- dd) Bei vorgelegten HartzIV Bescheiden.⁸⁰
- ee) Entreicherung bzw. Unverhältnismäßigkeit bei Eröffnung des Insolvenzverfahrens über das Vermögen des Einziehungsadressaten.⁸¹
- ff) Entreicherung, wenn der inhaftierte Verurteilte nachgewiesen über kein Vermögen mehr verfügt.⁸²
- gg) Bei schwerer Krankheit und Rückkehr in den Heimatstaat.⁸³
- hh) Schulden beim Finanzamt, Abgabe einer eidesstattlichen Versicherung, Bezug von staatlichen Unterstützungsleistungen nach dem SGB II.⁸⁴

5. Vollstreckung der Einziehungsentscheidung, Durchsuchung nach § 459g Abs. 3 StPO

Die Durchsuchung gem. § 459g Abs. 3 StPO ist nur zulässig, wenn die begründete Aussicht besteht, dass die Durchsuchung zum Auffinden von Vermögenswerten führt, die für die Vollstreckung der Wertersatzeinziehung verwertet werden können.⁸⁵

6. Entschädigung Tatverletzter im Vollstreckungsverfahren, § 459h Abs. 2 StPO

Das Finanzamt kann Verletzter der Steuerstraftat sein, aus welcher der Einziehungsbetroffene "etwas erlangt" hat.⁸⁶ Wird die Gewerbesteuer von der Gemeinde erhoben, so ist die Gemeinde Verletzte der Hinterziehung der Gewerbesteuer.⁸⁷

⁷⁹ LG Stralsund, Beschl. v. 30.1.2019 – 26 Qs 2/19.

⁸⁰ AG Lübeck, Beschl. v. 11.6.2019 - 76 Cs 720 Js 44047/18

⁸¹ AG Kiel, Beschl. v. 5.4.2019 - BwR 48 Cs 544 Js 13662/12 für Entreicherung, weitere Vollstreckung unverhältnismäßig; AG Mannheim, 4 Ls 622 Js 24240/16 für Unverhältnismäßigkeit A.A. OLG München, Beschl. v. 12.2.2019 – 3 Ws 939/18, weder Entreicherung noch Unverhältnismäßigkeit (Schutz durch Verbot der Einzelzwangsvollstreckung, § 89 InsO).

⁸² LG Mannheim, Beschl. v. 3.9.2019 – 19 StVK 246/19.

⁸³ AG Nürtingen, Beschl. v. 30.1.2018 - 16 Ds 85 Js 92420/17.

⁸⁴ LG Bochum, Beschl. v. 24.4.2020 – II-12 KLS- 450 Js 18/16-6/19.

⁸⁵ LG Lübeck, Beschl. v. 18.10.2019 - 6 KLS 6/16.

⁸⁶ OLG Hamburg, Beschl. v. 26.10.2018; OLG Stuttgart, Beschl. v. 25.10.2017 – 1 Ws 163/17.

⁸⁷ LG Hamburg, Beschl. v. 16.5.2018 – 618 Qs 14/18.

Strafprozessrecht

Rechtsanwalt Dr. Mayeul Hiéramente, Hamburg

Der irrlichternde 5. Strafsenat – Kein heimlicher Zugriff auf Alt-E-mails nach § 100a StPO, zugleich eine Anmerkung zu BGH, Beschl. v. 14.10.2020 – 5 StR 229/19

I. Einleitung

Die Kommunikation per E-Mail ist weder aus dem Berufs- noch dem Privatleben wegzudenken. Aufgrund der einfachen und ubiquitären Nutzung schlummert in E-Mail-Postfächern eine Masse an Informationen, die tiefgreifende Einblicke in die wirtschaftlichen Verhältnisse von Unternehmen und das Privatleben der jeweiligen Nutzer erlaubt. Dabei ist es keine Seltenheit, dass sich über ein E-Mail-Postfach die Kommunikation des Nutzers über Jahre oder gar Jahrzehnte zurückverfolgen und analysieren lässt. Die Nutzung von E-Mails ist darüber hinaus auch deshalb sensibel, weil sich der Bürger hierfür der Hilfe Dritter bedienen muss. So ist der Bürger für die

Nutzung eines E-Mail-Postfachs regelmäßig auf die Mitwirkung eines externen Providers angewiesen, bei dem auch Kopien der erhaltenen und versandten E-Mails gespeichert werden. Eine rein lokale Speicherung von E-Mails ist heutzutage eher die Seltenheit. Dies wirft die strafprozessuale Frage auf, unter welchen Bedingungen Strafverfolgungsbehörden auf beim Provider gespeicherte E-Mails zugreifen dürfen und ob derartige Zugriffe offen zu erfolgen haben oder ob ggfs. auch ein heimlicher Zugriff gestattet ist.

