Obergericht des Kantons Zürich

II. Strafkammer

Geschäfts-Nr.: SB240422-O/Z19/hb-nk

Mitwirkend: Oberrichter lic. iur. Spiess, Präsident, Oberrichterin lic. iur. Ohnjec und Oberrichter lic. iur. Weder sowie die Gerichtsschreiberin MLaw Blumer

Beschluss vom 15. August 2025

in Sachen

A._____,
Beschuldigter, Berufungskläger und Anschlussberufungsbeklagter

bis 9. Oktober 2024 amtlich verteidigt durch Rechtsanwalt lic. iur. X1._____,
ab 10. Oktober 2024 amtlich verteidigt durch Rechtsanwältin lic. iur. X2._____,

gegen

B._____ Bürgschaftsgenossenschaft,
Privatklägerin

vertreten durch Rechtsanwältin MLaw Y._____,

sowie

Staatsanwaltschaft II des Kantons Zürich,
Anklägerin, Berufungsbeklagte und Anschlussberufungsklägerin

betreffend **mehrfache qualifizierte Widerhandlung gegen das Betäubungsmittelgesetz etc. und Widerruf**

Berufung gegen ein Urteil des Bezirksgerichtes Dielsdorf, I. Abteilung, vom 19. Januar 2024 (DG230011)

Erwägungen:

I. Verfahrensgang

1. Mit Urteil vom 19. Januar 2024 sprach das Bezirksgericht Dielsdorf, I. Abteilung, den Beschuldigten von den Vorwürfen des mehrfachen Betrugs im Sinne von Art. 146 Abs. 1 StGB sowie der mehrfachen Urkundenfälschung im Sinne von Art. 251 Ziff. 1 StGB frei. Schuldig sprach es den Beschuldigten der mehrfachen Widerhandlung gegen das Betäubungsmittelgesetz im Sinne von Art. 19 Abs. 1 lit. b und c in Verbindung mit Art. 19 Abs. 2 lit. a BetmG sowie der Widerhandlung gegen das Betäubungsmittelgesetz im Sinne von Art. 19 Abs. 1 lit. c BetmG. Es bestrafte den Beschuldigten mit einer Freiheitsstrafe von 10 Jahren und 9 Monaten und widerrief den bedingten Vollzug der mit Strafbefehl der Staatsanwaltschaft Graubünden vom 14. Februar 2020 ausgesprochenen Geldstrafe von 30 Tagessätzen zu Fr. 230.–. Weiter verwies das Bezirksgericht den Beschuldigten im Sinne von Art. 66a StGB für 10 Jahre des Landes und verpflichtete ihn, Fr. 800'000.– als Ersatzforderung für den unrechtmässig erlangten Vermögensvorteil an den Staat zu zahlen. Es entschied über die Verwendung der beschlagnahmten Barschaft und weiterer beschlagnahmter Gegenstände sowie über die Frage der Vernichtung der Spuren und Spurenträger. Schliesslich regelte es die Kostenfolgen (Urk. 118 S. 100 ff.).

2. Gegen das mündlich eröffnete Urteil (Prot. I S. 26 ff.) liess der Beschuldigte rechtzeitig Berufung anmelden (Urk. 65; Art. 399 Abs. 1 StPO). Am 18. April 2024 meldete die B._____ Bürgschaftsgenossenschaft Berufung an (Urk. 95), liess sie jedoch mit Eingabe vom 9. September 2024 zurückziehen (Urk. 119). Die schriftliche Berufungserklärung des Beschuldigten erfolgte ebenfalls innert Frist (Urk. 122; Art. 399 Abs. 3 i.V.m. Art. 90 StPO). Das mit der Berufungserklärung gestellte Gesuch des Beschuldigten um Wechsel der amtlichen Verteidigung wurde mit Verfügung vom 30. September 2024 abgewiesen (Urk. 128). Nach erneutem Ersuchen des amtlichen Verteidigers sowie einer Eingabe des Beschuldigten (Urk. 131 und 132) wurde mit Verfügung vom 9. Oktober 2024 Rechtsanwalt lic. iur. X1._____ mit Wirkung ab 9. Oktober 2024 als amtlicher Verteidiger

des Beschuldigten entlassen und als neue amtliche Verteidigerin Rechtsanwältin lic. iur. X2._____ bestellt (Urk. 133). Am 21. Oktober 2024 wurde über die Fortsetzung der Sicherheitshaft verfügt (Urk. 140). Am 22. Oktober 2024 liess der Beschuldigte erklären, nicht beabsichtigt zu haben, die Berufung bezüglich des Freispruchs gemäss Dispositiv-Ziffer 1 zu erklären, und die Berufungsklärung vom 26. September 2024 in diesem Punkt zurückzuziehen (Urk. 142). Mit Verfügung vom 29. November 2024 wurde das Haftentlassungsgesuch des Beschuldigten abgewiesen (Urk. 164). Mit Beschluss vom 9. Dezember 2024 wurde vom Rückzug der Berufung des Beschuldigten betreffend Dispositiv-Ziffer 1 Vormerk genommen. Sodann wurde die B._____ Bürgschaftsgenossenschaft als Privatklägerin zugelassen und von ihrer Konstituierung als Zivil- und Strafklägerin sowie ihrem Rückzug der Berufung Vormerk genommen. Gleichzeitig wurde der Privatklägerin sowie der Staatsanwaltschaft II des Kantons Zürich Frist angesetzt, zu erklären, ob Anschlussberufung erhoben werde, oder um einen Nichteintretensantrag zu stellen (Urk. 168). Mit Eingabe vom 18. Dezember 2024 erklärte die Vertreterin der Staatsanwaltschaft II des Kantons Zürich Anschlussberufung (Urk. 172).

3. Am 27. Januar 2025 stellte die Verteidigung den Antrag, es sei das Berufungsverfahren zweizuteilen und in einem ersten Teil der Verhandlungsgegenstand einstweilen auf die Frage der Verwertbarkeit der SkyECC-Daten zu beschränken und sodann ein zweiter Teil innert der in Art. 408 Abs. 2 StPO vorgesehenen Frist anzuberaumen (Urk. 183). In der gleichen Eingabe beantragte die Verteidigung weiter, es sei auf die Anschlussberufung der Anklägerin nicht einzutreten sowie es seien Rohdaten der im Recht liegenden Chatdateien zu edieren (Urk. 183). Zu dieser Eingabe nahm die Staatsanwaltschaft am 12. Februar 2025 Stellung (Urk. 191). Die Antwort der Verteidigung darauf datiert vom 10. März 2025 (Urk. 193). Mit Beschluss vom 9. April 2025 wurde dem Antrag der Verteidigung entsprochen und die Parteivertreter wurden angehalten, am anberaumten

Gerichtstermin vom 6. Juni 2025 ausschliesslich zur Frage der Verwertbarkeit der SkyECC-Daten zu plädieren (Urk. 202).

4. Am 17. April 2025 liess der Beschuldigte verschiedene Beweisergänzungsantrage stellen (Urk. 208), welche mit Verfügung vom 23. April 2025 der Staatsanwaltschaft und der Privatklägerin zur Stellungnahme zugestellt wurden (Urk. 209). Die Stellungnahme der Staatsanwaltschaft datiert vom 9. Mai 2025 (Urk. 214) und eine diesbezügliche Antwort der Verteidigung vom 19. Mai 2025 (Urk. 221). Am 20. Mai 2025 reichte die Staatsanwaltschaft Beilagen in französischer und englischer Sprache ein und beantragte, diese seien zu den Akten zu nehmen (Urk. 222 und 223/1-3). Am 21. Mai wurde der Verteidigung Frist zur Stellungnahme zu diesem Antrag angesetzt (Urk. 224). Diese datiert vom 23. Mai 2025 (Urk. 226). Die Übersetzungen der Beilagen wurden am 27. Mai 2025 nachgereicht (Urk. 227 und 228/1-2) und der Verteidigung mit dem Hinweis zugestellt, dass das rechtliche Gehör zum damit zusammenhängenden Beweisantrag der Staatsanwaltschaft vom 20. Mai 2022 am Verhandlungstermin vom 6. Juni 2025 wahrzunehmen sei (Urk. 229). Die von der Staatsanwaltschaft eingereichten Unterlagen wurden zu den Akten genommen.

5. Die Berufungsverhandlung vom 6. Juni 2025 wurde auf das Thema der Verwertbarkeit der SkyECC-Daten beschränkt durchgeführt. Sie fand in Anwesenheit des Beschuldigten und seiner amtlichen Verteidigung sowie der Vertretung der Staatsanwaltschaft II des Kantons Zürich statt (Prot. II S. 20 ff.).

