COMPLIANCE UND WIRTSCHAFTSSTRAFRECHT

Digitale Ermittlungen im Wandel: Was Beschuldigte und Verteidiger jetzt wissen müssen

Aktuelle Rechtsprechung und Gesetzgebung zu technischen und verdeckten Ermittlungen im Internet Einleitung Der Staat rüstet auf – digital. Krypto-Handys werden geknackt, Fahrzeugdaten ausgewertet, V-Personen im Darknet …

AUTOR / ANSPRECHPARTNER

Georg Mörchel

Rechtsanwalt

2026-08-14

Aktuelle Rechtsprechung und Gesetzgebung zu technischen und verdeckten Ermittlungen im Internet

Einleitung

Der Staat rüstet auf – digital. Krypto-Handys werden geknackt, Fahrzeugdaten ausgewertet, V-Personen im Darknet eingesetzt, und Ermittler tarnen sich mit falschen Identitäten in Online-Foren. Was noch vor wenigen Jahren wie Science-Fiction klang, ist längst gelebte Ermittlungspraxis. Die Gerichte halten mit: In schneller Folge haben der Bundesgerichtshof (BGH), der Europäische Gerichtshof für Menschenrechte (EGMR) und der Europäische Gerichtshof (EuGH) grundlegende Entscheidungen zu Zulässigkeit und Grenzen dieser Methoden getroffen. Gleichzeitig arbeitet der Gesetzgeber an einer neuen Rechtsgrundlage für den Einsatz verdeckter Ermittler und Vertrauenspersonen. Dieser Beitrag gibt einen Überblick über die wichtigsten aktuellen Entwicklungen – für alle, die in Ermittlungsverfahren mit Bezug zu digitalen Beweismitteln betroffen sind oder werden könnten.

I. Kryptokommunikation im Visier: EncroChat, Sky ECC und ANOM – eine Bestandsaufnahme der Rechtsprechung

Der Ausgangspunkt: Massenüberwachung mit richterlichem Segen

EncroChat, Sky ECC und das FBI-Phantom ANOM haben eines gemeinsam: Sie galten als unknackbare Kommunikationsplattformen für ein Millionenpublikum – und wurden von Strafverfolgungsbehörden jahrelang im Stillen mitgelesen. Im Fall EncroChat infiltrierten französische Behörden die Server des Dienstes und leiteten ab März 2020 Millionen von Chatnachrichten ab. Auf Grundlage einer Europäischen Ermittlungsanordnung (EEA) erhielten deutsche Staatsanwaltschaften Zugang zu diesen Daten. Seither stehen Hunderte von Verfahren in Deutschland unter der Frage: Dürfen diese Beweise verwertet werden?

Der BGH setzt den Rahmen – und hält ihn aufrecht

Den rechtlichen Grundstein legte der. Strafsenat des BGH mit seinem Grundsatzbeschluss vom 2. März 2022 (5 StR 457/21): EncroChat-Daten sind in deutschen Strafverfahren verwertbar, soweit die Taten dem Straftatenkatalog des § 100b Abs. 2 StPO (Online-Durchsuchung) unterfallen. Der BGH wandte dabei die restriktivste Verwendungsschranke des § 100e Abs. 6 StPO an – als Ausdruck einer verhältnismäßigkeitsgeleiteten Abwägungslösung.

Dieser Rahmen wurde seitdem von übergeordneten Gerichten bestätigt und weiterentwickelt:

Der EuGH urteilte am 30. April 2024 (C-670/22), dass für die Rechtmäßigkeit einer EEA maßgeblich ist, ob die Datenübermittlung in einem vergleichbaren innerstaatlichen Fall zulässig gewesen wäre – und verweist damit auf das nationale Recht.

Das Bundesverfassungsgericht bestätigte mit Nichtannahmebeschluss vom 1. November 2024 (2 BvR 684/22), dass die BGH-Lösung verfassungsrechtlich unbedenklich ist.

Die Cannabis-Frage: Verwertbar trotz KCanG?

Eine neue, brisante Rechtsfrage entstand durch das Inkrafttreten des Konsumcannabisgesetzes (KCanG) am 1. April 2024: Wenn der Besitz und Handel von Cannabis nun nur noch als Vergehen eingestuft ist – dürfen dann EncroChat-Daten, die auf Basis der schwereren alten Rechtslage erhoben wurden, noch verwendet werden?