Diese Frage schien in der gerichtlichen Praxis weitgehend geklärt. So haben Bundesverfassungsgericht und Bundesgerichtshof eine Beschlagnahme der E-Mails nach § 94 StPO als zulässig erachtet.¹ Da es sich hierbei jedoch um eine offene Ermittlungsmaßnahme handelt, sind die Ermittlungsbehörden dazu verpflichtet, den Beschuldigten nach § 33 Abs. 1, § 35 Abs. 2 StPO hierüber in Kenntnis zu setzen. Diese Benachrichtigung darf nicht aus ermittlungstaktischen Gründen zurückgestellt werden.² Daneben ist nach Ansicht der Rechtsprechung eine heimliche Überwachung der laufenden E-Mail-Kommunikation unter den Voraussetzungen des § 100a Abs. 1 StPO zulässig.³ Die Ermittlungsbehörden können bei ausreichender Schwere des Tatvorwurfes mithin um gerichtliche Anordnung einer Telekommunikationsüberwachung (TKÜ) ersuchen und – befristet auf die Laufzeit der Anordnung (3 Monate) – die ausgetauschten E-Mails mitlesen. Der 5. Strafsenat überrascht nun mit einer Entscheidung, die auch einen heimlichen Zugriff auf Alt-E-mails – also E-Mails die vor Erlass einer TKÜ-Anordnung erhalten oder versandt wurden – nach § 100a Abs. 1 S. 1 StPO zulassen will. Die Ermittlungsbehörden sollen auf diese Weise ermächtigt werden, auch in der gesamten Historie des E-Mail-Accounts zu stöbern.

II. Die Entscheidung des 5. Strafsenats

Hintergrund des Verfahrens waren Ermittlungen wegen des Vorwurfs der Marktmanipulation. Zur Beweisführung hatte das Instanzgericht auf E-Mails zurückgegriffen, die versandt worden waren, bevor eine TKÜ-Anordnung nach § 100a Abs. 1 StPO aF erlassen worden war. Der Zugriff erfolgte insoweit heimlich.

Der 5. Strafsenat führt insoweit zunächst aus, dass die spezifische Gefährdungslage für die Freiheitsverbürgung des Art. 10 Abs. 1 GG auch dann bestehe, wenn die E-Mails nach Kenntnissnahme durch den Empfänger beim Provider gespeichert bleiben. Durch die Endspeicherung werde der von Art. 10 Abs. 1 GG zuvörderst geschützte Kommunikationsinhalt infolge der Nutzung eines bestimmten Kommunikationsmediums auf einem vom Kommunikationsmittler bereitgestellten Speicherplatz in einer von keinem Kommunikationsteilnehmer beherrschbaren Sphäre abgelegt. Ein Zugriff auf die dort zwischen- oder endgespeicherten E-Mails sei nach § 100a Abs. 1 StPO aF zulässig. Einem Zugriff stehe auch nicht entgegen, dass das Bundesverfassungsgericht insoweit auch eine Beschlagnahmemöglichkeit für zulässig erachtet habe. Insoweit werde die Anwendung von § 100a StPO nicht durch § 94 StPO verdrängt.

Nachdem die Anwendbarkeit des § 100a Abs. 1 StPO aF dem Grunde nach bejaht wurde, widmet sich der 5. Strafsenat der Frage, ob die Befugnis zur TKÜ auch E-Mails betreffe, die vor Anordnung versandt bzw. empfangen wurden. Dies wird ohne kritische Auseinandersetzung bejaht, wobei der 5. Strafsenat zwei Argumente in den Vordergrund rückt: Zum einen begründet der Senat eine Befugnis nach § 100a Abs. 1 StPO mit einem Erstrechtschluss im Hinblick auf § 94 StPO. Wenn der Zugriff auf Altdaten nach § 94 StPO zulässig sei, müsse dies erst recht für § 100a Abs. 1 StPO aF gelten. Zum anderen führt der Senat einen Umkehrschluss ins Feld. Aus den neu eingeführten Regelungen zur Quellen-TKÜ, die nur eine Überwachung der laufenden Telekommunikation zulassen, müsse man schließen, dass diese Begrenzung für die „normale“ TKÜ nicht gelte.

