Case Review

On the admissibility of evidence obtained via Operation Trojan Shield (ANOM)

Review of Federal Court of Justice, judgement from 9 January 2025

BGH (1. Strafsenat), Urt. v. 09.01.2025 - 1 StR 54/24, NJW 2025, 1584; BeckRS 2025, 23

Michel Hoppe[*]

A. Circumstances of the case

The defendant had conducted his illegal activities in Germany using encrypted mobile telephones sold under the brand "*Anom*" which, unbeknownst to him, had been developed and put into circulation by the US Federal Bureau of Investigations (FBI). Although the chat function hidden in the devices' calculator was end-to-end encrypted, the FBI retained the necessary codes to decrypt all messages. Copies of all messages send were transmitted and stored on a server located in another undisclosed member state of the European Union. According to the FBI, one of that country's courts had allowed for the server's contents to be copied every two to three days up until a set date and eventually forwarded to the FBI. A few days later, the Federal Criminal Police Office (*Bundeskriminalamt*) would then be able to access any decrypted information relating to Germany.

On 31 March 2021, the attorney general's office (*Generalstaatsanwaltschaft*) formally requested legal assistance from the FBI, which while allowing for the transmitted information to be processed and admitted as evidence, denied further assistance in the form of witnesses or documents. Based on one of these transmissions, the defendant was sentenced by the Regional Court (*Landgericht*) of Tübingen to seven years and six months imprisonment for trading various drugs in non-insubstantial quantities in 35 cases. His

---

[*] Law student, HHU Düsseldorf. Head of the Department for Criminal Law. Student Assistent, Chair of German and Foreign Public Law, European Law and Public International Law (*Lehrstuhl für Deutsches und Ausländisches Öffentliches Recht, Völkerrecht und Europarecht*, Prof. Dr. Kreuter-Kirchhof). The author gives his thanks to Professor Till Zimmermann for his advice. All opinions, errors and omissions are entirely the author's.

proceeds and the secured cocaine were confiscated.

B. Background

The defendant appealed the sentence strictly on points of law (*Revision*, section 333 of the Code of Criminal Procedure - StPO), as opposed to also on points of fact (*Berufung*, section 312 StPO). Appeals of this nature directed against judgements handed down by Regional Courts are decided on by the Federal Court of Justice (*Bundesgerichtshof* – BGH) according to section 135 paragraph 1 of the Courts Constitution Act (*Gerichtsverfassungsgesetz* – GVG). The defendant argued that the prosecutorial authorities, on which the onus of proof would supposedly lie, had not demonstrated that their behaviour conformed to rule of law principles. On the contrary, the FBI had "shopped" for a territory which – unlike the US – would allow for the measures described being performed without reasonable suspicion, and the German authorities had accordingly appropriated the fruits of these illegal activities. He accused the parties involved of acting on the basis of foreign warrants whose existence or contents were dubious, analogous to violating the hearsay rule. The lack of opportunities to take action against the collection of his data in the first place breached due process as well.

C. Ruling

Due to various legal errors in determining whether several statutory violations had been committed by one act (*Tateinheit*, section 52 of the German Criminal Code - StGB) or if there had been several offences which were merely to be adjudicated at the same time (*Tatmehrheit*, section 53 StGB), the sentence was altered to just 23 cases of trading drugs. However, the defendant's argument regarding the inadmissibility of his communications was fully rejected.

D. Arguments

The Federal Court of Justice reaffirms that the inadmissibility of evidence is to be considered an exception to the principles of ex officio examination (section 244 paragraph 2 StPO) and free appraisal of evidence by the judge (section 261 StPO). Criminal courts are thus, in principle, at liberty also to accept evidence gained from foreign authorities. Lacking a specific, explicit prohibition to admit the evidence in question, its inadmissibility could only stem from an unwritten exception founded on the illegality of the investigations, or on a human rights violation perpetrated in the process of using the

evidence. The legality of investigatory measures is not judged by the standards of the requesting state but by the domestic law of the state from which information has been requested. As a basic rule, foreign legal systems and their contents would have to be respected. At the same time, a breach of law on the part of the requesting state could be constituted by a violation of rule of law principles, by their own standards rather than genuinely by the standards of foreign law.[1] Germany had, however, not breached the rule of law merely by trusting that the US had acted in accordance with US law. To the contrary, the principle of mutual trust would have to be applied to the US just as it is to other rule-based, constitutionally established states.

