have competence in both law and technology; expert dependence is a natural consequence of this. In Section 4.4.2, we see that experts are being used actively, and J2 mentioned that they are dependent on them to understand technical aspects, and P2 mentioned that some are able to explain concepts P2 could not explain themselves, and the court judgments show that technical experts were used. Expert testimony is important

because it translates technical processes into explanations that the court can use in its legal assessment.

Legal professionals, therefore, depend on experts, but this dependence raises further questions about independence and control. J1 mentioned in Section 4.4.2 that there are rarely independent experts on technical questions, and as we have seen, in this case, it is the police who present the technical evidence. This means that the technical explanation often comes from actors close to the investigation. The defence may still appoint its own experts, and technical expertise can therefore become part of the parties' contest over how the evidence should be understood. A3 mentioned that when one side has technical information and the other does not, it creates a very uneven landscape.

A related concern when defence-appointed technical experts are introduced is the quality of those experts. P2 said that some experts might be people with CV's saying what they are paid to say, and P1 introduced the concern that defence lawyers and judges might have too little technical competence to evaluate the quality of an alleged expert, and we know from P3 that the threshold for appearing as an expert in Norwegian courts is low. As A3 mentioned, it is up to the court to decide whether to believe the expert. Expert dependence also introduces a control problem. The court needs expert explanations to understand the technical evidence, but it must also assess the independence and quality of those explanations without strong technical competence of its own. Expert testimony helps bridge the gap between law and technology while raising a new question of control. We summarise the identified forms of expert use in Table 5.4, which also includes the positive functions and potential risks or control problems.

5.7 Overall Discussion

This section brings together the main findings from the discussion and considers their implications beyond the individual research questions. We first synthesise the overall pattern of the findings before outlining practical implications, limitations, and relevance to sustainability.

5.7.1 Synthesis of the Findings

Our main pattern across the research questions is that communication material from encrypted platforms is challenging because it undergoes many steps before it becomes evidentiary material, and its evidentiary value depends on this chain, in which selection, filtering, presentation, technical control, identification, and expert explanations are coupled. The evidentiary material can be very strong without being self-explanatory: it may appear precise and objective, but is still subject to

Table 5.4: Benefits and risks of expert use in technically complex evidence

Type of expert use	**Positive function**	**Risk or control problem**
Police or prosecution-linked technical experts	Provide direct knowledge of how the material was handled, processed, and presented	The explanation may come from actors close to the investigation, creating an **uneven landscape** if one side has more technical information than the other
Defence-appointed technical experts	Give the defence a way to challenge technical interpretations, identify weaknesses, and introduce alternative explanations	Their role may **become part of the parties' contest** over the evidence, and the court must assess whether the expert is independent or **saying what they are paid to say**
Independent technical experts	Could provide a more neutral technical explanation and help the court understand complex material	They appear to be **used rarely** in technical data questions, and the court may lack a clear routine for when such expertise should be introduced
Expert explanations generally	Translate technical processes into explanations that judges and lawyers can use in legal assessment	The court may depend on the same technical explanation that it must evaluate critically, creating a **control problem**

interpretation, requires context, and is evaluated as part of an overall assessment. The court and the defence cannot see the entire underlying dataset or the full international chain of evidence, so control is exercised through documentation, technical control points, contradiction, and an overall assessment; thus, the control is often indirect and partial. The central dilemma is that the same steps that make the evidentiary material manageable also form what becomes visible and challengeable. The main challenge is to ensure that the process from data to evidence is sufficiently transparent, understandable, and open to challenge.

5.7.2 Implications for Practice

Our findings have practical relevance beyond the concrete Sky ECC case examined here. Our study builds on limited material, but the findings point to broader challenges in cases where large amounts of data come from encrypted platforms. As we see in Figure 1.1, EncroChat and Sky ECC have already been mentioned in several serious criminal proceedings, suggesting that similar questions about documentation, access, selection, technical control and expert use are likely to become even more common in the coming years. We want to clarify that our aim is not to propose legal reforms, but to extract practical points from our findings. This is summarised in Table 5.5.

5.7.3 Limitations

We interviewed 11 participants in total. This means that we focused on depth rather than broad representativeness. The selection covers several central actor groups, but is not large enough to represent judges, defence lawyers, investigators or experts more broadly. The findings show experiences, evaluations, and patterns in this material, but they are not a basis for statistical generalisation.

Practical accessibility constraints affected recruitment, and we found participants through different channels: some were suggested by supervisors, others through networks and acquaintances of acquaintances, via email to institutional addresses, and through internet searches. This is useful for gathering relevant people in a small field, but it can introduce bias, as participants may be those with a special interest, capacity, or openness. Some actors were harder to recruit than others; the defence lawyers were especially difficult to recruit, and D2 came late. This may have shaped which perspectives are more strongly represented in the material.