II. Rückweisung des Verfahrens an die Vorinstanz

1. Die Verteidigung beantragt die Rückweisung des Verfahrens an die Vorinstanz. Ihren Antrag begründet sie damit, dass die durch die Staatsanwaltschaft neu eingereichten Unterlagen (Urk. 223 bzw. Urk. 228) zahlreiche richterliche Genehmigungsentscheidungen während des gesamten Zeitraums der Überwachung enthielten, die Vorinstanz hingegen davon ausgegangen sei, dass alleine der Entscheid des Tribunal de Grande Instance de Lille vom 14. Juni 2019 (Urk. 1/16/2=Urk. 228/1/3=Urk. 223/2/3) – in Kombination mit der Genehmigung

durch das Zwangsmassnahmengericht des Obergerichts des Kantons Zürich vom 19. Dezember 2022 (Urk. 1/16/5) – für die Rechtmässigkeit der gesamten Beweiserhebung im Ausland genüge. Mit dem Bundesgericht sei festzuhalten, dass der inländisch vorgesehene Grundrechtsschutz durch eine zwangsmassnahmengerichtliche Genehmigung auch dann gewahrt sein müsse, wenn die Beweisabnahme im Ausland erfolge, was vorliegend fehle, sowie, dass dieses Manko nicht durch eine richterliche Genehmigung in der Schweiz kompensiert werden könne (Urk. 230 Rz. 30 ff.).

2. Weist das erstinstanzliche Verfahren wesentliche Mängel auf, die im Berufungsverfahren nicht geheilt werden können, so hebt das Berufungsgericht das angefochtene Urteil auf und weist die Sache zur Durchführung einer neuen Hauptverhandlung und Fällung eines neuen Urteils an das erstinstanzliche Gericht zurück (Art. 409 Abs. 1 StPO). Erforderliche zusätzliche Beweiserhebungen im Berufungsverfahren stellen grundsätzlich keinen schwerwiegenden Mangel im Sinne von Abs. 1 dar, der eine Rückweisung an die erste Instanz rechtfertigt, sondern sind aufgrund des reformatorischen Charakters der Berufung und des Beschleunigungsgebots vom Berufungsgericht selbst vorzunehmen (BGer 6B_1075/2019 E. 4; BSK StPO-KELLER, 3. Aufl., Basel 2023, Art. 409 N 1a).

3. Der von der Verteidigung vorgebrachte Einwand betrifft die Frage der Verwertbarkeit der SkyECC-Daten. Zwar ist es in der Tat so, dass der Vorinstanz lediglich der Entscheid des Tribunal de Grande Instance de Lille (Urk. 1/16/2=Urk. 228/1/3=Urk. 223/2/3) samt Genehmigung durch das Zwangsmassnahmengericht des Obergerichts des Kantons Zürich vom 19. Dezember 2022 (Urk. 1/16/5) zur Verfügung stand und die Staatsanwaltschaft die weiteren Entscheide der französischen Gerichte erst kurz vor der Berufungsverhandlung vom 6. Juni 2025 einreichte. Es handelt sich hierbei aber um zulässige zusätzliche Beweiserhebungen vor Berufungsinstanz und nicht um einen Fehler der Vorinstanz, der nicht behoben werden kann. Vor diesem Hintergrund ist der Antrag des Beschuldigten auf Rückweisung des Verfahrens an die Vorinstanz abzu-

weisen. Vielmehr hat sich das Berufungsgericht mit der Frage der Verwertbarkeit der SkyECC-Daten selbst auseinanderzusetzen.

III. Frage der Verwertbarkeit der SkyECC-Daten

1. Vorbemerkungen

1.1. Anzumerken ist, dass die im Recht liegenden Akten es dem hiesigen Gericht nicht ermöglicht haben, sich ein schlüssiges und lückenloses Bild über die Erhebung der SkyECC-Daten zu machen. Hinsichtlich der Fragen zum Ablauf der Erhebung sowie der französischen Verfahren bzw. deren Zweck ergeben sie ein unvollständiges bzw. lückenhaftes Gesamtbild, sodass sich das hiesige Gericht, um den Hintergrund nachvollziehen zu können, Informationen aus dem Internet bzw. aus zur Frage der SkyECC-Daten ergangenen ausländischen Entscheiden holen musste. Es bleibt aber die Erkenntnis, dass auch eine fundierte Recherche nicht gewährleistet, dass keine Lücken bezüglich massgebender Fakten bestehen bleiben, zumal die an der Erhebung der Daten beteiligten Behörden hinsichtlich bestimmter Umstände ein Geheimhaltungsinteresse geltend machen.

1.2. Bei der Applikation SkyECC handelte es sich um eine serverbasierte Kommunikationsplattform, welche vom kanadischen Unternehmen "Sky Holding Global Inc." betrieben wurde und auf speziell präparierten Mobiltelefonen der Marken "Nokia", "BlackBerry", "Apple iPhone" und "Google Pixel" ihren Nutzern eine verschlüsselte Kommunikationsmöglichkeit anbot. Die jeweiligen Entschlüsselungscodes waren auf den Geräten der Benutzer gespeichert und die versendeten Daten konnten somit lediglich vom Absender und vom Empfänger eingesehen werden. Die Mobiltelefone waren vorkonfiguriert, wurden anonym gekauft und ein Abonnement konnte für bis zu sechs Monaten abgeschlossen werden; danach war der Kauf eines neuen Mobiltelefons notwendig. Die benötigte technische Lösung wurde durch die in Frankreich, Roubaix, domizilierte Firma "OVH SAS" implementiert. Diese betrieb zunächst zwei Server, den Hauptserver (Server 1) und den Backup-Server (Server 2), welche mit einem Intranet-Netzwerk verbunden waren. Ab September 2020 kam ein dritter Server dazu (vgl. dazu eingehender Urk. 1/16/3).

2. Erhebung der SkyECC-Daten

2.1. Am 13. Februar 2019 eröffnete die Staatsanwaltschaft Lille in Frankreich eine Voruntersuchung betreffend Beteiligung an einer kriminellen Vereinigung mit der Absicht der Vorbereitung von Verbrechen oder Vergehen, die mit zehn Jahren Freiheitsstrafe bestraft werden (Betäubungsmitteldelikte sowie Straftaten gegen die Gesetzgebung über kryptologische Mittel bzw. Verschlüsselungsverfahren; Urk. 1/16/2=Urk. 228/1/3=Urk. 223/2/3). An den Ermittlungen beteiligten sich im Rahmen einer gemeinsamen Ermittlungsgruppe neben den französischen, belgischen und niederländischen Strafverfolgungsbehörden auch Eurojust und Europol. Die niederländischen Behörden übermittelten eine Aufstellung von etwa 9'000 Mitteilungen französischer SkyECC-Nutzer aus dem Zeitraum 2016 bis Mitte 2017, deren Kommunikationsinhalte sich hauptsächlich auf den Handel mit Betäubungsmitteln (Kokain und Cannabis) bezogen. Auf Antrag der Staatsanwaltschaft Lille genehmigte am 14. Juni 2019 ein Richter des Tribunal de Grande Instance de Lille auf der Grundlage der Artikel 706-73, 706-73-1 und 706-95, 100, 100-1 und 100-3 bis 100-8 der französischen Strafprozessordnung (Code de procédure pénale) sowie des Artikels L.32 des französischen Gesetzbuchs über die Post und die elektronische Kommunikation (Code de postes et des communications électroniques) für die Dauer von einem Monat das Abfangen, das Aufzeichnen und die Transkription der elektronischen Kommunikation zwischen dem Haupt- und dem Sicherungsserver sowie der ein- und ausgehenden elektronischen Kommunikation des Hauptservers (Urk. 1/16/2=Urk. 228/1/3=Urk. 223/2/3; vgl. BGH, Beschluss vom 9. Januar 2025 - 1 StR 142/24 Rn. 13-18).

