Norwegian University of Science and Technology

Cryptology and Social Life: Cryptographic Evidence in Norwegian Courts

Tjerand Silde – Social Foundations of Cryptography Autumn School

NTNU | Norwegian University of Science and Technology

PART 1

Cryptology and Social Life

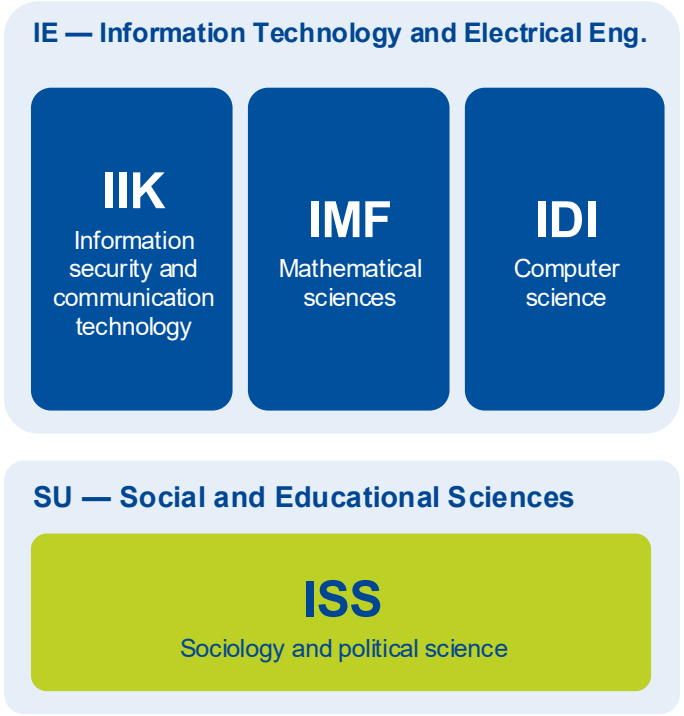
The Project

Cryptology and Social Life: The Idea

How cryptographic systems are designed, deployed, governed, and ultimately understood, trusted, and used in practice

Digital infrastructures as coupled technical, organizational and social problems

Four departments, two faculties, one project with seed-funding by the NTNU Community strategic area to get things started



The Team

Tjerand Silde

Associate Professor, IIK

Cryptographic protocols, privacy, quantum-safe cryptography.

Katrien De Moor

Professor, IIK

Human-centered design and evaluation, usable privacy and security.

Kristian Gjøsteen

Professor, IMF

Applied cryptography, security protocols, electronic identification.

Eric Monteiro

Professor, IDI

Public-sector digitalization, information infrastructures, system implementation

Emil André Røyrvik

Professor, ISS

Ethnography of organizations, governance, technology and culture.

Petter Grytten Almklov

Professor, ISS

Societal security, risk, and digitalization in organizations

Seed Funding

We got 200 KNOK in seed funding from the NTNU Community strategic area to get started

February 2025	December 2025	Spring 2026
Visit to the Social Foundations of Cryptography team in London Tjerand, Katrien, Emil and Petter	**Cryptology and Social Life workshop, Trondheim** 40 participants, 6 countries, 10 institutions, 3 keynotes	**Master's Thesis on Cryptographic Evidence in Norwegian Courts** Our first project and the main topic of this talk

The Workshop, Trondheim, December 2025

The Workshop Program

Keynote — Phil Rogaway: “Can Ethics Be Taught?”

Keynote — Rikke Bjerg Jensen: “Social Foundations of Cryptography: An Ethnography Talk”

Keynote — Jean-François Blanchette: “Legislating digital signatures: Lessons from a past cryptographic utopia”

Short talks:

- Kristian Gjøsteen: "EUDI wallets and sole control"
- Eirik Gjerde Buset: "Cryptographic evidence in Norwegian courts"
- Victor Morel: "Privacy compliance of TCF-based Android apps"
- Katherine Butcher: "Deepfakes, epistemic authority and E2EE"
- Mikaela Brough: "Security, privacy and grassroots environmentalism in the Philippines"
- Gergely Biczok: "Interdependent privacy and address books"
- Hans Heum: "Smittestopp contact tracing"
- Lorenzo Martinico: "The politics of surveillance in the UK"

Norwegian University of Science and Technology

PART 2

Cryptography in Court

EncroChat, Sky ECC, and how Norwegian courts dealt with them

EncroChat and Sky ECC

Cryptophones: modified commercial devices in closed ecosystems with pseudonymous IDs, disappearing messages, distress passwords, and remote wipe

EncroChat (c. 2013–2020): roughly 60,000 users and more than 120 million messages collected; in 2020, a French–Dutch–Europol joint investigation team copied the servers at OVH in Roubaix and pushed collection software (malware) to the users in the system

Sky ECC (shut down March 2021): a France–Belgium–Netherlands team copied a live server's memory and ran a man-in-the-middle to obtain keys; about a billion messages across 170,000 IDs, roughly 60% decrypted