It is worth noting that the participants comprise 10 men and 1 woman. This might affect which experiences and perspectives emerge. We do not analyse gender as a dimension, but we still find it important to be open about the imbalance. The participants had varying levels of proximity to the Sky ECC case and to communication material from encrypted platforms as evidence; some had direct experience from

Table 5.5: Actionable implications for handling communication material from encrypted platforms

Actor / stakeholder	**What needs to be in place**	**Concrete practical steps**
Police and prosecution	The process from large dataset to case material must be visible enough for others to understand how the evidence was shaped	Document **search terms, filtering criteria, selection decisions, technical control points, missing material, and known limitations**. Make clear what has been checked, what has not been checked, and what has been excluded or not followed up
Defence lawyers	The defence must have a practical possibility to challenge the material, not only formal access to selected excerpts	Ensure access to case material in usable formats, the possibility to request **new searches or supplementary material**, and technical support where needed to understand the dataset, metadata, and limitations
Courts and judges	The court must be able to assess technical evidence without assuming that the presented material is complete, neutral, or self-explanatory	Use **control questions** about search, selection, documentation, user identification, missing material, and technical verification. Assess the material together with other evidence, and consider whether uncertainty has been made visible enough
Technical experts	Expert explanations must help legal actors understand both the technical findings and the limits of those findings	Explain **methods, assumptions, uncertainty, scope, and limitations**. Be clear about what the technical material can show, what it cannot show, and whether conclusions go beyond the technical basis
Institutional / system level	Future cases involving datasets from encrypted platforms need clearer routines across actors and stages of the process	Develop shared guidance for **documentation, access, search logs, selection records, technical verification, expert use, and supplementary searches**, so that future cases are easier to assess, challenge, and compare

cases like this, whereas others had more general academic or institutional competence. This provides breadth but also means the interviews vary in how closely they relate to concrete criminal proceedings.

The interview guides were not identical across participants. The interviews with A1 and A2 were conducted earlier in the project and used separate interview guides, partly because they served a more exploratory, expert-oriented function. The shared interview guide covers Norwegian practice and the handling of evidence in Norwegian criminal proceedings. This role-based adaptation made the interviews more relevant to each participant. At the same time, this means that the interviews were not fully symmetrical. The interviews with A1 and A2 were conducted in English, while the rest were conducted in Norwegian. Because English is not our first language, follow-up questions may have come less naturally in these interviews than in the Norwegian ones. However, this limitation was mitigated by the audio recordings and later transcript review.

Only one researcher coded the material, so no intercoder comparison was conducted. This means that the coding and thematic grouping depend on one researcher's interpretation of the material. During the analysis, we became aware that strong institutional perspectives could temporarily affect the interpretation of the material. For example, after an interview with a defence lawyer, the defence perspective seemed very convincing, whereas after an interview with a police investigator, the police perspective could appear more convincing. It is important to clarify this possible bias [Cre09, p. 192]. To reduce this limitation, we analysed the material across all interviews rather than interview by interview.

The judgment material is limited to two judgments from the same case complex and therefore cannot represent Norwegian court practice more generally. This provides depth and enables us to connect the interviews to a concrete evidentiary context, but we cannot assess variation across different case complexes, courts, platforms, or investigative setups. We want to mention that we are not seeking to verify the underlying Sky ECC material, but to examine how such material is described, understood, challenged, and evaluated by institutional actors and in the selected judgments. The field is also still evolving, and new judgments, practices and technical clarifications might emerge after the data collection, meaning that these findings describe a particular moment in an evolving area of practice.

5.7.4 Sustainability Reflection

Our thesis aligns with the UN's Sustainable Development Goal 16 [Unia], which concerns peaceful and inclusive societies, access to justice, and effective, accountable, and inclusive institutions. In our thesis, we examine the practical possibility of understanding and challenging technically complex evidentiary material, and we

examine the right to a fair trial, which relates directly to target 16.3, which concerns equal access to justice for all and the rule of law. We can see a connection to target 16.6, which concerns effective, accountable and transparent institutions. This connection arises from our examination of transparency, responsibility, and how legal institutions handle evidentiary material.

We have found that communication material from encrypted platforms can serve as strong evidence. However, for the evidentiary material to be used fairly, insight, chain of custody, technical control points, and visible uncertainty must be present. These conditions give actors a better basis for fairly evaluating and challenging the material. We therefore support the view that institutions, such as the police, the prosecution, defence lawyers, and the courts, need routines and competence to handle large digital datasets in a transparent and verifiable way.

Our thesis is also related to SDG 9 [Unib], which concerns infrastructure, industrialisation, and innovation. These cases build on advanced digital technology and require institutional capacity to manage technological infrastructure. Sustainability in our thesis is therefore mainly about fair, responsible, and trustworthy institutions in addressing technologically complex evidence.

Chapter 6
Conclusion

This chapter concludes our thesis by bringing together the main findings from our analysis. We first summarise how communication material from encrypted platforms is handled and evaluated as evidence, then clarify the study's contribution and outline directions for future research.