2.2. Die Nachrichten der Nutzer und die damit verbundenen Metadaten konnten zwar abgefangen sowie die von SkyECC vergebenen Nutzerkennzahlen mit den IMEI-Nummern der Endgeräte in Verbindung gebracht werden. Eine Entschlüsselung der Nachrichten war jedoch nicht möglich. Auf Antrag der Staatsanwaltschaft Lille genehmigte ein Richter des Tribunal de Grande Instance de Lille die Verlängerung der Überwachungsmassnahme am 22. Juli 2019 zunächst für einen weiteren Monat (Urk. 228/1/4=Urk. 223/2/4). Anschliessend wurde die Massnahme am 20. August 2019 für weitere zwei und am 18. Oktober 2019 für weitere vier Mo-

nate (Urk. 228/1/9=Urk. 223/2/9), im Ergebnis also bis zum 20. Februar 2020, genehmigt (Urk. 228/1/8=Urk. 223/2/8).

2.3. Da nur die Hälfte der SkyECC-Kommunikation abgefangen werden konnte, beantragte der Polizeidivisionskommandant am 25. November 2019, den gesamten externen Netzwerkverkehr (Internet) der beiden Server zu überwachen. Am 13. Dezember 2019 erliess das Tribunal de Grande Instance einen Auftrag zur Überwachung des Hauptservers für vier Monate bis zum 13. April 2020 (Urk. 228/1/14=Urk. 223/2/14). Die Überwachung des Back-Up Servers sowie diejenige des internen Servers kamen dazu, wobei die Überwachungen laufend verlängert wurden (vgl. u.a. Urk. 228/1/6=Urk. 223/2/6, Urk. 228/1/7=Urk. 223/2/7, Urk. 228/1/11=Urk. 223/2/11, Urk. 228/1/17=Urk. 223/2/17, Urk. 228/1/5=Urk. 223/2/5, Urk. 228/1/9=Urk. 223/2/9).

2.4. Am 17. Dezember 2020 genehmigte ein Richter des Tribunal Judiciaire de Paris die Einrichtung der technischen Vorrichtung "Man-in-the-Middle" ("MITM") für vier Monate (Urk. 228/1/20=Urk. 223/2/20). MITM stellt einen an der externen Verbindung des Sicherungsservers angeschlossenen Server dar, welcher in der Lage war, die bei Versand einer Nachricht übermittelten kryptografischen Elemente, die für die Entschlüsselung der vom betreffenden Gerät erhaltenen individuellen Nachrichten erforderlich waren, zu erfassen. Der Zweck des MITM war es, die Schlüssel erhältlich zu machen, um die Kommunikation – welche im Rahmen der bisher erfolgten Überwachung der Server zwar abgefangen, aber nicht gelesen werden konnte – zu entschlüsseln.

2.5. Das Gerät wurde am 18. Dezember 2020 installiert und aktiviert (Urk. 228/1/7=Urk. 223/2/7, jeweils S. 12). Am 19. Februar 2021 verzeichneten die niederländischen Ermittler einen erheblichen Rückgang der entschlüsselten Nachrichten. Eine Untersuchung ergab, dass Änderungen in der Infrastruktur vorgenommen wurden und die verschlüsselten Daten nicht mehr nur über den Sicherungsserver, sondern auch über den Hauptserver liefen. Am 24. Februar 2021 genehmigte ein Richter des Tribunal Judiciaire de Lille die Installation eines zweiten, identischen Erfassungsgeräts auf dem Hauptserver für vier Monate (Urk. 228/1/25=Urk. 223/2/25). Am 9. März 2021 beschlagnahmte die Polizei die

drei Server in Roubaix (Urk. 228/1/27=Urk. 223/2/27). Gemäss Eurojust-Jahresbericht kam es im Zuge des Aktionstags am 9. März 2021 nicht nur zu einer Vielzahl von Festnahmen, sondern auch zu zahlreichen Hausdurchsuchungen und Beschlagnahmen in Frankreich, Belgien und den Niederlanden (vgl. https://www.eurojust.europa.eu/ar2021, S. 26, zuletzt besucht am 11. August 2025).

3. Funktionsweise der "Man-in-the-Middle"-Technik

3.1. Im Bericht der niederländischen Kriminalpolizei zur "Erklärung des Erhalts, der Übermittlung und Verarbeitung der abgefangenen Daten" wird unter dem Titel "7. Datenverarbeitung" festgehalten, dass die Analyse der auf dem Untersuchungsnetzwerk abgespeicherten IP-TAP-Daten aufgezeigt habe, dass die überwachte IP-Kommunikation verschlüsselte Kommunikation enthalten habe. Das für die lesbare Darstellung der Gespräche benötigte Schlüsselmaterial habe sich nicht in diesen, mit einem IP-TAP abgefangenen Streaming-Daten befunden, sondern sei mittels MITM erhalten worden. Sky (gemeint die in Canada domizilierte "Sky Global Holdings Inc. Jean-Francois") habe für die Verschlüsselung von Nachrichten zwischen zwei Nutzern eine sogenannte Public-Key-Verschlüsselung verwendet. Das bedeute, dass ein Nutzer über ein Schlüsselpaar – bestehend aus einem privaten und einem öffentlichen Schlüssel – verfüge. Ein Sender verwende den öffentlichen Schlüssel eines Empfängers, um die Nachrichten zu verschlüsseln. Der Empfänger verwende dann seinen privaten Schlüssel, um die Nachrichten zu entschlüsseln. In der Praxis sei diese Technik für die Nutzer der SkyECC-App fast unsichtbar; dieses Verfahren werde von der SkyECC-App ausgeführt. Der private Schlüssel eines Nutzers entschlüssle nur Nachrichten, die mit einem öffentlichen Schlüssel, der dem privaten Schlüssel des Nutzers gehöre, verschlüsselt seien. Daher sei es nur unter Verwendung des privaten Schlüssels des Empfängers einer Nachricht möglich, den Inhalt der verschlüsselten, abgefangenen Nachrichten zwischen zwei Nutzern lesbar darzustellen (Urk. 228/2/7=Urk. 223/3/7, jeweils S. 3 und 10).

Im genannten Bericht wird unter "9. Man-in-the-Middle" weiter angegeben, dass die holländischen Ermittler eine Konzeptionstechnik entwickelt hätten, um die auf jedem Telefon mit SkyECC-App gespeicherten "decryption elements" zu erhalten. Die Technik basiere auf der Installation eines Servers, der die Rolle des "Man-in-the-Middle" übernehme und an den Server 2 (Sicherungsserver) habe angebracht werden müssen. Dieser MITM-Server, der in demselben Datenzentrum in der Nähe von Server 2 sei, erhalte den Datenstrom von Nutzertelefonen an Server 2 und umgekehrt. Sobald sich ein SkyECC-Telefon an den Server 2 einlogge, sende der MITM-Server eine speziell erstellte Push-Nachricht, die normalerweise auf diesem Telefon nicht sichtbar sei, mit dem einzigen Zweck, eine Reaktion des Telefons und somit eine Freisetzung von Verschlüsselungselementen zu erhalten, die für die Entschlüsselung der vom Telefon empfangenen Individualnachrichten nötig seien. Die entsprechende Passage lautet in der Originalfassung bzw. auf Englisch wie folgt: "When a SKY phone logs in to server 2, the MITM server sends a specially designed push message that is normally invisible to this phone, with the sole purpose of urging the phone to react and thus release the encryption elements necessary to decrypt the individual messages received by the phone." Diese Daten würden mithilfe des MITM-Systems abgefangen und nicht an Server 2 retourniert. Alle weitere Kommunikation der Telefone werde ohne Änderungen an Server 2 weitergeleitet und umgekehrt, sodass die entschlüsselte Serverkommunikation normal weiterfunktioniere (vgl. Urk. 228/2/7=Urk. 223/3/7, jeweils S. 12).