A Real-World Law-Enforcement Hack: The Case of Encrochat

Martin R. Albrecht[1], Sunoo Park[2], Michael A. Specter[3], and Douglas Stebila[4]

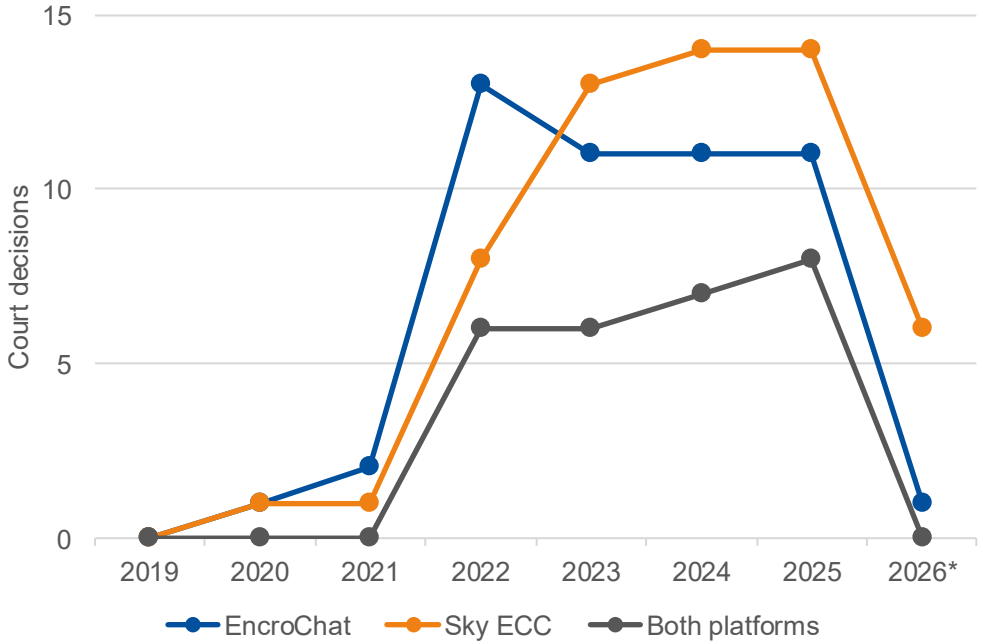
[1]King's College London, UK, martin.albrecht@kcl.ac.uk
[2]New York University, USA, sunoo.park@nyu.edu
[3]Georgia Tech, USA, specter@gatech.edu
[4]University of Waterloo, Canada, dstebila@uwaterloo.ca

25th June 2026

Abstract

In 2020, a coordinated law-enforcement effort infiltrated Encrochat, an end-to-end encrypted service provider, exfiltrating historical and real-time data and metadata over months. Encrochat was used extensively by organised crime, and the data from the operation was used as supporting evidence in over 6,000 arrests and related prosecutions across Europe. Encrochat's architecture was vertically integrated, with the company acting as both a device vendor and service provider; Encrochat sold modified Android smartphones with its own PKI and custom applications, including encrypted messaging based on the Signal protocol. In this work, we give the most detailed public account to date of Encrochat's infrastructure and how it was compromised.

Already in Norwegian Case Law



Norwegian court decisions mentioning EncroChat and/or Sky ECC (thesis Figure 1.1; Lovdata Pro search, May 22, 2026).

≈40

people convicted in ≈20 Norwegian cases on Sky ECC material by September 2023 (prosecutor, Advokatbladet)

≈1,250

Norwegian Sky ECC users, of about 170,000 worldwide (prosecutor)

HR-2022-1314-A: EncroChat material read under French law admitted by the Supreme Court — on three conditions (next slide)

The Supreme Court's Three Conditions

English version

HR-2022-1314-A

Instans	Noregs Høgsterett – Orskurd
Dato	2022-06-30
Publisert	HR-2022-1314-A
Stikkord	Straffeprosess. Bevisavskjæring. Data innhentet av utenlandske myndigheter fra kryptert datatrafikk. EncroChat.
Sammendrag	Politiet hadde fått tilgang til datamateriale som fransk politi hadde avlest fra et kryptert kommunikasjonsnettverk, og ønsket å bruke dette materialet som bevis i en norsk straffesak. Høyesterett uttalte at dersom innhentingen av materialet ikke kunne ha vært gjort lovlig i Norge - et spørsmål det ikke ble tatt standpunkt til - måtte tre vilkår være oppfylte for å kunne bruke materialet som bevis. Bevisene må være innhentet etter reglene som gjelder i det aktuelle landet. Tiltalte må ha rett til innsyn i alle opplysningene som er innhentet. Innhentingen må heller ikke være gjennomført på en måte som gjør at bruken som bevis vil være i strid med grunnleggende norske verdier. Høyesterett kom til at alle vilkårene var oppfylte. Til det siste vilkåret ble det lagt avgjørende vekt på at det ikke var tale om masseovervåking, og på at Stortinget gjennom strpl. § 216 o har åpnet for datainnhenting i situasjoner som i alle fall etter ordlyden ligger nær opp til den aktuelle situasjonen. Det ble også vist til at bruk av en kryptert kommunikasjonsplattform som i all hovedsak ble benyttet av kriminelle, ikke hadde krav på vern. Kravet om at materialet skulle avskjæres som bevis ble ikke tatt til følge. (Rt-sammendrag) Henvisninger: Straffeprosessloven (1981) §216o
Saksgang	Oslo tingrett TOSL-2021-30329 – Borgarting lagmannsrett LB-2021-164345, LB-2021-164360 og LB-2021-168568 –