6.1 Summary of Main Findings

In this thesis, we have examined how communication material from encrypted platforms is handled as evidence in Norwegian criminal proceedings, using a practice-oriented, descriptive approach. The study builds on interviews with different actors and two selected judgments. Our overall findings show that the evidentiary material has undergone several technical and investigative steps. A central finding is that the material can be strong without being self-explanatory, and its evidentiary value depends on how it is handled, presented, challenged, and understood.

When the Norwegian police gained access to the communication, foreign authorities had already captured, decrypted, and structured it as very large datasets. The evidentiary material, therefore, has to be searched, filtered, selected, and formatted before it reaches the court. As a result, the court and defence encounter excerpts, tables, timelines, chat logs, or presentations. This makes the material more manageable, but it significantly affects what is visible and what can be challenged.

The evaluation of the material involves several layers, of which technically correct decryption is only one. Another one is reliability, which depends on documentation, integrity, completeness and fragmentation. Credibility depends on language, slang, metadata and technical traces. User identification is critical, as a digital user, device, or Sky ECC-ID must be linked to a physical person. Fairness depends on whether uncertainty, missing material, and alternative explanations are sufficiently visible. The chain of custody is only partly visible, especially in the foreign parts of the chain. Documentation, mirror tests, checksums, and institutional trust support the

evaluation, and these mechanisms provide a point of control without giving full transparency in the chain.

We have identified some safeguards available in these cases, such as defence insight, the possibility of new searches, contradiction, control questions, and an overall assessment. Together, these reduce risk, but they do not eliminate it completely. We have seen that many of these safeguards work after the material has already been filtered and selected. Technical reports, documentation, mirror tests and checksums function as concrete practices. At the same time, we have not found any standard regime which supports the entire evidence chain. Legal actors rely on technical explanations and experts, who help the court understand the material. This is positive, but it also introduces a control challenge involving quality, independence, and proximity to one of the parties. The main point is therefore that **the process from collected data to evidence should be visible enough, understandable enough, and possible to challenge**.

6.2 Significance and Contribution

We were unable to identify prior empirical research examining how Norwegian legal actors have approached this type of complex technical material. Our study contributes insight into the practice of these actors in a field that remains insufficiently examined. We focused on how the actors actually describe, evaluate and handle the material. The interviews provide insight into experiences from different perspectives, while the analysis of the two judgments provides a concrete legal context. This combination connects the actors' experiences to how these questions appear in court. Our contribution is to shed light on how technical uncertainty is handled in Norwegian criminal proceedings.

Our study makes a complex evidentiary field more accessible to actors who need to deal with it in practice. We show that challenges arise from the interaction among technology, process, insight, and understanding. We provide a framework for discussing what should be visible when this kind of evidence is used, and we help concretise the questions the actors should ask about the material. Our study also shows that it is important to consider the entire chain from collection to evidence, and we make it clear that practical handling of such cases includes facilitating evaluation and challenge. This can be useful as a foundation for further routines, training or guidance for actors meeting such evidence. We highlight the need for greater understanding between legal and technical actors. The practical implications summarised in Table 5.5 show how these findings can be translated into more concrete points for police and prosecution, defence lawyers, technical experts and institutional actors.

6.3 Future Work

Our study has been exploratory, and we have identified many topics worth exploring further. First, future research could include more cases, more judgments, and a broader range of actors. This study is based on a limited number of interviews and judgments, so further studies could examine whether the same challenges also occur in other cases.

It would be interesting to examine the balance between thoroughness and efficiency in these types of cases. Are there, for example, risks of some criminals going free because there are not enough police resources to look further into the Sky ECC material? Or do we know whether the process described by P2 in Section 4.1.1 has had sufficient resources to expand the Norwegian Sky ECC network? In this study, we saw in Section 4.1.2 that P1 mentioned that a case could be cut short if it was considered sufficiently clarified, but we have not examined this further. This also enables further exploration of the selection by analysing search logs, process logs, or full case files, and looking closely at how searches are conducted, how the selection is made, what is actually left out, and how this is made visible to the defence and the court.

Another aspect we wanted to look into further, but which would be out of scope for this project, is to delve deeper into the defence lawyer's perspective and the defence strategies used to challenge this material. While D1 was criticising the usage of this material, D2 actually said that declaring this evidentiary material invalid would *"totally undermine the legal culture and pretty much society itself"*, so that would not happen. D2 therefore focused more on explaining that a better defence strategy would be to contest the identification moments, and cooperate more with the court, and not stay silent. D2 mentioned that this strategy could result in a reduced sentence, possibly by several years. Future research could examine which defence strategies were used in the Sky ECC cases, and whether the defence lawyers still support the same strategies they used when defending the accused.

In our study, we found that both judges and defence lawyers rely on experts, but this reliance introduces a new challenge about the quality of experts. Further research could examine how courts evaluate the quality of expert testimony and its technical explanations in cases involving digital evidence. It would also be possible to consider who should serve as an expert in these technically complex cases. The research could examine whether there is a need for more independent experts and why they are more often used in cases involving traditional evidence.

