Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

famos

Der Fall des Monats
im Strafrecht
Online-Zeitschrift

Herausgeber: Prof. Dr. Tobias Reinbacher, Lehrstuhl für Strafrecht, Strafprozessrecht und Medienstrafrecht,
Julius-Maximilians-Universität Würzburg
Redaktion: Prof. Dr. Tobias Reinbacher und die Mitarbeiterinnen und Mitarbeiter des Lehrstuhls
www.famos.jura.uni-wuerzburg.de

06
2026

Juni 2026

Finger weg von meinem Account!

Beweisverwertungsverbot / Telekommunikationsüberwachung / Online-Durchsuchung

§§ 100a Abs. 1 S. 2, 3, Abs. 5 S. 1; 100b Abs. 1 StPO

***famos*-Leitsätze**:

1. Rechtsgrundlage für die Überwachung und Aufzeichnung von Chatinhalten i.R.d. Account-Clonings ist die Quellen-TKÜ gem. § 100a Abs. 1 S. 2, 3.
2. Hiernach dürfen erst ab der richterlichen Anordnung versendete Chatinhalte erhoben werden.

BGH, Beschluss vom 20.01.2026 – 3 StR 495/25; veröffentlicht in NJW 2026, 1448.

1. Sachverhalt[1]

A steht unter Verdacht, mit Doping- sowie verschreibungspflichtigen und gefälschten Arzneimitteln zu handeln. Um ihn zu überführen, ordnet der Ermittlungsrichter beim AG auf Antrag der StA am 21.03.2022 gem. § 100a Abs. 1 S. 2 und 3, Abs. 2 Nr. 3, Nr. 7 lit. a, b StPO[2] die Überwachung und Aufzeichnung der Telekommunikation des A über einen Zeitraum von drei Monaten an. Daraufhin verschafft sich ein Sachbearbeiter des BKA in der Nacht des 30.03.2022 Zugang zum Telegram-Account des A über die Website des Messengerdienstes ohne Kenntnis und Mitwirkung des A oder des Telekommunikationsanbieters (Provider). Dabei nutzt er für die Anmeldung As Telefonnummer und fängt den zusätzlich benötigten Zwei-Faktor-Authentifizierungscode (2FA) mit technischen Mitteln ab (sog. „Aufschaltung“). Als A wenige Stunden später den fremden Zugriff bemerkt, unterbindet er ihn. Bis dahin können seine Chats vom 26.11.2021 bis zum 30.03.2022 gesichert werden.

In der Hauptverhandlung werden sodann Chatinhalte ab dem 01.02.2022 bis zum 26.03.2022 als Beweise eingeführt. Die Verteidigung widerspricht der Erhebung und Verwertung der Chatinhalte mit dem Argument, dass nach § 100a Abs. 5 S. 1 Nr. 1 lediglich die laufende Kommunikation überwacht werden dürfe. Die Strafkammer verwirft den Widerspruch mit der Begründung, die Datenerhebung falle in den Anwendungsbereich des § 100a Abs. 1 S. 1. Das LG verurteilt A u.a. wegen gewerbsmäßigen Handeltreibens mit Dopingmitteln in neun Fällen und stützt dies in zwei Fällen auf die erhobenen Chatinhalte. Die Verteidigung legt Revision zum BGH ein.

2. Probleme und bisheriger Meinungsstand

Die zentrale Problematik des Falls liegt in der Frage, ob ein **Beweisverwertungsverbot** bzgl. der erhobenen Chatinhalte besteht. Hierbei ist zwischen selbstständigen und unselbstständigen Beweisverwertungsverboten zu unterscheiden. Während erstere unabhängig von der Rechtmäßigkeit der Beweiserhebung entstehen, sind letztere durch eine rechtswidrige Beweiserhebung gekennzeichnet.[3] Handelt es sich zudem um ein ungeschriebenes,

[1] Der Sachverhalt wurde verändert, um die Hauptprobleme des Falles deutlicher hervortreten zu lassen.

[2] Alle nachfolgenden Normen sind, soweit nicht anders gekennzeichnet, solche der StPO.

