

DR. IUR. H. C. GERHARD STRATE
KLAUS-ULRICH VENTZKE
JOHANNES RAUWALD

RECHTSANWÄLTE

DR. IUR. H.C. GERHARD STRATE
KLAUS-ULRICH VENTZKE
JOHANNES RAUWALD
SINA AARON MOSLEHI
RECHTSANWÄLTE

Per beA
An das
Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

Hamburg, am 17.03.2025
168/22, 92/21

Aktenzeichen: 2 BvR 64/23

In dem Verfassungsbeschwerdeverfahren

des

1. **Murat Silgir**

2. 

wird im Hinblick auf den Beschluss der 1. Kammer des Zweiten Senats des Bundesverfassungsgerichts vom 01.11.2024 in dem Verfahren zum Aktenzeichen 2 BvR 684/22 hier ergänzend Stellung genommen:

Die Kammer erklärt in ihrem Beschluss (Rn. 93), dass „(e)ine Verletzung des allgemeinen Persönlichkeitsrechts des Beschwerdeführers aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG“ ausscheide.

Im weiteren führt sie aus, dass die Verwertung personenbezogener Informationen in einer gerichtlichen Entscheidung – wie im Falle der EncroChat-Daten – zwar in das allgemeine Persönlichkeitsrecht eingreife, dieses Recht jedoch nicht vorbehaltlos gewährleistet und eine Beschränkung zum Schutze überwiegender Allgemeininteressen zulässig sei.¹ Gemäß § 261 StPO dürften rechtmäßig erhobene oder in das Strafverfahren unter Wahrung der verfassungsrechtlichen Anforderungen eingeführte Informationen grundsätzlich verwertet werden.² Wurden diese rechtswidrig erlangt, bestehe von Verfassungs wegen kein Rechtsschutz, wonach ihre Verwertung stets unzulässig wäre. Die Annahme eines Beweisverwertungsverbotes stelle dabei die Ausnahme dar und sei „**nur nach ausdrücklicher gesetzlicher Vorschrift oder aus übergeordneten wichtigen Gründen im Einzelfall**“ anzuerkennen.³ Ein Beweisverwertungsverbot sei aber „**von Verfassungs wegen zumindest bei schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen, bei denen die grundrechtlichen Sicherungen planmäßig oder systematisch außer Acht gelassen worden sind, geboten.**“⁴

Diese Voraussetzungen waren in dem durch das Bundesverfassungsgericht nicht zur Entscheidung angenommenen Fall erfüllt. Die Datenerhebung durch die französischen Behörden erfolgte entgegen den Bestimmungen des § 100b StPO, da bereits kein Tatverdacht gegen den Beschwerdeführer im Zeitpunkt der Anordnung der Ermittlungsmaßnahme vorlag. Daraus folgt auch ein Beweisverwertungsverbot, weshalb das Gericht die Daten gemäß § 100e Abs. 6 Nr. 1 StPO nicht verwenden durfte (1). Ferner war die Verwertung der EncroChat-Protokolle bereits aufgrund der individualschützenden Vorschrift des Art. 31 Abs. 3 RL EEA bzw. § 91g Abs. 6 IRG durch die deutschen Behörden unzulässig (2). Aufgrund dessen verletzte die Verwertung der EncroChat-Daten – entgegen der Ansicht der 1. Kammer des Zweiten Senats des Bundesverfassungsgerichts – den Beschwerdeführer in seinem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

¹ Vgl. BVerfG, Beschluss vom 01.11.2024 – 2 BvR 684/22, Rn. 94 f.

² Vgl. BVerfG, Beschluss vom 01.11.2024 – 2 BvR 684/22, Rn. 96.

³ Vgl. BVerfG, Beschluss vom 01.11.2024 – 2 BvR 684/22, Rn. 97.

⁴ Vgl. BVerfG, Beschluss vom 01.11.2024 – 2 BvR 684/22, Rn. 98.

1.

Soweit das Bundesverfassungsgericht erklärt,

„[d]ass der Bundesgerichtshof die Verwertung der Informationen, (...) vor dem Hintergrund der von ihm vorgenommenen Abwägung der widerstreitenden Interessen davon abhängig macht, ob die Voraussetzungen der – nicht unmittelbar anwendbaren – § 100e Abs. 6, § 100b Abs. 2 Nr. 5 Buchstabe b StPO vorliegen und dabei auf eine Betrachtung zum Verwertungszeitpunkt abstellt, keinen verfassungsrechtlichen Bedenken [begegnet],“⁵

(Hervorhebungen durch den Unterzeichner)

ist dem nicht zuzustimmen. § 100e Abs. 6 StPO regelt die Weiterverwendung von Daten in anderen Verfahren. Der Bundesgerichtshof hatte den Grundgedanken dieser Vorschrift in seinem Beschluss vom 02.03.2022 (5 StR 457/21) aufgrund folgender Überlegungen herangezogen.

