# What Remains of the ordre public in Transnational Surveillance?

## A Commentary on the Decisions of the Federal Court of Justice and the Federal Constitutional Court in the ANOM Proceedings

**Thomas Wahl** *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

**Article**

## ABSTRACT

ANOM was an undercover law enforcement operation in which the American FBI distributed encrypted mobile phones with a hidden backdoor, allowing authorities to monitor previously untraceable criminals' communication in real time. Many details of the operation were kept confidential by law enforcement. The intelligence gathered led to hundreds of arrests worldwide, major drug seizures, and disruption of organised crime networks.

Continuing the discussion initiated by Lassalle and Lannier (→ related link), who retrace the EncroChat police operation in France, this article analyses two rulings by Germany's highest courts (the Federal Court of Justice and the Federal Constitutional Court) that approved the use of chat data obtained from the ANOM operation. Despite many differences between EncroChat and ANOM, both courts saw no reason to depart from the evidence-friendly case law they had each already established in the German EncroChat cases. The author argues that the approach adopted by the courts with regard to the public order (ordre public) under mutual legal assistance law does not do justice to the subject matter in ANOM and that statements against the admissibility of evidence should have been made.

**AUTHOR**

**Thomas Wahl**

Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

**CITATION SUGGESTION**

T. Wahl, "What Remains of the ordre public in Transnational Surveillance?", 2025, Vol. 20(4), eucrim, pp303–311. DOI: https://doi.org/10.30709/eucrim-2025-025

Published in
2025, Vol. 20(4) eucrim pp 303 – 311
ISSN: 1862-6947
https://eucrim.eu

# I. Introduction

The same legal outcome was reached in two criminal proceedings involving the ANOM operation, despite technical and legal differences in the collection of evidence from cryptophones. This is the main conclusion in both the decision of the German Federal Court of Justice (FCJ, *Bundesgerichtshof*) on 9 January 2025[1] and that of the Federal Constitutional Court (FCC, *Bundesverfassungsgericht*) on 23 September 2025.[2] Both courts held that evidence obtained via the decryption and surveillance of chat messages on ANOM devices was admissible in criminal proceedings against "German users". Both courts essentially followed the line of argumentation they had developed in the EncroChat case and later applied to the SkyECC case,[3] which also dealt with the admissibility of evidence of criminal activity obtained by investigators via the infiltration of encrypted mobile phones. However, the ANOM operation is unique in that it was not carried out by police authorities in EU countries, but by the U.S. Federal Bureau of Investigation (FBI), and much of the background to the operation has been deliberately kept obscure.

Having spoken out almost unanimously in favour of a ban on the use and exploitation of data obtained from abroad in the EncroChat and SkyECC proceedings, German legal scholars reinforced their position in the ANOM cases. In this context, a ban has been primarily derived from constitutional law, European law, and on domestic criminal procedural grounds.[4] This article contributes to the discussion by focusing on the legal basis for mutual legal assistance (MLA) in the two German decisions and by taking a closer look at the courts' arguments based on "*ordre public*".

Section II summarises the facts underlying the two decisions. Section III then outlines the main reasons given by the FCJ and the FCC in their decisions. Section IV comments on the judicial arguments, focusing on the reasoning behind the "*ordre public*" exception, before conclusions are drawn in Section V.

# II. The ANOM Case: Facts, Background, and Legal Question

The FCJ and the FCC based their decisions on the following facts:[5]

Following an investigation by US authorities into a company that sold cryptophones to members of criminal organisations for the purpose of encrypted communication, the FBI developed "ANOM" cryptophones to sell to these organisations. Although each ANOM device was end-to-end encrypted, the FBI was, unbeknownst to users, in possession of the codes enabling each sent message to be decrypted. Since the summer of 2019, the iBot server, which received a copy of each sent message, was located in "an EU Member State". The FBI first decrypted the messages in temporary storage on that server, then re-encrypted them, and finally forwarded them to the transfer server with a few days' delay. This enabled the communication of ANOM users to be continuously monitored.

In October 2019, a court order was issued in said EU Member State which enabled a copy of the server to be made and its content to be received by the US authorities until June 2021, in accordance with a bilateral mutual legal assistance treaty between that EU Member State and the United States. At the country's request, the FBI did not reveal the identity of the EU Member State, and it is not known why this EU Member State requested secrecy in this matter. The content of the court order(s) allowing the recovery and transmission of the data has also not been disclosed.

In September 2020, the German Federal Criminal Police Office (*Bundeskriminalamt*, BKA) was granted access to the decrypted content data for information purposes, with a link to Germany via an internet-based analysis platform. On 31 March 2021, the Frankfurt am Main General Public Prosecutor's Office (*Generalstaatsanwaltschaft Frankfurt am Main*) initiated proceedings against the users of ANOM cryptophones. On 21 April 2021, the Office submitted a request for mutual legal assistance to the U.S. Department of Justice, which consented to the use of the transmitted data in a letter dated 3 June 2021. It clarified, however, that the FBI would not provide support for the criminal proceedings in Germany, including witness testimonies or the authentication of documents.