3.2. In den Erwägungen im Entscheid des Tribunal Judiciaire de Paris vom 17. Dezember 2020, mit welchem die Einrichtung der MITM-Vorrichtung genehmigt wurde, wird festgehalten, dass die Entschlüsselung der einzelnen Nachrichten nicht allein auf der Grundlage der abgefangenen Daten erfolgen könne. Der Grund dafür sei, dass nur der Teil der kryptografischen Elemente, welcher von den Telefonen an die Server übertragen werde, aus den abgefangenen Daten wiederhergestellt werden könne; der andere Teil der kryptografischen Elemente sei hingegen nur auf den Telefonen gespeichert. Zur Funktionsweise der MITM-Technik wird erwogen, dass bei Authentifizierung eines SkyECC-Telefons bei Server 2 der MITM eine speziell gestaltete und normalerweise unsichtbare Push-

Nachricht an dieses Telefon generiere, deren einziger Zweck darin bestehe, das Telefon zu veranlassen, die kryptografischen Elemente zu übermitteln, die für die Entschlüsselung der von diesem Telefon empfangenen individuellen Nachrichten erforderlich seien. Diese Elemente würden von der MITM-Einrichtung erfasst, aber nicht an den Server 2 zurückgesendet. Weiter wird festgehalten, dass – da eine Analyse der SkyECC-Terminals nicht möglich sei – die Verschlüsselung der von den Nutzern ausgetauschten Daten, die alle über den Server in Roubaix liefen, nur durch die Installation eines Datenerfassungsgeräts umgangen werden könne. Der Einsatz dieses Geräts, das die bereits eingerichtete Überwachung der Server ergänze, sei die einzige Möglichkeit, die individuellen Nachrichten der Nutzer der SkyECC-Telefone zu klären. Schliesslich sei die Installation dieser Vorrichtung zu genehmigen, um die kryptografischen Elemente aller Telefone, die die SkyECC-Verschlüsselungslösung verwenden würden, zu erfassen, welche in Verbindung mit den aus den Überwachungsmassnahmen gewonnenen kryptografischen Elementen die Entschlüsselung der einzelnen, von diesen Telefonen empfangenen Nachrichten ermöglichen würden (Urk. 228/1/20=Urk. 223/2/20, jeweils S. 4).

3.3. Die Anwendung der MITM-Methode wurde per 17. Dezember 2020 gerichtlich genehmigt (Urk. 228/1/20=Urk. 223/2/20). Die Anklagesachverhalte B und C betreffen die Zeit vor und der Anklagesachverhalt D die Zeit nach der genannten Genehmigung. Die Verteidigung stellt in diesem Zusammenhang die Frage, wie es denn möglich gewesen sei, die Nachrichten aus der Zeit vor dem 17. Dezember 2020 zu entschlüsseln (vgl. Urk. 230 Rz. 108 ff.). Angesichts der oben zitierten Erläuterungen, wonach jeder Nutzer einen privaten und einen öffentlichen Schlüssel hat, wird davon ausgegangen, dass, sobald der bzw. die Schlüssel erhältlich gemacht werden konnten, die dazugehörige – auch davor abgefangene und gespeicherte – Kommunikation des betreffenden Nutzers entschlüsselt werden konnte.

3.4. Die Ausführungen im Bericht der niederländischen Kriminalpolizei sowie in dem die Anwendung der MITM-Methode genehmigenden Entscheid des Tribunal Judiciaire de Paris vom 17. Dezember 2020 machen deutlich, dass zwischen zwei

unterschiedlichen Datenabschöpfungsmethoden zu unterscheiden ist. Die Kommunikation zwischen den Nutzern der SkyECC-Telefone wurde mittels der zwei Server in Roubaix abgefangen bzw. die entsprechenden Daten wurden aus den Servern abgeleitet. Auf diese Art wurden die Daten gesammelt, konnten aber mangels entsprechender Schlüssel, die nicht auf die gleiche Weise wie die Kommunikation abgefangen werden konnten, nicht gelesen werden. Um die abgefangene Kommunikation lesbar zu machen, bestand als einzige damals technisch bekannte Methode diejenige des MITM, welche so funktionierte, dass mittels einer Push-Nachricht auf das SkyECC-Telefon eines Nutzers zugegriffen und dieses dazu gebracht wurde, den ihm zugewiesenen Schlüssel zu übermitteln (vgl. dazu auch die Verteidigung in Urk. 230 Rz 103 ff.). Die entsprechenden Schlüssel bzw. "decryption elements" waren nur auf den Telefonen gespeichert. Diese Entschlüsselungselemente wurden nicht vom Server, sondern mittels des MITM – im Sinne einer Trojanersoftware – von den Endgeräten ausgeleitet. Im Gegensatz zum Abfangen der Kommunikation des Beschuldigten durch Server in Roubaix, was keinen Zugriff auf das Endgerät des Beschuldigten voraussetzte, wurden die für die lesbare Darstellung seiner Kommunikation benötigten und nur auf seinem SkyECC-Telefon befindlichen Entschlüsselungselemente durch Zugriff auf sein Schweizer Endgerät erhältlich gemacht.

4. Verletzung des Territorialitätsprinzips

4.1. Im internationalen Strafrecht gilt der Grundsatz der Territorialität. Nach diesem kann ein Staat die mit seiner Souveränität verbundenen Befugnisse – darunter die Strafverfolgungsgewalt – nur innerhalb seines eigenen Gebietes ausüben. Die Staaten müssen somit gegenseitig ihre Souveränität beachten. In Anbetracht dieses Grundsatzes ist ein Staat auch nicht ermächtigt, Untersuchungs- und Strafverfolgungsmassnahmen auf dem Gebiet eines anderen Staates ohne dessen Zustimmung vorzunehmen. Von einem Staat oder seinen Beamten auf dem Gebiet eines anderen Staates ohne eine solche Zustimmung vorgenommene hoheitliche Akte sind somit unzulässig und stellen eine Verletzung der Souveränität und der territorialen Integrität des betroffenen Staates dar, was einer Verletzung des Völkerrechts gleichkommt. Eine Verletzung des Territorialitätsprinzips kann

auch erfolgen, wenn der verfolgende Staat sich mittels objektiv als unfair beurteilten Mitteln Beweismittel oder von Sicherungsmassnahmen betroffene Vermögenswerte namentlich unter Verletzung der für die internationale Rechtshilfe in Strafsachen geltenden Regeln beschafft. Nicht nötig ist, dass die Behörde auf ausländischem Gebiet gehandelt hat, um die Souveränität des ausländischen Staates zu verletzen; es genügt, dass ihre Handlungen Wirkungen auf dem Gebiet dieses Staates entfalten. Zu den amtlichen Handlungen, die das Territorialitätsprinzip und die Souveränität eines anderen Staates beachten müssen, zählt namentlich der Einsatz von technischen Überwachungsgeräten im Sinne von Art. 280 StPO. Der Einsatz von technischen Überwachungsgeräten im Hoheitsgebiet eines fremden Staates ist nach der Rechtsprechung nur zulässig, wenn die Strafbehörden dazu nach internationalem Recht ermächtigt sind oder der betroffene Staat nach den Regeln der internationalen Rechtshilfe sein (grundsätzlich vorgängig einzuholendes) Einverständnis erteilt hat. Unter Verletzung des Territorialitätsprinzips mittels technischer Überwachungsgeräte gewonnene Erkenntnisse sind absolut unverwertbar (BGE 146 IV 36 E. 2; bestätigt in den Urteilen 7B_120/2022 vom 5. Oktober 2023 E. 2.4; 1B_93/2021 vom 19. Juli 2021 E. 2; 1B_302/2020 vom 15. Februar 2021 E. 3; 7B_273/2023, 7B_274/2023, 7B_275/2023, 7B_276/2023 vom 11. April 2024 E. 2).

4.2. Sowohl das Bundesgesetz über internationale Rechtshilfe in Strafsachen (IRSG, SR 351.1) als auch entsprechende bilaterale Übereinkommen (einsehbar auf https://www.rhf.admin.ch/rhf/de/home/rechtshilfefuehrer/laenderindex.html) setzen für Beweiserhebungen eines ausländischen Staates in der Schweiz ein internationales Rechtshilfeersuchen voraus. Es besteht keine Rechtsgrundlage, welche Beweiserhebungen auf schweizerischem Hoheitsgebiet durch Organe eines fremden Staates ohne Kenntnis der zuständigen Schweizer Behörden bzw. ein entsprechendes Ersuchen zuliesse.

4.3. Die Verteidigung führt ins Recht, dass sich der Beschuldigte (und damit auch sein SkyECC-Handy) zum Zeitpunkt des Zugriffs auf sein SkyECC-Handy mittels der MITM-Methode in der Schweiz befunden habe (Urk. 230 Rz. 116), was von der Staatsanwaltschaft nicht in Frage gestellt wurde. Von diesem Umstand ist

daher auszugehen, zumal keine Hinweise für das Gegenteil vorliegen und der Beschuldigte zu diesem Zeitpunkt auch seinen Wohnsitz in der Schweiz hatte. Der Zugriff mittels der MITM-Methode auf das SkyECC-Handy des Beschuldigten gilt damit als auf Schweizer Gebiet erfolgt.

