Gert Raal & Margus Reudolph v. Estonia

App. Nos. 14711/25 and 14712/25

Joint Written Observations by the European Criminal Bar Association (ECBA) and Fair Trials intervening as third parties

1. The European Criminal Bar Association ('**ECBA**') and Fair Trials Europe (**Fair Trials**) (collectively, the '**Interveners**') seek to assist the Court in dealing with a recurrent factual matrix whereby one state imports decrypted communications obtained by another state and uses them in a criminal trial. The Court's approach to Article 6 and 8 in such cases may have implications in many future cases.

2. Further to earlier related interventions,[1] the Interveners will comment on these matters: (i) practitioner insights on ANOM cases; (ii) broader context on surveillance, evolving international legal frameworks and associated risks; (iii) the approach to Article 8 when evidence is imported via mutual assistance; (iii) the role of Article 6 in criminal proceedings involving such imported evidence.

3. These written comments address issues of general principle and not the facts or merits of the two individual applications. Any discussion of background facts refers to the much broader issue of the use of ANOM as a general topic only.

A. Practitioner insights

4. The ECBA and Fair Trials have had extensive discussions about ANOM scenarios and similar prosecutions in their networks (the ECBA's membership and the Legal Experts Advisory Panel ('**LEAP**') coordinated by Fair Trials). The observations below draw upon that expertise and seek to assist the Court with the realities encountered by practitioners, across Europe, on these issues.

5. In the experience of practitioners across the Contracting States, the defining characteristic of these cases is that the material placed before the domestic court is not raw evidence but a finished evidential product, generated by a foreign investigative authority and transmitted between States. The defence receives a curated set of decrypted communications, but not the underlying data, nor an account of the method by which the product was extracted and assembled, nor any means of establishing surrounding context or whether it is complete,

unaltered and correctly attributed to the accused. The processes that produced the evidence are, as a rule, shielded by claims of investigative secrecy or state security invoked by an authority beyond the domestic court's jurisdiction.

6. This gives rise to a structural inequality of arms that no measure of diligence on the part of the defence can cure. The prosecution proceeds with the benefit of the resources and techniques of international cooperation, while the defence is denied the very instruments — access to the source material and to the manner of its generation — required to subject decisive evidence to searching scrutiny. Compounding this, the prosecution frequently determines alone, from its own vantage point, which communications are relevant and disclosable, and which are withheld; the defence is excluded even from the prior exercise of defining the criteria by which incriminating and exculpatory material is identified. Practitioners are routinely required to demonstrate concrete indications of error or manipulation as an initial condition of any further disclosure, yet cannot identify such indications precisely because the material needed to do so is withheld. The result is a closed circle in which the defence is asked to prove the unreliability of evidence it has never been permitted to examine.

7. A second recurring feature compounds the first. Faced with material transmitted by a cooperating State, domestic courts tend, in reliance on mutual trust, to treat it as presumptively lawful in the manner it was obtained and presumptively reliable in technical terms. Where issues are raised by the defence, in practice, these are too often answered only by reference to the trust reposed in the transmitting authority. This, in turn, affects the sufficiency of reasoning that courts are able to provide for their decisions when such issues are raised.

8. Third, these cases are characterised by a situation whereby the judicial forum of the pre-trial detention decision-making or criminal charge determination is in no position to oversee the prosecutorial handling of what is disclosed and what is not. The court, like the defence, has no access to either the full technical process yielding the evidence supplied and/or the fuller body of evidence from which material has been selected in substantive terms. This produces a situation in which restrictions on access to relevant information and evidence rest entirely in the hands of prosecuting authorities, beyond judicial control.

B. The ANOM operation in broader international context

9. The Court is here dealing with one version a recurrent factual matrix in which communications are intercepted on a massive scale in one state, and a product drawn from that is then shared across borders, and a representational product is then relied upon downstream as the basis for coercive measures or at trial.

10. This includes the **EncroChat** operation (reviewed A.L. and E.J. v. France no. 44715/20 (Dec) (2024), §§4-34) and the **SkyECC** operation (at issue in Isha v Norway 7905/25 (communicated 6 May 2026)). These both involved investigative operations in one state (France) gaining access to the encrypted communications of entire user bases of these two systems with servers in France, on the premise that they were systems used for criminality. The content was then shared formally pursuant to European Investigation Orders or, for non-EU countries, mutual legal assistance. After initial litigation, it has become a practice for a bundle of basic French court orders to be supplied. However, trials continue to proceed on the basis of a presentational end product without the underlying raw data or the full information as to the forensic process followed.