III. Kein Zugriff auf Alt-E-mails nach § 100a Abs. 1 S. 1 StPO

Die Entscheidung des 5. Strafsenats ist sowohl im Ergebnis als auch in der Begründung untragbar. Die argumentativen Schwächen lassen den Leser – angesichts der grundrechtlichen Bedeutung der Thematik und der enormen praktischen Relevanz der E-Mail-Kommunikation für Wirtschafts- und Privatleben – sprachlos zurück.

¹ BVerfG, Urt. v. 16.6.2009 - 2 BvR 902/06; BGH, Beschl. v. 24.11.2009 – StB 48/09.

² BGH, Beschl. v. 24.11.2009 – StB 48/09; BGH, Beschl. v. 4.8.2015 – 3 StR 162/15.

³ Vgl. Übersicht bei Gercke in: Gercke/Julius/Temming/Zöllner, Strafprozessordnung, 6. Aufl. 2019, § 100a, Rn. 14; Günther in: MüKoStPO, 1. Aufl. 2014, StPO § 100a Rn. 138 f.; krit. Hauck in: Löwe-Rosenberg, StPO, 27. Aufl. 2018, § 100a, Rn. 77.

Der Senat leitet die Begründung mit einer Analyse der verfassungsgerichtlichen Rechtsprechung zum Anwendungsbereich des Art. 10 Abs. 1 GG ein und konstatiert, dass ein Zugriff auf beim Provider gespeicherte E-Mails einen Eingriff in den Schutzbereich des Fernmeldegeheimnisses darstellt.⁴ So richtig diese Bewertung ist, so wenig aussagekräftig ist sie jedoch für die Frage, ob § 100a Abs. 1 S. 1 GG eine geeignete Rechtsgrundlage für einen derartigen Eingriff darstellt. So ist die strafprozessuale Vorschrift zwar für Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG konzipiert. Dies erlaubt indes nicht den Umkehrschluss, dass sämtliche Eingriffe in das Grundrecht auf diese Rechtsgrundlage gestützt werden können.⁵ Ein Gleichlauf ist vom Gesetzgeber weder gewollt noch bei der Ausformulierung des § 100a StPO umgesetzt worden. § 100a StPO enthält keine Pauschalermächtigung für Eingriffe in Art. 10 Abs. 1 GG, sondern erlaubt nur die Überwachung der Telekommunikation.

Der Wortlaut des § 100a Abs. 1 S. 1 StPO wird vom 5. Strafsenat in der Folge dann auch gänzlich ignoriert, obwohl dieser eine zentrale Stellschraube für die Beantwortung der in der Rede stehenden Rechtsfrage darstellt. So ignoriert der Senat – trotz Rekurses auf den Aufsatz von Grözinger – vollständig, dass § 100a StPO bereits aufgrund der Wahl des Begriffs *Überwachung* nur als Grundlage für eine heimliche Kenntnisnahme des Inhalts einer *laufenden* Kommunikation dienen kann.⁶ Auch die genannte Aufzeichnung spricht deutlich gegen einen Datenzugriff in der Vergangenheit.

Neben dem Wortlaut sprechen auch gewichtige (norm-)systematische Gründe gegen die Annahme eines retrograden Zugriffs auf beim Provider gespeicherte E-Mails. So sieht der Gesetzgeber aufgrund der besonderen Eingriffstiefe heimlicher Ermittlungsmaßnahmen für die Anordnung einer TKÜ eine dreimonatige Befristung vor (§ 100e Abs. 1 S. 4 StPO). Eine solche Beschränkung würde *ad absurdum* geführt, wenn ein zeitlich unbegrenzter Zugriff in der Vergangenheit zulässig wäre.⁷ Deutlich wird dies auch an den Regelungen der Telekommunikations-Überwachungsverordnung, die in § 100a Abs. 4 S. 2 StPO in Bezug genommen wird. Dort heißt es in § 5 u.a.:

„Die zu überwachende Telekommunikation umfasst bei Überwachungsmaßnahmen nach § 100a Absatz 1 Satz 1 der Strafprozessordnung [...] die Telekommunikation, die

1. von der zu überwachenden Kennung *ausgeht*,
2. für die zu überwachende Kennung *bestimmt ist*,
3. in eine Speichereinrichtung, die der zu überwachenden Kennung zugeordnet ist, *eingestellt oder aus dieser abgerufen wird* oder [...]
5. zu einer der zu überwachenden Kennung aktuell zugeordneten anderen Zieladresse *um- oder weitergeleitet wird*, [...]