4.4. Festgehalten werden kann somit, dass die in Frankreich installierte MITM-Technik hinsichtlich des Zugriffs auf das SkyECC-Handy des Beschuldigten Wirkung auf dem Gebiet der Schweiz entfaltete. Wenn die Staatsanwaltschaft gegen die Entfaltung einer Wirkung der MITM-Methode auf dem Gebiet der Schweiz ausführt, bei der Untersuchung in Sachen SkyECC in Frankreich seien die Kommunikationsserver in Frankreich durch französische Behörden ausgeleitet worden, wodurch es sich aus französischer Sicht nicht um Souveränität verletzende extraterritoriale Hoheitsakte gehandelt habe (vgl. Prot. II S. 33), ist darauf hinzuweisen, dass dies lediglich auf die Methode des Abfangens der Kommunikation der Nutzer zutrifft. Hingegen konnten die zur lesbaren Darstellung der abgefangenen Nachrichten benötigten Entschlüsselungselemente auf diese Weise nicht erhältlich gemacht werden. Um die jedem Nutzer zugewiesenen Schlüssel zu erhalten, war es nötig, die MITM-Methode anzuwenden und eine Push-Nachricht direkt auf das Telefon des Nutzers zu schicken, um das Telefon zu veranlassen, den auf diesem gespeicherten Schlüssel zu übermitteln. Diese Methode bediente sich damit nicht lediglich der in Frankreich verorteten Server, sondern griff direkt in die Geräte der Nutzer ein und entfaltete damit ihre Wirkung im Falle des Beschuldigten in der Schweiz (so auch LG Berlin, Entscheid. v. 19.12.2024 – [525 KLs 8/22] 279 Js 30/22, E. 198 ff. betreffend Unverwertbarkeit der EncroChat-Daten infolge Verletzung des Territorialitätsprinzips durch Infiltration von EncroChat-Endgeräten mittels Trojanersoftware mit Wirkung auf deutsches Staatsgebiet).

4.5. Dass Frankreich die zuständigen Schweizer Behörden um Rechtshilfe im Zusammenhang mit der Anwendung der MITM-Methode auf Schweizer Staatsgebiet ersucht haben soll, geht aus den Akten nicht hervor und wird von der Staatsanwaltschaft auch nicht behauptet. Der Zugriff auf das Gerät des Beschuldigten erfolgte damit in unzulässiger Weise und stellt eine Verletzung der Souveränität und der territorialen Integrität der Schweiz dar, was – gemäss oben zitierter bun-

desgerichtlicher Rechtsprechung – einer Verletzung des Völkerrechts gleichkommt.

5. Absolute Unverwertbarkeit der SkyECC-Daten

5.1. Nach Art. 141 Abs. 1 StPO sind Beweise, welche in Verletzung von Art. 140 StPO erhoben wurden oder von der Strafprozessordnung als unverwertbar bezeichnet werden, in keinem Falle verwertbar. Die Staatsanwaltschaft beruft sich auf Art. 141 Abs. 2 StPO, gemäss welchem Beweise, selbst wenn sie in strafbarer Weise oder unter Verletzung von Gültigkeitsvorschriften erhoben wurden, verwendet werden dürfen, wenn sie zur Aufklärung schwerer Straftaten unerlässlich sind. Dies sei hier im Falle von Verbrechen gegen das Betäubungsmittelgesetz der Fall. Auch sei die Unerlässlichkeit gegeben, lasse sich nur dank der SkyECC-Daten nachweisen, dass der Beschuldigte mit Kokain gehandelt habe (Urk. 60 S. 1 f., Urk. 1/16/3 S. 7).

5.2. Gemäss der oben (E. 4.1) zitierten bundesgerichtlichen Rechtsprechung sind unter Verletzung des Territorialitätsprinzips mittels technischer Überwachungsgeräte gewonnene Erkenntnisse absolut unverwertbar (BGE 146 IV 36 E. 2; bestätigt in den Urteilen 7B_120/2022 vom 5. Oktober 2023 E. 2.4; 1B_93/2021 vom 19. Juli 2021 E. 2; 1B_302/2020 vom 15. Februar 2021 E. 3; 7B_273/2023, 7B_274/2023, 7B_275/2023, 7B_276/2023 vom 11. April 2024 E. 2). Für die Ausnahmeregel von Art. 141 Abs. 2 StPO bleibt vorliegend kein Raum und es kann festgehalten werden, dass die in den Akten liegenden SkyECC-Daten absolut unverwertbar sind. Zur Frage der Verwertbarkeit von durch nicht genehmigte Überwachungen gewonnenen Erkenntnissen vgl. entsprechende Erwägungen unten E. IV.1.3.1.

5.3. Die Aufzeichnungen über unverwertbare Beweise werden aus den Strafakten entfernt, bis zum rechtskräftigen Abschluss des Verfahrens unter separatem Verschluss gehalten und danach vernichtet (Art. 141 Abs. 5 StPO). Vorliegend befinden sich die aus Frankreich erhaltenen SkyECC-Daten auf CDs (Urk. 1/14/8 und Urk. 1/15/9). In weiteren Urkunden finden sich Transkriptionen der auf den

CDs erhaltenen Files (u.a. Urk. 1.1.5.1.-3., Urk. 1.1.6.1.-4., Urk. 1.1.7.1.-2., Urk. 1.1.8.1.-3.). Letztlich weisen sämtliche Akten der Sachverhalte B, C und D einen Bezug zu SkyECC-Daten auf: sowohl die Polizeiberichte als auch die Einvernahmen und Sachverständigengutachten. Dies liegt daran, dass die Übermittlung dieser SkyECC-Daten den Auslöser für die Anklageerhebung hinsichtlich der Sachverhalte B, C und D gab, wobei die SkyECC-Daten bezüglich der genannten Sachverhalte auch die einzigen Beweismittel darstellen. Die Unverwertbarkeit der SkyECC-Daten wirkt sich damit hinsichtlich der Sachverhalte B, C und D auf sämtliche Akten aus.

IV. Weitere Fragen im Zusammenhang mit der Erhebung und Verwertung von SkyECC-Daten

1. Voraussetzungen für die Gutheissung von ausländischen Rechtshilfeersuchen sowie die Verwertung von im Ausland erhobenen Beweisen

Der Vollständigkeit halber und der Bedeutung des Streitgegenstandes Rechnung tragend sind – trotz der Unverwertbarkeit der SkyECC-Daten infolge der Verletzung des Territorialitätsprinzips (vgl. dazu oben E. III.5) – die Fragen zu beantworten,

- (1) ob Schweizer Behörden einem französischen Rechtshilfeersuchen um Überwachung mittels der MITM-Technik entsprochen hätten (Frage der Voraussetzungen für die Gutheissung von ausländischen Rechtshilfeersuchen) sowie

- (2) ob mittels der in Frankreich erfolgten Serverüberwachung (und ohne auf das Schweizer Hoheitsgebiet zugreifenden MITM-Methode) erhobene SkyCC-Daten im vorliegenden Verfahren verwertbar wären (Frage der Verwertung von im Ausland erhobenen Beweisen).

1.1. Für die Beantwortung der beiden Fragen anwendbares Recht

1.1.1. Bei der Überwachung und dem Abfangen der SkyECC-Daten handelt es sich um eine geheime Überwachungsmassnahme nach Art. 269 ff. StPO. Ob in

der Schweiz einem ausländischen Rechtshilfeersuchen um Überwachungsmassnahmen zu entsprechen ist, richtet sich nach den Art. 269 ff. StPO (vgl. Art. 18a Abs. 4 IPRG). Ebenso befindet über die Verwertbarkeit eines im Ausland erhobenen Beweises das in der Schuldfrage entscheidende Gericht grundsätzlich nach den Vorgaben seiner Rechtsordnung. Dies gilt unabhängig davon, ob Überwachungsergebnisse rechtshilfeweise gewonnen oder aber im Ausland autonom, mithin unabhängig von einem (schweizerischen) Rechtshilfeersuchen erhoben worden sind und damit bei der Übernahme eines Strafverfahrens bereits vorliegen (BGer, 6B_1353/2023, 6.11.2024, E. 4.3.2.1 mit Verweis auf BGE 138 IV 169 E. 3.1).

1.1.2. Damit beantworten sich sowohl die Frage (1), ob Schweizer Behörden einem entsprechenden Rechtshilfeersuchen aus Frankreich entsprochen hätten, wie auch die Frage (2), ob mittels der in Frankreich erfolgten Serverüberwachung erhobene SkyECC-Daten im vorliegenden Verfahren verwertbar wären, nach Schweizer Recht.