References

[Alf26] Alfasoft, *NVivo 15 - The Most Trusted Qualitative Analysis Software (QDA) is Even Better*, 2026. last visited: Jun. 2, 2026. [Online]. Available: https://nvivo.de/en/.

[App24] Apple, *iMessage security overview*, Dec. 2024. last visited: May 24, 2026. [Online]. Available: https://support.apple.com/guide/security/imessage-security-overview-secd9764312f/web.

[APSS24] M. Albrecht, S. Park, et al., "The Case of EncroChat: A Real-World Law-Enforcement Hack", in *Real World Crypto 2024*, Mar. 2024. last visited: Mar. 2, 2026. [Online]. Available: https://www.youtube.com/watch?v=AeKRS6_zxoc.

[Aum18] J.-P. Aumasson, *Serious Cryptography - A Practical Introduction to Modern Encryption*. No Starch Press, 2018.

[BĆ25] V. Bajović and V. Ćorić, "Encrochat and Sky ECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision", *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 33, pp. 235–262, Sep. 2025. [Online]. Available: https://brill.com/view/journals/eccl/33/3/article-p235_002.xml?srsltid=AfmBOoqTfG1zrQinRHmoXDmpQ4CKzVoxylBIhUDLJH-OIcGxAumMiZag.

[Bun22] Bundesgerichtshof, *5 StR 457/21*, Judgment, 2022. last visited: Mar. 2, 2026. [Online]. Available: https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Strafsenate/5_StS/2021/5_StR_457-21.pdf?___blob=publicationFile&v=2.

[Bus25] E. G. Buset, *Cryptographic Evidence in Norwegian Courts*, Specialisation project report, Norwegian University of Science and Technology (NTNU), Unpublished project report, Nov. 2025.

[CM16] Colin and K. R. McCartan, *Real World Research*. Wiley, 2016.

[Cou21] Court of Appeal (England and Wales), *A v R [2021] EWCA Crim 128*, Judgment, 2021. last visited: Feb. 26, 2026. [Online]. Available: https://www.judiciary.uk/wp-content/uploads/2022/07/A-v-R.pdf.

[Cre09] J. W. Creswell, *Research design : qualitative, quantitative, and mixed methods approaches*. Sage, 2009.

[Eur21] Eurojust, "Eurojust Annual Report 2020", Eurojust, Tech. Rep., 2021, pp. 28–29. last visited: Mar. 5, 2026. [Online]. Available: https://www.eurojust.europa.eu/sites/default/files/assets/2021_04_14_eurojust_annual_report_2020_final.pdf.

[Eur25] Europol, *Operation Emma*, Dec. 2025. last visited: May 24, 2026. [Online]. Available: https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-emma.

[Eur26] Europol, *Operational Taskforce LIMIT*, Apr. 2026. last visited: May 24, 2026. [Online]. Available: https://www.europol.europa.eu/how-we-work/operations/operational-taskforce-limit.

[Goo24] B. Goodwin, *Ex-boxer fights US government over legality of Sky ECC cryptophone intercepts*, Nov. 2024. last visited: Mar. 2, 2026. [Online]. Available: https://www.computerweekly.com/news/366615638/Ex-boxer-fights-US-government-over-legality-of-Sky-ECC-cryptophone-intercepts.

[Goo26] Google, *Google Scholar*, 2026. last visited: May 22, 2026. [Online]. Available: https://scholar.google.com/.

[Inv23] Investigatory Powers Tribunal, *SF and Others v National Crime Agency (IPT/21/05/CH)*, Judgment, 2023. last visited: Mar. 5, 2026. [Online]. Available: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2023/05/SF-and-Ors-v-NCA-JUDGMENT-IPT-21-05-CH-and-Ors.pdf.

[Kri25] J. Kriukow, *20 minute NVivo tutorial: learn how to code qualitative data*, Jan. 2025. last visited: Mar. 18, 2026. [Online]. Available: https://www.youtube.com/watch?v=FpMm0SEqLzU.

[Kri26] J. Kriukow, *How to code the data in NVivo 15*, Jan. 2026. last visited: Mar. 18, 2026. [Online]. Available: https://www.youtube.com/watch?v=tWeVEjCk6FM.

[LA-2023-74900-3] Agder lagmannsrett, *LA-2023-74900-3*, Judgment, Nov. 2023. last visited: May 27, 2026. [Online]. Available: https://lovdata.no/dokument/LASTR/avgjorelse/la-2023-74900-3.

[LB-2021-164345] Borgarting lagmannsrett, *LB-2021-164345 – LB-2021-164360 – LB-2021-168568*, Ruling, Jan. 2022. last visited: Apr. 15, 2026. [Online]. Available: https://lovdata.no/dokument/LBSTR/avgjorelse/lb-2021-164345.