*„Bei innerstaatlichen Ermittlungen oder im Wege der europäischen Rechtshilfe ersuchten ausländischen Ermittlungsmaßnahmen wird der – durch Beweisverwertung fortdauernde oder sich vertiefende – Grundrechtseingriff regelmäßig bereits bei der Anordnung der Ermittlungsmaßnahme selbst limitiert (etwa Beschränkung auf besonders schwere Straftaten oder Fälle qualifizierten Verdachts). Kann diese Beschränkung in Fällen wie dem vorliegenden nicht geleistet werden, weil hier durch einen anderen Mitgliedstaat in originärer Anwendung seines nationalen Rechts in die Grundrechte Betroffener eingegriffen wird, **sind die dadurch möglichen Unterschiede bei den Eingriffsvoraussetzungen auf der Ebene der Beweisverwendung zu kompensieren.** Hierfür kann auf die in strafprozessualen Verwendungsbeschränkungen verkörperteten Wertungen zurückgegriffen werden, mit denen der Gesetzgeber dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz bei vergleichbar eingriffsintensiven Mitteln Rechnung trägt (vgl. auch BVerfG, Urteil vom 19. Mai 2020 – 1 BvR 2835/17, BVerfGE 154, 152 ff. Rn. 216 ff.). Im vorliegenden Fall können aufgrund des Gewichts der Maßnahme zur Wahrung des Verhältnismäßigkeitsgrundsatzes – auch um jede denkbare Benachteiligung auszuschließen – **die Grundgedanken der Verwendungsschranke mit dem höchsten Schutzniveau (§ 100e Abs. 6 StPO) fruchtbar gemacht werden.**“⁶*

(Hervorhebungen durch den Unterzeichner)

⁵ Vgl. BVerfG, Beschluss vom 01.11.2024 – 2 BvR 684/22, Rn. 99.

⁶ Vgl. BGH, Beschluss vom 02.03.2022 – 5 StR 457/21 -, juris, Rn. 68.

Der Bundesgerichtshof prüfte den Punkt der rechtmäßigen Anordnung der Ermittlungsmaßnahmen lediglich nach französischem Recht und legte hierbei den Grundsatz des wechselseitigen Vertrauens falsch aus. Eine Prüfung, ob die Anordnung der Telekommunikationsüberwachung auch nach deutschen Maßstäben zulässig gewesen wäre, erfolgte nicht. Nach dem Grundsatz des wechselseitigen Vertrauens ist lediglich zu vermuten, dass die Anordnung der Maßnahme in Frankreich nach den dort geltenden Vorschriften zulässig war. Die Frage der Verwertbarkeit der Daten in einem deutschen Strafverfahren hat sich indes vollständig nach der deutschen Rechtsordnung zu richten.

Dafür muss überprüft werden, ob die Anordnung der ausländischen Ermittlungsmaßnahme auch nach der deutschen Strafprozessordnung rechtmäßig gewesen wäre. Ansonsten würde der Grundsatz des wechselseitigen Vertrauens zu einer Rechtsangleichung verschiedener nationaler Strafprozessordnungen führen, und mithin zu einer Ausweitung der Kompetenzen der Ermittlungsbehörden. Dies war von dem europäischen Gesetzgeber hingegen ersichtlich nicht gewollt. So betont auch der Gerichtshof der Europäischen Union in seinem Urteil vom 30.04.2024, dass der „*Erlass einer Europäischen Ermittlungsanordnung allein vom Recht des Anordnungsstaates abhängt.*“⁷ Ferner führte der Gerichtshof aus:

*„Sodann ergibt sich aus dem Wortlaut von Art. 6 Abs. 1 Buchst. b der Richtlinie 2014/41 sowie aus der Unterscheidung in Art. 1 Abs. 1 dieser Richtlinie, auf die in Rn. 71 des vorliegenden Urteils hingewiesen worden ist, dass, wenn „die in der EEA angegebene Ermittlungsmaßnahme“ in der Erlangung von Beweismitteln besteht, die sich bereits im Besitz der zuständigen Behörden des Vollstreckungsstaats befinden, d. h. der Übermittlung dieser Beweismittel an die zuständigen Behörden des Anordnungsstaats, **eine solche Anordnung nur unter der Voraussetzung erlassen werden kann, dass diese Übermittlung „in einem vergleichbaren innerstaatlichen Fall unter denselben Bedingungen [hätte] angeordnet werden können**“.*

(...)