German public prosecution services subsequently conducted individual criminal proceedings against users of ANOM devices in Germany, most of which concerned drug trafficking and the proliferation of weapons. Criminal courts convicted the individuals, the decrypted chat messages exchanged via the ANOM devices regularly being the only supporting evidence.

The defendants argued that Sec. 261 of the German Code of Criminal Procedure (*Strafprozessordnung*, StPO) had been violated and that the evidence had to be excluded. The reasoning was that, unlike in the EncroChat case, the court order(s) was/were not known ("orders from hearsay"), and a verification on the basis of rule-of-law standards has been impossible. They also argued that, regardless of any concrete grounds for suspicion, the FBI had engaged in abusive "forum shopping", which the German law enforcement authorities adopted as their own and thus continued the abusiveness.

Overall, it can be noted that the ANOM and EncroChat/SkyECC operations have little in common. In both cases, the main focus was on monitoring a private telecommunications server via infiltration software. Information initially came to Germany through police channels, and the use of the data was subsequently approved through judicial assistance.[6] There are some striking differences between the operations however.[7] In contrast to EncroChat/SkyECC, ANOM is characterised by:

- Mobile phones (cryptophones), developed by the state (USA) and distributed under the control of police forces (the FBI) using front companies;
- Investigators being able to read seemingly fully encrypted messages at any time thanks to their own decryption codes;
- Unclear reasons for the secrecy surrounding the geographical outsourcing of the evidence collection (to an unknown state hosting the server in the EU) and the content of the court surveillance orders, due to the FBI's confidentiality agreement.

# III. The Reasoning

## 1. The FCJ's main line of argumentation

In its judgment of 9 January 2025, the FCJ first reiterated the main principles for the use of evidence collected in a foreign legal order and the German approach to exclusionary rules:

- A prohibition against the use of evidence is an exception that requires justification, given that the primary objective of criminal proceedings is to reach a just and materially correct decision;
- The admissibility of evidence obtained through mutual legal assistance (MLA) shall be governed by the law of the requesting state (*lex fori*);

- The legality of investigative measures in the requested state shall not be reviewed against the standards of the requesting state's legal system;
- In international cooperation in criminal matters, it is rather necessary to respect the structures and content of foreign legal systems and views, even if they do not correspond in detail to domestic – in this case, German – views; otherwise, the sovereignty of the other state would be called into question;
- Mere non-compliance with German law in a foreign investigation does not in itself constitute grounds for a (dependent) prohibition on the use of evidence;
- The inadmissibility of evidence may result from a violation of the principles of national and European *ordre public* (Section 73, sentence 1 IRG[8]) or guarantees of binding international law with individual legal protection – such as Art. 3 of the European Convention on Human Rights (ECHR) – during the collection of evidence.

With regard to the case at issue, the FCJ further examined the consequences of a potential violation of Art. 31 para. 1 of the Directive regarding the European Investigation Order (i.e., the failure to notify an EU Member State on whose territory an interception order is used and from which no technical assistance is needed to carry out the interception). According to the FCJ, a violation by the "unknown third state party which is an EU Member State" (i.e., the state hosting the server) of the notification obligations does not lead to the exclusion of evidence, as the state's interest in investigating the case outweighs the defendant's right to privacy and communication.

The following main part of the FCJ's judgment was dedicated to the findings of a possible violation of the *ordre public*, which the FCJ rejected by arguing as follows:

- A lack of knowledge regarding both the identity of the monitoring third country and the content of the decisions taken there does not constitute a violation of fundamental principles of the rule of law. The reason for this is because the principle of mutual trust requires that the legality of official acts and investigative measures carried out abroad be assumed at first. This principle also applies to mutual legal assistance with the USA. Only if there are reliable indications that the requested state has not acted in accordance with the law can the presumption of lawful action be refuted. Such non-lawful conduct does not arise specifically from the FBI's failure to disclose information, as confidentiality commitments and source protection are not foreign to German criminal proceedings either. Investigative measures do not have to be completely transparent.
- The FBI operation was not a groundless mass investigation and mass data analysis and thus essentially a secret service measure for which there would be no legal basis in criminal proceedings.
- Since this was not a case of indiscriminate mass surveillance, intercepting ANOM data was not disproportionate, but rather a permissible criminal investigation tactic (*zulässige kriminalistische List*).
- The essence of the German and European principle of a fair trial was not violated, since the proceedings as a whole were not unfair. The requirements of a functioning criminal justice system must also be taken into account in this context.
- In addition, the minimum standards of the rule of law were not violated by the defendant not having had the opportunity to have the orders reviewed by a court. Although the lack of primary legal remedies deprives the defendant of legal protection, this does not affect the essence of the relevant fundamental rights (telecommunications secrecy and the general right of personality), either institutionally or individually (through the use of the ANOM findings). The German Code of Criminal Proced-

ure also provides for comparable measures with regard to telecommunications surveillance in Sec. 100a StPO.