[3] *Heinrich*/*Reinbacher*, Examinatorium Strafprozessrecht, 4. Aufl. 2024, S. 146.

also ein im Gesetz nicht verankertes Beweisverwertungsverbot, ist nach der h.M. eine Abwägung zwischen dem staatlichen Interesse an der Strafverfolgung und den Rechten des Betroffenen durchzuführen (sog. **„Abwägungslehre“**).[4] Da in unserem Fall kein selbstständiges geschriebenes Beweisverwertungsverbot ersichtlich ist, kommt nur ein ungeschriebenes Beweisverwertungsverbot in Betracht, das aus der Rechtswidrigkeit der Maßnahme folgen könnte. Ob die Beweiserhebung hier rechtswidrig war, hängt insbesondere davon ab, ob die vom Ermittlungsrichter angeordnete Maßnahme von einer Rechtsgrundlage gedeckt ist.

Ursprünglich gab es lediglich die **„klassische TKÜ“** gem. § 100a Abs. 1 S. 1. Dabei wird die Telekommunikation „in der Leitung“ nach der h.M. vom Provider heimlich abgefangen und der Ermittlungsbehörde zur Verfügung gestellt.[5] Aufgrund der zunehmenden Verschlüsselung von Kommunikation über Messengerdienste wie WhatsApp oder Telegram (z. B. Ende-zu-Ende Verschlüsselung) ist dieses Vorgehen stark erschwert bis unmöglich geworden.[6] Deshalb hat der Gesetzgeber im Jahr 2017 die **Quellen-TKÜ** nach § 100a Abs. 1 S. 2, 3 und die **Online-Durchsuchung** nach § 100b Abs. 1 eingeführt.[7] Die Quellen-TKÜ setzt zur Überwachung der Kommunikationsinhalte „an der Quelle“, also vor der Verschlüsselung der Nachrichten auf dem Endgerät bzw. nach der Entschlüsselung auf dem Empfängergerät an.[8] Dagegen dürfen bei der Online-Durchsuchung nicht nur die Kommunikationsdaten, sondern sämtliche Daten auf dem System des Betroffenen erhoben werden.[9] Beide Maßnahmen erlauben dazu einen direkten, heimlichen Zugriff mit technischen Mitteln – insbesondere durch die Installation von Spähsoftware – auf das vom Betroffenen genutzte IT-System.[10] Bei der Quellen-TKÜ darf dabei gem. § 100a Abs. 5 S. 1 Nr. 1 lit. a im Gegensatz zur Online-Durchsuchung grds. nur die laufende Telekommunikation überwacht bzw. aufgezeichnet werden und die Maßnahme ist gem. § 100e Abs. 1 S. 4 auf drei Monate beschränkt. Die Online-Durchsuchung ist hingegen gem. § 100e Abs. 2 S. 4 auf einen Monat begrenzt. Beide Maßnahmen können gem. § 100e Abs. 1 S. 5 bzw. Abs. 2 S. 5 verlängert werden. Aus dem Wortlaut des § 100a Abs. 1 S. 2 ergibt sich, dass die Quellen-TKÜ subsidiär gegenüber der klassischen TKÜ ist.[11] Welche Rechtsgrundlage im Einzelnen die richtige ist, entscheidet sich zunächst daran, ob ein **IT-System** vorliegt. Der Begriff ist sehr weit auszulegen, nämlich als Einheit aus technischen Anlagen und Bauelementen, denen eine gemeinsame Funktion zukommt und die der Verarbeitung und Übertragung von Daten dienen.[12] Ob ein IT-System vorliegt, ist insbesondere im Rahmen von Zugriffen auf eine Cloud[13] oder der Schaffung eines Zweitzugangs zu fremden Accounts, bspw. über den Webclient eines Messengerdienstes, also einer Aufschaltung (technisch sog. „**Account-Cloning**“[14]), umstritten.

