Isha v Norway **(app. no 7905/25);** *Emmen v Norway* **(app. no 9417/25)**

Joint observations of the European Criminal Bar Association & Fair Trials

1. The European Criminal Bar Association ('**ECBA**') and Fair Trials Europe ('**Fair Trials**') (together, the '**Interveners**') seek to assist the Court in two parts.

2. The first part deals with the procedural significance, under Article 6 § 1, of the technical differences between EncroChat and Sky ECC, as well as addressing questions (b) to (e) and (h) from a forensic perspective. The second part addresses the counterbalancing safeguards required where the defence does not have access to the underlying data or to the full cross-border forensic chain.

3. The Interveners adopt, without repeating here, previous comments on the lawfulness of the originating measures, mutual trust or the evidential onus placed on the defence, on which the Interveners have already commented.[1]

4. The perspectives and arguments herein are representative of those consistently emerging from discussions and activities over several years within the collective legal community of the ECBA, Fair Trials, and the Legal Experts Advisory Panel ('**LEAP**') on EncroChat, Sky ECC and cross-border evidence sharing.

PART 1 – THE FORENSIC PERSPECTIVE

5. This part treats together two issues which cannot be separated in practice. The investigative pathway – EncroChat or Sky ECC – determines which errors can occur and which technical records exist. Access to those different records, in turn, determines whether the defence can test the evidence relied on at trial.

Two pathways, two error profiles

6. The EncroChat and Sky ECC operations used two different methods of collection, each with its own sources of error. In the EncroChat operation, the French authorities placed an implant on the handsets, distributed as an apparent update. On the account accepted by the Court of Appeal of England and Wales, a first stage copied the data still held in the handset's message database, typically some seven days of communications, and was repeated several times on each device; a second stage copied new messages from the working memory of the sending device.[2] What reaches the trial court is thus a copy of what a particular handset held at a particular moment. A message erased by its user or

by a self-destruct timer before collection, or composed on a handset that was not (or no longer) infected, may be absent from the record; another may survive only in the data taken from the counterpart's handset. Reverse engineering of an infected handset, reported in August 2026, indicates that implants frequently failed and had to be reinstalled, and that a coding error inverted the direction of call records, 'to' effectively meaning 'from'. A French official reportedly declined to explain that error, invoking national defence secrecy.[3]

7. Sky ECC data were obtained at the level of the service's servers in France. Encrypted traffic was captured from 2019; a capability to decrypt it was developed only in late 2020 and was then applied retrospectively to the stored traffic, alongside a short period of live interception in early 2021.[4] Here the record is the output of a decryption process applied to captured traffic. Its completeness depends on whether capture was continuous and whether the key material needed for each message was available; its attribution depends on each decrypted message being assigned to the right sender and recipient. In a report of 22 June 2022, considered by the Court of Appeal of Basel-Stadt, the Netherlands Forensic Institute found that data processed with the police 'Toolbox' method were not entirely complete when compared with examined handsets, and that 73.7 per cent of messages had been successfully decrypted.[5]

What the pathway means for Article 6

8. Three consequences follow. First, 'authenticity' and 'integrity' (question (b)) mean different things on each pathway. For EncroChat, the question is whether the record faithfully reproduces what the handset held when collected, and whether the handset has been correctly identified; for Sky ECC, whether the decrypted text corresponds to the captured traffic and has been attributed to the right sender and recipient. The records that answer these questions differ accordingly: implant and collection logs and device identifiers in the first case, capture logs, decryption logs and failure rates in the second.

9. Secondly, gaps are not evidentially neutral. A message may be missing because it was never sent, because it was erased before collection, because capture or

decryption failed, or because it was dropped during selection or processing. Each explanation bears differently on the meaning of the surrounding messages and on the possibility that a gap conceals exculpatory content. A court which bridges gaps by reference to the 'overall context' draws its inference from the very material whose completeness is in issue. Only the technical pathway records can show which explanation applies.