## 2. The FCC's main line of argumentation

In its order (*Beschluss*) of 23 September 2025, the FCC essentially shared the FCJ's argumentation and approach, particularly with regard to the exceptional character of accepting evidential exclusionary rules in German criminal procedure, the principal non-review of the sovereign decisions of the requested state against the standard of the requesting state's law, and the general adherence to the structures and substantive content of foreign legal orders and perspectives, even if they are not necessarily consistent with domestic views in an individual case. The FCC also emphasised the importance of the principle of mutual trust in international cooperation in criminal matters, which leads to the "as-long-as" formula: It must be assumed that principles of the rule of law and human rights protection have been observed in the foreign state, as long as this is not refuted by the facts of the case. In the present case, there were no indications that suggested an undermining of mutual trust, according to the FCC.

Among other things, the FCC highlighted two aspects of the case that supplement the FCJ's ruling:

- Lack of knowledge regarding the unknown EU country hosting the server is irrelevant, as the legality of the collection procedure is fundamentally irrelevant to the usability of the data. Furthermore, the manner of collection and the maximum scope (= users of the devices) were limited, as specified by the FBI.

- The argument that there were insufficient opportunities to influence the course and outcome of the proceedings is invalid, because the complainant could have commented on the communications surveillance affecting him and, in particular, called into question the authenticity of these communications in the German proceedings. Even if the lack of influence in the unknown EU state were considered deficient and questionable from a constitutional point of view, this would be irrelevant here, because the collection of evidence in the requested state is insignificant for the question of the prohibition of evidence in the *lex fori*, as laid out above.

# IV. Commentary

The ANOM operation did not lead the FCJ and FCC to deviate from the approach taken in the EncroChat/SkyECC proceedings. This outcome has been achieved primarily through adherence to the traditional approach of applying the "*forum regit actum*" principle to the question of the use of evidence collected abroad, negating the need for legality control of measures taken in the "surveilling state", and placing a strong emphasis on the maxim of mutual trust that governs international cooperation in criminal matters. The FCJ and FCC rulings have met with fierce opposition in the German legal literature. Above all, scholars have criticised the defendant's inability to obtain sufficient legal protection, the disproportionality of the operation in placing all purchasers of the mobile phones under general suspicion, and the failure to follow up on concrete indications of forum shopping.[9] The discussion in the next subsections will be guided by three key questions, viewed through the lens of mutual legal assistance (MLA):

- Is the approach of applying the *forum regit actum* principle to all questions regarding the use of foreign evidence still up to date in the present context?

- What is the yardstick for an *ordre public* assessment (national or European)?

- What arguments can be raised against the courts' findings with regard to the *ordre public* in the ANOM case?

## 1. The *lex fori*-approach – Still up to date?

This subsection examines whether, in transnational surveillance police operations such as those in ANOM (and also in EncroChat), the "preliminary question" – assessing foreign evidence under the *lex fori* standard, coupled with the factual exclusion of reviewing the legality of the measure in the "requested state" – can still be followed.

The German courts' statement that the admissibility of evidence obtained through MLA is governed exclusively by the national law of the requesting state (*lex fori*), combined with the statement that the sovereign decisions of the requested state are not, in principle, subject to review under the standards of the requesting state's legal system,[10] appears irrefutable. However, it should be noted that this maxim was developed in "traditional" MLA situations, those in which German judicial authorities issued a request for a specific investigative measure to a foreign state, which then executed the measure.[11] In these situations, the German judicial authorities at least had the opportunity to influence the investigative measure in the foreign state (including the possibility of asking for "German" safeguards in accordance with the *forum regit actum principle*[12]). At the later trial stage, it was possible to review whether procedural flaws that did not comply with German criminal procedure order had consequences on the use of the evidence collected abroad.[13]

Departing from this concept, the EncroChat case and, even more strikingly, the ANOM case each reveal a completely different scenario: A foreign police force conducted investigations into an initially undefined number of persons, thereby encroaching upon their fundamental right to privacy through surveillance measures (using infiltration techniques), and then distributed the "final product" (data collected on users in other countries) to police forces in other territories for their use. Judicial authorities in these territories were hardly, if at all, involved in these law enforcement operations from the outset, and the evidence was primarily transmitted through police channels. Only retrospectively was an MLA request submitted by the judicial authorities – purely as a formality – in order to have the authorisation for use rubber-stamped.

The courts' statement that "evidence was obtained '*by way of mutual legal assistance*'" must be viewed with considerable scepticism. Most notably, the courts failed to address fundamental issues, including the completely different quality of information gathering compared to previous MLA practice, the relationship between police assistance and judicial assistance, and the consequences arising from this. By separating the state *gathering* evidence from the state *utilising* evidence, the FCJ and the FCC have created a dangerous loophole: Defence rights can no longer be systematically asserted anywhere, especially when the location and manner of data collection remain secret. While the verifiability of data collection under French law was used as an argument for compliance with fair trial principles in the EncroChat case,[14] this is completely absent in the ANOM case.