1.2. Voraussetzungen der Überwachungsmassnahmen nach Art. 269 ff. StPO

1.2.1. Die Überwachung der Telekommunikation setzt nach Art. 269 Abs. 1 lit. a StPO den dringenden Tatverdacht auf ein sog. Katalogdelikt (Art. 269 Abs. 2 StPO) voraus. Der Tatverdacht muss nach der Rechtsprechung auf "konkreten Umständen und Erkenntnissen" beruhen und eine gewisse Wahrscheinlichkeit des Schuldspruchs schaffen (BSK StPO-JEAN-RICHARD-DIT-BRESSEL, 3. Aufl., Basel 2023, Art. 269 N 35).

1.2.2. Die Staatsanwaltschaft liess die SkyECC-Daten des Beschuldigten als Zufallsfund vom Zwangsmassnahmengericht des Obergerichts des Kantons Zürich am 19. Dezember 2022 genehmigen (Urk. 1/16/5). In diesem Zusammenhang ist auf einen danach zur Operation ANOM – Kommunikationsüberwachung sämtlicher rund 12'000 (vermeintlich) abhörsicherer Geräte (ANOM-Kryptohandys) – ergangenen Bundesgerichtsentscheid hinzuweisen, in welchem dieses erwog, dass Art. 296 ff. StPO auf Beweise, welche nicht von schweizerischen Strafbehörden,

sondern von ausländischen Behörden erlangt worden seien, keine Anwendung fänden (Urteil vom 11. Januar 2024, 7B_159/2022 und 7B_160/2022 [= BGE 150 IV 139] E. 5.6.). Es handle sich im Falle der durch die Überwachung erlangten Daten über den dortigen Beschuldigten, deren Zurverfügungstellung man gezielt rechtshilfeweise angefragt habe, auch nicht um Zufallsfunde (a.a.O. E. 5.8.). Demnach sei das Zwangsmassnahmengericht für einen Genehmigungsentscheid gestützt auf Art. 278 i.V.m. Art. 274 StPO nicht zuständig gewesen; die Prüfungskompetenz hinsichtlich der Verwertung obliege dem Sachrichter (a.a.O. E. 5.7. f.). Diese Rechtsprechung bestätigte das Bundesgericht in einem die SkyECC-Daten betreffenden Fall (Entscheid vom 11. Juli 2024, 7B_76/2024 E. 3.2.). Vor diesem Hintergrund entfaltet die Genehmigung des Zufallsfunds durch das Zwangsmassnahmengericht des Obergerichts des Kantons Zürich vom 19. Dezember 2022 hinsichtlich der Frage der Verwertbarkeit der SkyECC-Daten keine Wirkung.

1.2.3. Der Entscheid des Tribunal de Grande Instance de Lille vom 14. Juni 2019 erging im Rahmen der polizeilichen Vorermittlungen (enquête préliminaire) nach Art. 75 ff. CPP (Code de procédure pénale) wegen Beteiligung an einer kriminellen Vereinigung zur Vorbereitung eines Verbrechens oder Vergehens, das mit Freiheitsstrafe von zehn Jahren bestraft wird (Handel mit Betäubungsmitteln und bandenmässige Einfuhr von Betäubungsmitteln sowie Straftaten gegen die Gesetzgebung über kryptologische Mittel; Urk. 1/16/2=Urk. 228/1/3=Urk. 223/2/3, jeweils S. 1). Seine Entscheidung begründete der französische Richter damit, dass nach den bisherigen Ermittlungen SkyECC-Endgeräte für kriminelle Zwecke verwendet würden. Dieser Verdacht gründete auf der Beschlagnahme der SkyECC-Telefone im Zusammenhang mit dem Betäubungsmittelschmuggel im Hafen von Anvers, der Heimlichkeit der Verkaufsprozesse sowie der Aufstellung von über die 9'000 SkyECC-Nachrichten (Urk. 1/16/2=Urk. 228/1/3=Urk. 223/2/3, jeweils S. 1 f.).

Die Lektüre der gesetzlichen Bestimmungen des CPP zur enquête préliminaire (Art. 75 ff. CPP) ergibt, dass diese Voruntersuchung die Prüfung, ob sich genügend Indizien für die Eröffnung eines Ermittlungsverfahrens gegen einen konkreten Beschuldigten finden lassen, bezweckt und keinen konkreten Tatverdacht ge-

gen eine bestimmte Person voraussetzt. Hinsichtlich der in der Voruntersuchung anwendbaren Massnahmen wird nur verlangt, dass die Notwendigkeiten der Voruntersuchung die Massnahme erfordern. Auch die vorliegenden durch die französischen Behörden ergriffenen auf Art. 76 CPP gestützten Überwachungsmassnahmen sowie die Infiltrierung von Mobiltelefonen nach Art. 706-102-1 i.V.m. Art. 706-95-11 CPP erforderten keinen konkreten individualisierten Tatverdacht (vgl. dazu eingehender LG Berlin, Entscheid. v. 19.12.2024 – [525 KLs 8/22] 279 Js 30/22, E. 120 ff.).

1.2.4. Nicht in Frage gestellt wird, dass gegen den Beschuldigten zum Zeitpunkt der Anordnung und Durchführung der in Frankreich erfolgten Massnahmen der Serverüberwachung bzw. des Abfangens und Aufzeichnens der Kommunikation kein konkreter Verdacht auf eine Straftat bestanden hat.

1.2.5. Ebenso wenig bestand zum Zeitpunkt der Anordnung und Durchführung der Massnahme ein ausreichender Tatverdacht, der nach Schweizer Recht eine Überwachungsmassnahme gegen sämtliche SkyECC-Nutzer gerechtfertigt hätte. In Anbetracht der Gesamtzahl von rund 170'000 SkyECC-Nutzern werden im Entscheid des Tribunal de Grande Instance de Lille vom 14. Juni 2019 wenig Argumente für einen dringenden Tatverdacht gegen alle Nutzer angeführt, wenn lediglich auf den Betäubungsmittelschmuggelfall im Hafen von Anvers, die Heimlichkeit der Verkaufsprozesse sowie die Aufstellung von über die 9'000 SKYECC-Nachrichten verwiesen wird (Urk. 1/16/2=Urk. 228/1/3=Urk. 223/2/3, jeweils S. 1 f.). Der Entscheid legt nicht dar, inwiefern die konkreten Verdachtsmomente sämtliche rund 170'000 SkyECC-Nutzer beträfen. Die Nutzung einer Verschlüsselungstechnologie vermag für sich alleine keinen Anfangsverdacht zu begründen, zumal in der Tat nicht nur (möglicherweise) Kriminelle an Geräten mit dermassen hohen Sicherheitsstandards interessiert sein dürften, sondern z.B. auch Journalisten, politische Aktivisten oder Mitarbeiter von Unternehmen (vgl. so LG Berlin, Beschl. v. 1.7.2021 – [525 KLs] 254 Js 592/20 [10/21], E. 235). Schliesslich verstösst es gegen das Legalitätsprinzip und den Grundsatz individueller strafrechtlicher Verantwortung, wenn lediglich aus dem Profil und der Kommunikation einzelner Anwender entscheidende Schlussfolgerungen auf sämtliche Nutzer gezogen werden,

ohne dass konkrete Inhalte oder andere relevante Informationen zu einem spezifischen Angeklagten vorliegen (vgl. EGMR vom 26.9.2023, Yüksel Yalçınkaya vs. Türkei, 15669/20, § 326). Im oben erwähnten Bundesgerichtsentscheid zu ANOM-Überwachungen in den USA im Rahmen von – so die dortige Vorinstanz – präventiven polizeilichen Vorermittlungen erwog das Bundesgericht hinsichtlich des dringenden Tatverdachts gegen alle Nutzer, die Oberstaatsanwaltschaft habe nicht plausibel dargelegt, wie es den Strafbehörden der USA möglich gewesen wäre, gegen die Erwerber von etwa 12'000 ANOM-Kryptogeräten bereits konkrete Verdachtsmomente zu begründen (Urteil vom 11. Januar 2024, 7B_159/2022 [=BGE 150 IV 139] und 7B_160/2022 E. 5.5.). Das Bundesgericht liess für die Zulässigkeit der Überwachung sämtlicher rund 12'000 Geräte im ANOM-Fall damit nicht lediglich konkrete Verdachtsmomente gegen einzelne Erwerber genügen. SkyECC verfügte über rund 170'000 Nutzer. Angesichts der um ein Vielfaches grösseren Anzahl Nutzer als im Falle von ANOM-Geräten kann hier noch weniger von konkreten Verdachtsmomenten gegen sämtliche Erwerber der SkyECC-Geräte ausgegangen werden.