11. The **ANOM** operation, at issue in this case, shares similar core features in so far as (i) the operation started from the premise of suspicion of the entire user base of the system; (ii) there was, on that basis, bulk collection, without prior individualised suspicion; (iii) states where the devices were used were then able to request (in bulk) the data relating to such uses via mutual legal assistance; and (iv) there are several stages of processing between the original data capture and the ultimate trial product. However, the ANOM scenario presents certain specificities which place it at the most acute end of the scale in terms of these issues, namely (a) the additional layer of cross-border process, in that the communications were accessed not by the US directly but by a third state (Lithuania) which was not even identified by the US documents; (b) the fact that the relevant judicial authorisations (in Lithuania) are not supplied with the data; (c) the combination of these, which increases the amount of procedural and technical information that is unknown to either the trial state's courts or the defence, increasing the strain upon principles of mutual trust. In relation to these

issues, the Court's attention is drawn to the June 2026 article of LEAP member Mr Christian Lödden[2] (the '**Lödden article**') which asserts, based on hitherto unseen evidence, that US and Lithuanian authorities materially misstated the factual position when seeking authorisations of the Lithuanian court.

12. The Interveners observe that there is a current international emphasis upon enabling further such operations, in the interest of combating cyber-enabled offending. Thus, in parallel to the then-emerging successes of the EncroChat, Sky ECC and ANOM / Operation Trojan Shield operations, States Parties of the United Nations ('**UN**') negotiated the UN Convention against Cybercrime ('**UNCC**') (agreed in October 2024, and signed from October 2025) which replicates at global level many of the provisions of the Council of Europe Treaty on Cybercrime (ETS 185). The UNCC requires states to possess a range of investigative powers (Chapter IV), e.g. empowering its authorities and ensuring they have the capability to search or access communication systems or to perform real-time traffic data collection or content interception. It then sets forth an MLA framework (Chapter V), which provides for exchange of evidence spontaneously or on request. Its human rights safeguards (Article 6) are broad and unspecific. The treaty has been met with great concern among civil society.[3] This highlights the important function to be played by case-law principles.

13. The Interveners also invite the Court to have regard to the international consensus on encryption. In Podchasov v Russia 33696/19 (2024), the Court, whilst accepting that '*encryption can also be used by criminals*' relied on UN content in observing that '*In the digital age, technical solutions for securing and protecting the privacy* […]*, including* […] *encryption, contribute to ensuring the enjoyment of other fundamental rights, such as freedom of expression* […] *Encryption, moreover, appears to help citizens and businesses to defend themselves against abuses of information technologies*' (§76). There is an echo of that dual reality in the observations of the Higher Court of the Canton of Zürich, when expressing its concerns about the hacking of all 177,000 users of Sky ECC that '*it is not only (potentially) criminals who are likely to be interested in devices with such high security standards, but also, for example, journalists, political activists, or employees of companies*'.[4] The Interveners

suggest that this duality must remain in sharp focus in the evaluation of any measures which target the entire user base of a system to investigate crime.

14. Finally, and without overstating the proximity of these issues to those at hand, the Interveners recall the numerous troubling revelations in recent years of abusive government-sponsored surveillance, e.g. targeting of activists and journalists through the NSO Group's Pegasus malware, or the surveillance of e.g. activists concerned with rescue in the mediterranean sea by Italian intelligence services using Graphite spyware.[5] This highlights the risk that intrusion capabilities for fighting crime may be used for illegitimate purposes.

15. The Interveners therefore invite the Court to resist any dilutions of fundamental principles in ANOM and similar cases, as these will form the backbone of safeguards against abuse in a fast-developing legal and technical landscape.

C. Observations on the role of Article 8

16. The Interveners contend that a Contracting State may only import and attach penal consequences to material obtained outside its jurisdiction if the original evidence gathering exercise was compatible with basic Convention values.

