

**Schriftliche Stellungnahme
zu der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des
Deutschen Bundestages am 14. April 2021**

**zu dem Entwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung
und zur Änderung weiterer Vorschriften (BT-Drucksache 19/27654)**

Das mit dem Regierungsentwurf verfolgte Ziel, das Strafprozessrecht in einer Vielzahl von Einzelaspekten behutsam zu modernisieren und den wandelnden gesellschaftlichen sowie technischen Rahmenbedingungen anzupassen, wird begrüßt. Hervorzuheben ist, dass der Entwurf insbesondere wichtige neue Ermittlungsinstrumente wie beispielsweise die retrograde Auskunft von Postdienstleistern oder die automatische Kennzeichenerfassung bietet und bestehende Instrumente nachjustiert. Hier sollen lediglich einzelne Aspekte aufgegriffen werden:

I) § 95a StPO-E (Artikel 1 Nr. 7)

Mit der Regelung des § 95a Abs. 1 StPO-E löst der Entwurf das praktisch immer häufiger auftretende Problem, dass ein bisher noch verdeckt geführtes Ermittlungsverfahren frühzeitig offengelegt werden muss, da die Staatsanwaltschaft in einem frühen Stadium der Ermittlungen zur Aufklärung des Sachverhalts bei einem Provider – und damit bei einem Dritten – gespeicherte Daten des Beschuldigten beschlagnahmen muss. De lege lata ist dem Beschuldigten daraufhin die Beschlagnahme nach § 33 Abs. 1, § 35 StPO bekannt zu machen, da sie nur als offene Maßnahme zulässig ist (vgl. dazu jüngst BGH, Beschluss vom 14. Oktober 2020 – 5 StR 229/19, Rn. 21, sowie bereits BGH, Beschluss vom 4. August 2015 – 3 StR 162, 15, NStZ 2015, 704, 705). Dadurch bekommen der Beschuldigte sowie etwaige Mittäter oder Teilnehmer Kenntnis von den Ermittlungen, was einerseits einen Beweismittelverlust befürchten lässt, indem Beweismittel vernichtet oder Aussagen abgesprochen werden, andererseits die Gefahr begründet, dass weitere verdeckte Maßnahmen ins Leere laufen. Zwar bietet § 100a Abs. 1 StPO eine Ermächtigungsgrundlage für den verdeckten Zugriff auf „ruhende Emails“, sie betrifft aber nur *aktive* Emailkonten (vgl. BGH, Beschluss vom 14. Oktober 2020 – 5 StR 229/19, Rn. 22ff.). Somit besteht für den verdeckten Zugriff auf *inaktive* Emailkonten keine entsprechende strafprozessuale Maßnahme. Das Problem kann auch nicht dadurch gelöst werden, dass die Benachrichtigung von der Beschlagnahme zurückgestellt wird, da insoweit keine gesetzliche Grundlage besteht (vgl. BGH, Beschluss vom 4. August 2015 – 3 StR 162/15, Rn. 2, NStZ 2015, 704;

auch nicht in entsprechender Anwendung des § 101 Abs. 5 StPO, „allein Sache des Gesetzgebers“; BGH Beschluss vom 24. November 2009 – StB 48/09, Rn. 19, NStZ 2010, 345, 346). Für die Staatsanwaltschaft stellt sich dadurch im Einzelfall die herausfordernde Entscheidung, einerseits durch eine Beschlagnahme und der damit verbundenen Benachrichtigung das Verfahren unter Gefährdung des Ermittlungserfolges frühzeitig offenzulegen oder andererseits die Beschlagnahme zunächst zurückzustellen, weiter verdeckt zu ermitteln, dabei aber die Gefahr in Kauf nehmend, dass zu einem späteren Zeitpunkt die Beschlagnahme ins Leere läuft, weil die zu beschlagnahmenden Daten bereits vom Täter gelöscht wurden.

Es ist daher ausdrücklich zu begrüßen, dass der Gesetzgeber mit § 95a StPO-E im Begriff ist, die Benachrichtigungspflicht auf richterliche Anordnung zurückstellen zu lassen, sofern der Untersuchungszweck gefährdet wäre, eine Straftat von erheblicher Bedeutung vorliegt und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre. Die beabsichtigte Regelung zur Zurückstellung der Benachrichtigung harmoniert mit der Strafprozessordnung und ist ihr – wie verdeckte Maßnahmen insgesamt – auch nicht wesensfremd. So kann die Benachrichtigung bereits bei bestimmten verdeckten Maßnahmen gemäß § 101 Abs. 5 StPO zurückgestellt werden, wenn eine Gefährdung des Untersuchungszwecks besteht, namentlich bei der Rasterfahndung (§ 98a StPO), der Postbeschlagnahme (§ 99 StPO), der Telekommunikationsüberwachung (§ 100a StPO), der Online-Durchsuchung (§ 100b StPO), der akustischen Wohnraumüberwachung (§ 100c StPO), der akustischen Überwachung außerhalb von Wohnraum (§ 100f StPO), der Observation mit technischen Mitteln (§ 163f, § 100h StPO), dem Einsatz technischer Mittel bei Mobilfunkendgeräten (§ 100i StPO), der Speicherung und dem Abgleich von Daten aus Kontrollen (§ 163d StPO) und der Ausschreibung zur Beobachtung bei polizeilichen Kontrollen (§ 163e StPO). Der Entwurf zu § 95a Abs. 1 Nr. 1 StPO-E orientiert sich dabei an dem Katalog des § 100a Abs. 2 StPO, so dass insoweit im Wesentlichen ein Gleichklang zwischen der Beschlagnahme des *inaktiven* Emailkontos und der *aktiven* Email-Überwachung nach § 100a StPO hergestellt wird.