[LB-2022-147596] Borgarting lagmannsrett, *LB-2022-147596*, Judgment, Feb. 2023. last visited: Apr. 15, 2026. [Online]. Available: https://lovdata.no/dokument/LBSTR/avgjorelse/lb-2022-147596.

[LB-2023-104594] Borgarting lagmannsrett, *LB-2023-104594*, Judgment, Dec. 2023. last visited: Apr. 15, 2026. [Online]. Available: https://lovdata.no/dokument/LBSTR/avgjorelse/lb-2023-104594.

[LB-2024-142625] Borgarting lagmannsrett, *LB-2024-142625*, Judgment, Jun. 2025. last visited: May 31, 2026. [Online]. Available: https://lovdata.no/dokument/LBSTR/avgjorelse/lb-2024-142625.

[Lov26a] Lovdata, *Lovdata*, 2026. last visited: May 22, 2026. [Online]. Available: https://lovdata.no/sok?q.

[Lov26b] Lovdata, *Lovdata Pro*, 2026. last visited: May 22, 2026. [Online]. Available: https://lovdata.no/pro/#myPage.

[MdRE+24] J. Meeuwissen, R. de Roo, et al., "Forensic advisers working for all district courts and courts of appeal in the Netherlands: An overview and discussion", *Journal of Forensic Sciences*, vol. 69, pp. 182–188, 1 Jan. 2024.

[Met26] Meta, *What end-to-end encryption on Messenger means and how it works*, 2026. last visited: May 24, 2026. [Online]. Available: https://www.facebook.com/help/messenger-app/786613221989782.

[OR23] J.-J. Oerlemans and S. Royer, "The future of data-driven investigations in light of the Sky ECC operation", *New Journal of European Criminal Law*, vol. 14, pp. 434–458, 4 2023. [Online]. Available: https://doi.org/10.1177/20322844231212661.

[OvT22] J.-J. Oerlemans and D. A. van Toor, "Legal Aspects of the EncroChat Operation: A Human Rights Perspective", *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 30, 3-4 2022. [Online]. Available: https://brill.com/view/journals/eccl/30/3-4/article-p309_006.xml.

[Sag23] G. Sagittae, "On the lawfulness of the EncroChat and Sky ECC-operations", *New Journal of European Criminal Law*, vol. 14, pp. 273–293, 3 Sep. 2023. [Online]. Available: https://journals.sagepub.com/doi/10.1177/20322844231159576.

[SE24] K. Sæter and E. Engdal, "Til sammen 105 års fengsel for narkonettverk", *Dagens Næringsliv*, Apr. 2024. last visited: May 10, 2026. [Online]. Available: https://www.dn.no/kriminalitet/oslo-tingrett/kripos/kokain/til-sammen-105-ars-fengsel-for-narkonettverk/2-1-1628499.

[Sig26] Signal, *Speak Freely - Share Without Insecurity*, 2026. last visited: May 31, 2026. [Online]. Available: https://signal.org/.

[Sik26] Sikt, *Sikt – Norwegian Agency for Shared Services in Education and Research*, 2026. last visited: May 31, 2026. [Online]. Available: https://sikt.no/en/about-sikt.

[Sto24a] H. Stolt-Nielsen, "Syv personer dømt etter mafiaparagrafen i norgeshistoriens største narkotikasak", *Aftenposten*, Apr. 2024. last visited: May 10, 2026. [Online]. Available: https://www.aftenposten.no/norge/i/8qlRxW/syv-personer-doemt-etter-mafiaparagrafen-i-norgeshistoriens-stoerste-narkosak.

[Sto24b] R. Stoykova, "A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings", *Computer Law & Security Review*, vol. 55, p. 106 040, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364924001067.

[Tjo19] A. Tjora, *Qualitative Research as Stepwise-Deductive Induction*. Routledge, 2019.

[TOSL-2022-185848] Oslo tingrett, *TOSL-2022-185848*, Judgment, Apr. 2024. last visited: May 16, 2026. [Online]. Available: https://lovdata.no/dokument/TRSTR/avgjorelse/tosl-2022-185848.

[Unia] United Nations, *16 Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels*. last visited: May 23, 2026. [Online]. Available: https://sdgs.un.org/goals/goal16#targets_and_indicators.

[Unib] United Nations, *9 Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation*. last visited: May 23, 2026. [Online]. Available: https://sdgs.un.org/goals/goal9#targets_and_indicators.

[Uni26a] University of Oslo, *Nettskjema*, 2026. last visited: May 28, 2026. [Online]. Available: https://nettskjema.no/.

[Uni26b] University of Oslo, *Nettskjema-diktafon*, 2026. last visited: May 28, 2026. [Online]. Available: https://www.uio.no/english/services/it/adm-services/nettskjema/help/nettskjema-dictaphone.html.

[Uni26c] University of Oslo, *Transcribe with Autotekst*, 2026. last visited: Jun. 3, 2026. [Online]. Available: https://autotekst.uio.no/en.