Nevertheless, the EU member state hosting the server had been obliged to inform the German authorities about their cross-border surveillance according to Article 31 paragraph 1 of the EIO Directive. The EIO Directive is a piece of legislation passed by the European Union, concerning especially the conditions under which a warrant issued by a member state is recognized and must therefore be executed as a European Investigation Order (EIO) by the other member states, including for the purposes of an interception of telecommunications. The circumstance that the EIO is a directive and not a regulation directly applicable in the member states and by their authorities[2] did not hinder the Court's intermediary conclusion that, due to the breach of Article 31 paragraph 1 EIO directive, the investigation had technically been illegal. Although Article 31 paragraph 3 letter b of the Directive only prohibits the intercepting EU member state in certain cases from using the material obtained, no such restrictions are placed on the notified state.[3] Still, there had been a violation of a provision erected in order to protect the accused's individual rights, enabling the Court to apply the so-called *Abwägungslösung* in order to possibly deduce a rule of inadmissibility in favour of the defendant. At first sight, the duty to notify the other member state serves to exclusively protect that member state, as indicated by the preclusion in case that they do not intervene within 96 hours.[4] In view of Article 7 of the EU Charter of Fundamental Rights, Article 31 paragraph 1 is nevertheless classified by the Court as safeguarding the citizenry as well.

The aforementioned *Abwägungslösung* is the method widely applied for the purposes of deriving an implicit rule of inadmissibility from a procedural violation where there is no such explicit statutory rule. Subject to this formula, not all illegal investigatory measures

[1] Frank Zimmermann, 'Die Verwertbarkeit von Auslandsbeweisen im Lichte der EncroChat-Ermittlungen' (2022) 2 ZfIStw 173, 176.

[2] See Consolidated Version of the Treaty on the Functioning of the European Union [2016] OJ C202/01, art 288.

[3] Thomas Wahl, 'Verwertung von im Ausland überwachter Chatnachrichten im Strafverfahren. Zugleich Besprechung der EncroChat-Beschlüsse des OLG Bremen v. 18.12.2020 – 1 Ws 166/20, und OLG Hamburg v. 29.1.2021 – 1 Ws 2/21' (2021) 16 ZIS 452, 457.

[4] Zimmermann (n 1) 178.

lead to the evidence obtained being rendered inadmissible. Rather, the arguments for and against admitting the evidence are balanced against each other, taking into account the public interest in the investigation, the availability of other evidence, the weight of the offence as well as the intensity of the suspicions surrounding the defendant on one hand, and on the other hand whether the authorities had acted in good faith, whether the protective purpose of the breached provision applies to the breach in question and whether the authorities could hypothetically have acted within the confines of the law (*hypothetischer Ersatzeingriff*).

Initially, the Court identifies the offences in question as grave, being punishable with up to fifteen years imprisonment. Furthermore, the insights gained are deemed to be of considerable value to the investigations, while there had been no other comparably promising alternatives. Nor is there anything to suggest that the German authorities had intentionally circumvented stricter German rules, namely the sections 100a and following of the StPO. In fact, if the phones would have been distributed and surveilled by Germany, section 100a StPO would have been applicable. Lastly, the data collected was unrelated to the "taboo" core of the private sphere in the sense of the fundamental right to human dignity and one's personality. No protection of trust could be granted to someone who acquired a communications tool specifically for criminal purposes.

Consequently, the Court examines exclusively whether the *ordre public* or individual safeguards established by binding international law had been violated. A breach of Germany's sovereignty by virtue of accessing German data is rejected on grounds that such a breach would ultimately have been salvaged by the domestic attorney general's request for information. The fact that the US did not disclose the EU country which hosted the FBI's server also does not evidently hint at illegal behaviour on the side of the Americans, as the protection of a confidential source is not foreign to German law either. Reasonable suspicion that criminal deeds were being perpetrated was present in the use of the "*Anom*" phones, without such considerations constituting a general and unfounded suspicion targeted against telecommunication or even encryption which would touch the core guarantee of the right to private correspondence (Article 10 of the Basic Law – GG). Rather, those phones had been sold in sufficiently disreputable circles, for a high price of €1,000 to €1,500, suggesting that they should be used for grave offences. The FBI had also not provoked the criminal activities in question beyond providing the "*Anom*" phones methods of communication.

In conclusion, the Regional Court had correctly admitted the decrypted messages as evidence. The Court of Justice counters the defendant's argument regarding a "hearsay warrant" by noting that the Regional Court had not taken the messages as gospel but had instead scrutinised their authenticity.