17. That principle has three related sources. First, it is uncontroversial that at the point of enforcing an act of another state within their territory, Contracting States are '*obliged to refuse their co-operation if it emerges that the conviction is the result of a flagrant denial of justice*' (Drozd & Janouzek v France & Spain (1992), §110). Second, that same principle translates into the area of qualified rights: the Court has indicated that restrictive (confiscation) measures at the point of execution of MLA cannot be presumed to be '*in the general interest*' for the purposes of the qualifications in Article 1(3) of the First Protocol if it would '*result from … proceedings which … may … consist of a flagrant denial of justice*' (Shorazova v Malta (2012), §112). Third, the principle equally applicable to the use of evidence obtained requested from a third state: most simply, evidence is subject to exclusion where it is established that there is a 'real risk' that it was obtained abroad incompatibly with Article 3 (El Haski v Belgium (2012), §§81-89). The common thread is that a Contracting State cannot indifferently take on and attach concrete internal coercive consequences to a process in a third state which conflicts with fundamental Convention values.

18. That principle necessarily presupposes a power in the trial state's court to assess, at a high level, whether the originating process fundamentally conflicted with Convention standards. Such a power is entirely appropriate and uncontroversial in a classic MLA context not subject to the specificities of EU law systems.

19. In this regard, the Interveners submit that the approach should, as in any international context, involve the familiar dynamic applying a core standard which avoids applying Convention standards to third states like for like. Such analysis would involve an assessment, at a high level, of whether the interception exercise was compatible with the principles in Roman Zakharov v Russia [GC] 47143/06 (2015), §§227-234/260, as summarised in Big Brother Watch.

20. As part of the lawfulness issue (Roman Zakharov §§228-231), the analysis would involve an assessment of whether the state carrying out the interception did so on a Convention-sufficient legal basis. Further, since the '*in accordance with the law*' test ultimately serves to protect against arbitrariness, the analysis would also extend matters such as those ventilated in the Lödden article, i.e. material misstatement of facts which call into question the core judicial orders.

21. The necessity in a democratic society aspect (Roman Zakharov §232) would include the issue whether the authorisations proceeded on the basis of '*reasonable suspicion*', which is part of this analysis (Zakharov §260). The Court has indeed stated that '*telephone tapping is a very serious interference with a person's rights and that only* ***very serious reasons*** *based on a* ***reasonable suspicion*** *that* ***the person*** *is involved in* ***serious criminal activity*** *should be taken as a basis for authorising it* (Iordachi & Others v Moldova (2009) §51). The authority allowing interception '*must be capable of verifying the existence of a* ***reasonable suspicion*** *against the person concerned, in particular, whether there are* ***factual indications for suspecting that person*** *of* […] ***criminal acts or other acts that may give rise to secret surveillance measures***' (Roman Zakharov §260). The Court distinguishes that from surveillance of a '***"general" or "exploratory"***' nature (originally Klass & Others v Germany (1978)). Notably, the Court's practical approach involves an assessment of the reasoning in prosecutorial requests and the judicial authorisations granted: see e.g. Adomaitis v Lithuania (2022) §§85-86 or Draksas v Lithuania (2012) §56.

22. The Interveners therefore contend that there must be a rational assessment by the importing trial state's court of whether the measures in the originating state(s) were ordered on a basis reasonably corresponding to the core Convention distinction between targeted investigation and a broad exploratory exercise. Any other approach would allow a Contracting State to import, via MLA, the fruit of widespread exploratory interceptions concerning people or activities on its own territory, which the above case-law would prohibit it from carrying out internally. In the Interveners' view, what requires assessment is the specifics of the judicial orders at the point of authorisation of the interception.

23. In the case of Operation Trojan Shield, the national court (and this Court) could legitimately have regard to features which have troubled national courts, e.g. the Swiss Federal Court's concern as to there being insufficient material to impute liability to 11,800 users merely by virtue of using a hardened encryption system.[6] The Interveners point out that the Court has itself looked askance at national approaches involving the imputation of criminal responsibility to individuals simply by virtue of their using an encrypted system, when applying the individualised liability requirements of Article 7 (Yüksel Yalçinkaya v Türkiye [GC] 25669/20 (2023)) which are transposable to the person-specific concept of reasonable suspicion. The analysis would have to have in mind the duality referred to above: citizens also use encryption legitimately. The analysis could also take account of FBI materials stating that from the 11,800 users in question there appear to have been some 800 arrests made around the world. It is unclear if the other 11,000 are just more elusive, or not all criminals after all.

24. Should a national court reach the conclusion that the originating exercise was carried out in breach of Article 8 – e.g. because there was some fundamental unlawfulness and/or because it was an impermissible mass exploratory exercise – it should give full effect to that finding: see the Article 6 section infra.