*Daraus folgt, dass eine Anordnungsbehörde, wenn sie Beweismittel erlangen möchte, die sich bereits im Besitz der zuständigen Behörden des Vollstreckungsstaats befinden, eine Europäische Ermittlungsanordnung **davon abhängig machen muss**, dass alle im Recht ihres eigenen Mitgliedstaats für einen vergleichbaren innerstaatlichen Fall vorgesehenen Bedingungen erfüllt sind.*“⁸

(Hervorhebungen durch den Unterzeichner)

⁷ Vgl. EuGH, Urteil vom 30.04.2024 – C-670/22, Rn. 92.

⁸ Vgl. EuGH, Urteil vom 30.04.2024 – C-670/22, Rn. 91 ff.

Dies steht auch im Einklang mit dem Sinn und Zweck der Vorschrift des Art. 6 Abs. 1 b) RL EEA, die insbesondere einen „*ungewollten Kompetenzzuwachs für die nationalen Strafverfolgungsbehörden [vermeiden]*“ soll.⁹

Darüber hinaus ergibt sich aus der RL EEA selbst, dass vor allem im Rahmen der grenzüberschreitenden Telekommunikationsüberwachung die Vorschriften des überwachten Mitgliedstaates (hier Deutschland) im Zeitpunkt der Erhebung maßgeblich sind. Diese sieht in Kapitel V dafür besondere Vorschriften vor.

Gemäß Art. 31 Abs. 1 RL EEA muss der überwachende Staat grundsätzlich *vor* der Überwachung den überwachten Staat über die Datenerhebung unterrichten oder dies *umgehend* nachholen. Die Unterrichtungspflicht soll sicherstellen, „*dass eine EEA nicht dazu führen kann, innerstaatliche Befugnis- und Verfahrensnormen zu umgehen*“ und „*ergänzt insoweit den Artikel 6 Absatz 1 Buchstabe b der RL EEA.*“¹⁰

Der deutsche Gesetzgeber baute diesen Schutz noch weiter aus und normierte – anders als Art. 31 Abs. 3 RL EEA – in der Umsetzungsvorschrift des § 91g Abs. 6 IRG eine **Verpflichtung** der deutschen Behörden, wonach sie dem überwachenden Mitgliedstaat (hier Frankreich) innerhalb von 96 Stunden mitteilen müssen, dass die Überwachung zu beenden ist, soweit sie in einem vergleichbaren innerstaatlichen Fall nicht genehmigt werden würden. Die Verpflichtung soll dabei verhindern,

„dass sensible Daten, die aus einer Telekommunikationsüberwachung auf deutschem Hoheitsgebiet gewonnen werden, im europäischen Ausland auch dann verwendet werden, wenn die Überwachung nach deutschem Recht nicht zulässig wäre. Zum Schutz der Grundrechte von betroffenen Personen und zum Schutz der deutschen Staatssouveränität ist Absatz 6 deshalb als verbindliche Regel ausgestaltet.“¹¹

Dass der Gesetzgeber die Verwendung von rechtswidrig erhobenen Daten aus Telekommunikationsüberwachungsmaßnahmen auf deutschem Hoheitsgebiet im Ausland verhindert wissen will, zeigt, dass nichts anderes für die Verwendung eben dieser Daten in deutschen Strafverfahren gelten darf. Um eine Umgehung der **individualschützenden Norm** des § 31 RL EEA¹² zu verhindern, muss daher – zumindest für den Fall der Telekommunikationsüberwachung – stets geprüft werden, ob die Voraussetzungen der §§ 100a ff StPO für die ergriffene ausländische Ermittlungsmaßnahme **im Zeitpunkt ihrer Anordnung** vorlagen.

⁹ Vgl. BT-Drs. 18/9757, S. 23.

¹⁰ Vgl. BT-Drs. 18/9757, S. 44 f.

¹¹ Vgl. BT-Drs. 18/9757, S. 75.