E. Commentary

The aforementioned ruling extends the arguments brought forward in a prior ruling by the Federal Court of Justice in 2021.[5] There, French authorities (after obtaining a warrant) had gained access to a French Server enabling encrypted anonymous communications between users of specially sold "*EncroChat*" mobile phones. There had been reason to believe that people suspected of being involved in organized drug trade had used these phones in their operations. The decryption of a few thousand messages confirmed that these indeed related to illegal activities of the sort described. After obtaining another warrant, the authorities installed an intercepting device. First findings ascertained that 63.7% of all phones were used for criminal activities, with the rest being inactive or not yet surveyed. Europol informed the *Bundeskriminalamt* of serious felonies, after which the attorney general directed an EIO towards France, directed at the data relating to Germany and its use in German criminal procedures. The ensuing criminal procedures became the subject of many trials.

I. Standard of review

In its revision of a decision regarding one of these trials, the Federal Court had already recognized section 261 StPO as a sufficient basis for using information gained from the exchange in question.[6] It mentioned the rebuttable presumption for EU member states to act in compliance with EU law and especially the fundamental rights guaranteed by it.[7] The same presumption of legality is granted to the United States in the case at hand. Nevertheless, in both cases the Court assesses the question of proportionality. In the French case, this extends to both the proportionality of the EIO (Article 6 paragraph 1 letter b of the Directive) as well as the proportionality of the use of evidence. This differs from earlier, more restrictive jurisprudence where merely general principles of international law such as the right to a fair trial under Article 6 of the ECHR had been considered.[8] Section 100e paragraph 6 of the StPO regulates the usability of personal data obtained by remote searches and acoustic surveillance for criminal proceedings different from the one originally intended (*Zweckänderung*). Although the Court of Justice denied the immediate applicability of that provision (more explicitly in the French case than in the American one), it was applied analogously in order to specify the principle of

[5] BGH, Beschluss vom 02.03.2022 – 5 StR 457/21, NJW 2022, 1539.

[6] Demanding a more specific authorisation: Kai Cornelius, 'Anmerkung zu BGH, Beschluss vom 02.03.2022 – 5 StrR 457/21' (2022) 42 NStZ 1546, 1547; Anja Schmidt, 'Zur strafprozessualen Verwertbarkeit der Daten aus der Überwachung verschlüsselter Mobiltelefone durch einen anderen Mitgliedstaat der EU' (2022) 134 ZStW 982, 1004 ff.

[7] Directive 2014/41/EU of the European Parliament and of the Council of 3 April regarding the European Investigation Order in criminal matters [2014] OJ L130/1, recital 19.

[8] cf Wahl (n 3) 457-58, referring to BGH, Beschluss vom 21.11.2012 – 1 StR 310/12, NStZ 2013, 596.

proportionality, in the context of section 261.[9] These are, in principle, suitable limits to the use of evidence acquired from foreign authorities, within or outside the EU.

II. Probable cause

First and foremost, the use as evidence thus required that certain facts gave rise to the suspicion that serious offences had been committed or attempted (section 100b paragraph 1 and section 100c paragraph 1). Whether the strict requirements for undisclosed operations are met in situations resembling *Anom* and *EncroChat* is, ultimately, the most important but also divisive problem facing the judiciary. Previously, lower-tier decisions affirming the compatibility of the French measures with section 100e paragraph 6 had been criticized for substituting a general suspicion of every single user of *EncroChat* (or, consequently, the legitimate use of any other encrypted messaging services) for the required individual suspicion. From the point of view of sections 100e paragraph 6, considering the constitutional protection of personal data and storage, surveillance could not be used against initially unsuspicious citizens in order to discover the required suspicious facts.[10] The inappropriateness of these measures seems evident if one considers that had necessarily been no accusation of any specific offence.[11] Despite all this, Court of Justice nevertheless held it as sufficient that *EncroChat* was not a business model coincidentally suited for criminal activities, but indeed a network aligned towards committing sufficiently serious offences. These suspicions had been repeatedly and consistently confirmed when analysing the data. Thus, it seems that the use of information gained from mass surveillance of encrypted messengers is justified at least if those services are high-priced enough,[12] even though their users could theoretically be law-abiding citizens who are at the same time militant defenders of their own privacy. Assuming a hypothetically legal substitutionary measure is therefore highly problematic.