Hierbei vertritt **eine Ansicht**, dass beim Einsatz des Account-Clonings auf kein IT-

---

4 BGH NJW 1999, 959, 961; BeckRS 2018, 28269 Rn. 24 ff.; *Bhatti*, JuS 2026, 400.

5 BT-Drs. 18/12785, S. 48; *Niedernhuber*, JA 2018, 169, 170.

6 BT-Drs. 18/12785, S. 48; *Rückert*, in MüKo, StPO, Bd. 1, 2. Aufl. 2023, § 100a Rn. 119.

7 BT-Drs. 18/12785, S. 48 ff.

8 BT-Drs. 18/12785, S. 48 f.; *Köhler*, in Schmidt/Köhler, StPO, 69. Aufl. 2026, § 100a Rn. 14a, 14b.

9 BT-Drs. 18/12785, S. 54; *Rückert*/*Meyer-Wegener*/*Safferling*/*Freiling*, JR 2023, 366, 370.

10 *Niedernhuber*, JA 2018, 169, 170 f.; *Rückert*/*Meyer-Wegener*/*Safferling*/*Freiling*, JR 2023, 366, 370.

11 BT-Drs. 18/12785, S. 51; *Wolter*/*Greco*, in SK-StPO, Bd. 2, 6. Aufl. 2023, § 100a Rn. 77.

12 *Hauck*, in Löwe-Rosenberg, StPO, Bd. 3/1, 27. Aufl. 2019, § 100a Rn. 105 f.; *Rückert*, in MüKo (Fn. 6), § 100b Rn. 22.

13 *Rückert*, in MüKo (Fn. 6), § 100a Rn. 214 ff.

14 Vgl. *Rückert*, in MüKo (Fn. 6), § 100b Rn. 38 ff.

System zugegriffen wird.[15] Daher komme als Rechtsgrundlage für die Aufzeichnung der Chats nur § 100a Abs. 1 S. 1 in Betracht.[16] Es werde dabei gerade nicht auf den gesamten Server des Providers, welcher stets ein IT-System darstellt, zugegriffen. Vielmehr würden ausschließlich die spezifischen Chatinhalte vom Server über den Zweitzugang an die Ermittlungsbehörden übermittelt.[17] Zudem sei in diesen Fällen die Eingriffsintensität gering, sodass die strengeren Einschränkungen der Quellen-TKÜ nicht geboten seien. Auch die Mitwirkung des Providers sei hierbei nicht notwendig.[18] Nach dieser Ansicht wurde also im konkreten Fall, bei welchem ein Account-Cloning von den Ermittlungsbehörden eingesetzt wurde, nicht in ein IT-System eingegriffen, sodass die richtige Rechtsgrundlage nur § 100a Abs. 1 S. 1 sein konnte. Diese beschränke die Überwachung nicht auf die laufende Kommunikation, sodass auch der Zugriff auf retrograde, also vergangene Chatinhalte zulässig sei.[19] Im vorliegenden Fall hätten folglich alle Chatinhalte erhoben und verwertet werden dürfen.

Eine **andere Ansicht** bejaht in den Fällen des Account-Clonings einen Eingriff in ein IT-System.[20] Durch dieses Vorgehen werde eine neue Kommunikationsleitung zu einem Gerät, meist dem Server des Providers, geschaffen, von dem jegliche Chatnachrichten des Betroffenen ohne dessen Einverständnis in Kopie an die Ermittlungsbehörde übermittelt werden.[21] Dieser neu geschaffene Zugriff stelle einen Eingriff in die Integrität des dem Betroffenen zugewiesenen Speicherplatzes auf dem Server des Providers dar. Mithin liege ein IT-System vor. Außerdem sei die Eingriffsintensität hier hoch, da beim Account-Cloning Veränderungen der Kommunikationsdaten vorgenommen werden könnten, bspw. durch das Versenden weiterer Nachrichten durch die Polizeibeamten über den Account des Betroffenen.[22] Folglich seien die deutlich strengeren Voraussetzungen der Quellen-TKÜ und Online-Durchsuchung, insbesondere der Einschränkungen bzgl. Veränderungen, notwendig. Darüber hinaus sei die Mitwirkung des Providers für Maßnahmen nach § 100a Abs. 1 S. 1 zwingend erforderlich, sodass diese Rechtsgrundlage beim Account-Cloning, welches typischerweise ohne Zutun des Providers stattfindet, von vornherein ausscheidet.[23] Deshalb sei beim Überwachen verschlüsselter Messengerinhalte grds. § 100a Abs. 1 S. 2, 3 die Rechtsgrundlage für den Zugriff auf die ab dem Anordnungszeitpunkt versendeten Chatnachrichten.[24] Wegen der Beschränkung in § 100a Abs. 5 S. 1 Nr. 1 dürften retrograde Chatinhalte nur nach § 100b Abs. 1 erhoben werden.[25] Da beim Account-Cloning der gesamte Chatinhalt zwischen den Endgeräten des Betroffenen und der Ermittlungsbehörde synchronisiert wird, sei die Auswahl einzelner Chatinhalte derzeit technisch unmöglich. Die Beschränkung des § 100a Abs. 5 S. 1 Nr. 1 werde also nicht eingehalten. Deswegen sieht ein **strengerer Teil der Lit.** innerhalb dieser