10. Thirdly, validating a method does not verify a dataset. Reports on the general reliability of a collection or decryption method, and comparisons with handsets seized from other persons, show that the method can produce accurate results. They cannot show that a particular dataset is complete, unaltered and correctly attributed. Confirmation obtained through live monitoring in one operation, or in one period, says nothing about data produced by retrospective decryption in another. The Grand Chamber has held that the fact that the data concerning an applicant tallied with another dataset verified by an expert 'did not necessarily remove the applicant's procedural rights with respect to that original data'.[6]

11. The pathway also determines how much of the chain lies within the trial State's control. If it received data directly and in near real time (as with EncroChat data), receipt, storage and processing are domestic acts which should be documented; foreign secrecy cannot shield those records. If it received a single delivery of data already decrypted abroad (as with Sky ECC data), that delivery is the earliest point within national reach. It must be preserved as received, and the trial State must obtain from the originating State the information needed to explain it. In *Yalçınkaya* the Court found fault with domestic courts which 'did not address the matter of how the integrity of the data obtained from the server had been ensured'.[7] The less of the chain the trial State controls, the more demanding the counterbalancing required (question (d)).

The minimum forensic record

12. Electronic evidence is 'inherently more prone to destruction, damage, alteration or manipulation'.[8] Forensic practice responds with two basic rules, set out in the Council of Europe's Electronic Evidence Guide: no action should materially

change data which may later be relied upon in court, and a record of every action taken should be kept so that an independent third party can repeat those actions and achieve the same result.[9] These rules are preconditions of verifiability. Where they were not observed, or their observance is not documented, neither the defence nor the court can establish that what is presented at trial is what was collected; and where material has not been preserved, the defence cannot verify its own assumptions as to the relevance of that material.[10]

13. In the Interveners' submission, where such data are relied upon, Article 6 §§ 1 and 3(b) require that the defence have access at least to:
    a. the raw data in the form in which they reached the trial State, as a bit-for-bit copy in native format rather than a spreadsheet or PDF generated from them, together with the hash values computed on receipt;
    b. a chain-of-custody record for every transfer and processing step, stating who acted, when, with which tool and version, with input / output hash values, and including parsing, merging and de-duplication, time-zone conversion, translation and the criteria by which the national subset was selected;
    c. the integrity-verification record: verification logs for each stage and documentation of known anomalies, including periods in which collection or decryption failed wholly or partly, and measures taken to remedy them;
    d. the complete communications and metadata of the account attributed to the accused and, as explained below, of the accounts of its counterparts;
    e. access to these items should not depend on a prior showing of irregularity by the defence, for the reasons given in the Interveners' earlier submissions.

Communications and metadata of counterparts

14. Data relating to counterparts belong to the evidential picture. Messages of other users naming, describing or addressing the account holder are used to attribute an account to the accused and to establish what was said. On the EncroChat pathway, a message may survive only in the record of the handset on which it was composed. Such data form part of the prosecution case or, at least, of the material in the possession of the authorities 'with potential relevance' to the

defence.[11] The defence must be able to establish whether a message missing from the accused's record exists in the counterpart's, and whether other contacts of the same account referred to its user in circumstances inconsistent with the attribution relied upon. The Court has recognised the importance of the defence having an opportunity to be involved in defining the criteria by which potentially relevant material is identified within a larger dataset.[12] The privacy of third parties can be protected by confidentiality orders or controlled access; it cannot justify withholding material on which the prosecution itself relies.

15. The same applies to metadata. Device identifiers, timestamps, network data and location information are needed to test attribution and chronology, and may be exculpatory where they place a device somewhere the accused was not. They also show where a device was when it was intercepted, and therefore which legal regime governed the interception. Within the European Union, notification under Article 31 of Directive 2014/41/EU is owed to the Member State 'on whose territory the subject of the interception is located';[13] for Norway, a corresponding duty arises under Article 20 of the 2000 EU Mutual Assistance Convention.[14] Without location metadata, neither the defence nor the court can know whether that regime was engaged, let alone whether it was respected.