Einige Landgerichte und Oberlandesgerichte verneinten dies. Das LG Berlin sprach einen Angeklagten im Mai 2024 frei: Da Cannabisdelikte nicht mehr im Katalog des § 100b StPO enthalten seien, fehle es an der Verhältnismäßigkeitsvoraussetzung für die Verwertung.

Der BGH widersprach klar: Mit Urteil vom 30. Januar 2025 (5 StR 528/24) hob er diesen Freispruch auf. Entscheidend sei der Zeitpunkt der Datenübermittlung, nicht der spätere Verurteilungszeitpunkt. Zum Zeitpunkt der EEA-Anforderung im Jahr 2020 waren die Taten als Verbrechen nach § 29a Abs. 1 Nr. 2 BtMG strafbar und im Katalog des § 100b StPO enthalten – die Daten wurden damit rechtmäßig übermittelt und bleiben verwertbar.

Sky ECC und ANOM: Die Grundsätze gelten entsprechend

Für den Kryptodienst Sky ECC (Belgien/Frankreich, Überwachung ab Ende 2020) gelten nach Auffassung des BGH dieselben Maßstäbe: Der. Strafsenat stellte in seinem Beschluss vom 9. Januar 2025 (1 StR 142/24) fest, dass die SkyECC-Daten aufgrund des vergleichbaren Verfahrensablaufs und der identischen Rahmenbedingungen (Serverstandort in Frankreich, verdeckte Verkaufsstrukturen, vollständige kriminelle Ausrichtung) verwertbar sind. Verstöße gegen Benachrichtigungspflichten führen nach der BGH-Abwägungslösung nicht zwingend zu einem Beweisverwertungsverbot.

Das OLG Frankfurt bestätigte diese Linie zuletzt mit Beschluss vom 1. April 2025 (7 Ws 46/25) und erstreckte sie auf Chat-Inhalte aus beiden Diensten.

Praktische Konsequenz: Wer wegen Drogenhandels, Waffenhandels oder anderer schwerer Delikte angeklagt ist und seine Kommunikation über EncroChat, Sky ECC oder ANOM abgewickelt hat, muss mit der vollständigen Verwertbarkeit dieser Chats rechnen – sofern die Taten zum Tatzeitpunkt Katalogtaten im Sinne des § 100b Abs. 2 StPO darstellten. Die Verteidigung sollte gleichwohl stets prüfen, ob im konkreten Einzelfall Verstöße gegen Benachrichtigungspflichten (Art. 31 RL EEA, § 91g Abs. 6 IRG) vorliegen, die im Rahmen der Abwägung Gewicht erlangen können.

II. Der Cyberbunker: Wenn Hosting zur Mitgliedschaft in einer kriminellen Vereinigung wird

Der Fall

Im rheinland-pfälzischen Traben-Trarbach betrieben acht Angeklagte von 2013 bis 2019 ein Rechenzentrum in einem ehemaligen NATO-Bunker. Ihr Versprechen an die Kunden: „stay online – no matter what!" – ein garantierter Schutz vor behördlichem Zugriff. Rund 84 Prozent der Kunden nutzten die Server für illegale Zwecke: Betäubungsmittelmärkte, Phishing-Plattformen, Kreditkartenbetrug, Verbreitung kinderpornografischer Inhalte.

Das Urteil des BGH vom 12. September 2023 (3 StR 306/22)

Das LG Trier hatte die Angeklagten wegen mitgliedschaftlicher Beteiligung an einer kriminellen Vereinigung (§ 129 StGB) verurteilt. Der BGH bestätigte das Urteil dem Grunde nach und präzisierte: Da der Betrieb des Cyberbunkers auf das Ermöglichen staatlicher Kontrolle entzogener Internetaktivitäten ausgerichtet war und die Betreiber auch nach Kenntnis konkreter Straftaten aktiv für den Weiterbetrieb sorgten, sei das Geschäftsmodell keine neutrale Infrastruktur mehr.