[WBJ+25] S. Westers, M. Berkenpas, et al., "From code to courtroom - The role of encryption in the Dutch criminal justice system", in *Legal and Ethical Issues in Digital Policing*. Koninklijke Boom uitgevers, 2025, pp. 109–131. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1918059/FULLTEXT01.pdf#page=111.

[Wha26] WhatsApp, *About end-to-end encryption*, 2026. last visited: May 24, 2026. [Online]. Available: https://faq.whatsapp.com/820124435853543.

Appendix A

Interview Guide

Felles intervjuguide

Instruksjoner til meg selv

Ikke vær partisk

Still spørsmål åpent, ikke-ledende

Husk å takke for tiden

Om jeg er usikker på om jeg forstår hva de mener, kan jeg legge inn "forstår jeg riktig at du mener ...?"

Info om samtykke osv.

Max tid: 5 min

- Opptak
- Kan velge å ikke svare på hvilke som helst spørsmål
- Interessert i dine personlige tanker og erfaringer, det finnes ingen feil svar
- Du har muligheten til å ta tilbake noe du har sagt hele tiden
- Mer informasjon finnes i infoskrivet
- Kjapp intro til oppgaven
    - Hvordan kryptert informasjon brukes og forstås som bevis i norske rettsaker
    - Hvordan teknisk usikkerhet håndteres i praksis, og hvordan ulike aktører forholder seg til dette
    - Kun ment som bakgrunnsintervju, for å forstå praksis og arbeidsflyt, ikke for å evaluere rettslige vurderinger
- Varighet + struktur

Tema 1 – Oppvarming – Rollen og arbeidsflyten rundt kryptert kommunikasjon

Max tid: 8 min

Spørsmål 1.1

- Kan du beskrive din rolle i saker der kryptert kommunikasjon inngår som bevis?

Spørsmål 1.2

- Hvordan opplever du at slikt materiale typisk beveger seg gjennom prosessen, fra etterforskning til bruk i retten, sett fra ditt perspektiv?
- Når du først blir involvert i slike saker, hva opplever du at du allerede må ta for gitt om materialet du får?

Notat

- Ikke avbryt eller korriger
- La informanten sette begreper

Oppfølgingsspørsmål

- Hvis roller blir uklare:
    - På hvilke tidspunkt er du selv involvert, og hvor går ansvaret videre til andre aktører
- Hvis uklart hvor bearbeidet materiale er
    - Hvordan ser materiale vanligvis ut når det når deg?

Hva får jeg ut av spørsmålet/Hvorfor dette spm?

- Presis aktørkartlegging (til metodekapittelet)
- Språk og begreper aktøren bruker
- Bedre presisjon i de resterende temaene

Relevante RQs

- RQ1 – legal and procedural challenges
    - Indirekte ved å avdekke praksis
- RQ2 – hvordan aktører vurderer pålitelighet
- RQ3 – beviskjede og samarbeid
    - Synliggjør hvem som er involvert

Tema 2 – Seleksjon og filtrering i praksis

Max tid: 12 min

Spørsmål 2.1

- Når store mengder kryptert kommunikasjon blir tilgjengelig i en sak, hvordan foregår seleksjon og filtrering i praksis?

Notat

- Ikke vær partisk
- Ikke vurder, kun få kjennskap til praksis

Oppfølgingsspørsmål

- Hvis utfordringer ikke blir nevnt
    - Hvilke utfordringer oppstår i forbindelse med slik seleksjon og filtrering?
- Hvis tidspunkt er uklart
    - På hvilket stadium i prosessen skjer denne seleksjonen, er det tidlig i etterforskningen, underveis, eller nærmere tiltale?
- Hvis ansvar og roller er uklart
    - Hvem er det i praksis som bestemmer hva som blir tatt videre, og hva som blir lagt til side
- Hvis det mangler begrunnelse for at det blir som det blir
    - Hvilke typer vurderinger ligger til grunn for valgene?
- Hvis dokumentasjon ikke blir nevnt
    - Blir det dokumentert hva som velges bort?
- Hvis konsekvenser av seleksjon over tid ikke nevnes
    - Når utvalget først er gjort, opplever du at det da finnes informasjon som i praksis ikke lenger lar seg etterprøve?
- Hvis veldig abstrakt svar
    - Kan du beskrive et eksempel på en sak hvor et stort datamateriale blir snevret inn?
- "Har du opplevd at en melding eller en chatlog så ganske belastende ut alene, men så endret betydningen seg når du fikk mer kontekst?"
- "Har du opplevd at det kom nytt materiale senere som endret forståelsen av det som allerede var lagt frem?"

Hva får jeg ut av spørsmålet/Hvorfor dette spm?