HR-2022-1314-A (June 30, 2022): EncroChat material read by French police, admitted in a Norwegian trial — Lovdata

Foreign-collected material may be used as evidence in Norwegian Courts if

1. it was collected under the rules of the country where it was collected
2. the accused has a right of access to all the information collected
3. the collection was not done in a way that makes its use contrary to fundamental Norwegian values

Decisive for (3): no mass surveillance, and Parliament has opened for data reading in nearby situations (§ 216o). A platform "mainly used by criminals" had no claim to protection.

How We Got Involved

It started in the news

The Sky ECC trials made headlines from 2023: the largest drug case in Norwegian history, and a crucial piece of evidence was a French spreadsheet.

Then the courts reached out

In spring 2025, I was engaged as an expert witness in the ongoing cases — on the encryption Sky ECC used, and on how the data was collected through Europol's man-in-the-middle attack on the end-to-end encrypted service.

Expert witness testimony

April 2025

Borgarting Court of Appeal, Oslo LB-2024-142625

May 2025

Oslo District Court

June 2025

Gulating Court of Appeal, Bergen LG-2025-43360

September 18, 2026

Next testimony — tomorrow

Two Vocabularies for the Same Object

What the cryptographer sees

Integrity
hashes, checksums

Authentication
a key or an ID was used

Confidentiality
side-stepped by the operation

Provenance
where the bytes came from

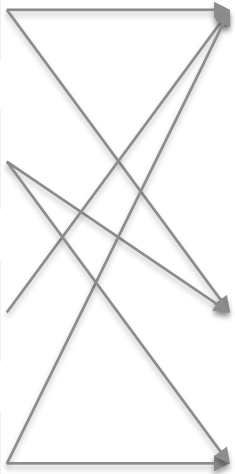
What the court asks

Reliability
usable, documented, complete?

Credibility
can meaning be anchored in context?

User identification
does the ID belong to this person?

Fairness
is uncertainty visible enough to challenge?



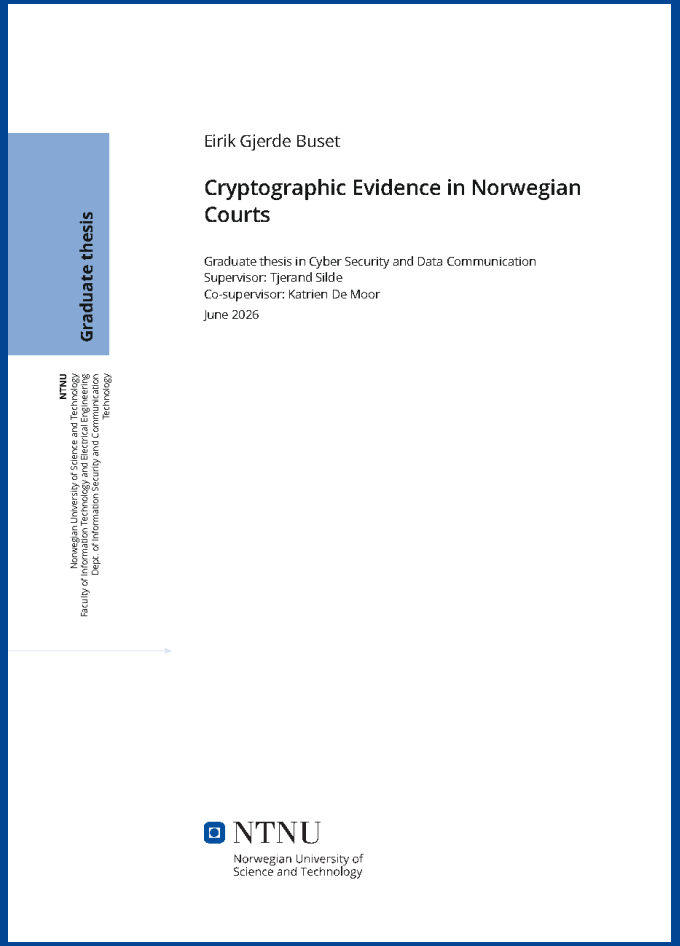
A digital signature shows that a person's key was used, not that the person signed — and mathematical proof does not translate automatically into legal proof.