---

15 BGH BeckRS 2020, 49703 Rn. 19, 32 ff.; *Graf*, in BeckOK, StPO, 59. Ed., Stand: 02.04.2026, § 100a Rn. 81, 84.

16 BGH BeckRS 2020, 49703 Rn. 19, 32 ff.

17 BGH BeckRS 2020, 49703 Rn. 27, 33.

18 BGH BeckRS 2020, 49703 Rn. 25.

19 BGH BeckRS 2020, 49703 Rn. 32 ff.; NJW 2021, 1252 f.; *Köhler*, in Schmidt/Köhler (Fn. 8), § 100a Rn. 6e; a. A. *Grözinger*, GA 2019, 441, 451 ff.

20 BT-Drs. 19/26424, S. 13 f.; *Rückert*/*Meyer-Wegener*/*Safferling*/*Freiling*, JR 2023, 366, 369; *Rückert*, in MüKo (Fn. 6), § 100b Rn. 39.

21 *Rückert*/*Meyer-Wegener*/*Safferling*/*Freiling*, JR 2023, 366, 369 f.

22 *Rückert*, in MüKo (Fn. 6), § 100b Rn. 39a.

23 *Rückert*/*Meyer-Wegener*/*Safferling*/*Freiling*, JR 2023, 366, 369; *Wolter*/*Greco*, SK-StPO (Fn. 11), § 100a Rn. 32.

24 *Henrichs*/*Weingast*, in KK-StPO, 9. Aufl. 2023, § 100a Rn. 26a, 44; *Köhler*, in Schmidt/Köhler (Fn. 8), § 100a Rn. 14a, 14b, 14h; *Rückert*, in MüKo (Fn. 6), § 100b Rn. 39.

25 *Henrichs*/*Weingast*, in KK-StPO (Fn. 24), § 100a Rn. 26a; *Köhler*, in Schmidt/Köhler (Fn. 8), § 100a Rn. 14a, 14b, 14h.

Ansicht bei solchen Maßnahmen § 100b Abs. 1[26] als einzig verbleibende Rechtsgrundlage.[27] Dies gelte auch, wenn lediglich die Überwachung der zukünftigen Kommunikation bezweckt wird. In unserem Fall läge daher nach dieser Ansicht ein Eingriff in ein IT-System vor, und dieser hätte insgesamt nach § 100b Abs. 1 angeordnet werden müssen.

Nach der **weiteren Ansicht in der Lit.** hätten nur die Chatinhalte vom 21.03.2022 bis zum 26.03.2022 nach § 100a Abs. 1 S. 2, 3 erhoben und im Gerichtsprozess verwertet werden dürfen. Bzgl. der retrograden Chatinhalte hätte zusätzlich eine Anordnung nach § 100b Abs. 1 ergehen müssen, für die gem. § 100e Abs. 2 S. 1 eine besondere Kammer des LG zuständig ist. Da eine solche Anordnung vorliegend nicht erging, wäre die Erhebung der retrograden Chatinhalte rechtswidrig. Nach der **strengeren Ansicht in der Lit.** hätte hingegen von vornherein eine Anordnung nach § 100b Abs. 1, 100e Abs. 2 S. 1 ergehen müssen. Eine solche Erhebung wäre nach § 100b Abs. 1 auch unabhängig von der fehlenden Anordnung rechtswidrig gewesen, weil hier keine Katalogtat i.S.d. § 100b Abs. 2 vorliegt.