- Kartlegger hvordan store datamengder snevres inn i praksis
- Empiri om hvordan datasett blir ufullstendige
- Innsikt i
    - Hva som aldri når retten

    - Hvilke deler av materiale som blir sett på som relevant
- Grunnlag for å se på
    - Incomplete datasets
    - Selective presentation
    - Access and disclosure

Relevante RQs

- RQ2 – hvordan aktører vurderer pålitelighet
- RQ4 – safegards mot selektive bevis

Tema 3 – Presentasjon av kryptert kommunikasjon som brukes som bevis i retten

Max tid: 12 min

Spørsmål 3.1

- Når kryptert kommunikasjon blir presentert i retten, hvordan blir dette materialet typisk fremstilt og strukturert i praksis?

Notes

- Ikke vær partisk, unngå ord som problem, mangler, skjevhet
- Ikke vurder

Oppfølgingsspørsmål

- Hvis formen for presentasjon er uklar
    - I hvilken form møter retten dette materiale?
        - Utdrag, sammendrag, tidslinjer?
- Hvis teknisk usikkerhet ikke nevnes
    - Hvordan håndteres usikkerhet eller manglende kontekst når materialet presenteres?
- Hvis forenkling ikke nevnes
    - Er det deler av materialet som i praksis forenkles i retten?
- Har du opplevd at presenterte utdrag ga et annet inntrykk enn det fulle kommunikasjonsforløpet ville gjort?
    - Gav det mer klarhet eller tyngde enn det var grunnlag for?
-

Hva får jeg ut av spørsmålet/Hvorfor dette spm?

- Gir empiri om hvordan teknisk materiale oversettes til rettslig forståelig former
- Viser
    - Hvordan narrativer bygges
    - Hva som anses som nok dokumentasjon
- Danner grunnlag for å kunne se på
    - Evidence artifacts presented in courts
    - Selective presentastion
    - Judicial strategies of caution

Relevante RQs

- RQ2 – hvordan aktører vurderer pålitelighet
- RQ4 – safegards mot selektive bevis

Tema 4 – Beviskjede og utenlandsk samarbeid i praksis

Max tid: 12 min

Spørsmål 4.1

- Når kryptert kommunikasjon som politiet har fått tilgang til gjennom samarbeid med utenlandske myndigheter, hvordan oppleves beviskjeden og informasjonsflyten i praksis fra ditt ståsted?

Notes

- Fokuser på hvordan det faktisk håndteres i praksis, ikke hvordan det burde ha vært

Oppfølgingsspørsmål

- Hvis utenlandsk samarbeid nevnes overfladisk
    - Hvilken informasjon følger vanligvis med materialet når det kommer fra utenlandske myndigheter
- Hvis tillit ikke nevnes
    - Er det deler av prosessen eller materialet som man i praksis ikke har full innsikt i, men likevel må forholde seg til?
- Hvis dokumentasjon ikke nevnes
    - Hva type dokumentasjon finnes det i praksis rundt innhenting og overlevering av materialet?
- Har dere bedt om mer innsyn eller mer materiale, men ikke fikk det? Hva var det konkret dere mente manglet?
- Hva er det viktigste du skulle ønske du visste mer om når materiale kommer fra utenlandske myndigheter?

Hva får jeg ut av spørsmålet/Hvorfor dette spm?

- Gir empiri på forhold som ikke kommer frem av dommer eller lovdata
- Synliggjør
    - Hva aktører vet
    - Hva de må stole på uten egen verifisering
- Gir grunnlag for å kunne se på
    - Cross border data handling
    - Chain of custody in practise
    - Drøfting av institusjonell tillit under teknisk usikkerhet

Relevante RQs

- RQ1 – prosessuelle utfordringer
- RQ3 – mekanismer for transparens og beviskjede

Tema 5 – Uformelle standarder og praksiser

Max tid: 8 min

Spørsmål 5.1

- Er det sider ved **arbeidet** med kryptert kommunikasjon, som i praksis sjelden blir problematisert eller stilt spørsmål ved?

Notes

- Ikke antyd at noe bør være problematisert
- La informanten selv beskrive hva som blir tatt for gitt

Oppfølgingsspørsmål

- Hvis generelt
  - Kan du si litt mer konkret hva som blir tatt for gitt i slike saker?
- Hvis "godt nok" ikke kommer frem
  - Hva oppfattes i praksis som tilstrekkelig dokumentasjon eller undersøkelse, uten at man går videre?
- Hvis praksis fremstilles som fullstendig planlagt og gjennomtenkt
  - Opplever du at dette varierer mellom saker, eller mellom aktører?
- Hvis ikke ekspertvitner nevnes
  - I noen saker brukes ekspertvitner. Hvis det er aktuelt i din erfaring, er det noen sider ved dette som sjelden blir problematisert?
- Er det noe ved digitale eller dekrypterte bevis som du opplever at retten eller påtalemyndigheten ofte tar litt for mye for gitt?

Hva får jeg ut av spørsmålet/Hvorfor dette spm?