NTNU | Norwegian University of Science and Technology

PART 3

Master's Thesis by Eirik Gjerde Buset

Cryptographic Evidence in Norwegian Courts — questions, method, case, findings



The Study and Its Questions

MSc thesis, June 2026 — Eirik Gjerde Buset, supervised by Tjerand Silde and Katrien De Moor

How material from encrypted platforms is handled, evaluated, and challenged as evidence in Norwegian criminal proceedings

Descriptive and practice-oriented: it was not a normative assessment of the law, nor a technical verification of the material

No prior empirical research on Norwegian practice was found, and very little elsewhere either

Six research questions

RQ1	Procedural challenges
RQ2	Reliability, credibility and fairness
RQ3	Transparency and chain of custody across borders
RQ4	Safeguards against selective presentation
RQ5	Standards guiding forensic experts
RQ6	Reliance on expert testimony

Method: Qualitative and Practice-Oriented

2	2	3	3	1
judges	defense lawyers	police investigators	academic experts	recent law graduate

Role-based emphasis: judges on assessment and safeguards; defense on access and contradiction; police on collection and selection; academics on technical uncertainty; the law graduate on education

Contrast: the EncroChat paper reconstructed its story from 3,000+ pages of documents; this study asked the people involved in these kind of cases in Norway

The Case Behind the Judgments

Oslo District Court TOSL-2022-185848 and Borgarting Court of Appeal LB-2024-142625

Seven defendants; indictments built on Sky ECC material Kripos received from Europol, split into 54 events

Main hearing Sep 19 – Dec 12, 2023, 26 witnesses; appeal 26 court days, 18 witnesses. Described as “probably the largest drug case in Norwegian history”

The defense's complaint was that evidence for the strictest penalty had reached them as an Excel sheet; the prosecutor saw “no difficult legal questions”

Advokat Marius Dietrichson forsvarer en av de sju tiltalte. Til venstre advokatene Camila Alexandra Aas og Vidar Lind Iversen (bak til høyre). Foto: Nina Schmidt

Kan man dømmes til lovens strengeste straff basert på bevis forsvarene bare har fått se på et regneark?

Seks menn og én kvinne står tiltalt i det som trolig er Norgeshistoriens største narkotikasak. Forsvaret er kritiske til at de ikke får se originalbevisene fra appen Sky ECC - en meldingstjeneste som ifølge aktoratet i hovedsak er benyttet til narkotika-kriminalitet.

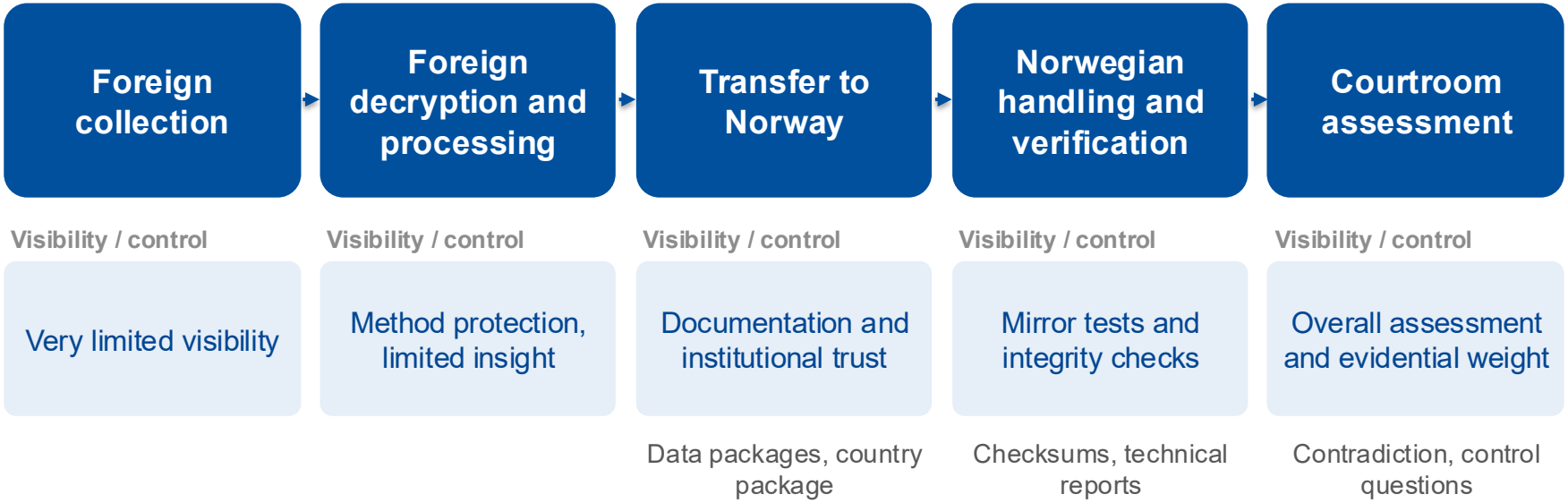
Nina Schmidt
REDAKTØR

PUBLISERT 20.09.2023 - 04:00 SIST OPPDATERT 20.09.2023 - 07:51

Ifølge påtalemyndigheten har alle de sju tiltalte brukt det krypterte

“Can you be sentenced to the law's strictest penalty on evidence the defense has only seen in a spreadsheet?”
— Advokatbladet, September 20, 2023, on the opening day of the trial