3. Kernaussagen der Entscheidung

Die Verfahrensrüge des A hat bzgl. der Verwertung der retrograden Chatinhalte Erfolg, sodass der BGH das vorinstanzliche Urteil in zwei Fällen aufhebt und zu neuer Verhandlung an eine andere Strafkammer des LG zurückverweist.

Die Erhebung der retrograden Chatinhalte sei rechtswidrig erfolgt. Entgegen der Auffassung des LG stelle die „Aufschaltung" auf den Telegram-Account des A eine Quellen-TKÜ gem. § 100a Abs. 1 S. 2, 3 dar. Eine solche Maßnahme sei ein Eingriff in ein IT-System, da Messengerdienste wie Telegram regelmäßig ein solches darstellten. In dieses habe das BKA ohne Mitwirkung des Providers mit technischen Mitteln eingegriffen, sodass die Maßnahme nicht von § 100a Abs. 1 S. 1 erfasst sei. Damit weicht der BGH ausdrücklich von der Auffassung des Ermittlungsrichters beim BGH ab, welcher in einem ähnlich gelagerten Fall § 100a Abs. 1 S. 1 als Rechtsgrundlage sah.[28] Der BGH begründet seine Ansicht damit, dass der Zugriff ohne Mitwirkung des Providers stattfindet und Kommunikationsdaten auch verändert werden können.

Zwar habe der Gesetzgeber bei der Einführung der Quellen-TKÜ die „Aufschaltung" noch nicht im Sinn gehabt, jedoch sei sie vom Wortlaut, Normzweck und der Eingriffsintensität erfasst. In der Folge hätte also die Beschränkung des § 100a Abs. 5 S. 1 Nr. 1 eingehalten werden müssen. Danach hätten lediglich die nach der richterlichen Anordnung versendeten Chatnachrichten überwacht und aufgezeichnet werden dürfen. Hierbei sei auf den Zeitpunkt der Anordnung der konkreten Maßnahme und nicht auf den Zeitpunkt einer früher angeordneten Überwachung abzustellen. Folglich hätten die vor dem 21.03.2022 versendeten Chatinhalte nur im Rahmen einer Online-Durchsuchung erhoben werden dürfen. Diese scheiterte – unabhängig vom Vorliegen der weiteren Voraussetzungen – bereits an der fehlenden Anordnung durch eine besondere Kammer des LG gem. § 100e Abs. 2 S. 1. Aufgrund der rechtsgrundlosen Erhebung der retrograden Chatinhalte liege diesbezüglich ein Beweiserhebungsverbot vor. Die nach der st. Rspr.[29] für die Annahme eines Beweisverwertungsverbots zudem erforderliche

---

[26] § 100b wurde vom BVerfG am 24.06.2025 (BeckRS 2025, 19413) wegen Verletzung des Zitiergebots lediglich für mit der Verfassung unvereinbar erklärt. Daher kann die Norm trotz ihrer Verfassungswidrigkeit weiter als Rechtsgrundlage herangezogen werden.

[27] *Köhler*, in Schmidt/Köhler (Fn. 8), § 100a Rn. 14b; § 100b Rn. 2a; *Rückert*, in MüKo (Fn. 6), § 100b Rn. 39 ff.; *Rückert*/*Meyer-Wegener*/*Safferling*/*Freiling*, JR 2023, 366, 369 f.

[28] Zur Aufschaltung auf einen WhatsApp-Account: BGH BeckRS 2020, 49703 Rn. 19, 32 ff.

[29] BVerfG BeckRS 2024, 33588 Rn. 97; BeckRS 2025, 25383 Rn. 25; BGH NJW 2007, 2269, 2271; NJW 2025, 1584, 1586

Abwägung nahm der BGH mit folgenden Erwägungen vor.