While it may be true that foreign law does not need to be examined against the standards of German law, a sound assessment of *ordre public* cannot be made if the legality of an investigative measure is unclear or even not verifiable, as in ANOM. Therefore, it must be pleaded for the approach that German courts cannot completely disregard the question as to what impact unlawful conduct by foreign authorities should have on German criminal proceedings.[15] In this context, it is extremely regrettable that the FCJ and FCC adopted a highly "German-centric" approach, ignoring developments in other countries where courts are increasingly questioning the reliability of digital evidence gathered through law enforcement's infiltration of cryptophones.[16]

There were several indications that the FBI's actions were unlawful, which the German courts should have been aware of.[17] Not to forget: There was also controversy in the United States over whether the information obtained through the infiltration of cryptophones was admissible as evidence and whether it met the requirements of the US law of evidence.[18] However, if the admissibility of the evidence is legally controversial even under US law, i.e., under the law of the originator of the action, why should other states overlook this?

## 2. The yardstick for an *ordre public* assessment – Did the FCJ/FCC get it right?

The courts' interpretation of *ordre public* as the ultimate limit on the admissibility of foreign evidence will be examined in this subsection. This examination will be followed by a proposal for a new approach to the issue, which shall also guide the continued analysis of the ANOM case (subsection 3 below).

Both the FCJ and the FCC derive a potential prohibition of the evidence collected abroad from scaling the *ordre public*. Both courts reduce the scope of *ordre public* to a minimum standard. In the words of the FCC:[19]

> The limits on the use of evidence [in the sense of *ordre public*] are breached if the collection of evidence abroad did not meet the indispensable minimum level of fundamental rights protection and the minimum standards under international law insofar as it binds the Federal Republic of Germany in accordance with Art. 25 of the Basic Law.

The deeper meaning of this formula is rarely clarified, and it can be debated whether such clarification is in fact possible. The decisive clue, however, can be discerned from the central norm in Germany's law on international cooperation in criminal matters: Sec. 73 IRG.[20] This provision distinguishes two types of *ordre public* in two distinct sentences:

- The rendering of mutual assistance is not permissible if it contradicts core principles of the German legal system (= national/German *ordre public*).
- If the request is subject to an EU instrument of judicial cooperation (e.g., the European Investigation Order), the rendering of assistance is not permissible if executing the request would go against basic principles as set out in Art. 6 TEU (= European *ordre public*).

Although the wording of the provision submits its applicability only if MLA is "rendered" (i.e. Germany as the requested state), it also applies by analogy to outgoing requests (i.e. Germany as the requesting state), as the phrasing expresses the central limit of protection of individual rights in "transnational criminal proceedings based on division of labour" (*international-arbeitsteiliges Strafverfahren*).[21] It follows that the principles underlying Sec. 73 IRG also apply to evidence collected abroad and "entering" Germany.

Against this background, the first criticism that arises is that the FCJ and FCC do not distinguish clearly enough between the national/German and European *ordre public*. The latter only applies in the realm of "EU MLA". In the ANOM case, the key questions are "who is who" and "who did what". According to the underlying facts of the case, the "third party EU Member State" did not conduct its own investigative measures, such as filtering or analysing the copied data. It merely acted as a "service" for the US authorities (FBI), as it was not permitted to place the server on US territory. "EU MLA" in the form of the EIO Directive only applies if the requested (i.e. executing) State *carries out* one or more specific investigative measures to obtain evidence (on its territory)[22]. In the present case, however, it was the FBI, as a US authority, that carried out the investigative measure, as the "final evidence product" stems from its own analysis (wherever this occured) and not from the EU. Therefore, from the perspective of the authorities in countries that received the data,

the US is the "requested" State and not an EU country that merely functioned as a conduit or extended arm for the US.

As a result, only the national *ordre public* applies in the case of cooperation with non-EU Member States. This may entail higher standards than the "European *ordre public*", given that EU MLA instruments are based on a much higher level of mutual trust, which forms the basis for the concept of mutual recognition of judicial decisions. By overly emphasising the governance of mutual trust in MLA, the FCJ and FCC level this distinction and create a hurdle that is almost impossible for the individual to overcome.

In this context, a second criticism emerges: According to the courts, the *ordre public* should only come into play if the *essence* of a fundamental right – in particular the right to a fair trial (as enshrined in Art. 6 ECHR) – has been violated. It is unclear, however, why the national *ordre public* requires a further reduction of the minimum standard already set (see above) to another minimum standard, i.e., the essence of a right's violation. As *Böse* rightly stated: When evaluating evidence, German courts are fully bound by the principle of fair trial, and restricting the *ordre public* is not justifiable.[23] Similarly, the FCJ's argument that it "only" had to determine whether the proceedings as a whole were fair is flawed.[24] This approach is a consequence of the ECtHR's self-restraint, as the ECHR does not lay down rules on the administration of evidence.[25] This cannot be applied to a domestic court that must determine whether evidence, potentially obtained unlawfully (including foreign evidence), is admissible in terms of domestic law (see 1. above).