¹² Vgl. EuGH, Urteil vom 30.04.2024 – C-670/22, Rn. 132.

Eine solche Prüfung hätte vorliegend ergeben, dass die Anordnung der Maßnahme nach deutschen Maßstäben rechtswidrig gewesen wäre **(a)** und das Fehlen eines Tatverdachts zu einem Beweisverwertungsverbot geführt hätte **(b)**.

a)

Eine heimliche Online-Durchsuchung setzt nach § 100b StPO den Verdacht einer Straftat voraus. Die Vorschrift schränkt den Kreis der Anlasstaten zudem auf die in seinem Abs. 2 aufgezählten Katalogtaten ein. Der Tatverdacht muss sich dabei auf „*bestimmte Tatsachen*“ beziehen. Vage Anhaltspunkte, bloße Vermutungen oder allgemeine Erfahrungssätze reichen nicht, um eine solche Maßnahme zu rechtfertigen.¹³

Ein solcher Tatverdacht lag weder gegen den Beschwerdeführer noch gegen die sonstigen Nutzer der EncroChat-Handys im Zeitpunkt der Anordnung der Maßnahme vor.

Soweit der Bundesgerichtshof meint, dass die Einleitung des Verfahrens gegen Unbekannt durch die französischen Behörden unbedenklich war, weil die Geräte nicht offiziell im Handel erhältlich und sehr teuer in Anschaffung und Betrieb waren,¹⁴ ist dem entgegenzuhalten, dass der Preis von ca. 1.500,00 € für Anschaffung und halbjährliche Nutzung keinesfalls in einem Kostenbereich liegt, der typischerweise nur durch Straftaten erwirtschaftet werden kann. Darüber hinaus kann eine solch generalisierende Aussage vorliegend bereits aufgrund der sehr unterschiedlichen subjektiven Wahrnehmung davon, was als „*teuer*“ empfunden wird, nicht getroffen werden.

Auch die Nutzung der Handys selbst konnte keinen Tatverdacht gegen die einzelnen EncroChat-User rechtfertigen. Anhaltspunkte dafür, dass alle oder der ganz überwiegende Teil von ihnen eine kriminelle Zielsetzung verfolgten, lagen nicht vor. Dies war bereits aufgrund der hohen Anzahl von über 60.000 Nutzern, von denen mehr als 30.000 durch die ergriffenen Maßnahmen der französischen Behörden abgehört wurden, nahezu ausgeschlossen. Zudem würde eine solche Annahme auf einen Generalverdacht der Begehung (schwerere Straftaten) gegen alle Personen hinauslaufen, die verschlüsselte Telekommunikationsdienste wie EncroChat benutzen. Für einen solchen besteht jedoch keine rechtliche Grundlage.¹⁵

Soweit sich der Tatverdacht lediglich gegen die Betreiber richten sollte, ist nicht ersichtlich, wie das Ausspähen der Telekommunikationsdaten der einzelnen Nutzer Erkenntnisse hinsichtlich von ihnen begangener Straftaten liefern sollte. Für die Anordnung einer Telekommunikationsmaßnahme gegen „Dritte“ wäre zudem eine „*sichere Tatsachenbasis*“ notwendig gewesen,¹⁶ welche hier ebenfalls nicht vorlag.

¹³ Vgl. BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07 –, juris Rn. 250 f.

¹⁴ Vgl. BGH, Beschluss vom 02.03.2022 – 5 StR 457/21 –, juris, Rn. 35.

¹⁵ Vgl. BVerfG, Stattgebender Kammerbeschluss vom 9. Februar 2005 – 2 BvR 1108/03 –, juris Rn.20.

¹⁶ Vgl. BVerfG, Urteil vom 12. März 2003 – 1 BvR 330/96 –, BVerfGE 107, 299-339.

b)

Aus der nach deutschen Maßstäben rechtswidrigen Datenerhebung der EncroChat-Protokolle folgt ferner ein Beweisverwertungsverbot. Wie das Bundesverfassungsgericht zutreffend ausführte, zieht nicht jede rechtswidrige Beweiserhebung ein Beweisverwertungsverbot nach sich. Ein solches kann sich nach den Umständen des Einzelfalls aufgrund eines besonders schwerwiegenden Rechtsverstoßes ergeben, wenn übergeordnete wichtige Gründe das staatliche Interesse an der Wahrheitsforschung und die Belange einer funktionstüchtigen Strafrechtspflege überwiegen.¹⁷

Dies war hier der Fall.