Bei der Einführung der verletzten Norm, § 100a Abs. 1 S. 2, 3, habe der Gesetzgeber die Möglichkeit einer retrograden Überwachung gesehen und sich mit § 100a Abs. 5 S. 1 Nr. 1 ausdrücklich dagegen entschieden. Wird diese vom Gesetzgeber getroffene, eingriffsmindernde Beschränkung nicht eingehalten, handle es sich bei der Überwachungsmaßnahme um einen besonders intensiven Eingriff in das IT-System-Grundrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[30] Lasse man dennoch die Verwertung der retrograden Kommunikation zu, könnte dies zu einer Begünstigung rechtswidriger Beweiserhebungen führen und damit zu Lasten desjenigen gehen, der durch diese Regelung geschützt werden sollte. Überdies stünden die A vorgeworfenen Taten einem Beweisverwertungsverbot nicht entgegen, da es sich zwar um schwere Straftaten i.S.d. § 100a Abs. 2 Nr. 3, jedoch nicht um besonders schwere i.S.d. § 100b Abs. 2 handelt. Die Abwägung führe im konkreten Fall dazu, dass ein Beweisverwertungsverbot bzgl. der retrograden Chatinhalte vorliegt. Da lediglich zwei Verurteilungen auf den unverwertbaren Inhalten beruhten, hebt der BGH nur diese auf, § 337 Abs. 1.

4. Konsequenzen für Ausbildung und Praxis

Mit dem Beschluss klärt der BGH erstmals höchstrichterlich die Rechtsgrundlage für die Erhebung von Chatinhalten beim Account-Cloning. Diese Entscheidung ist insbesondere für die Praxis hilfreich, denn sie verschafft Ermittlungsrichtern und der StA Klarheit darüber, von welcher Rechtsgrundlage solche Maßnahmen erfasst sind. Soll auf Chatinhalte, die vor der richterlichen Anordnung versendet wurden, zugegriffen werden, ist dies nur unter den strengeren Voraussetzungen des § 100b Abs. 1 möglich. Diese lagen in unserem Fall unabhängig von der Anordnung gem. § 100e Abs. 2 S. 1 mangels Katalogtat i.S.d. § 100b Abs. 2 nicht vor, sodass auch der materielle Tatbestand des § 100b nicht erfüllt war. Die Überwachung und Aufzeichnung der danach versendeten Chatinhalte ist hingegen auch von § 100a Abs. 1 S. 2, 3 gedeckt. Werden retrograde Chatinhalte nicht gem. § 100b Abs. 1 erhoben, führt dies regelmäßig zu einem Beweisverwertungsverbot. Die Ausführungen des BGH zur Abwägung bieten zudem Richtwerte für die konkrete Einzelfallprüfung. Darüber hinaus ist auf die Relevanz eines rechtzeitigen Widerspruchs des Verteidigers in der Hauptverhandlung bzgl. der Beweiserhebung hinzuweisen. Anderenfalls ist die Rüge des Beweiserhebungsverbots nach der Widerspruchslösung des BGH präkludiert.[31]

Für die juristische Ausbildung ist insbesondere die Prüfung eines Beweisverwertungsverbots im strafprozessualen Teil einer Klausur von großer Bedeutung.[32] Allerdings ist zu beachten, dass die heimlichen Maßnahmen nach §§ 100a ff. nicht zum Pflichtstoff des ersten Staatsexamens in Bayern – in Würzburg jedoch zum strafrechtlichen Schwerpunkt – gehören und deshalb im Staatsteil der Prüfung keine vertieften Kenntnisse, u.a. zum Streitstand um den Begriff des IT-Systems, erwartet werden können. Vielmehr müsste auf die relevanten Normen hingewiesen werden. Von den Studierenden wird dann vor allem die präzise Arbeit mit dem Gesetz verlangt.

5. Kritik

Grundsätzlich ist die Entscheidung des BGH nachvollziehbar und im Ergebnis überzeugend. Wirkt der Provider nicht mit und ist eine Änderung der Kommunikationsdaten möglich, sind bei solchen Maßnahmen zwingend die vom Gesetzgeber eingeführten eingriffsmindernden Beschränkungen des § 100a Abs. 5 bzw. § 100b Abs. 4 notwendig, um den Eingriff

[30] BVerfG BeckRS 2025, 19413, Rn 220 ff., 235.

[31] St. Rspr. BVerfGE 130, 1; BGH NJW 1992, 1463, 1466; NJW 2006, 707.