To make the assessment of *ordre public* more precise and to move away from the highly undetermined, casuistic approach of German case law, the following question should be asked: Would a tolerable situation still be guaranteed in terms of German fundamental rights and fundamental principles of its criminal procedure if the foreign standard were incorporated into German criminal procedure law for the purpose of obtaining evidence?[26]

## 3. Arguments in favour of an *ordre public* breach in the ANOM case

Taking this standpoint (as formulated in the previous paragraph) as the basis for the *ordre public* assessment, two arguments become apparent in the ANOM case that merit a different view to that taken by the FCJ and FCC.

### a) Surveillance beyond the core values of German telecommunication surveillance law

Clandestine access to phone data through telecommunication surveillance by German law enforcement is considered a serious interference into the fundamental rights of the Basic Law (the German constitution: *Grundgesetz*).[27] To navigate this legal issue, the FCC developed several core principles that have been implemented through rather restrictive legislation in Sec. 100a et seq. StPO. In order to comply with fundamental rights, German legal requirements stipulate that surveillance orders can only be issued for serious offences that are listed and that the principle of proportionality must be observed in several respects. In addition, the German law provides for "securing mechanisms", such as requirements governing surveillance software, the permissible scope of alterations to the information technology system, their rescissions, documentation obligations, etc.[28] Notably, the FCC itself emphasised that surveillance can only be ordered on occasion of a concrete event and that the initial suspicion is concretised *ex ante* with regard to the specific list offence.[29] Indiscriminate surveillance of mobile telephones belonging to initially unknown users is therefore prohibited under German law,[30] particularly given that suspicion based on facts and events for a specific serious offence, as enshrined in the telecommunication surveillance provisions must be seen as one of the "core principles" of the German *ordre public*.[31]

The FBI's ANOM operation clearly contradicted these principles. This also cannot be discarded by the FCJ's and FCC's argument that the purchase of the ANOM crypto mobile phone *per se* establishes suspicion because "only criminals bought them". This would subject any person, criminal or not, to general suspicion of criminality and would lead to a suspicion *in rem* rather than *in personam* as is fundamentally required by German law.[32] Operating with statistical probabilities does not establish suspicion. Taken to its logical conclusion, according to the line of argumentation advanced by the FCJ and the FCC, the mere fact of holding a numbered account in the Cayman Islands would also be sufficient to give rise to suspicion of a (serious?) money laundering criminal offence.[33]

If the German BKA accepts evidence gathered in the manner of the ANOM operation, it accepts material that German law enforcement authorities would never have been permitted to collect.[34] Regardless of whether the FBI itself engaged in forum shopping or power shopping (*Befugnisshopping*), using the ANOM chats in Germany amounts to illicit power shopping on the part of the German law enforcement authorities themselves through the self-appropriation of data, which is not in line with the core principles of the German legal order.[35]

### b) Disrespect for essential defence rights

Eventually, neither the FCJ nor the FCC have adequately addressed the German *ordre public* standard with regard to defence rights in digital investigations. As part of the right to a fair trial, it is common ground in Germany that the defendants and their defence council must be able to question both the lawfulness and the means and manner of enforcement of coercive measures. In digital investigations, this includes the right to have access to and voice concern over the computer data, data files established during the investigative phases, the selection process of the data by the police, their compilation, and, finally, the integrity and authenticity of the data.[36] This is consistent with the aforementioned securing mechanisms, which are framed by the German law on telecommunications surveillance as well as the procedure of digital investigations formalised in German legal practice.[37]

The FCC deemed it sufficient to be able to challenge the communication surveillance and the authenticity of the data at any time after transmission (based on reports by the BKA). However, this falls short of the fundamental principles of the German legal system, which require the *entire* "chain of custody" and data analysis to be subject to challenge.

In its existing case law on electronic evidence, and thus in determining a – potentially lower – standard of European *ordre public*, the ECtHR has also emphasised the importance of access to raw data in order to enable counter-arguments to be put forward.[38] The ECtHR likewise also emphasised the need to subject the content and integrity of the raw material to independent scrutiny.[39] Therefore, it is not only the point in time at which evidence is used in a German criminal proceeding that is decisive, but also the point in time at which it is collected, in order to ascertain whether the essential IT forensics standards have been met.[40] By failing to disclose the circumstances of the data collection and analysis, and by refusing to provide assistance in national criminal proceedings in other states, the FBI deprives the person concerned of this essential right.[41] Ultimately, the FCC is engaging in a circular argument: If the person concerned is never provided with information regarding a chain of custody, they cannot invoke it in proceedings. This blatantly contradicts the principle of fairness.