Der Verpflichtete hat der berechtigten Stelle [...] *den tatsächlichen Einrichtungszeitpunkt* sowie die tatsächlich betroffene Kennung mitzuteilen. Dies gilt entsprechend für die Übermittlung einer Information zum *Zeitpunkt der Beendigung* einer Überwachungsmaßnahme.“

Die TKÜV ist ersichtlich für eine Maßnahme ausgelegt, die der Kenntniserlangung der Ermittlungsbehörden von einer laufenden, der Anordnung nach §§ 100a Abs. 1 S. 1, 100e StPO nachfolgenden Telekommunikation dienen soll. Das Erfordernis der Protokollierung der „tatsächlichen Einrichtungszeit“ verdeutlicht, dass der Gesetzgeber sowohl hinsichtlich des Beginns als auch des Endes der Maßnahme eine zeitliche Begrenzung vornehmen wollte.

Schließlich ist die Beschränkung auf die laufende Kommunikation auch deutlich im Wortlaut der aktuellen Fassung des § 100a StPO niedergelegt. So recurriert § 100a Abs. 1 S. 3, Abs. 5 S. 1 Nr. 1 a) StPO im Hinblick auf die Quellen-TKÜ ausdrücklich auf die *laufende* Kommunikation. Diese Beschränkung gilt – anders als der 5. Strafsenat meint – auch für die „normale“ TKÜ.

Dies ergibt sich eindeutig aus der *Gesetzesbegründung* in der BT-Drs. 18/12785. Es ist insoweit äußerst verwunderlich, dass der 5. Strafsenat diese Begründung als Beleg für die eigene Rechtsauffassung heranzieht. So betont der Gesetzgeber an zahlreichen Stellen und mit klaren Wor-

⁴ Zur Diskussion s. Hauck in: Löwe-Rosenberg, StPO, 27. Aufl. 2018, § 100a, Rn. 76 ff. mwN.

⁵ Zur Problematik im Hinblick auf den Telekommunikationsbegriff s. bereits Wolter/Greco in: SK-StPO, 5. Aufl. 2016, § 100a, Rn. 18; *Hiéramente/Fenina* StraFo 2015, 365, 371.

⁶ S. ausführlich Grözinger GA 2019, 441, 443 ff. Vgl. auch Wolter/Greco in: SK-StPO, 5. Aufl. 2016, § 100a, Rn. 34. Zum Aspekt der laufenden Kommunikation s. auch Hauck in: Löwe-Rosenberg, StPO, 27. Aufl. 2018, § 100a, Rn. 92.

⁷ Grözinger GA 2019, 441, 444.

ten, dass insoweit ein Gleichlauf zwischen Quellen-TKÜ und „normaler“ TKÜ gewollt ist. Um diesen Gleichlauf sicherzustellen, hat der Gesetzgeber gerade die technischen Vorkehrungen in § 100a Abs. 5 S. 1 Nr. 1 a) StPO eingefügt.⁸ Die folgenden Passagen aus der Gesetzesbegründung zeigen dies in unmissverständlicher Klarheit:

„Die Regelung des § 100a StPO enthält *derzeit* unstreitig eine Rechtsgrundlage zur Erhebung derjenigen Kommunikationsinhalte, die während der Übertragung von einem Kommunikationsteilnehmer zu einem anderen während des *laufenden* Übertragungsvorgangs im öffentlichen Telekommunikationsnetz überwacht und aufgezeichnet werden können.“ (BT-Drs. 18/12785, S. 48).