Testing the record: witnesses and experts

16. Records do not answer every question. Officers and technicians whose reports on the receipt, processing and analysis of the data are relied upon are witnesses against the accused within the autonomous meaning of Article 6 § 3(d).[15] Questioning them is often the only way to establish whether collection collapsed wholly or partly at any point, how that was dealt with, and which steps were taken without being recorded. In a recent German Sky ECC trial, officers testified that data received through Europol had been merged and de-duplicated with unidentified tools, and machine-translated and pre-selected for relevance before an interpreter saw them; that columns of the transmitted files could not be explained and had been disregarded; that identifiers had been left out of evidential tables for the sake of clarity; and that country codes were missing for

data dated before 23 March 2020. A witness who had worked on the data at Europol declined, for want of authorisation, to say in which formats they had been held.[16] Requests to examine such witnesses fall to be assessed under the *Murtazaliyeva* criteria,[17] and restrictions placed by foreign or EU bodies on what officials may say must be examined by the trial court and counterbalanced.

17. Equality of arms extends to expert evidence. Where the only forensic assessment comes from a body linked to the trial State authorities, refusing the defence an alternative expert opinion may breach Article 6 § 1.[18] Where nothing in the file shows that the data were ever examined to verify their integrity, the accused has 'a legitimate interest in seeking their examination by independent experts'; the courts must respond to that concern.[19] A defence expert can do nothing without the raw data and the chain-of-custody records, nor are those useful without an expert: these are two sides of one guarantee.

PART 2 – COUNTERBALANCING SAFEGUARDS

18. The Interveners now address the safeguards required where the defence has access neither to the underlying data nor to the chain by which decrypted communications become evidential packages for use at trial or where the originating State keeps parts of the above-mentioned process confidential.

19. The specific features of electronic evidence do not 'in the abstract call for the safeguards under Article 6 § 1 to be applied differently'.[20] As such, the prosecution is to disclose all material evidence in its possession for or against the accused,[21] irrespective of reports derived therefrom.[22] The question is whether the safeguards secured the overall fairness of the proceedings.[23]

20. The Court has distinguished a mass of data whose content the prosecution itself did not know, which raises no issue of non-disclosure 'in the classic sense', from data selected by the prosecution alone, without the involvement of the defence or judicial supervision.[24] This distinction calls for particular care where the material transmitted by the originating State has already been selected from a larger dataset. The trial State may not possess the larger collection, yet the

material used at trial may already reflect a prior selection exercise. The trial State cannot therefore bring the case within the first situation merely because the selection was made abroad (see §11 above). Equal access to the extracts does not answer whether potentially exculpatory material has been excluded. The Belgian Court of Cassation has held that the accused is entitled to know the selection criteria relevant to their identification and alleged criminal involvement.[25] The issue is whether the defence can challenge that selection.[26]

21. Restrictions on disclosure are permissible only if strictly necessary, and the difficulties they cause to the defence must be sufficiently counterbalanced by the procedures followed by the judicial authorities, regard being had to the importance of the undisclosed material.[27] What is required is not an invariable right to the entire raw collection, but an effective opportunity to test evidential selection and context, through safeguards responding to the disadvantage actually sustained (see § 12-17 above).[28] Analytically, these may be grouped into those concerning defence access and those concerning judicial scrutiny.[29]

Defence access

22. First, the defence must be able to understand contest the grounds on which, and by whose decision, material is withheld.[30] Second, the participation of the defence in defining the criteria for identifying relevant material is an important safeguard, and the refusal of further technically feasible searches of material already selected may raise an issue under Article 6 § 3 (b) (see § 14 above).[31] Third, the defence should have a genuine opportunity to comment on the full extent of the decrypted material concerning the accused.[32] Illustratively, the Noord-Holland District Court, Netherlands, ordered that the defence should have access to Hansken, the national police tool for access to and searching the underlying electronic material held in the Netherlands, observing that this had become current practice in other cases[33] (see §§ 13(d), 14 and 15 above). Fourth, where material is held by the originating State, the domestic court should consider a targeted request, and give reasons if it declines to make one (see §§ 7 / 14 above). The practical significance of access to the wider dataset is

illustrated by the Court of Appeal of Basel-Stadt. In a Sky ECC case, it found that access limited to selected chats prevented the defence from checking the selection made at source or whether other conversations involving the account's correspondents contained potentially exculpatory material. The court regarded that restriction as a further ground for excluding the chats under Swiss law.[34]