Bemerkenswert ist die Einziehungsentscheidung: Der BGH stellte klar, dass alle aus der Tätigkeit des Cyberbunkers erzielten Einnahmen als Taterträge i.S.d. § 73 Abs. 1 StGB einzuziehen sind – auch solche aus der (wenigen) legalen Servernutzung, da die maßgebliche Straftat die mitgliedschaftliche Beteiligung an der Vereinigung selbst war.

Bedeutung für die Praxis: Das Cyberbunker-Urteil setzt eine klare Grenze: Wer als IT-Dienstleister oder Hosting-Provider wissentlich und aktiv kriminelle Nutzer schützt und unterstützt, kann strafrechtlich als Mitglied einer kriminellen Vereinigung haften. Die Haftungsprivilegierung des (früheren) § 10 TMG / heutigen § 7 DDG schützt nicht vor Strafbarkeit, wenn konkrete Kenntnis von Straftaten mit aktivem Weiterhosting verbunden wird.

III. Verdeckte Ermittler, V-Personen und die Grenze zur Tatprovokation – ein Rechtsgebiet im Umbruch

Der rechtliche Rahmen

Der Einsatz verdeckter Ermittler (§§ 110a ff. StPO) ist in der Strafprozessordnung geregelt; der Einsatz von Vertrauenspersonen (V-Personen) und Informanten hingegen basiert bislang allein auf den Generalklauseln der §§ 161, 163 StPO sowie auf verwaltungsinternen Richtlinien (RiStBV). Beide Methoden sind im Internet in besonderem Maße verbreitet – sei es das Auftreten unter falscher Identität in einschlägigen Foren, die Bestellung von Beweismitteln im Darknet oder die gezielte Kontaktaufnahme zu Verdächtigen in sozialen Netzwerken.

Tatprovokation: Das Verfahrenshindernis ist gefestigt

Eine der folgenreichsten Entwicklungen der letzten Jahre ist die endgültige Abkehr von der sog. „Strafzumessungslösung”: Wer durch staatliche Stellen – also durch Polizei, verdeckte Ermittler oder V-Personen – zur Begehung einer Straftat verleitet wird, obwohl er zuvor nicht tatbereit war, ist Opfer einer rechtsstaatswidrigen Tatprovokation. Die Folge ist nicht mehr nur eine mildere Strafe, sondern ein Verfahrenshindernis, das zur Einstellung des Verfahrens führt (§§ 206a, 260 Abs. 3 StPO).

Diese Linie wurde durch den EGMR in der Entscheidung „Furcht ./. Deutschland” vom 23. Oktober 2014 (Nr. 54648/09) erzwungen: Der Gerichtshof verwarf die bisherige Strafzumessungslösung als unvereinbar mit Art. 6 Abs. 1 EMRK (Recht auf ein faires Verfahren). Der BGH vollzog den Wandel mit Urteil vom 10. Juni 2015 (2 StR 97/14, BGHSt 60, 276): Die rechtsstaatswidrige Tatprovokation begründet nunmehr ein Verfahrenshindernis – der Strafverfolgungsanspruch des Staates ist in diesen Fällen verwirkt.

Der BGH festigte diese Rechtsprechung erneut mit Urteil vom 20. Dezember 2023 (2 StR 175/23) und bestätigte, dass die EGMR-Vorgaben und die darauf beruhende nationale Rechtsprechung zum Verfahrenshindernis bei rechtsstaatswidriger Tatprovokation durch V-Personen wie durch verdeckte Ermittler gleichermaßen gelten.

Die „Keuschheitsprobe” – erlaubt oder Verstoß?

Bei der sogenannten Keuschheitsprobe (im angloamerikanischen Raum: „integrity test”) soll ein Verdächtiger durch staatliche Stellen auf die Probe gestellt werden: Er wird zu einer strafbaren Handlung aufgefordert, und es wird beobachtet, ob er dieser Aufforderung nachkommt. Die Zulässigkeit ist eng begrenzt: Der BGH hat klargestellt, dass ein solcher Test nur dann rechtsstaatlich unbedenklich ist, wenn bereits ein konkreter Verdacht besteht und der Betroffene auf eigene Initiative handelt, ohne erheblich durch staatliche Stellen bedrängt oder manipuliert zu werden. Wer hingegen gezielt und ohne ausreichenden Anfangsverdacht unter Druck gesetzt wird, ist Opfer einer unzulässigen Tatprovokation – mit der Folge des Verfahrenshindernisses.

