Implikationen des EGMR Urteils Yüksel Yalcinkaya v. Türkiye (157669/20) für sog. EncroChat-Fälle

1. Nutzung eines Kryptodienstes als Beweis für strafbares Handeln

Zunächst ist zu berücksichtigen, dass sich die zugrunde liegenden Sachverhalte erheblich unterscheiden: Denn in dem Fall, über den der EGMR zu entscheiden hatte, war allein die Nutzung des Kommunikationsdienstes „ByLock“ der entscheidende Beweis für die Mitgliedschaft in der FETÖ/PDY gewesen. Die abstrakte Nutzung des Dienstes, ohne Ansehung der darüber versendeten Nachrichten, diente den türkischen Gerichten demnach als Beweis für die Begehung einer Straftat und war Grundlage für eine Verurteilung. Dies ist in den EncroChat-Urteilen anders: Hier liegen konkreten Nachrichten vor, die die Gerichte auswerten und aus denen sie die Begehung von Straftaten ableiten (etwa, weil über EncroChat Handelsgeschäfte vereinbart wurden etc.).

Die deutschen Ermittlungsbehörden sowie die deutschen Gerichte leiten allerdings z.T. aus der Nutzung von EncroChat einen *Tatverdacht* für die Begehung von Straftaten ab. Man könnte also unter Verweis auf das Urteil des EGMR darlegen, dass allein die Nutzung eines Kryptodienstes für eine Verurteilung nicht ausreicht und das Gleiche auch für die Frage des Bestehens eines Tatverdachtes gelten müsse. Die relevante Passage aus dem Urteil wäre m.E. Rn. 337 ff. Dort stellt der EGMR fest, dass die türkischen Gerichte die Behauptung, der Beschwerdeführer habe ByLock für organisationsbezogene Zwecke genutzt, nicht auf konkrete tatsächliche Feststellungen gestützt habe. Vielmehr seien sie allein von der ursprünglich vom MİT vorgebrachten Behauptung, ByLock sei „ausschließlich" von den Mitgliedern der FETÖ/PDY genutzt worden, ausgegangen.

Diese Behauptung scheint sich vor allem auf die technischen Merkmale der ByLock-App zu stützen, wie die Verschlüsselung, die Erfordernis, einen VPN zu verwenden und die automatische Löschung von Inhalten und einzelne entschlüsselte Nutzerprofile und Inhalte. Der EGMR stellt dann fest, dass die App „ByLock“ allerdings 2014-2016 frei verfügbar im Google Playstore war und 500.000 bis 1 Millionen Mal heruntergeladen worden sei. Außerdem seien einige der technischen Merkmale, aufgrund derer die türkischen Ermittlungsbehörden eine Nutzung ausschließlich von Mitgliedern der FETÖ/PYD angenommen habe, auch von anderen Diensten angeboten worden. Das Gericht fährt dann wie folgt fort:

> „340 While it is not the Court’s intention to draw any substantive conclusions from these factual assertions, they point to some palpable lacunae in the “exclusivity” and “organisational use” argument, which called for further explanation by the domestic courts as to how it was ascertained that ByLock was not, and could not have been, used by anyone who was not a “member” of the FETÖ/PDY within the meaning of Article 314 § 2 of the Criminal Code (see, for a similar finding, in the context of Article 5 § 1 of the Convention, Akgün, cited above, § 173). This is particularly so bearing in mind, once again, the apparently layered structure of the organisation, as noted in paragraph 266 above. The Court notes that the domestic courts, including the Court of Cassation in their landmark judgments, accepted the findings made primarily by the MİT, in an extrajudicial context, regarding the

> allegedly exclusive and organisational nature of ByLock and did not thoroughly scrutinise those findings."

Damit könnte man dafür argumentieren, dass die deutschen Gerichte ebenfalls nicht schlicht die Behauptung, EncroChat werde vor allem für kriminelle Zwecke genutzt, zur Konstruktion des Tatverdachts gegen alle Nutzer hätten übernehmen dürfen.