Nach der Rechtsprechung des Bundesgerichtshofs

*„dürfen mit Blick auf die Grundsätze eines **rechtsstaatlichen Verfahrens** die aus einer Telekommunikations-Überwachungsmaßnahme gewonnenen Erkenntnisse **nicht als Beweismittel verwendet werden, falls wesentliche sachliche Voraussetzungen für die Anordnung der Überwachungsmaßnahme fehlen.**“¹⁸*

(Hervorhebungen durch den Unterzeichner)

Das Erfordernis eines qualifizierten Tatverdachts gegen den Betroffenen ist eine wesentliche sachliche Voraussetzung für die Anordnung einer Maßnahme nach § 100b StPO. An ihn knüpfen sich nicht nur die Rechte des Beschuldigten selbst, sondern auch die entsprechenden Eingriffsbefugnisse der Strafverfolgungsbehörden.¹⁹ Der jeweilige Verdachtsgrad verhindert, dass die Ermittlungsbehörden willkürlich grenzenlos und ohne konkreten Bezug zu einer Straftat Daten erheben und sammeln.²⁰ Die Anordnung einer Maßnahme nach § 100b StPO ohne jeglichen Tatverdacht gegen die betroffene Person ist daher unter keinem rechtlichen Gesichtspunkt vertretbar und objektiv willkürlich.²¹

¹⁷ Vgl. BGH, Beschluss vom 03.05. 2018 – 3 StR 390/17 – juris Rn. 24.

¹⁸ Vgl. BGH, Beschluss vom 7. März 2006 – 1 StR 316/05 –, BGHSt 51, 1-9 –, juris Rn. 7 m.w.N.

¹⁹ Vgl. BGH, Beschluss vom 29. August 1989 – 1 StR 453/89 –, juris Rn. 3; *Mavany* in Löwe-Rosenberg StPO Band 5/1, 27. Aufl. 2020, § 152 Rn. 28.

²⁰ Vgl. *Peters* in MüKo StPO, 2. Aufl. 2024, § 152 Rn. 34.

²¹ Vgl. BVerfG, Stattgebender Kammerbeschluss vom 30. November 2021 – 2 BvR 2038/18 –, juris; BVerfG, Urteil vom 12. März 2003 – 1 BvR 330/96 –, BVerfGE 107, 299-339 –, juris Rn. 78, 80 ff; LG Berlin, Beschluss vom 27. Juni 2008 – 525 Qs 102/08 –, juris Rn. 4; Diemer in KK StPO, 9. Aufl. 2023, § 152 Rn. 3.

Auch die besondere Schwere der aufzuklärenden Tat vermag an diesem Ergebnis nichts zu verändern. Würde man im Rahmen der Verhältnismäßigkeitsprüfung zu dem Schluss kommen, dass die Ergreifung einer Maßnahme nach § 100d StPO ohne Vorliegen eines Tatverdachts dennoch aufgrund der Schwere der Tat nicht zu einem Beweisverwertungsverbot führt, würde der Schutzzweck des Tatverdachtserfordernisses in den Fällen der §§ 100 a ff StPO gänzlich leerlaufen²² und zu einer vom deutschen Gesetzgeber nicht gewollte *Wahrheitserforschung um jeden Preis*²³ führen.

c)

Die in dem Ausgangsverfahren erhobenen Daten unterlagen damit – nach deutschen Maßstäben – einem Beweisverwertungsverbot. Sie durften daher vom Tatgericht nicht verwendet werden.

2.

Ein Beweisverwertungsverbot ergibt sich zudem aus der Vorschrift des Art. 31 Abs. 3 RL EEA bzw. § 91g Abs. 6 IRG selbst. Diesbezüglich hatte der Unterzeichner bereits in seinem ergänzenden Schriftsatz an das Bundesverfassungsgericht vom 16.12.2024 in Bezug auf das Urteil des Gerichtshofs der Europäischen Union vom 30.04.2024 umfangreiche Ausführungen gemacht, sodass – um Wiederholungen zu vermeiden – auf diesen verwiesen wird.



Dr. iur. h.c. Gerhard Strate
Rechtsanwalt

²² Nach diesen Vorschriften ist eine (besonders) schwere Straftat bereits Tatbestandsvoraussetzung.

²³ Vgl. OLG Hamburg, Beschluss vom 29.06.2007 – 3-30/07, NStZ-RR 2008, 144.