## V. Conclusion

The two rulings discussed here, by the Federal Court of Justice and the Federal Constitutional Court, have consistently upheld the approach taken in the EncroChat and SkyECC criminal proceedings, even in the –

somewhat different – ANOM operation. The hotly debated question in Germany as to whether data obtained by foreign authorities through the infiltration of encrypted mobile phones using Trojans can be used in criminal proceedings with a connection to Germany has essentially been unanimously answered with a clear "yes" by both courts. The differences in the ANOM case, primarily arising from the state authorities luring offenders by distributing the mobile phones themselves via front companies, were resolved by the German courts primarily through arguments based on – almost unshakeable – mutual trust in mutual legal assistance, the virtual impossibility of reviewing the legality of foreign investigative measures, and the exclusion of prohibitions on the use of evidence under the *lex fori*. The main argument of both courts was that the limits of national and European *ordre public* were not exceeded.

The aim of this article was to demonstrate that the legal reasoning of both courts regarding mutual legal assistance could well have – and indeed should have – taken a different direction. Focusing solely on examining German rules on the use of evidence, regardless of the legality of the measure in the "requested state", falls short when it comes to the information gathering underlying the ANOM case. The courts' interpretation of the *ordre public* standard is too narrow and must be corrected by considering how the foreign rule would look like if it were incorporated into the German law of criminal procedure. Would this then give rise to contradictions with our fundamental principles? The answer to this question in the ANOM case is: Yes!

---

1. BGH, Urteil vom 9.1.2025 – 1 StR 54/25. The full text (in German) is available at: https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Strafsenate/1_StS/2024/1_StR__54-24.pdf?__blob=publicationFile&v=1. A press release in English is available at: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2025_en/2025002.html;jsessionid=1EB69E7D3CD3F4F1FD8BB40D1BEDF199.internet992?nn=19778950. All hyperlinks in this article were last accessed on 13 March 2026.↩
2. BVerfG, Beschluss vom 23.9.2025 – 2 BvR 625/25. The full text (in German) is available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2025/09/rk20250923_2bvr062525.html. The English version of the decision is available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2025/09/rk20250923_2bvr062525en.html . A press release in English is available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2025/bvg25-088.html?nn=68080.↩
3. For the EncroChat case, see the FCJ's landmark ruling: BGH, Beschluss vom 2.3.2022 – 5 StR 457/21. The full text (in German) is available at: <https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Strafsenate/5_StS/2021/5_StR_457-21.pdf?__blob=publicationFile&v=1>. A summary of the decision in English is provided by T. Wahl, "Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases", (2022) *eucrim*, 36-37. Constitutional complaints against criminal convictions following the assessment of the transmitted EncroChat data from France to Germany have remained unsuccessful (cf. BVerfG, Press Release No. 77/2023 (in German), <Bundesverfassungsgericht - Homepage - Unzulässige Verfassungsbeschwerde gegen strafrechtliche Verurteilung nach Auswertung übermittelter EncroChat-Daten>, and BVerfG, Press Release No. 104/2024 in English at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2024/bvg24-104.html). On declaring evidence admissible involving SkyECC, see BGH, Beschluss vom 9.1.2025, 1 StR 142/24. The full text of the decision (in German) is available at: https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Strafsenate/1_StS/2024/1_StR_142-24.pdf?__blob=publicationFile&v=1.↩
4. For the different approaches taken in the EncroChat case already, see J. Geneuss, "Entscheidungsanmerkung – Verwendung und Verwertung von EncroChat-Daten nach Inkrafttreten des Konsumcannabisgesetzes", (2026) *Zeitschrift für Internationale Strafrechtswissenschaft (ZfIStw)*, 104.↩
5. BGH, *op. cit.* (n. 1), mn. 12, 13; BVerfG, *op. cit.* (n. 2), mn. 8, 9, 31.↩
6. In the EncroChat case, the investigating judge in Lille, France approved a European Investigation Order; in the ANOM case, the U.S. Department of Justice approved an MLA request under the German-American Mutual Legal Assistance Treaty.↩
7. Cf. R. Esser, "Zur Unverwertbarkeit von Beweisen aus TK-Überwachungsmaßnahmen im Ausland („Anom")", (2025) *Wirtschaftsstrafrecht und Haftung im Unternehmen (ZWH)*, 325; L. Lafleur, "Die EncroChat-Verfahren aus Sicht der Justiz", in: K. Pfeffer (ed.), *Policing Crime Chat Networks – Lessons from the EncroChat Operation*, 2024, p. 17, 30 et seq., who justifies the use of evidence obtained in the EncroChat operation but – on the basis of the differences – sees the red line exceeded in the FBI's Anom case.↩
8. Act on International Mutual Assistance in Criminal Matters (*Gesetz über die Internationale Rechtshilfe in Strafsachen,* IRG). The English translation of the Act is available under: <https://www.gesetze-im-internet.de/englisch_irg/index.html>.↩
9. With regard to the FCJ's judgment (*op. cit.* (n. ##)), see M. Böse, "Anmerkung", (2025) *JuristenZeitung (JZ)*, 937; Esser, *op. cit.* (n. 7); R. Michalke, "Anmerkung", (2025) *Neue Juristische Wochenschrift (NJW)*, 1589; L. Zeyher, "Anmerkung", (2025) *Strafverteidiger (StV)*, 512; A. Althaus, "Vertrauen statt Kontrolle?", (2025) *HRRS*, 87. With regard to the FCC's decision (*op. cit.* (n. 2)) : J. Marinitsch, „Anmerkung" (2025) *MMR*, 961. See also S. Pschorr and L. Wörner, "Strafverfolgung in Deutschland aufgrund US-amerikanischer Daten", (2023) *StV*, 274. At the heart of data-driven (criminal) investigations spanning multiple countries lies the more fundamental question: does the end justify the means? (cf. S. Gless, "Heiligt der Zweck die Mittel 2.0?", (2026) 144 *Schweizerische Zeitschrift für Strafrecht (ZStrR)*, 80).↩
10. BGH, *op.cit.* (n. 1), mn. 8; BVerfG, *op. cit.* (n. 2), mn. 27.↩
11. For an overview, see T. Hackner, "Vor § 68 IRG", in: Schomburg/Lagodny, *Internationale Rechtshilfe in Strafsachen*, 6th ed. 2020, mn. 11 et seq.↩
12. The "*forum regit actum*" principle in this sense refers to the collection of evidence (e.g., Art. 4(1) 2000 EU MLA Convention, Art. 9(4) EIO Directive) and is not to be confused with the application of the "*forum regit actum*" principle if it comes to the use of the evidence transmitted.↩