- Avdekker standarder og terskler i praksis
- Viser
  - Hva som blir sett på som godt nok
  - Hvor man i praksis slutter å stille spørsmål
- Gir mulighet for å se på
  - Judicial strategies of caution
  - Fairness without full transparency
  - Expert knowledge as a trust mechanism

Relevante RQs

RQ2 – hvordan aktører vurderer pålitelighet og rettferdighet

RQ6 – hvordan dommere og advokater er avhengig av ekspertvitner

Tema 6 - Avslutning

Max tid: 5 min

Spørsmål 6.1

- Er det noe du mener forsvarersiden ser tydeligere enn andre aktører i disse sakene?
- Er det noe ved bruken eller forståelsen av slik kommunikasjon som bevis du opplever ofte blir forenklet eller misforstått i diskusjoner om slike saker?

Notes

- Still spørsmålet rolig, uten oppfølgingspress

Oppfølgingsspørsmål

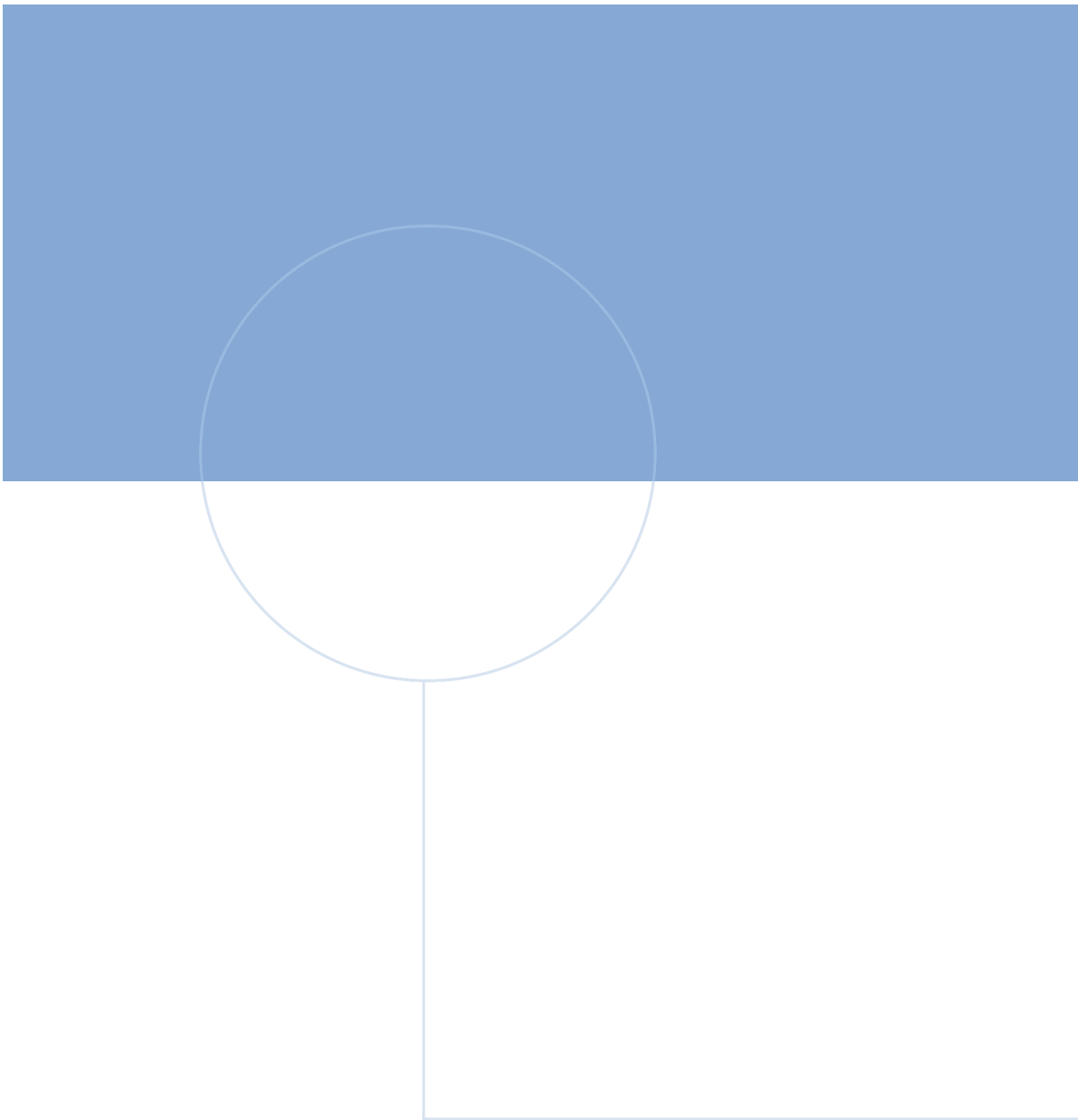
- Nei

Hva får jeg ut av spørsmålet/Hvorfor dette spm?

- Åpner for uventede perspektiver
- Gir materiale til discussion kapittel
- Kan avdekke problemer jeg ikke var klar over

Relevante RQs

- Ingen direkte



NTNU

Norwegian University of
Science and Technology