The Evidence Chain



After thesis Figure 5.1

The Challenges at a Glance

Scale
About a billion messages, 170,000 IDs

Selection before court
Search terms and priorities shape the case before a judge sees it

Partial visibility
The foreign part of the chain is closed by design

Completeness
Known and unknown unknowns; one-way dialogues

Interpretation
Slang, timestamps, system events, technically true but misleading

Identification
A key, an ID, or a phone is not (necessarily) a (unique) person

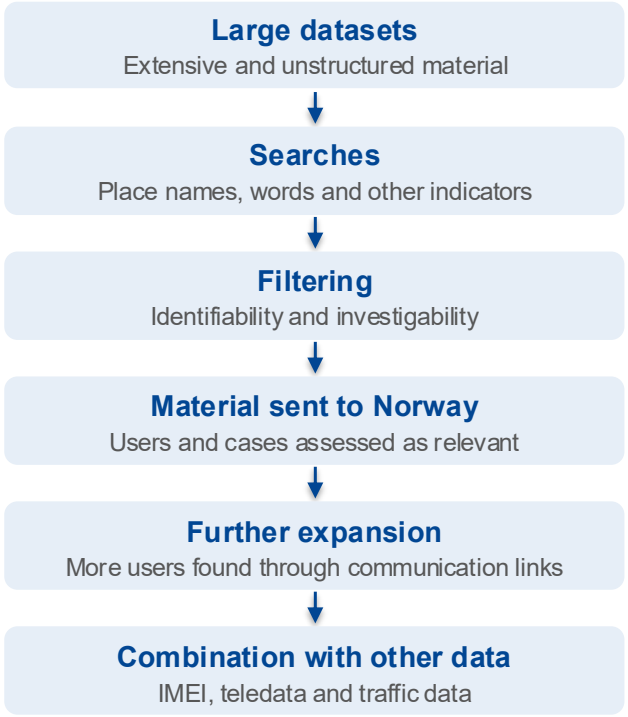
Expert dependence
Courts rely on explanations they cannot check

Safeguards act late
Contradiction and control questions come after filtering

Weak regulation
No standard covers the whole chain; handling varies by case

Synthesized from the thesis (chapters 4–5)

Theme A — Finding the Needle



After thesis Figure 4.2

- Searches on Norwegian place names and words
- Filtering: can the user behind the ID be identified — and are the acts concrete enough to investigate?
- JSON → database → CSV → Excel, chosen for its low entry barrier (P2)
- Expansion through contacts; combined with IMEI, teledata and traffic data; ~950 Sky ECC IDs received
- · “Finding the needle in the haystack” (P3)
  · Nobody can read everything from 170,000 users (P2)
  · A full presentation would run to millions of lines (D1)

Selection Happens Early and Is Inevitable

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: excerpts, tables, timelines, slides	The material may appear cleaner, more coherent and more complete than the dataset
Courtroom assessment	Lets the court evaluate the material within ordinary procedure	Assessment begins after prior processing has shaped what is visible and challengeable

Thesis Table 5.1

"Some degree of selection will inevitably have to take place" **— judge J2**

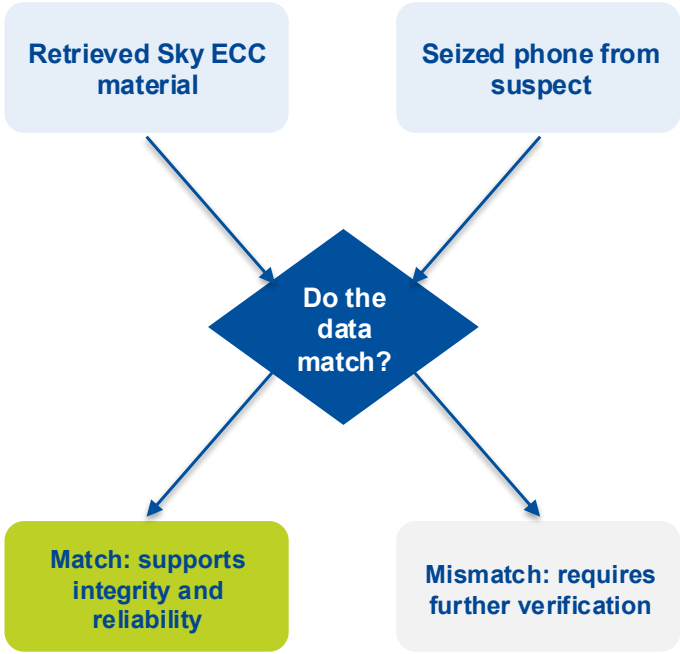
"Always a balancing of thoroughness and efficiency" **— judge J1**