D. Article 6: procedural and remedial obligations

25. In Yalçinkaya, the Grand Chamber held that equality of arms principles applied, in full, to the context of electronic evidence. On the facts, it found that the fact of the applicant having access to a second-hand product (ByLock reports) did not mean the applicant had no right or interest in the underlying data (§327)

which was prejudiced by his '*inability to verify first-hand the integrity of the evidence in question*' (§330). The Yalçinkaya judgment then focuses on the response of national courts to defence complaints about this (e.g. §§331-334).

26. The Interveners' core point is that since a national court must grapple with the (i) the question of lawfulness of the evidence, and (ii) the question of its completeness, accuracy and reliability as evidence, these issues must be the subject of equality of arms. This equality of arms demands sufficient information as to the legal and technical '*origin story*' of the evidence, and availability of the raw material on which the second-hand product is based. In default, the defence are not able to comment effectively, undermining fairness.

27. In the Interveners' view, a national court accepting a downstream evidential product without ensuring due scrutiny of how it was arrived or its underlying basis also effectively allows a situation '*a procedure whereby the investigating authority itself* […] *attempts to assess what may or may not be relevant to the case*', which '*cannot comply with* […] *Article 6 § 1*' (Natunen v Finland 21022/04 (2009) §47). That situation is very far from that in in other cases where restrictions are '*under the assessment of the trial judge*' (ibid §48): the whole process is shrouded in opacity and lies entirely outside the court's scrutiny.

28. In that context, the Interveners submit that a court fails in its duty to give adequate reasons, or to ensure equality of arms, if it deals with all such issues by reference to mutual trust, which does not operate in the usual way here.

29. Typically, presumptions of trust are amenable to challenge by the defence based on evidence available in the public domain, objective facts or the individual's knowledge: see e.g. M.S.S. v Belgium & Greece [GC] 30696/09 (2011) / Tarakhel v Switzerland [GC] 29217/12 (2014) (public reports on asylum reception conditions in a destination state); (Bivolaru & Moldovan v France & Spain 40324/16 and 12623/17 (2021) (public reports and judgments etc. on destination prison conditions); Shorazova, §§110-111 (public reports, decisions etc. questioning the underlying criminal case); Avotiņš v Latvia [GC] 17502/07 (2016) (objective procedural facts combined with the individual's knowledge raised against the presumption of original Article 6 compliance). Notably, the Court said in Avotiņš that such issues should be '*examined in adversarial*

proceedings leading to reasoned findings' (§121). In short, a presumption being rebuttable is an effective and practical concept.

30. The realities are quite different within the opaque new transnational model at issue, the more so in the case of ANOM given its radical opacity discussed supra. Applied in that context, the presumption is de facto unassailable.

31. The Interveners point out recent decisions of national courts, which have bucked the maximalist trend in the admission of Sky ECC, EncroChat and ANOM evidence and the associated reliance on mutual trust. Thus the judgment of the Audiencia Provincial of Spain of 26 January 2026[7] recognised that the sole and decisive evidence, emanating from Sky ECC servers, could not be properly verified and that '*el derecho a un proceso equitativo exigía que en este caso se hubieran permitido a las defensas el acceso a los datos en bruto*'. On 19 January 2026, a judge at the Tribunale di Imperia excluded[8] EncroChat evidence on the basis of '*the potential alterability of the material submitted* […] *given that what reaches the trial is* […] *the result of filtering the data found on the phone, which cannot be further analyzed*' in the absence of the underlying raw data. More recently, in June 2026, the Tribunale di Catanzaro issued a European Investigation Order to the French authorities for the preservation of the original evidence, in order to enable the defence to exercise rights of challenge[9] – a decision which highlights that there can also be a dialogue with the originating state with a view to achieving overall fairness.

32. Further in relation to trial fairness, the Interveners register reservations about the principle in Bykov v Russia [GC] 4738/02 (2009) §90-91, whereby evidence obtained in breach of Article 8 may yet be used at trial without producing violation of Article 6, unless it produces specific unfairness. The principled alternative originally put by Judge Loucaides ('*I cannot accept that a trial can be 'fair'* […] *if a person's guilt* […]*is established through evidence obtained in breach of* […] *the Convention*' (Khan v UK 35394/97 (2000)) would offer an appropriate solution in cases where the evidence in question is decisive – i.e. where there could have been no criminal prosecution but for the evidence being encountered amid e.g. an unlawful or impermissibly exploratory exercise.[10]