23. Access to the minimum forensic record should not depend on a prior showing of irregularity by the defence (see § 13(e) above). As a relevant example, see the practice of the Dutch courts which routinely allow the defence access to the complete Dutch-held dataset (communications, metadata and traffic data – roughly what is referred at § 13(d)) (but not the French-held raw data) without any requirement for the defence to raise any particular reasons (cf. §13(e)).[35]

Judicial scrutiny

24. The trial court's own examination becomes a counterbalancing safeguard where access cannot be given or when certain parts of the process are kept confidential. There is an onus on the court to subject those issues to 'the most searching scrutiny'.[36] Confirmation that the data were lawfully collected does not answer how their integrity was ensured,[37] nor, in the Interveners' submission, a substantiated objection that the communications presented at trial omit context relevant to their interpretation (see §§ 8-9 above). The defence is entitled to a specific and explicit reply to the arguments decisive for the outcome,[38] which a court does not give where it leaves unanswered a specific and pertinent objection to the completeness, coherence or attribution of decisive evidence.[39] The Interveners emphasise that the less of the evidential process the trial State can scrutinise, the more counterbalancing safeguards it must ensure (see § 11).

25. That scrutiny is not provided by reliance on trust in the originating State. By analogy, the Court has examined whether the safeguards offset the prejudice to the defence, despite assumption of good faith.[40] Nor is it provided by corroboration alone, which does not remove the defence's procedural rights in respect of the contested data,[41] or by inference from the messages that remain, gaps not being evidentially neutral (see §§ 8-9 above). Where the defence

cannot test the prosecution's inferences against material beyond the selected extracts, the court must support them with sufficient and pertinent reasoning.[42]

26. The greater the weight attached to that evidence, the greater the need to explain how the restriction was counterbalanced. If a handicap is not counterbalanced, the consequence is not automatic, and reliance on reports without direct examination of the raw data does not alone render proceedings unfair.[43] Rather, it follows from the assessment of overall trial fairness, in which the weight of the evidence and the (in)sufficiency of the measures are decisive.[44] The Interveners submit that, where no adequate measure is adopted and the evidence is decisive, the evidence must be disregarded to avoid breach of Article 6.

27. Of course, domestic law may require reasons for a disclosure request, and courts may examine their validity.[45] But the expectation must be realistic. Where this Court held the lack of specificity against applicants, the defence had obtained searches on parameters of its own choosing, a full readable copy of the files and the accused's own knowledge of the communications,[46] or overviews of the seized items and an unused judicial remedy.[47] Even then, it was not required to explain its strategy.[48] Conversely, where inadequate disclosure had prevented the applicant from making a specific argument about the relevance of undisclosed material, that lack of specificity could not be held against him.[49] A recent Italian judgment illustrates this further. In proceedings concerning Sky ECC evidence obtained from France, the Court of Cassation held that defence requests for additional documentation were not merely exploratory, particularly where counsel had demonstrated unsuccessful attempts to obtain from the French authorities the documents necessary to assess and prepare measures to safeguard fundamental rights.[50]