13. Cf. T. Wahl, "Grundlagen: Internationale Zusammenarbeit in der Telekommunikationsüberwachung", in: U. Sieber, N. von zur Mühlen, and T. Wahl, *Rechtshilfe zur Telekommunikationsüberwachung*, 2021, pp. 127 et seq.↩
14. BGH, Urt. v. 30.1.2025 – 5 StR 528/24, (2025) *Neue Zeitschrift für Strafrecht (NStZ)*, 371; Marinitsch, *op. cit.* (n. 9).↩
15. The necessity for a legality of the measure according to the law of the requested state is the prevailing approach in German legal literature. See T. Wahl. *op. cit.* (n. 13), p. 134 with further references.↩
16. It was revealed rather blatantly that an Australian court initially denied placing the server for the ANOM operation on Australia's territory (A. Althaus and J. Samek, "Vertrauen statt Rechtsstaat: Die ANOM-Entscheidungen des BVerfG und BGH im Lichte neuer Erkenntnisse, (2025)(6) *KriPoZ*, 396). For EncroChat and SkyECC, see S. Gless, (2026) 144 *ZStrR*, *op. cit.* (n. 9), 80; Joint Defence Team "EncroChat and SkyECC: Why European Courts are Questioning the Reliability of Digital Evidence", <https://www.joint-defense-team.com/post/encrochat-skyecc-digital-evidence-reliability-europe>.↩
17. C. Nestler, "Anmerkung", (2022) *StV*, 280; S. Pschorr, "Keine verfassungsrechtlich bedenklichen Erkenntnisse über die Erhebung von ANOM-Telekommunnikationsdaten?", *jurisPR-StrafR* 23/2025 Anm. 1.↩
18. Cf. Gless, (2026) 144 *ZStrR*, *op. cit.* (n. 9), 86; A. Milch, "'SkyECC has fallen' – Der New Yorker Paukenschlag und seine Bedeutung für Europas Kryptoverfahren", (2026) *Recht Digital (RDi)*, 46.↩
19. BVerfG, *op. cit.* (n. 2), mn. 29.↩
20. The provision is also cited by the FCJ (BGH, *op. cit.* (n. 1), mn. 19).↩
21. S. Gless, T. Wahl, and F. Zimmermann, "§73 IRG", in: Schomburg/Lagodny, *op. cit.* (n. 11), mn. 4; K. Ambos/A. M. Gronke, "Rechtshilfehindernisse und ordre public", in: K Ambos, S. König and P. Rackow (eds.), *Rechtshilferecht in Strafsachen*, 2nd ed. 2020, I, mn. 69. For details on the concept of the "international-arbeitsteiliges Strafverfahren", see Authors, in: Schomburg/Lagodny, *op. cit.* (n. 11), Einleitung, mn. 145 et seq. The concept reflects a shared responsibility in transnational cooperation states act collectively rather than independently. The main focus of the concept is which conclusions can be drawn for the protection of the individual who must be seen as a legal subject (*Rechtssubjekt*) in transnational criminal proceedings.↩
22. Art. 1(1) of Directive 2014/41/EU regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, 1.↩
23. Böse, *op. cit.* (n. 9), 940.↩
24. BGH, *op. cit.* (n. 1), mn. 36, 37.↩
25. ECtHR, 11 July 2017, *Moreira Ferreira v. Portugal (no. 2),* Appl. no. 19867/12, para. 83 with further references.↩
26. T. Wahl, "Verwertbarkeit von im Ausland überwachter Chatnachrichten im Strafverfahren", (2021) *Zeitschrift für internationale Strafrechtsdogmatik (ZIS)*, 452, 454; F. P. Schuster, *Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess*, 2006, p. 130.↩
27. See, recently, BVerfG, Beschluss vom 24.6.2025, 1 BvR 180/23, mn. 172.↩
28. See, for a summary, S. Gless and T. Wahl, "The Handling of Digital Evidence in Germany", in: M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence – Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, 2021, pp. 49, 54 et seq.↩
29. BVerfG, Beschluss vom 18. 4. 2007 - 2 BvR 2094/05= (2007) NJW, 2749, 2751; BVerfG, Urteil vom 27.02.2008 - 1 BvR 370, 595/07 = official case reports E 120, 274, 328 et seq.↩
30. LG Saarbrücken, Urteil vom 3. Juni 2024 – 4 KLs 16/24 –, juris, mn. 38; S. Pschorr, "EncroChat und (k)ein Ende?", (2025) *Strafverteidiger Forum (StraFo)*, 167, 169 with further references.↩