Defense lawyers "at the mercy of the police selection process" **— reported by P3**

A client acquitted because the defense found messages the police had not presented **— D2**

Theme B — “Reliability Is a Chain”

- Documentation, provenance, chain of custody come first; transparency is “the core of reliability” (P3)
- Mirror tests: received Sky ECC data compared with a seized phone
- Identical checksums at Kripos and the Netherlands Forensic Institute; media files checked at the District Court
- Logged decryption attempts (including failures); technical reports
- Protecting decryption methods ≠ documenting the handling chain — only the first has a claim to secrecy (P3)



The mirror test (after thesis Figure 4.3)

A Checksum Answers a Narrow Question

Practice or control	What it supports	What it cannot show
Technical reports	Document what was done during decryption or processing	Only the process described; depends on detail and availability
Documentation and traceability	Who handled the material, what was done, and when	Varies between cases; may not cover the international chain
Mirror tests	Received data matches data from seized devices	Only material that can be compared; not collection or selection
Checksums and hash sums	Specific files or data have not changed	Not completeness, correct interpretation or representativeness
Laboratory standards and accreditation	Quality control in some forensic lab settings	Much digital evidence handling occurs outside laboratories

Thesis Table 5.3. Digital forensics is less regulated than other forensic disciplines, and much of the handling happens outside laboratories (P3); documentation varies from case to case (P1, J1).

Practical Limits to Verification

Police handling of digital material is poorly regulated and varies between practices (P1, P3); digital forensics is less regulated than other forensic disciplines

ISO-accredited laboratories exist abroad, but much of the handling of digital traces happens outside any laboratory (P3)

Verifiability depends on what was secured early: teledata that is not retained cannot be recreated (P2); documentation varies from case to case (P1, J1)

Information about which tools were used can be inconsistent or contradictory (D1); it is easily assumed that the material had more quality control than it did (J1)

Much of what is known about these processes surfaced only through legal disputes (A2); confidence in foreign handling often rests on trust and varies by jurisdiction (L1)

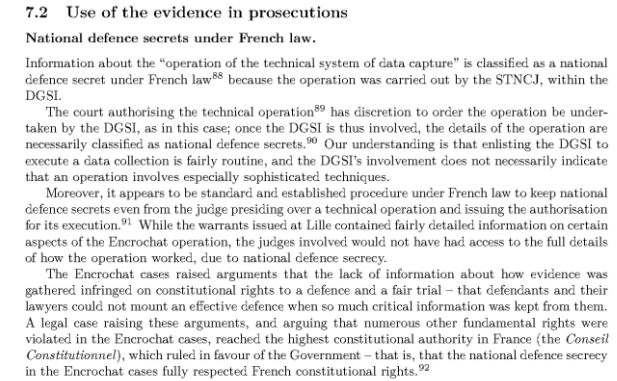
The Foreign Part of the Chain

"We have no insight into what happens before the material reaches the Norwegian police" (D1) — the complaint that opened the 2023 trial

France: the operation was run by an intelligence service — a national defense secret, withheld even from the authorizing judge; upheld by the constitutional council in 2022

UK courts asked whether data was taken in transit or at rest; France declined to answer, and both sides argued from expert guesswork; transfer questions reached the CJEU

Borgarting: French personnel could not be questioned; answers relayed from unnamed Europol colleagues weighed less



7.2 Use of the evidence in prosecutions

National defence secrets under French law.

Information about the "operation of the technical system of data capture" is classified as a national defence secret under French law[88] because the operation was carried out by the STNCJ, within the DGSI.

The court authorising the technical operation[89] has discretion to order the operation be undertaken by the DGSI, as in this case; once the DGSI is thus involved, the details of the operation are necessarily classified as national defence secrets.[90] Our understanding is that enlisting the DGSI to execute a data collection is fairly routine, and the DGSI's involvement does not necessarily indicate that an operation involves especially sophisticated techniques.