33. Finally, the Interveners respectfully draw attention to the question of entrapment. Clearly, a state actor capturing data from an encrypted system is not within the classic person-bound entrapment concept, with its associated clear exclusionary consequence (Ramanauskas v Lithuania [GC] 74420/01 (2008)). But the protective rationale – ensuring state activity is on the right side of the line between passive investigation and incitement – appears relevant where the state has created and promoted a system which it intends to be an instrument of crime (and, Lödden argues, then withheld the states' active role when obtaining court orders for the relevant interceptions). Three safeguards appear relevant in this context: (i) such an issue, if raised, should be subject to adversarial testing (Bannikova v Russia 18757/06 §§57-58); (ii) if the issue is raised, prosecution ought to be in a position to demonstrate that it did not exceed passive investigation (Ramanauskas §§69-70); and (iii) there must be previous informed judicial authorisation for what took place (Ramanauskas §53). All of which further underline the importance of the defence being placed sufficiently in the picture as to the underlying process to raise such a challenge effectively.

Vânia Costa Ramos
Chair of the ECBA

Chryssa Mela
Director, Fair Trials Europe

Alexis Anagnostakis
ECBA Human Rights Officer

Rapporteurs:
Alex Tinsley
ECBA Human Rights Committee | Senior Legal Consultant, Fair Trials

Simona di Dio
Advocacy and Networks Coordinator, Fair Trials

Constança Calçada Soares
ECBA Human Rights Committee

Lorenzo Farnetti
ECBA Intern

[1] Fair Trials and the ECBA previously intervened in Silgir (No 2) v Germany 22234/25 (communicated 31 October 2025). Fair Trials' intervention is available here: https://www.fairtrials.org/app/uploads/2026/04/Fair-Trials-Silgir-No-2-amicus-FINALwebsite.pdf. The ECBA's intervention is supplied with this one (via regular mail only).

[2] Lödden, Makepeace, StV 2026, 441 "ANOM Leaks" – Fact and Fiction Regarding ANOM and Project "Trojan Shield", available at https://research.wolterskluwer-online.de/document/31a873e8-e8bc-3af7-8ac8-9de069b73a65 (EN supplied).

[3] See 'Joint Statement on the signing of the UN Convention on Cybercrime', 24 October 2025 (available via https://www.hrw.org/news/2025/10/24/joint-statement-on-the-signing-of-the-unconvention-on-cybercrime), signed by inter alia Human Rights Watch, Article 19, Access Now, Privacy International, and the Electronic Frontier Foundation: the UNCC '*creates legal regimes to monitor, store, and allow cross-border sharing of information in a manner that would undermine trust in secure communications and infringe on human rights*'.

[4] Decision of 15 August 2025, available at: https://www.gerichte-zh.ch/fileadmin/user_upload/entscheide/oeffentlich/SB240422-O1.pdf (DE).

[5] See Camera dei Diputati, report of the Parliamentary Committee on the Security of the Republic, 4 June 2025, available at: https://documenti.camera.it/_dati/leg19/lavori/documentiparlamentari/IndiceETesti/034/004/INTERO.pdf), from p. 16.

[6] Urteil vom 11. Januar 2024 (available at https://search.bger.ch/ext/eurospider/live/fr/php/aza/http/index.php?lang=fr&type=highlight_simple_query&page=1&from_date=&to_date=&sort=relevance&insertion_date=&top_subcollection_aza=all&query_words=anom&rank=1&azaclir=aza&highlight_docid=aza%3A%2F%2F11-01-2024-7B_159-2022&number_of_ranks=5) §5.5: '*The Public Prosecutor's Office also fails to provide a plausible explanation as to how the US law enforcement authorities could have already established concrete grounds for suspicion against the purchasers of approximately 12,000 ANOM crypto devices*'.

[7] Audiencia Provincial València, sentencia 24/2026 (1 January 2026) (https://www.poderjudicial.es/search/AN/openDocument/480d2acbedd213aaa0a8778d75e36f0d/20260129).

[8] Tribunale di Imperia, ordinanza 19 gennaio 2026 (supplied / EN supplied).

[9] See the decision of the Court of Cassation Sez. VI no. 27520 of 2026 (9 June 2026), available at https://www.cortedicassazione.it/resources/cms/documents/27520_07_2026_pen_noindex.pdf.

[10] See the fuller observations on this topic within the ECBA's previous intervention, §§21-25.