und

„Ebenso wie bei der Sprach- und Videotelefonie darf das Ausleiten von Messenger-Nachrichten am Endgerät nur dann erfolgen, wenn dies ein *funktionales Äquivalent* zur Überwachung und Ausleitung der Nachrichten aus dem Telekommunikationsnetz darstellt. Die vorgeschlagenen Änderungen setzen folglich ausschließlich das Ziel um, den technischen Entwicklungen der Informationstechnik Rechnung zu tragen und – ohne Zugriff auf weitere gespeicherte Inhalte des informationstechnischen Systems – eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist. Um die *funktionale Äquivalenz auch in zeitlicher Hinsicht* zu gewährleisten, ist technisch sicherzustellen, dass über Messenger-Dienste versandte Nachrichten *erst ab dem Zeitpunkt der Anordnung* durch das Gericht bzw. – in Eilfällen – der Staatsanwaltschaft ausgeleitet werden dürfen. *Auch im Rahmen der herkömmlichen Telekommunikationsüberwachung können Kommunikationsinhalte erst von diesem Zeitpunkt an ausgeleitet werden.* (BT-Drs. 18/12785, S. 50).

und

„Soll hingegen eine Ausleitung aller Nachrichten in zeitlich unbegrenzter Hinsicht erfolgen, würde das über die *herkömmlichen Möglichkeiten der Telekommunikationsüberwachung weit hinausgehen* und eine – wenngleich auf Kommunikationsinhalte eines Kommunikationsdienstes begrenzte – „kleine“ Online-Durchsuchung darstellen. Das Ausleiten von Nachrichten, die vor dem Anordnungszeitpunkt abgesendet oder empfangen wurden, findet seine Rechtsgrundlage folglich nicht in § 100a StPO, sondern in der für die Online-Durchsuchung neu geschaffenen Ermächtigungsgrundlage des § 100b StPO. (BT-Drs. 18/12785, S. 50).

und

„Um die *funktionale Äquivalenz* mit der herkömmlichen Telekommunikationsüberwachung zu gewährleisten, dürfen nur solche Kommunikationsinhalte und -umstände erhoben werden, die auch *während des laufenden Übertragungsvorgangs* im öffentlichen Telekommunikationsnetz in verschlüsselter Form erhoben werden könnten.“ (BT-Drs. 18/12785, S. 51).

und

„Um die *funktionale Äquivalenz* zur herkömmlichen Telekommunikationsüberwachung *auch in zeitlicher Hinsicht* zu gewährleisten, dürfen *nur zukünftige Kommunikationsinhalte* erhoben werden [...].“ (BT-Drs. 18/12785, S. 53).

Der Gesetzgeber hat insoweit für die Quellen-TKÜ keinen anderen zeitlichen Anwendungsbereich definiert, sondern dafür Sorge getragen, dass auch beim Einsatz technischer Mittel zur Umgehung einer Verschlüsselung nur das funktionelle Äquivalent – die laufende Kommunikation – überwacht wird.⁹ Dieses Verständnis dürfte im Übrigen auch beim Bundesverfassungsgericht vorgeherrscht haben, als es im Hinblick auf die Quellen-TKÜ darauf hinwies, dass die mit der Infiltration einhergehende „Gefährdung weit über die hinaus [geht], die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist.“¹⁰ U.a. auf diese Entscheidung hat der Gesetzgeber mit der Reform des § 100a StPO reagiert. Insoweit sind durch den Gesetzgeber sowohl rechtliche Schranken definiert (§ 100a Abs. 1 S. 3 StPO) als auch technische Begrenzungen gefordert worden (§ 100a Abs. 5 S. 1 Nr. 1 a) StPO). Es ist angesichts der Gesetzesbegründung und -ausgestaltung abwegig, hier einen Umkehrschluss ziehen zu wollen.¹¹ Die

⁸ S. ausführlich BT-Drs. 18/12785, S. 46 ff.

⁹ S. auch *Bruns* in: KK-StPO, 8. Aufl. 2019, StPO § 100a Rn. 7; *Gercke* in: Gercke/Julius/Temming/Zöller, StPO, 6. Aufl. 2019, § 100a, Rn. 30.

¹⁰ BVerfG, Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, Rn. 188.

¹¹ S. bereits *Grözinger* GA 2019, 441, 446 mwN.

Gesetzesreform belegt gerade die vom Gesetzgeber intendierte zeitliche Beschränkung sämtlicher TKÜ-Maßnahmen. Es verwundert insoweit auch nicht, dass sich der 5. Strafsenat insoweit auf keine belastbare Quelle zu stützen vermag. Der Autor der in Bezug genommenen Kommentartabelle¹² ist als erkennender Richter in diesem Beschluss jedenfalls keine geeignete (externe) Referenz.