II) § 99 Abs. 2 StPO-E (Artikel 1 Nr. 8)

Ebenfalls positiv ist zu bewerten, dass sich der Entwurf der praxisrelevanten und umstrittenen Frage annimmt, ob und gegebenenfalls auf Basis welcher Rechtsgrundlage auf retrograde, nicht mehr im Gewahrsam des Postdienstleisters befindliche Postdaten zugegriffen werden kann bzw. unter welchen Voraussetzungen ein dahingehender Auskunftsanspruch besteht. Der Bundesgerichtshof hatte bekanntlich mit Beschluss vom 20. Februar 2019 – StB 51/18 (NStZ-RR-

2019, 280) festgestellt, dass de lege lata keine Rechtsgrundlage dafür existiere, namentlich seien weder § 94 noch § 99 StPO einschlägig; auch nicht in analoger Anwendung. Zu einer Änderung dieser Rechtslage sei allein der Gesetzgeber berufen. Der vorliegende Entwurf stellt mit § 99 Abs. 2 StPO-E ein insbesondere für Staatsschutzstrafverfahren wichtiges praxisgerechtes Instrument in Aussicht. Es zeigt sich gerade in Ermittlungsverfahren im Zusammenhang mit terroristischen Anschlagplanungen, dass beispielsweise Täter unter Nutzung des Internets einzelne Gegenstände zur Herstellung eines Sprengsatzes bestellen. Für die Tataufklärung sind Auskünfte der Postdienstleister im Sinne von § 99 Abs. 2 StPO-E, wie etwa Absender oder Maß und Gewicht der Postsendung, immens wichtig.

III) § 163g StPO-E (Artikel 1 Nr. 27)

Die Schaffung einer bundesgesetzlichen Regelung über die automatische Kennzeichenerfassung zu Fahndungszwecken wird ebenso begrüßt. Durch die nunmehr vorgenommene Streichung der „bestimmten Stellen“ in § 163g Abs. 1 StPO-E (vgl. noch Referentenentwurf vom 6. Oktober 2020) wird die Maßnahme – bei vergleichbarer Eingriffstiefe – auch mobil möglich sein, so dass beispielsweise geparkte Fahrzeuge miterfasst werden können. Die vom BVerfG (vgl. Beschluss vom 18. Dezember 2018 – 1 BvR 142/15, Rn. 115, NJW 2019, 827, 836) aufgezeigte Grenze des Übermaßverbotes wird durch die Tatbestandsmerkmale „örtlich begrenzt“ und „nur vorübergehend und nicht flächendeckend“ für die Praxisanwendung klar und greifbar berücksichtigt.

Es bleibt zu überlegen (vgl. Bundesrat Drucksache 57/1/21 Nr. 12), in § 163g StPO-E ebenfalls zu regeln, dass Daten für eine gewisse beschränkte Dauer zu speichern sind, damit sie bei schwersten Straftaten wie terroristischen Anschlägen oder Amoklagen mit anderweitig erhobenen Daten abgeglichen werden können.

IV) § 120 Abs. 2 Satz 1 Nr. 4 GVG-E (Artikel 4 Nr. 7)

Die Erweiterung der evokativen Zuständigkeit des Generalbundesanwalts beim Bundesgerichtshof auf alle Fälle des Kriegswaffenkontrollgesetzes sowie der Versuchsfälle nach dem Außenwirtschaftsgesetz unter den bisherigen Voraussetzungen des § 120 Abs. 2 Satz 1 Nr. 4 GVG wird ausdrücklich befürwortet und spiegelt den Bedarf der forensischen Praxis wider. Der Generalbundesanwalt beim Bundesgerichtshof kann dadurch – bei Vorliegen der übrigen Voraussetzungen des § 120 Abs. 2 Nr. 4 Buchstaben a oder b GVG – auch die Verfolgung von

OStA b. BGH Dr. Moldenhauer

Straftaten nach dem Kriegswaffenkontrollgesetz im Zusammenhang mit besonders gefährlichen konventionellen Kriegswaffen an sich ziehen, sofern dem Fall eine besondere Bedeutung im Sinne des § 120 Abs. 2 S. 1 Nr. 4 GVG zukommt; dies kann bei einem staatschutzfeindlichen Charakter mit geheimdienstlichen Strukturen der Taten im Einzelfall geboten sein.

Karlsruhe, 9. April 2021

Dr. Gerwin Moldenhauer