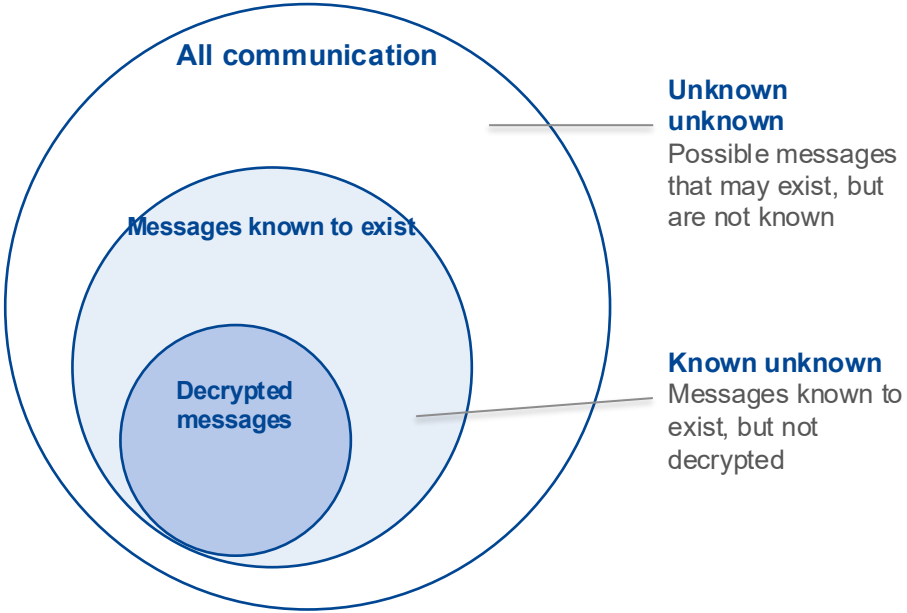
Moreover, it appears to be standard and established procedure under French law to keep national defence secrets even from the judge presiding over a technical operation and issuing the authorisation for its execution.[91] While the warrants issued at Lille contained fairly detailed information on certain aspects of the Encrochat operation, the judges involved would not have had access to the full details of how the operation worked, due to national defence secrecy.

The Encrochat cases raised arguments that the lack of information about how evidence was gathered infringed on constitutional rights to a defence and a fair trial – that defendants and their lawyers could not mount an effective defence when so much critical information was kept from them. A legal case raising these arguments, and arguing that numerous other fundamental rights were violated in the Encrochat cases, reached the highest constitutional authority in France (the *Conseil Constitutionnel*), which ruled in favour of the Government – that is, that the national defence secrecy in the Encrochat cases fully respected French constitutional rights.[92]

The EncroChat paper, §7.2 "National defense secrets under French law" (CRYPTO 2026)

Institutional trust fills the gap: cooperation inside the ECHR area is easier to trust (L1).

Theme C — Known and Unknown Unknowns



Based on thesis Figure 4.5

- P2's distinction: messages known to exist but not readable, and messages nobody knows are missing
- One-way dialogues with missing replies; the Court of Appeal: use with caution when only one side is visible — messages may not have arrived, been read, or been recalled
- The defense made the same point on day one in 2023: many messages missing, threads one-way, meaning a matter of interpretation
- A statement to the court about completeness that later proved wrong when new datasets arrived from abroad (D1)

Six Ways the Material Needs Interpreting

Interpretive issue	Example from the material	Potential evidential risk
User identification	A device, account or key cannot automatically be linked to one person; phones are swapped in some milieus	Wrong attribution of actions
Language and slang	“10 yay” needs context to mean 10 kg of cocaine; “har 40, har nettopp solgt 60” may be a sales pitch or boasting	Misinterpretation of content
Metadata	Timestamps may not reflect local time	Incorrect reconstruction of sequence or timing
System- vs user-generated data	System activity mistaken for deliberate user action	False inference about conduct
Fragmented communication	One-way communication, missing replies	Incomplete understanding of meaning
Technically correct but misleading	“BankID is approved at the highest security level” — true, yet supports less than it seems	Overstated evidential value

Thesis Table 4.1. The Borgarting court tied persons to Sky ECC IDs from message content, travel routes, teledata, pictures, addresses and continuity over time — a separate assessment, not a technical inference.

The “Gold Mine” Problem

Digital evidence looks precise, stable and machine-generated — so it can seem more objective than it is.

Judges are trained in law, not technology; next to witnesses who forget, disagree or lie, data looks like a gold mine.

— after P3 and J1

Sources of error

- Hypothesis blindness — police reports that later reversed who controlled a device (D1)
- Tool presentation that steers attention through sequencing and visual emphasis (P3)
- Misleading terminology: “signing” is not signing (A1)
- The Danish telecom-data scandal: more than 10,000 cases reviewed (J1)
- AI-assisted selection adds a new layer of uncertainty (D1)

Theme D — Everyone Depends on Experts

- Legal actors have limited technical competence — and, as A3 stresses, it is not their job to have it (L1: absent from legal education)
- Courts rarely bring in independent experts on data questions (J1); the police's own data investigators usually present the material (P3, D1)
- The threshold for appearing as an expert is low — room for self-declared experts and pseudoscience (P3)

Type of expert use	Positive function	Risk or control problem
Police- or prosecution-linked experts	Direct knowledge of how the material was handled and presented	Uneven landscape if one side has more technical information
Defense-appointed experts	Challenge interpretations, identify weaknesses, alternative explanations	Part of the parties' contest; is the expert independent?
Independent experts	A more neutral technical explanation	Rarely used on data questions; no clear routine for when to call them
Expert explanations in general	Translate technical processes for judges and lawyers	The court depends on the explanation it must evaluate critically

Two Defense Strategies

Challenge the material in principle

- No insight into the chain before the material reaches Norway; the prosecutor is silent about it (D1; Dietrichson, 2023)
- Electronic evidence is especially vulnerable to change when the chain is long
- Using it to convict would violate ECHR Article 6; “better that more guilty go free than accepting rules that shake the control mechanisms of a state under the rule of law” (Bratlien, 2023)