31. It is a matter of dispute whether the information gathering underlying the ANOM operation constitutes source telecommunications surveillance (as provided for in section 100a(1), second and third sentences StPO) or an online search (as provided for in section 100b StPO). See, for the distinction in general: Gless and Wahl, *op. cit.* (n. 28), p. 54. The fundamental principles are the same, however, in both provisions: an order may only be issued in respect of listed offences, the requirements of proportionality, and the need for a specific suspicion of a listed offence against a particular person.↩
32. R. Eschelbach, "§100a", in: H. Satzger, W. Schluckebier and R. Werner (eds.*), StPO Kommentar*, 6th. ed. 2025, mn. 21. The German courts' assumption both in the EncroChat case and ANOM case, namely that there is no case of indiscriminating mass surveillance, is opposed by the vast majority of scholars in legal literature (see, among others, Böse, *op. cit.* (n. 9), 939; Esser, *op. cit.* (n. 7), 328; Zeyher, *op. cit.* (n. 9), 514; B. Derin and T. Singelnstein, "»Encrochat« – Verwendung durch verdachtsunabhängige Massenüberwachung im Ausland erlangter Daten in deutschen Strafverfahren", (2022) *StV*, 130); F. Deutsch and T. Eggendorfer, "EncroChat – Perspektive des Rechts und der Informatik", in: Pfeffer (ed.), *op. cit.* (n. 7), p. 37.↩
33. Another aspect emerges in view of the essential requirements of German law: It is impossible for an ANOM-like police operation (comparable to a state-instigated "honeypot") to initially filter out individuals suspected of having committed a list offence, as required by Sec. 100a et seq. StPO.↩
34. Nothing else can apply if the data transfer is regarded as a chance discovery (*Zufallsfund*) or if the collection of data is seen as having been carried out for a different purpose, and the German rules of use for other purposes are applied, as done by the FCJ and FCC. Here, too, the basic requirements regarding the suspicion of a list offence and the proportionality of the original measure must be met firsthand (cf. Eschelbach, "§100e", in: Satzger et al., *op. cit.* (n. 32), mn. 20, 21; Pschorr. (2025) StraFo, *op. cit.* (n. 30), 169 with regard to Sec. 479(2), 161(3) StPO).↩
35. Similarly, Pschorr and Wörner, (2023) *StV*, *op. cit.* (n. 9), 281, who describe "secret service management without a mandate" ("*geheimdienstliche Geschäftsführung ohne Auftrag*"), which leads to intolerable power shopping (*nicht tolerierbares Befugnisshopping*).↩
36. Gless and Wahl, *op. cit.* (n. 28), pp. 68 et seq. with further references. For the crucial importance of reliability, traceability, and completeness of the right of access to files from a Swiss perspective, see Gless, (2026) 144 *ZStrR, op. cit.* (n. 9), 93 et seq. For the standard developed by the ECtHR, see J-J. Oerlemans and S. Royer, "The future of data-driven investigations in light of the SkyECC operation", (2023) 14(4) *New Journal of European Criminal Law (NJECL),* 434.↩
37. Gless and Wahl, *op. cit.* (n. 28), pp. 68 et seq.↩
38. ECtHR (GC), 26 September 2023, *Yüksel Yalçınkaya v. Türkiye*, Appl. no. 15669/20, para. 331.↩
39. ECtHR, *Yüksel Yalçınkaya*, *op. cit.* (n. 38), para. 332.↩
40. F. Meyer, "Übermittlungsvoraussetzungen und Verwertbarkeit von EncroChat-Daten, (2024) *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)*, 243, 250, 251. For the "ECHR standard", see also R. Stoykova, "Encrochat: The hacker with a warrant and fair trials?", (2023) 46 *Forensic Science International* 301602.↩

41. For a similar result, see Böse, *op. cit.* (n. 9), 940, also referring to ECJ, 30 April 2024, Case C-670/22, *M.N. {EncroChat]*, paras. 105, 130; Esser, *op. cit.* (n. 7), 329.↩

## * Author statement

The author would like to thank Indira Tie and Dr. Anna Pingen from the eucrim team for their careful review of the manuscript and their valuable comments.



## About eucrim