2. Zugriff auf Rohdaten

Entscheidend dürfte im Hinblick auf den Zugang zu den Rohdaten für Angeklagte, bzw. die Verteidigung, folgende Passage aus dem Urteil des EGMR sein:

> "327. The Court reiterates in this connection that the requirement of disclosure to the defence of "all material evidence" for or against the accused, which is an aspect of the right to adversarial proceedings (see Rowe and Davis, cited above, § 60), cannot be construed narrowly, in the sense that it cannot be confined to evidence considered as relevant by the prosecution. Rather, it covers all material in the possession of the authorities with potential relevance for the defence, even if not at all considered, or not considered as relevant by the prosecution authorities (see Rook, cited above, § 58). Accordingly, the fact that the applicant had access to all the ByLock reports included in the case file does not necessarily mean that he had no right or interest to seek access to the data from which those reports had been generated.
>
> 328. Similarly, the fact that the domestic courts found the ByLock data pertaining to the applicant to tally with another set of data that had been verified by an expert (see paragraph 80 above) did not necessarily remove the applicant's procedural rights with respect to those former data. It is stressed in this connection that the ByLock data in question were critical in the applicant's case, as it was those data which triggered the criminal proceedings against him. Essentially, they served not only to gather the individualised information on the applicant's alleged use of ByLock, but also constituted the basis for it to be characterised as an exclusively organisational communication tool (see the findings in the MİT report noted in paragraph 115 above) and thus led directly to the applicant's conviction. It may, moreover, not be excluded that the ByLock material potentially contained elements which could have enabled the applicant to exonerate himself, or to challenge the admissibility, reliability, completeness or the evidential value of that material (see Matanović, cited above, § 161)."

Diese Passage passt grundsätzlich gut auf den Zugang zu Rohdaten in den EncroChat-Fällen. Der EGMR relativiert diese Grundsätze aber im Anschluss, indem er ausführt, das Recht auf Zugang zu Beweismitteln sei kein absolutes (Rn. 329). Dem Betroffenen müssten aber zumindest die Gründe dafür erläutert werden, warum keine Einsicht in die Rohdaten erfolgen könnte. Zudem müssten die Daten von einer unabhängigen Stelle überprüft werden. Diese Prüfung müsste sich gerade auch auf die Rohdaten beziehen:

> “333. That said, given in particular the absence of any concrete information in the case file to suggest that the data in question had at any point been subjected to examination for verification of their integrity, whether at the time of their submission to the judicial authorities in December 2016 or subsequently, the Court considers that the applicant had a legitimate interest in seeking their examination by independent experts and that the courts had the duty of properly responding to him.”

Da es dem Beschwerdeführer nicht möglich gewesen sei, unmittelbaren Zugang zu den Beweismitteln zu erhalten, um die Daten selbst zu prüfen, hätten die Gerichte zum Ausgleich immerhin feststellen müssen, dass die Integrität und Richtigkeit der Daten in jeder Hinsicht sichergestellt worden waren, insbesondere auch in der Zeit vor der Übermittlung der Datenpakete an die Justizbehörden (Rn. 334):

> „The Court considers that, in principle, the inability of the defence to have direct access to the evidence and to test its integrity and reliability first-hand places a greater onus on the domestic courts to subject those issues to the most searching scrutiny.“

Nach dieser Argumentation müssten die Rohdaten in den EncroChat-Fällen den Betroffenen ebenfalls zur Verfügung gestellt werden, oder es müsste zumindest ein Gutachten über die Authentizität und Integrität dieser Daten von einer unabhängigen Stelle erstellt werden.

Allerdings führt der EGMR auch aus, dass der Beschwerdeführer – da er schon keinen Zugang zu den Rohdaten erhalten hätte – zumindest Zugang zu dem gesamten ihn betreffenden entschlüsselten Materials hätte erhalten müssen, um sich dazu äußern zu können (Rn. 335). In den EncroChat Fällen werden die entschlüsselten Daten den Akten beigefügt und den Betroffenen zur Verfügung gestellt. Es ist höchstens fraglich, ob es sich dabei wirklich um das gesamte einen Nutzer betreffende Material handelt. Ohne einen Abgleich mit den Rohdaten ist das kaum zu überprüfen.

Zusammenfassend lassen sich m.E. einige der Passagen als Stütze für Anträge auf Beiziehung der Rohdaten sowie Anträge auf Erstellung von IT-forensischer Gutachten auf Grundlage der Rohdaten herbeiziehen. Da in den EncroChat-Fällen lediglich der Tatverdacht auf die Nutzung der Handys gestützt wurde, nicht aber die Verurteilungen, sind die Passagen, welche die Nutzung des Kryptodienstes als Beweismittel betreffen, nur bedingt übertragbar.