Work inside the material

- Invalidating this material “would totally undermine the legal culture and pretty much society itself” — it will not happen (D2)
- When the messages are incriminating, the fight moves to identification: does this ID, this phone, belong to this person?
- Look for what confirms and what excludes the link; cooperate with the court rather than stay silent — it can cut a sentence by years (D2)

Thesis sections 4.3.2, 4.4.3 and 6.3; Advokatbladet, September 20, 2023

What Protects the Process — And When

- Contradiction and a well-prepared defense: the evidence was “twisted and turned quite thoroughly” (P2) — as it should be (J2)
- Judges' control questions and a checklist under development; reviewing the police's internal quality assurance (J1)
- New searches with the police present (D2); the overall assessment against everything else in the case (D1, J1, J2)

Most safeguards act after filtering and selection have already shaped what is visible (after thesis Figure 5.2)

The Central Dilemma

The same steps that make the material manageable also determine what becomes visible and challengeable.

The material can be very strong without being self-explanatory. Evaluation has four layers — and technically correct decryption is only one of them.

Reliability
technically usable, documented, complete?

Credibility
meaning anchored in context?

User identification
digital user → physical person?

Fairness
uncertainty visible enough to challenge?

Thesis Table 5.2 and §5.7.1

Practical Implications by Actor

Actor	What needs to be in place	Concrete practical steps
Police and prosecution	The process from dataset to case material must be visible enough for others to understand how the evidence was shaped	Document search terms, filtering criteria, selection decisions, control points, missing material; say what was checked, not checked, excluded
Defense lawyers	A practical possibility to challenge the material, not only formal access to excerpts	Access in usable formats; new searches and supplementary material; technical support to understand the dataset
Courts and judges	Assess technical evidence without assuming it is complete, neutral or self-explanatory	Control questions on search, selection, documentation, identification, missing material; assess with other evidence
Technical experts	Explanations that convey both the findings and their limits	State methods, assumptions, uncertainty, scope; say what the material cannot show
Institutional level	Clearer routines across actors and stages	Shared guidance on documentation, access, search logs, selection records, verification, expert use

Thesis Table 5.5

NTNU | Norwegian University of Science and Technology

PART 4

Path Forward

From evidence to identity: the new project on digital identity wallets

Future Challenges: Digital Evidence and AI

1

Scale becomes the norm

Every takedown (EncroChat, Sky ECC, ANOM, Exclu, Ghost, MATRIX) yields datasets nobody can read in full; documenting the selection becomes the evidence question

2

AI in the loop

AI-assisted search, filtering, translation of slang, and chat summaries: a defense lawyer already flags uncertainty about the output — who audits the technical work?

3

Synthetic media

Deepfakes and generated messages: a checksum proves a file is unchanged, not that it is genuine

4

Attribution at scale

Identity wallets and BankID move “who is who” from investigative reconstruction to cryptographic credentials — but a key is still not a person

5

Long-lived evidence

Signatures and hashes must stay verifiable for decades while algorithms are retired; agility and re-signing become evidentiary questions

6

Lawful-access pressure

“Only criminals use this” arguments — privacy features as suspicion — put ordinary privacy technologies at risk

From Evidence to Identity

Real privacy

what the cryptography delivers

- Unlinkability, selective disclosure, minimal data sharing — properties a protocol has or lacks
- Today's EUDI Wallet architecture does not deliver the unlinkability the regulation requires

Expected privacy

what users and the law are promised

- Citizens will expect a wallet to reveal only what is needed — the law says so
- The gap between promise and delivery is where trust is won or lost

Perceived privacy

what people believe, and how they act on it

- Mental models diverge from technical assumptions — honest users make honest mistakes
- Trust, risk perception and security culture form through the technology, not before it

Why it matters for society

Critical infrastructure everyone will depend on

Sovereignty: less dependence on foreign platforms

Fairness: usable for all groups, not only experts

Accountability: a key is still not a person

The New Project: Digital Identity Wallets

- NTNU internal call “A more resilient society”; award letter September 16, 2026.
- Four four-year PhD positions, one per department, 2027–2031 (≈15 MNOK)
- Goal: secure, privacy-preserving, and democratically aligned digital identity wallets for Norway

Three knowledge needs

KN1
Robust and usable privacy-enhancing technologies

KN2
Societal practices and consequences of wallets in Norway and Europe

KN3
Provably secure, deployable, quantum-safe wallet designs

Four PhDs, Four Departments, One Project

PhD 1
IMF

Quantum-safe verifiable credentials

PhD 2
IIK

Privacy technologies and system analysis of digital wallets

PhD 3
IDI

Digital infrastructure in the public sector

PhD 4
ISS

Security culture, trust and society

Thanks! Questions?

tjerand.silde@ntnu.no
tjerandsilde.no

ntnu.edu/iik/cryptosocial