1.2.6. Die Vorinstanz erwog, dass gemäss den Darlegungen der Staatsanwaltschaft die Ermittlungen gegen die Betreiberin von SkyECC-Geräten (die in Canada domizilierte "Sky Holding Global Inc.") geführt worden seien, welche über die in Roubaix, Frankreich, domizilierte Firma OVH SAS mehrere Server für die Verwendung von SkyECC betrieben habe. In Frankreich sei am 13. Februar 2019 gegen die Betreiber eine Voruntersuchung wegen Beteiligung an einer kriminellen Vereinigung zur Vorbereitung eines Verbrechens oder Vergehens (Handel mit Betäubungsmitteln und bandenmässige Einfuhr von Betäubungsmitteln sowie Verletzung der Gesetzgebung über kryptologische Mittel) eingeleitet worden. Damit stützten sich laut Vorinstanz die in Frankreich durchgeführten Überwachungsmassnahmen, aus welchen erstmals SkyECC-Daten erlangt worden seien, auf einen konkreten Tatverdacht in Bezug auf schwere Straftaten. Der Tatverdacht habe wegen Gehilfenschaft bzw. Beihilfe zu schwerem Handel mit Betäubungsmitteln und bandenmässiger Einfuhr von Betäubungsmitteln und Verletzung der französischen Gesetzgebung über die Verwendung kryptologischer Mittel bestan-

den (vgl. Urk. 118 S. 28-32 E. 4.1.5.). An anderer Stelle stellt sich die Staatsanwaltschaft auf den Standpunkt, es habe gegen die Betreiber von SkyECC wie auch deren Nutzer ein hinreichend konkreter dringender Tatverdacht bestanden (vgl. Urk. 232 S. 3). In dieser Hinsicht ist festzuhalten, dass – kann vorliegend weder von einem konkreten Tatverdacht hinsichtlich des Beschuldigten noch hinsichtlich aller Nutzer der SkyECC-Telefone ausgegangen werden – ein solcher auch hinsichtlich der den Betreibern bzw. der Betreiberin vorgeworfenen Gehilfenschaft zu Betäubungsmitteldelikten nicht vorliegen kann, zumal sich Gehilfenschaft aus den den Nutzern vorgeworfenen Delikten ableitet. Bezüglich der den Betreibern bzw. der Betreiberin vorgeworfenen Delikte gegen die Gesetzgebung über Verschlüsselungsdienste bzw. kryptologische Mittel ist darauf hinzuweisen, dass es sich dabei nicht um eine Katalogtat nach Art. 269 Abs. 2 StPO handelt – sollte nach schweizerischem Recht überhaupt ein strafbares Verhalten vorliegen.

1.3. Fazit

1.3.1. Im Lichte vorstehender Ausführungen ist festzuhalten, dass der nach Art. 269 Abs. 1 lit. a StGB für die Anordnung einer Überwachungsmassnahme erforderliche dringende Tatverdacht zum Zeitpunkt der Serverüberwachung und dem Abfangen und Aufzeichnen der Kommunikation des Beschuldigten nicht bestanden hat. Festzuhalten ist an dieser Stelle, dass Erkenntnisse, welche durch nicht genehmigte Überwachungen erlangt worden sind, gestützt auf Art. 281 Abs. 4 i.V.m. Art. 277 Abs. 1 i.V.m. Art. 141 Abs. 1 StPO absolut unverwertbar und die entsprechenden Aufnahmen zu vernichten sind (vgl. BGE 145 IV 42 E. 4.5; vgl. auch BSK StPO-GLESS, 3. Aufl., Basel 2023, Art. 141 N 81 und 84). Letzteres muss auch bezüglich Überwachungen gelten, welchen eine Genehmigung nicht erteilt worden wäre.

1.3.2. Dies hat zur Folge, dass einem Rechtshilfeersuchen französischer Behörden um Überwachung des SkyECC-Handys des Beschuldigten mittels der MITM-Technik seitens der Schweizer Behörden nicht entsprochen worden wäre. Aus dem gleichen Grund des fehlenden dringenden Tatverdachts wäre den ausschliesslich mittels der in Frankreich erfolgten Serverüberwachung erhobenen

SkyECC-Daten in einem Schweizer Verfahren Verwertbarkeit versagt worden.

2. Rohdaten

2.1. Schliesslich ist – der Vollständigkeit sowie der Bedeutung der Frage im Zusammenhang mit (elektronischen) SkyECC-Daten wegen – die von der Verteidigung ins Feld geführte Thematik anzusprechen, wonach es sich bei den auf den CDs übermittelten Daten nicht um Rohdaten, auf welche nach Rechtsprechung ein Beschuldigter Anspruch habe, handle.

2.2. Die Verteidigung beantragt – wie vor Vorinstanz (Urk. 59 Rz. 27) – die rechtshilfeweise Edition der Rohdaten. Für elektronische Daten bedeute dies, dass diese in ihrer ursprünglichen, unbearbeiteten Form vorliegen müssten, um die Rechte der Verteidigung zu wahren. Die im Recht liegenden Daten seien aufgrund der massenhaften Überwachung durch Europol seit 2021 einer Bearbeitung oder "Verdünnung" unterzogen worden, was die Anklagebehörde nicht bestreite. Damit liege nahe, dass die vorliegenden Daten nicht originär seien. Die in den Akten liegenden zu PDF-Dateien konvertierten Excel-Tabellen, welche im Rahmen der polizeilichen Ermittlungen erstellt und visuell aufbereitet worden seien, seien nicht die eigentlichen Rohdaten, die durch die ausländischen Behörden erlangt worden seien. Bei Rohdaten handle es sich um Daten, die unmittelbar aus den erzeugenden Quellen stammten. Bei einer Konvertierung in Excel-Files oder PDFs könne es sich schon begrifflich nicht um die ursprünglichen Dateiformate handeln. Die Rohdaten würden neben Tabellen mit Meta-Informationen zu den Chattabellen und den Chattexten selbst unter Umständen auch (entlastende) Fotos, Videos und Audioaufnahmen enthalten (vgl. Urk. 183 Rz. 15-20, Urk. 59 Rz. 26 f., Urk. 230 Rz. 90 ff.).

2.3. Die Staatsanwaltschaft entgegnet dazu, der Ursprung der in Frankreich erhältlich gemachten Daten sei in den Akten ausführlich dokumentiert. Alle Rohdaten seien auf den in den Akten abgelegten CDs enthalten. Wie diese zu lesen seien, ergebe sich aus den auf den CDs enthaltenen Hinweisen. Für alle Mediendateien (Bilder, Audio, Video) seien die Hashwerte in den Daten bzw. Chatverläufen

sauber ausgewiesen und könnten überprüft werden. Zum (technischen) Ablauf verweist die Staatsanwaltschaft auf das Factsheet (Urk. 61), aus welchem hervorgehe, wie die Daten bei ihnen angekommen und zu lesen seien (Urk. 60 S. 2). Der Antrag auf Edition von Rohdaten sei demnach abzuweisen (Urk. 191 S. 2). Die Staatsanwaltschaft beruft sich weiter auf den von ihr im Rahmen des Berufungsverfahrens eingereichten Bericht des Niederländischen Forensischen Instituts "NFI" vom 22. Juni 2022 zur "Vollständigkeit und Genauigkeit der Dekodierung von SkyECC-Nachrichten mit der Toolbox-Methode" (Urk. 228/2/1=Urk. 223/3/1). Es handle sich dabei um einen ausführlichen Bericht, welcher zeige, dass die durch die Überwachungsmassnahmen erlangten Daten korrekt und vollständig seien und die verwendete Entschlüsselung das korrekte Ergebnis bringe. Die Untersuchung sei anhand von neuen SkyECC-Datenbanken aus drei Mobiltelefonen vorgenommen worden. Im Bericht würden Verschlüsselung, Übermittlung und Speicherung der SkyECC-Kommunikation ausführlich, aber für einen technisch interessierten Laien verständlich erläutert (Urk. 232 S. 5 f.). Die Verteidigung entgegnet dazu, aus dem Bericht ergebe sich, dass die umfangreichen, ursprünglich als pcap-Dateien vorliegenden Datenmengen nachträglich verarbeitet worden seien. Zwar bestätige der Bericht, dass die Ergebnisse dieser Methode durch das NFI validiert worden seien, dies aber ohne dass deren Funktionsweise im Verfahren unabhängig überprüft werden könnte. Die Prüfung von Herkunft, Vollständigkeit, Authentizität und Relevanz der Beweismittel sei nicht möglich, was ein klarer Verstoss gegen das Recht auf ein faires Verfahren im Sinne von Art. 6 EMRK sei (Urk. 230 Rz. 90 ff.). Zur Frage, ob es sich bei den CSV-Daten um Rohdaten handle, sowie zur SHA 1-Thematik beantragt die Verteidigung die Befragung einer sachverständigen Person (Urk. 236 S. 3).