Der Reformentwurf: V-Personen endlich gesetzlich regeln

Das Bundesjustizministerium hat Anfang 2024 einen Referentenentwurf zur erstmaligen gesetzlichen Kodifizierung des Einsatzes von V-Personen und verdeckten Ermittlern vorgelegt. Anlass waren vor allem zwei Beschlüsse des BVerfG (16. Dezember 2020 und 9. Dezember 2022), die den V-Personen-Einsatz als besonders schweren Grundrechtseingriff qualifizierten und eine gesetzliche Grundlage forderten.

Der Entwurf sieht u.a. vor: - Ausdrückliche materielle Grenzen für die Tatprovokation und deren Rechtsfolgen - Schutz des Kernbereichs privater Lebensgestaltung auch beim V-Personen-Einsatz (Verweis auf § 100d StPO) - Regelungen zur Dokumentation und richterlichen Kontrolle

Der Entwurf ist in der politischen Diskussion auf erhebliche Widerstände gestoßen: Das Land Niedersachsen erteilte dem Vorhaben bereits Ende Januar 2024 eine klare Absage.

Praxisrelevanz: Solange eine gesetzliche Regelung fehlt, gelten für den V-Personen-Einsatz die durch Rechtsprechung entwickelten Schranken. Eine Verwertbarkeit der von V-Personen gewonnenen Informationen ist an enge Voraussetzungen geknüpft: Das Gespräch darf nicht verbotswidrig fixiert worden sein, der Beschuldigte darf nicht zu selbstbelastenden Äußerungen gedrängt worden sein, und es darf insbesondere keine rechtsstaatswidrige Tatprovokation vorgelegen haben.

Was bedeutet das für Sie?

Die Entwicklungen der vergangenen Jahre zeigen: Digitale Ermittlungen sind rechtlich komplex, die Verwertbarkeit von Beweismitteln hängt von zahlreichen Faktoren ab, und die Rechtsprechung ist noch nicht in allen Bereichen abgeschlossen.

Für Beschuldigte und Verteidiger gilt daher: In jedem Verfahren, in dem digitale Beweismittel eine Rolle spielen – sei es aus Kryptodiensten, Fahrzeugdaten, OSINT-Recherchen oder verdeckten Ermittlungen –, sollte frühzeitig geprüft werden:

Wie wurden die Daten erhoben? Gab es eine richterliche Anordnung? War die Europäische Ermittlungsanordnung rechtmäßig?

War die Tat zum Zeitpunkt der Datenerhebung eine Katalogtat i.S.d. § 100b Abs. 2 StPO? Hat sich die Rechtslage seither geändert (z.B. durch das KCanG)?

Wurde ein Verwertungswiderspruch rechtzeitig und ordnungsgemäß erhoben?

Lag beim Einsatz von V-Personen oder verdeckten Ermittlern eine rechtsstaatswidrige Tatprovokation vor?

Wir beraten und begleiten Sie in allen Phasen des Ermittlungs- und Strafverfahrens – von der ersten Durchsuchung bis zur Revision. Sprechen Sie uns an.

Dieser Beitrag gibt den Stand der Rechtsprechung und Gesetzgebung zum Zeitpunkt der Veröffentlichung (Mai 2026) wieder und ersetzt keine anwaltliche Beratung im Einzelfall.

BERGISCHE SEKUNDANZ

Rechtsanwälte Lichtinghagen & Partner

IHR ANSPRECHPARTNER

Georg Mörchel

IT-, Datenschutz- und Wirtschaftsrecht

Rechtsanwalt

BERGISCHE SEKUNDANZ – Rechtsanwälte Lichtinghagen & Partner mbB

0221 / 9854 – 9999

kanzlei@bergische-sekundanz.de

Bornerhof 5–7, 51643 Gummersbach

bergische-sekundanz.de

Online weiterlesen

Aktuelle Fassung dieses Fachbeitrags

bergische-sekundanz.de · Zum Fachbeitrag

Hinweis zur Einordnung

Dieser Fachbeitrag dient der allgemeinen Information und ersetzt keine rechtliche Beratung im Einzelfall.