III. Rule of law

A breach of the right to fair trial – leading to the inadmissibility of the evidence – may also be inferred from the lack of information regarding the French investigative measures, by

[9] Regarding section 261 as a sufficient legal basis, see n 6. Affirming the immediate applicability of section 100e paragraph 6: OLG Hamburg, Beschluss vom 29.01.2021 – 1 Ws 2/21, BeckRS 2021, 2226 (decision by the Higher Regional Court of Hamburg); KG Berlin, Beschluss vom 30.08.2021 – 2 Ws 79/21, 2 Ws 93/21, NStZ-RR 2021, 353 (decision by the Higher Regional Court of Berlin). Denying a change of purpose, but also the usability of the evidence: LG Berlin, Beschluss vom 1.7.2021 – (525 KLs) 254 Js 592/20 (10/21), NStZ 2021, 696, 702 [81] – [83] (decision by the Regional Court of Berlin).

[10] Benjamin Derin and Tobias Singelnstein, 'Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat)' (2021) 41 NStZ 449, 452. Accordingly: LG Berlin (n 9) 698 [30] – [33].

[11] cf Zimmermann (n 1) 182.

[12] More explicit than the BGH in 2021 in this regard, foreshadowing the argument in the 2025 decision: KG Berlin (n 9) 354.

virtue of them being classified as military secrets.[13] Their concealment hinders counsel from charging an expert with producing a qualified evaluation of the technological framework.[14] It has been proposed that this be applied to the *Anom* case as well.[15]

None of the decisions discussed here had to deal with the question whether evidence is rendered unusable if German authorities intentionally circumvented stricter domestic requirements.[16] The full extent of Germany's involvement in the French case had not been known to the Federal Court when it made its 2021 decision.[17] Even if one does not infer abusive intent from these circumstances, one should nevertheless not compare the case at hand to cases where evidence is collected on the initiative of private citizens and not in long-term operations by foreign governments with the tacit approval of the German authorities.[18] Germany's responsibility for the procedure is aggravated by the provision of section 91g paragraph 6 of the Act on International Mutual Assistance in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen* – IRG), according to which German authorities may not just deny their authorization to foreign surveillance but must do so relatively swiftly if the measure would not be authorized in a comparable domestic case.[19] Aside from Germany's conduct, it is also clear that the US have actually acted contrary to the Court's presumption of legality and intentionally circumvented their own constitutional requirements in setting up the administrative triangle.[20]

IV. Conclusions

After the Court of Justice of the European Union had confirmed the decoupling of the legality of the collection of evidence from the legality of any transmissions,[21] the use of evidence gained from digital infiltration committed by foreign governments and more generally from measures of questionable legitimacy under German law ultimately became a question of the national approach to probable cause.[22] The BGH has continued its lax attitude towards justifying individual suspicions regarding the users of encrypted communications, all while refusing to monitor the rule of law in other jurisdictions. There

[13] Zimmermann (n 1) 189; Frank Meyer, 'Zusammenfassung und Besprechung von EuGH (GK), Urteil v. 30.4.2024' (2024) 7 GSZ 243, 250.

[14] LG Berlin, Beschluss vom 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22), MMR 2023, 453 [72] (decision by the Regional Court of Berlin).

[15] Meyer (n 13) 252.

[16] In favour: Jan-Hendrik Labusga, 'Anmerkung zu LG Berlin, Beschl. v. 1.7.2021 – (525 KLs) 254 Js 592/20 (10/21)' (2021) 41 NStZ 702, 704. Also EuGH (Große Kammer), Urteil vom 30.04.2024 – C/670/22 (MN), NJW 2024, 1723, 1728 [91] – [94] (decision by the Court of Justice of the European Union).

[17] LG Berlin (n 14) 456.

[18] LG Berlin (n 9) 701 [77].

[19] Reinhart Michalke, 'Anmerkung zu BGH, Urteil vom 9.1.2025 – 1 StR 54/24' (2025) 78 NJW 1589, 1589-90.

[20] ibid 1590.

[21] Meyer (n 13) 245.

[22] Karsten Gaede, 'Anmerkung zu EuGH, Urteil vom 30.4.2024 – C-670/22 (MN)' (2024) 77 NJW 1731, 1732.

is also reason to believe that the standards used to determine whether domestic requirements have been abusively bypassed are too narrow. Although the *EncroChat* and *Anom* measures seem to be effective, admitting their findings as evidence in criminal procedures lends credence to the expansion of the surveillance state and could lead to its extension into domains and communities not related to the black market. It would therefore be best to forsake the more collective-oriented approach and return to a case-by-case evaluation of every single user on their own merits.