2.4. Aus dem in Art. 29 Abs. 2 BV bzw. Art. 6 Ziff. 3 EMRK verankerten Anspruch auf rechtliches Gehör, welcher einen wichtigen und deshalb eigens aufgeführten Teilaspekt des allgemeineren Grundsatzes des fairen Verfahrens von Art. 29 Abs. 1 BV bzw. Art. 6 Ziff. 1 EMRK darstellt, ergibt sich für die beschuldigte Person das grundsätzlich uneingeschränkte Recht, in alle für das Verfahren wesentlichen Akten Einsicht zu nehmen und an der Erhebung wesentlicher Be-

weise mitzuwirken oder sich zumindest zum Beweisergebnis zu äussern, wenn dieses geeignet ist, den Entscheid zu beeinflussen. Das Akteneinsichtsrecht soll sicherstellen, dass die beschuldigte Person als Verfahrenspartei von den Entscheidgrundlagen Kenntnis nehmen und sich wirksam und sachbezogen verteidigen kann. Die effektive Wahrnehmung dieses Anspruchs setzt notwendigerweise voraus, dass die Akten vollständig sind. In einem Strafverfahren bedeutet dies, dass die Beweismittel, jedenfalls soweit sie nicht unmittelbar an der gerichtlichen Hauptverhandlung erhoben werden, in den Untersuchungsakten vorhanden sein müssen und dass aktenmässig belegt sein muss, wie sie produziert wurden. Damit soll die beschuldigte Person in die Lage versetzt werden, zu prüfen, ob sie inhaltliche oder formelle Mängel aufweisen, und gegebenenfalls Einwände gegen deren Verwertbarkeit erheben kann. Dies ist Voraussetzung dafür, dass sie ihre Verteidigungsrechte überhaupt wahrnehmen kann, wie dies Art. 32 Abs. 2 BV verlangt. Die Anklagebehörde muss dem Gericht sämtliches Material zuleiten, das mit der Tat als Gegenstand eines gegen eine bestimmte Person erhobenen Vorwurfs in thematischem Zusammenhang steht. Sie muss dem Gericht und der beschuldigten Person respektive der Verteidigung sämtliche Spurenvorgänge zur Kenntnis bringen, die im Verfahren – und sei es auch nur mit geringer Wahrscheinlichkeit – Bedeutung erlangen können. Die Ermittlungs- und Untersuchungsbehörden dürfen grundsätzlich kein von ihnen erhobenes oder ihnen zugekommenes Material zurückbehalten, das einen Bezug zur Sache hat. Die Dokumentationspflicht gilt auf allen Verfahrensstufen, also auch bereits im polizeilichen Ermittlungsverfahren. Dabei ist zu berücksichtigen, dass auch ergebnislose oder unergiebige Ermittlungen in ihrem negativen Ausgang einen für die Urteilsfällung relevanten Gehalt aufweisen können. Wichtig ist, dass sich aus der Hauptakte der Bestand der verhandlungsrelevanten Beiakten jederzeit feststellen lässt und die richterliche Verfahrensgestaltung ebenso wie die Gewährung von Akteneinsicht diese zusätzlichen Materialien einbezieht. Gemäss der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ist der beschuldigten Person ein Recht auf Einsicht in möglicherweise sachdienliche Aktenteile ausserhalb der Ermittlungsakte zu gewähren, wobei von der beschuldigten Person verlangt werden kann, spezifische Gründe für ihr Gesuch vorzubringen. Nicht zulässig ist es, die

Triage im Rahmen der verdeckten Ermittlung ohne verfahrensrechtliche Kontrollmechanismen den Strafverfolgungsbehörden zu überlassen. Den Parteirechten ist im Zusammenhang mit den ausgesonderten Aufzeichnungen der Fernmeldeüberwachung Rechnung zu tragen. Die beschuldigte Person hat das Recht, den Archivdatenträger mit den Aufzeichnungen der Fernmeldeüberwachung nach den Vorgaben von Art. 101 f. StPO einzusehen, um sich anhand der Gesprächsaufzeichnungen ein Bild über die von den Strafbehörden vorgenommene Triage zu machen (Urteil des Bundesgerichts 6B_403/2018 vom 14. Januar 2019 E. 2.3.1. ff.; vgl. auch Urteile des Bundesgerichts 6B_1188/2020 vom 7. Juli 2021 E. 1.1.3 und BGE 129 I 85, 89 E. 4.1. f.). Die Anforderung der Offenlegung "aller Sachbeweise" gegenüber der Verteidigung kann nicht auf von der Anklage als relevant erachtete Beweise beschränkt werden. Sie umfasst vielmehr das gesamte sich im Besitz der Behörden befindliche Material, das für die Verteidigung potenziell relevant ist. Die Tatsache, dass der Beschwerdeführer Zugang zu allen im Akt enthaltenen ByLock-Berichten hatte, bedeutet folglich nicht, dass er kein Recht hatte, Zugang zu jenen Daten zu verlangen, auf denen diese Berichte beruhten (EGMR vom 26.9.2023, Yüksel Yalçınkaya vs. Türkei, 15669/20, § 327). Elektronische Beweise unterscheiden sich in vielen Aspekten von herkömmlichen Formen der Beweise, etwa was ihre Natur und die für ihre Gewinnung, Sicherstellung, Verarbeitung und Auswertung erforderlichen besonderen Technologien betrifft. Noch entscheidender ist, dass sie besondere Fragen hinsichtlich ihrer Verlässlichkeit aufwerfen, weil sie ihrer Art nach anfälliger für Zerstörung, Beschädigung, Änderung oder Manipulation sind (EGMR vom 26.9.2023, Yüksel Yalçınkaya vs. Türkei, 15669/20, § 312).

2.5. Festgehalten werden kann, dass die in den Akten im Excel-Format vorliegenden Daten nicht ihrer ursprünglichen Form entsprechen. Auch kann nicht in Frage gestellt werden, dass hinsichtlich des Inhalts der Kommunikation eine Triage – um die relevanten Nachrichten herauszusuchen – stattgefunden hat sowie eine nachfolgende Zusammenstellung der Nachrichten im Excel-Dokument erfolgt ist. Dass es sich mit dem Bericht des NFI für das Gericht verifizieren liesse, dass die Daten ihrer ursprünglichen Form entsprechen, kann nicht ohne Weiteres be-

jaht werden. Allerdings kann in Anbetracht des Umstands, dass die SkyECC-Daten unverwertbar und aus den Akten zu entfernen sind (vgl. oben E. III.5), auf Weiterungen zur in Frage stehenden Qualifikation als Rohdaten verzichtet werden. Aus dem gleichen Grund erübrigt sich auch die von der Verteidigung beantragte Befragung von Sachverständigen.

Es wird beschlossen:

1. Der Antrag des Beschuldigten auf Rückweisung des Verfahrens nach Art. 409 StPO wird abgewiesen.

2. Die im Recht liegenden SkyECC-Daten sind unverwertbar und werden aus den Akten entfernt.

3. Schriftliche Mitteilung an die amtliche Verteidigung des Beschuldigten, die Vertretung der Privatklägerin sowie die Staatsanwaltschaft II des Kantons Zürich.

4. Gegen diesen Entscheid kann unter den einschränkenden Voraussetzungen von Art. 93 des Bundesgerichtsgesetzes **bundesrechtliche Beschwerde in Strafsachen** erhoben werden.

   Die Beschwerde ist innert **30 Tagen**, von der Zustellung der vollständigen, begründeten Ausfertigung an gerechnet, bei der II. strafrechtlichen Abteilung des Bundesgerichtes (1000 Lausanne 14) in der in Art. 42 des Bundesgerichtsgesetzes vorgeschriebenen Weise schriftlich einzureichen.

   Die Beschwerdelegitimation und die weiteren Beschwerdevoraussetzungen richten sich nach den massgeblichen Bestimmungen des Bundesgerichtsgesetzes.

Obergericht des Kantons Zürich
II. Strafkammer

Zürich, 15. August 2025

Der Präsident:	Die Gerichtsschreiberin:
lic. iur. Spiess	MLaw Blumer