28. The Court has treated as material data that 'potentially contained elements' enabling the accused to exonerate himself or to challenge the admissibility, reliability, completeness or evidential value of the evidence,[51] and has measured the required specification by whether the defence pointed to a 'specific issue' which further searches could clarify.[52] The Interveners submit that a request

identifying relevant categories of material and the issue they may clarify is sufficiently reasoned. Examples include the other communications of an attributed account and of its counterparts, or the selection criteria (see §§ 13(b), 13(d) and 14 above). Such requests differ from an unrestricted "fishing expedition", for they identify a line of enquiry without presuming knowledge of its result.[53] What is more, where the originating State maintains that parts of its process must remain confidential, the measures relied upon to counterbalance the resulting handicap must match the pathway and the gap they are meant to fill. Such measures include access to the raw data and logs by a defence expert under confidentiality undertakings; appointment of a court-appointed expert with full access, with the defence allowed participation in the definition of the terms of reference and cross-examination; evidence from the foreign technicians, in writing or by video link and subject to cross-examination, and judicial scrutiny of the secrecy claim itself. The reported reconstruction of the EncroChat implant from open-source components shows claims of secrecy may reach further than the interest they protect (see § 6). The Interveners submit that if no adequate measure is available and the evidence is decisive the only course consistent with Article 6 is to disregard it.[54]

Rapporteurs (in alphabetical order by surname)

- **Cristiana Bianco**, ECBA Human Rights Committee, LEAP Member
- **Federico Cappelletti**, ECBA Human Rights Committee
- **Paul Vlad Ciocotisan**, ECBA member
- **Lorenzo Farneti**, ECBA intern member
- **Aleksandra Horvat**, ECBA Human Rights Committee
- **Gwen Jansen-de Wolf**, ECBA Vice-Chair
- **Christian Lödden**, LL.M., LEAP member
- **Anna Rothwell**, ECBA member
- **Alex Tinsley**, Fair Trials; LEAP member; ECBA Human Rights Committee

REFERENCES

[1] Fair Trials, written comments in *Silgir v Germany (No. 2)* 22234/25 (https://www.fairtrials.org/app/uploads/2026/04/Fair-Trials-Silgir-No-2-amicus-FINALwebsite.pdf) §§ 22-27 and 36-50; joint written observations of the ECBA and Fair Trials in *Raal and Reudolph v Estonia* 14711/25 and 14712/25 (https://www.fairtrials.org/app/uploads/2026/08/Gert-Raal-Margus-Reudolph-v.-Estonia-Joint-Written-Intervention-FT-ECBA-.pdf), §§ 6-7, 16-24 and 28-30.

[2] *R v A, B, D and C* [2021] EWCA Crim 128 (https://www.bailii.org/ew/cases/EWCA/Crim/2021/128.html) §§ 12 and 14 (citing §§ 148-149 of the trial ruling); see also *A.L. and E.J. v France* (dec.) 44715/20 and 47930/21 (2024), §§ 4-34.

[3] D. Campbell and B. Goodwin, 'Revealed: Cyber spies used malware from GitHub to hack EncroChat cryptophone network', *Computer Weekly*, 17 August 2026 (analysis by Invasys of an infected handset; the implant used the open-source toolkit Frida and the Android vulnerability CVE-2019-2215) (available at https://www.computerweekly.com/news/366649396/Revealed-Cyber-spies-used-malware-from-GitHub-to-hack-EncroChat-cryptophone-network).

[4] The Court's statement of the subject matter of the case; Fair Trials, *Silgir (No. 2)*, § 6.

[5] Appellationsgericht Basel-Stadt, judgment of 3 October 2025, [case no. SB.2023.48] (https://94c729d2-2086-4ed5-85ea-a1b2171133a1.usrfiles.com/ugd/69f7d7_2925c1946073430bac384c33573004af.pdf) reasons pp. 18-19, referring to the NFI report of 22 June 2022, pp. 20 and 24.

[6] *Yüksel Yalçınkaya v Türkiye* [GC] 15669/20 (2023), § 328.

[7] Ibid., § 334.

[8] Ibid., § 312.

[9] Council of Europe, *Electronic Evidence Guide*, version 3.0 (2022), Principles 1 (data integrity) and 2 (audit trail); see also ISO/IEC 27037:2012 on the identification, collection, acquisition and preservation of digital evidence.

[10] *Natunen v Finland* 21022/04 (2009), § 47.

[11] *Yalçınkaya*, §§ 307 and 327.

[12] *Sigurður Einarsson and Others v Iceland* 39757/15 (2019), §§ 89-90.