Ebenso wenig ist ein Erst-Recht-Schluss im Hinblick auf die Zulässigkeit der Beschlagnahme von E-Mails nach § 94 StPO statthaft. Es ist nicht erklärlich, wie der 5. Strafsenat hier argumentativ einen Erst-Recht-Schluss herzuleiten gedenkt. Zum einen handelt es sich bei der Vorschrift des § 94 StPO um eine Regelung, die einen gänzlich anderen Regelungsinhalt aufweist (*Beschlagnahme vs. Überwachung*). Es ist auch in der Rechtsprechung des Bundesgerichtshofs anerkannt, dass § 94 StPO wesensverschieden ist.¹³ Zum anderen verbietet sich ein Rückschluss bereits deshalb, weil der Gesetzgeber bewusst gänzlich unterschiedliche Grundlagen für heimliche und offene Ermittlungsmaßnahmen geschaffen hat. Das Bundesverfassungsgericht betont insoweit auch die besondere Eingriffstiefe heimlicher Maßnahmen.¹⁴ Ein Erst-Recht-Schluss von Äpfeln auf Birnen ist nicht zulässig.

Schließlich steht die Interpretation des 5. Strafsenats auch verfassungsrechtlich auf wackeligen Füßen. So hat der Gesetzgeber richtigerweise darauf hingewiesen, dass ein Rückgriff auf Alt-E-mails einer „kleinen Online-Durchsuchung“ gleichkäme und daher nur unter den Voraussetzungen des § 100b StPO zulässig sein könne.¹⁵ Der 5. Strafsenat, der sich in der Entscheidung nur mit vereinzelt E-Mails zu befassen hat, blendet insoweit aus, welche tiefgreifenden Einblicke ein (heimlicher) Zugriff auf Jahre oder Jahrzehnte von E-Mails erlauben würde. So ist die E-Mail weit mehr als nur ein Mittel der direkten Kommunikation zwischen Individualpersonen. Bei einer Vielzahl von Aktivitäten im Netz (Warenbestellungen, Dienstleistungen im Internet, Newsletter, Blogs, etc.) ist die E-Mail zu hinterlegen, so dass die Sichtung von E-Mail-Postfächern gleichzeitig eine Analyse des Nutzerverhaltens im Internet ermöglicht. Der Zugriff auf E-Mail-Postfächer ist äußerst sensibel und bedarf daher einer Rechtsgrundlage, die der besonderen Eingriffstiefe Rechnung trägt.

IV. Fazit

Die Entscheidung des 5. Strafsenats kann getrost als Ausreißer eingestuft werden. Sie darf nicht Schule machen und ist bei nächster Gelegenheit zu revidieren. Ein Zugriff auf Datenbestände, die vor Anordnung einer TKÜ entstanden sind, ist nach § 100a Abs. 1 S. 1 StPO weiterhin unzulässig.

¹² Köhler in: Meyer-Goßner/Schmitt, 63. Aufl. 2020, § 100a, Rn. 6c.

¹³ S. z.B. BGH, Beschl. v. 4.8.2015 – 3 StR 162/15.

¹⁴ BVerfG, Urt. v. 16.6.2009 – 2 BvR 902/06, Rn. 68 mwN.

¹⁵ BT-Drs. 18/12785, S. 50.

Entscheidungskommentare

Medizinstrafrecht

Rechtsanwältin Kathie Schröder, Frankfurt a.M.

BVerfG Beschluss vom 15.01.2020 – 2 BvR 1763/16

Die Einstellung von Ermittlungen nach einer Hinderung einer Patientin, ein Krankenhaus zu verlassen, indem sie über eine längere Zeit rechtswidrig fixiert wurde, verstößt gegen das verfassungsgemäße Recht der effektiven Strafverfolgung.

1. Grundsätzlich ergibt sich aus den Grundrechten der körperlichen Unversehrtheit sowie der Freiheit eines jeden Einzelnen nach Art. 2 Abs. 2 Satz 1 und Satz 2 i.V.m. Art. 1 Abs. 1 Satz 2 GG kein Anspruch eines Einzelnen auf eine (effektive) Strafverfolgung Dritter.