[32] Vgl. *Heinrich*/*Reinbacher* (Fn. 3), S. 146 ff.

in die Grundrechte (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1 GG) des Betroffenen zu rechtfertigen. Somit ist es überzeugend, dass § 100a Abs. 1 S. 1 das Account-Cloning als Rechtsgrundlage nicht erfasst. Auch, dass nur die Online-Durchsuchung die Erhebung von retrograden Chatinhalten erfasst, ist nicht zu beanstanden. Dass die Quellen-TKÜ hierfür nicht in Frage kommt, geht schon ausdrücklich aus § 100a Abs. 5 S. 1 Nr. 1 hervor.

Von welcher Rechtsgrundlage die Erhebung zukünftiger, also ab der richterlichen Anordnung versendeter, Chatinhalte erfasst ist, bedarf einer näheren Betrachtung. Für den strengeren Teil der Literatur spricht zunächst der eindeutige Wortlaut des § 100a Abs. 5 S. 1, wonach bei der Maßnahme „technisch sicherzustellen" ist, dass nur die ab der richterlichen Anordnung getätigte Kommunikation überwacht und aufgezeichnet wird, sowie dass nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind. Daher könne jedes Account-Cloning ausschließlich von § 100b Abs. 1 gedeckt sein. Das Problem ist dabei hauptsächlich die automatische Synchronisation sämtlicher Chatinhalte, also auch der retrograden Nachrichten, innerhalb aller angemeldeten Geräte. Dieser Vorgang kann beim Account-Cloning nicht verhindert werden, da über den Server des Providers nicht durch Hacking die Kontrolle erlangt wird. Vielmehr wird beim Provider der Anschein erweckt, das neu verknüpfte Endgerät gehöre dem Accountinhaber. Es ist daher zur Bestimmung der Rechtsgrundlage für die Erhebung zukünftiger Chatinhalte zwischen zwei Konstellationen zu unterscheiden. Zum einen könnte das BKA die Chatinhalte direkt im eingeloggten Webclient überwachen und sichern. Dabei wäre es ausgeschlossen, dass die Beschränkungen in § 100a Abs. 5 S. 1 technisch sichergestellt werden können, da hierbei auch Nachrichten versendet und ältere Nachrichten jederzeit eingesehen werden könnten. Hier wäre die Erhebung zukünftiger Chatinhalte richtigerweise ausschließlich auf § 100b Abs. 1 zu stützen. Zum anderen könnte eine Software dazwischengeschaltet werden, die die Chatinhalte aus dem Webclient ausliest und die älteren Inhalte anhand der Timestamps rausfiltert. Die nun formatierten Chatinhalte würden dann den gesetzlichen Anforderungen entsprechend den BKA-Beamten zur Verfügung gestellt. Zwar würden auch die retrograden Inhalte an ein Endgerät des BKA übermittelt werden, allerdings wäre kein Zugriff durch die BKA-Beamten auf diese möglich. Somit wäre eine rechtswidrige Beweiserhebung technisch ausgeschlossen, sodass der gesetzgeberische Wille bzgl. der eingriffsmindernden Beschränkung erfüllt wäre und sodann § 100a Abs. 1 S. 2, 3 greifen würde. Bei der technischen Sicherstellung ist zudem nicht auf die Ausleitung aus dem IT-System, sondern auf die Unmöglichkeit der Kenntnisnahme durch die BKA-Beamten abzustellen. Diese nicht allzu strenge Auslegung der technischen Sicherstellung ist verfassungskonform[33] und empfehlenswert. Wie das BKA das Account-Cloning konkret durchführt, ist nicht bekannt. In diesem Fall wurde jedenfalls keine solche erforderliche Software dazwischengeschaltet, denn anderenfalls hätte das BKA die retrograden Chatinhalte erst gar nicht sichern können. Auch wenn die Entscheidung des BGH im Ergebnis überzeugt, wäre es wünschenswert gewesen, wenn er sich in der Begründung intensiver mit der technischen Sicherstellung beim Account-Cloning und der Definition des IT-Systems auseinandergesetzt hätte, anstatt dieses bzgl. Messengerdiensten einfach anzunehmen.

(Jessica Belz/Simon Nixdorf)

[33] Vgl. BVerfG BeckRS 2016, 44821 Rn. 234; BeckRS 2025, 19412 Rn. 59 f.