[13] CJEU, C-670/22 *M.N. (EncroChat)* [GC], EU:C:2024:372, §§ 114 and 119.

[14] This applies to Norway by virtue of the Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the application of certain provisions of the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and the 2001 Protocol thereto, OJ L 26, 29.1.2004, p. 3, Article 1(1); in force since 1 January 2013.

[15] *Butkevich v Russia* 5865/07 (2018), § 98.

[16] Landgericht Berlin, judgment of 12 September 2025, [case no. 532 Ks 3/25], a constitutional complaint is pending (BVerfG 2mBvR 1307/26). Further details can be supplied to the Court.

[17] *Murtazaliyeva v Russia* [GC] 36658/05 (2018), § 158.

[18] *Bönisch v Austria* 8658/79 (1985), §§ 32-34; *Stoimenov v the former Yugoslav Republic of Macedonia* 17995/02 (2007), §§ 38-42.

[19] *Yalçınkaya*, § 333.

[20] Ibid., §§312-313.

[21] *Rook v Germany* 1586/15 (2019), §58; *Yalçınkaya*, §307.

[22] *Yalçınkaya*, §327.

[23] Ibid., §313.

[24] *Sigurður Einarsson* §§90-91, citing *Rowe and Davis v the United Kingdom* [GC] 28901/95 (2000), §63.

[25] Court of Cassation, 18 June 2024, ECLI:BE:CASS:2024:ARR.20240618.2N.25 (https://juportal.be/content/ECLI:BE:CASS:2024:ARR.20240618.2N.25/NL?HiLi=eNpLtDK2qs60MrAutjI0tFIq0DMy0TMwMjHQy1OyzrQyhAoHwIX9QMJGGMJA1bUAuGwR4g==) §§16-17.

[26] Compare Matanović v Croatia 2742/12 (2017), §§182–186.

[27] *Rook*, §59; *Yalçınkaya*, §308.

[28] Ibid., §330.

[29] Ibid., §§330–337.

[30] Ibid, §331, citing *Matanović*, §183.

[31] *Sigurður Einarsson*, §§90–91.

[32] *Yalçınkaya*, §335.

[33] Rechtbank Noord-Holland, 21 April 2022, ECLI:NL:RBNHO:2022:3650 (https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBNHO:2022:3650). Notably, the facility was originally possible for EncroChat and some other platforms but not Sky ECC data. It was promised in 2023 that it would be extended to Sky ECC (see Nederlands Forensisch Instituut, 20 March 2023 https://www.forensischinstituut.nl/nieuws/nfi-maakt-inzage-cryptocommunicatie-op-werkplek-advocaten-mogelijk). To the best of the Interveners' collective knowledge, it still has not happened, and derived Excel sheets have continued to be accepted in Sky ECC cases.

[34] 3 October 2025, SB.2023.48, section III.5.2.

[35] Rechtbank Amsterdam, 16 October 2025 ECLI:NL:RBAMS:2025:7675 (https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2025:7675).

[36] *Yalçınkaya*, §334.

[37] Ibid., §334; see also §310.

[38] *Yalçınkaya*, §305.

[39] Compare ibid., §§334, 341

[40] Compare *Yalçınkaya*, §§317, 330–337.

[41] Ibid., §328.

[42] *Yalçınkaya*, §337.

[43] Ibid §332.

[44] Ibid., §§310, 330, 345.

[45] *Rook*, §59; *Yalçınkaya*, §308.

[46] *Rook*, §§68, 70, 72.

[47] *Sigurður Einarsson*, §92.

[48] *Rook*, §§65, 70.

[49] *Matanović*, §§179, 186.

[50] Corte di cassazione, Sixth Criminal Division, judgment no. 27520/2026, § 1.1.

[51] *Yalçınkaya*, §328.

[52] *Sigurður Einarsson*, §90.

[53] Compare *Sigurður Einarsson*, §90.

[54] Compare, in EU law, Article 14(7) of Directive 2014/41/EU as interpreted in M.N., §§ 130-131.